NATO STANDARDIZATION AGENCY
AGENCE OTAN DE NORMALISATION

MILITARY COMMITTEE LAND STANDARDIZATION BOARD (MCLSB)

20 September 2010 NSA(ARMY)1022(2010)C-IED/2298

MCLSB

STANAG 2298 C-IED (EDITION 1) – NATO WEAPONS INTELLIGENCE TEAM (WIT) CAPABILITIES STANDARDS

Reference:
NSA(ARMY)0891(2010)C-IED/2298 dated 13 August 2010 (Edition 1) (Ratification Draft 1)

1. The enclosed NATO Standardization Agreement, which has been ratified by nations as reflected in the NATO Standardization Document Database (NSDD), is promulgated herewith.

2. The reference listed above is to be destroyed in accordance with local document destruction procedures.

ACTION BY NATIONAL STAFFS

3. National staffs are requested to examine their ratification status of the STANAG and, if they have not already done so, advise the MCLSB NSA, through their national delegation as appropriate of their intention regarding its ratification and implementation.

Cihangir AKSIT, TUR Civ
Director, NATO Standardization Agency

Enclosure:
STANAG 2298 C-IED (Edition 1)

NATO Standardization Agency – Agence OTAN de normalisation
B-1110 Brussels, Belgium - Internet site: http://nsa.nato.int
E-mail: army@nsa.nato.int – Tel +32 2 707 5584 – Fax +32 2 707 5718

STANAG 2298
(Edition 1)

NORTH ATLANTIC TREATY ORGANIZATION

(NATO)

NATO STANDARDIZATION AGENCY
(NSA)

STANDARDIZATION AGREEMENT
(STANAG)

SUBJECT: NATO WEAPONS INTELLIGENCE TEAM (WIT) CAPABILITIES STANDARDS

Promulgated on 20 September 2010

Cihangir AKSIT, TUR Civ
Director, NATO Standardization Agency

RECORD OF AMENDMENTS

No.	Reference/date of amendment	Date entered	Signature

EXPLANATORY NOTES

AGREEMENT

1. This STANAG is promulgated by the Director NATO Standardization Agency under the authority vested in him by the NATO Standardization Organisation Charter.

2. No departure may be made from the agreement without informing the tasking authority in the form of a reservation. Nations may propose changes at any time to the tasking authority where they will be processed in the same manner as the original agreement.

3. Ratifying nations have agreed that national orders, manuals and instructions implementing this STANAG will include a reference to the STANAG number for purposes of identification.

RATIFICATION, IMPLEMENTATION AND RESERVATIONS

4. Ratification, implementation and reservation details are available on request or through the NSA websites (internet http://nsa.nato.int; NATO Secure WAN http://nsa.hq.nato.int).

FEEDBACK

5. Any comments concerning this publication should be directed to NATO/NSA – Bvd Leopold III - 1110 Brussels - Belgium.

STANAG 2298
(Edition 1)

NATO STANDARDIZATION AGREEMENT
(STANAG)

NATO WEAPONS INTELLIGENCE TEAM CAPABILITY STANAG

Annexes:

A. NATO WIT Tasks.
B. NATO WIT Minimum Standards of Proficiency.
C. NATO WIT Reports.
D. NATO WIT General Equipment List.
E. Lexicon

Related documents:

AJP-3.15 – Allied Joint Doctrine for Countering the Improvised Explosive Device (C-IED)
STANAG 2294 – Standard NATO Agreement for Countering Improvised Explosive Device training Standards
STANAG 2370 / AEODP-3 – Standard NATO Agreement / Allied Explosive Ordnance Disposal for Principles of Improvised Explosive Device Disposal
STANAG 2221/ AEODP-6 – Standard NATO Agreement / Allied Explosive Ordnance for Explosive Ordnance Disposal Reports and Messages

AIM

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

AGREEMENT

2. Nations are to train and equip WIT for C-IED to the standards defined in this STANAG.

GENERAL

3. **Background**. The NATO C-IED exploitation system comprises of three different levels, as stated in AJP-3.15. The NATO Exploitation Process is shown schematically at Figure 1[2]. Level 1 (L1) conducted by WIT, is the on site, initial[3] exploitation capability and

[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 Level 2 will be dependant on the theatre or phase of an operation and therefore alternative arrangements may be made for exploitation above Level 1.
[3] Limits of exploitation are to be determined by theatre SOPs.

the low level technical and tactical analysis support to the local commander on the ground. Level 2 (L2) provides a laboratory based technical and forensic exploitation capability, for a more detailed examination of recovered evidence[4]. Level 3 (L3) is a reach-back capability, providing in depth technical and forensic examination and an analysis exploitation capability. This STANAG is principally concerned with describing Level 1 capabilities. Level 2 and 3 capabilities are not included in this STANAG.

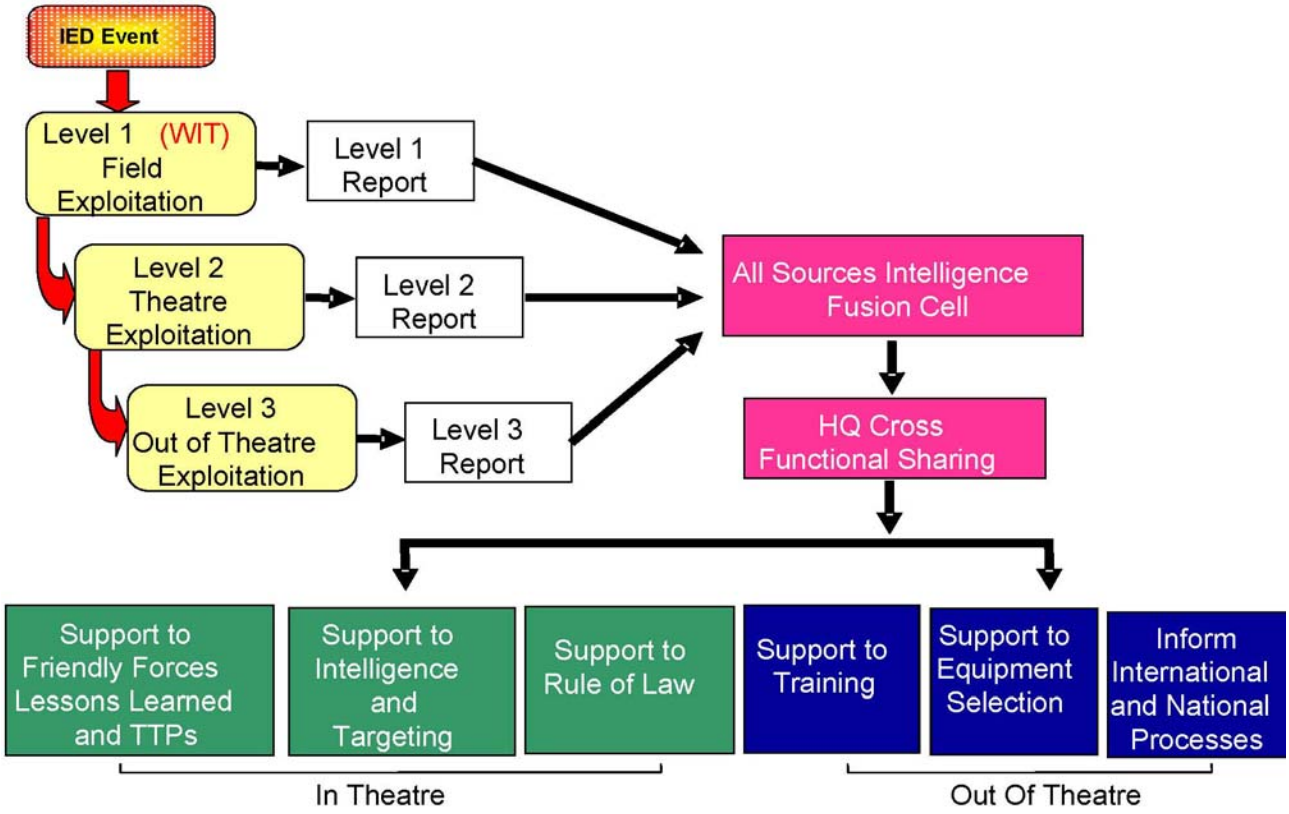

Figure 1 – The NATO Exploitation System

4. **WIT Capability:**

a. 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 evidence for exploitation; tasks to be carried out are described in Annex A. WIT ensure the collection and non intrusive examination of materiel and locations and tactical questioning of detained personnel and interviewing of witnesses often conducted forward of a dedicated facility. The WIT's purpose is to inform commanders of the threat, enemy TTPs, and the IED system and/or changes to these. The output will save lives by increasing combat effectiveness and provide intelligence to defeat the IED system.

b. WIT are part of the Technical Intelligence (TECHINT)[5] function of materiel and personnel exploitation[6]. The main output of the examination and analysis process is to

[4] The use of the word "evidence" in this STANAG refers to an intent to potentially utilise recovered materiel 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.
[5] TECHINT is an intelligence functional discipline

inform 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.

c. Materiel 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 materiel and observation of tactical factors at the scene of the event. This multiple source process makes extensive use of non-traditional intelligence collection, including the collection of forensic and biometric information, data recovered from electronic devices and digital systems, as well as hard copy documents. WIT 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. **Key Considerations:**

a. **Optimising 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.

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

c. **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 recovered physical items are handled appropriately to ensure they remain admissible as evidence.

d. **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 evidence to support more detailed investigation, as necessary. Most IED evidence is catalogued and forwarded for forensic examination at L2 laboratories, the evidence can then be transferred to L3 laboratories for more detailed forensic examination in support of the strategic intelligence plan.

e. **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 rigorously reviewed to ensure it has the lowest possible security classification to optimise information sharing amongst friendly forces.

6. **WIT Outputs - In Theatre:**

a. **Support to Friendly Forces Lessons Learned and Tactics Techniques and Procedures (TTPs)**. WIT provide reports based upon information gained from the tactical scenario, IED components, precursor materials, witnesses and associated documentation

[6] Personnel and materiel exploitation procedures are defined in AJP 2.5

gathered from the IED scene. These reports allow commanders to develop Lessons Learned and adapt their TTPs to mitigate the IED threat. WIT reports can also assist in the development of defensive technical countermeasures and influence the choice of equipment procurement.

b. **Support to Intelligence and Targeting**. When information and evidence collected by WIT is analysed using technical, forensic and biometric disciplines, the results can 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.

c. **Support to Rule of Law**. Information and materiel collected by WIT may provide items for further exploitation in order to identify and potentially convict perpetrators, by linking IED events to individuals.

7. WIT Outputs – Out of Theatre:

a. **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. WIT reports should be used to support the Lessons Learned process, in order that the most current training can be provided in the form of a robust C-IED Training package, in order to Prepare the Force to Attack the Network and Defeat the Device.

b. **Support to Equipment Selection**. WIT reports on device construction, method of operation and IED effects, provide detailed technical intelligence that will facilitate technical counter-measures and procurement for C-IED.

c. **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.

DETAILS OF THE AGREEMENT

8. This STANAG:

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, including the Immediate Report and the L1 Exploitation Report (Annex C).

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).

IMPLEMENTATION OF THE STANAG

8. This STANAG is implemented when a nation has issued the necessary orders or instructions to authorities and units concerned to put the standards and procedures detailed in this agreement into effect.

ANNEX A TO
STANAG 2298
(Edition 1)

NATO WEAPONS INTELLIGENCE TASKS

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

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

b. **Planning Site Exploitation**. Central to the role of WIT will be the planning and execution of exploitation of an IED event. Where ever 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 and secure by an appropriate organisation.

c. **Collection of Materiel and Triage.** When a WIT is deployed they normally assume the lead for the collection of materiel encountered as part of deliberate and routine operations. The decision regarding what materiel to collect and exploit 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[7]. Items assessed as of lesser value[8] should be left. 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 (HVT) should be afforded particular priority. In general, the following materiel 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 sometimes at L2 facilities but normally at a L3 facility.

(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 exploit IED components. These may include: car alarms, doorbells, mobile phones, two-way radios, batteries, electronic components, wires, wiring harnesses and timers.

(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.

[7] Some items may hold important biometric evidence and therefore should not be discounted.
[8] Such as unaltered religious publications, landline telephones without display screen, electrical / electronic peripherals with no memory storage, unaltered open source publications (newspapers, magazines)

d. **Visual Recording.** Visual recording of the scene is vital to understand the tactical scenario. WITs must be capable of accurately recording by photographs and / or video the exploitation site and evidence. Viewing images of an item, as opposed to consistently handling a particular piece of materiel, will also preserve uncontaminated materiel 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 evidence (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 (using latent fingerprinting techniques for example). Typical examples may be vehicles used in events or large items of furniture identified during a search. However, consideration should be given to the removal of forensically useful sections of larger pieces of evidence for exploitation. eg removal of door handles, mirrors or gear knobs for biometric analysis.

g. **Biometric Information / Data Capture**. WIT need to be proficient in the use of biometric equipment in order to capture data from individuals and materiel 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 ensure all the circumstances of the event are recorded.

i. **Chain of Evidence Protocols.** In all cases, chain of evidence is to be ensured in order to allow further exploitation. The chain of evidence protocols may vary depending on the nations or the operational theatre, but excellent collection can be ruined if the 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 provide templates which meet the requirements of WIT reporting. Contained in the AEODP-6, the EOINCREP provides a template for the WIT Immediate Report and the IEDTECHREP provides a template for the L1 Exploitation report. Annex C provides guidance on WIT reports. WIT are responsible for producing the following reports :

(1) **Immediate Report**. It is vital to ensure that the correct context is applied to evidence collected from an exploitation site. It should contain the circumstances in which the materiel 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. The Immediate 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 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 materiel evidence was recovered or not. The report will include details pertaining to the IED event and will go into as much detail on the technical construction of the device as possible. In particular, any new trends of construction or materiel should be highlighted. 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 evidence is to be exploited further.

l. **Briefs**. Team leaders need to be prepared to brief 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 reports should be consulted in order to identify local trends and integrate results into assessments and historical/technical records.

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, weapons systems and munitions as applicable.

NATO WEAPONS INTELLIGENCE TEAM MINIMUM CAPABILITY REQUIREMENTS

1. Typically a WIT consists of between 2 and 4 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. WIT should be established in accordance with national procedures and function best 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
Be able to describe the NATO Exploitation Process
Be able to describe the NATO L1 Exploitation Process
Be able to describe how Forensic and Biometrics relates to the Exploitation Process
Be able to describe EOD responders and their roles
Be able to describe the L1 Exploitation Team's equipment
Be able to describe the maintenance requirements of a L1 Exploitation Team's equipment
Be able to describe the use and function of the theatre IED database
Be able to describe the use and function of biometric databases
Be able to describe the Intelligence Cycle and the Intelligence Surveillance and Target Acquisition contribution
Be able to contribute to and support the L2 and L3 exploitation information requirement
Technical Knowledge
Be able to describe and identify the different IED types
Be able to identify the components and materiel / parts used to construct IEDs
Be able to identify and describe the different types of Home-made Explosives, precursor components and their effects
Be able to identify and describe the different types of commercial and military explosive main charges and their effects
Be able to understand the principles of explosive safety
Be able to identify the main types of military ordnance
Be able to identify electronic and electrical components and describe how they can be used in making IEDs
Be able to describe how materiel should be preserved for forensic and biometric exploitation
Be able to conduct exploitation within and supporting the NATO and national biometrics collection systems
Be able to effectively employ the WIT equipment provided

Be able to identify weapons and weapon systems associated to the theatre of operations

Tactical Knowledge
Be able to identify and assess an IED event including TTPs and how they relate to the ground
Be able to identify and assess IED indicators, vulnerable points, firing points
Be able to advise on development of Friendly Force TTPs
IED Event Response
Be able to plan and conduct the exploitation of an IED event when directed by the Chain of Command
Be able to conduct a reconnaissance of the IED event site
Be able to conduct questioning of witnesses and persons at the IED event site
Be able to conduct in-depth on site investigation dependant upon the tactical situation
Be able to complete a general and detailed visual record of an IED event
Be able to preserve evidence and maintain site integrity including a mass casualty event
Be able to conduct evidence collection without contaminating the evidence at the event site
Be able to conduct evidence packaging and labelling for transport to an evidential standard
Be able to describe the storage, handling and transportation of explosive materials
Be able to conduct explosive evidence (small samples of high explosive and detonators) collection in accordance with current safety standards
Be able to conduct fingerprint collection
Be able to conduct blast estimation and crater (seat of explosion) analysis of the event site
Be able to conduct fragmentation analysis of the event site
Be able to complete appropriate L1 Exploitation reports
Be able to conduct on scene threat assessment to identify adversary TTPs

ANNEX C TO
STANAG 2298
(Edition 1)

NATO WEAPONS INTELLIGENCE TEAM REPORTS

1. Immediate Report Guideline format is at appendix 1.

2. Level 1 Exploitation Report Guideline format is at appendix 2

APPENDIX 1 TO
ANNEX C TO
STANAG 2298
(Edition 1)

IMMEDIATE REPORT GUIDELINE

1. **Preliminaries:**

   a. Event and category type.

   b. Date-Time-Group (DTG) of the event.

   c. Event number.

   d. Location.

   e. Map with location.

   f. Target.

   g. Casualties.

   h. Damage.

   i. Description of the IED: probable IED type and brief description of evidence recovered from site or turned in.

   j. EOD/IEDD/Exploitation tasking: What EOD/IEDD/Specialist exploitation assets were tasked to respond to the event?

   k. Evidence status:

      (1) For IED / Mine(nuisance): was evidence recovered? Is the evidence being sent to L2 ?

      (2) For UXO / Explosive Remnants of War (ERW) / Cache / weapons add a separate sheet describing the details.

2. **Background**. This paragraph describes the event, including its context with previous events in the area and the presence of witnesses or detainees.

3. **Tactical Summary / Recommendation**:

   a For IED, describe the enemy TTPs and their impact on friendly forces.

   b For UXO / Mine (nuisance) / ERW / Weapons, explain if they are related to IED activities (hotspots, previous IED events, enemy cells etc).

4**.** **Annexes**: Provide relevant number of annexes as required for map, photos etc

APPENDIX 2 TO
ANNEX C TO
STANAG 2298
(Edition 1)

LEVEL 1 EXPLOITATION REPORT GUIDELINE

1. **Outcome of the IED Event**:

a. Provide relevant details on casualties (KIA, WIA, nationality, affiliation).

b. Provide relevant details on battle damage assessment (vehicle, buildings, and infrastructure).

c. Provide relevant details on requirement for further exploitation (priority, what is required from L2 and L3).

2. **Device Description**. Provide relevant details on primary device description, presence of secondary devices and description.

3. **Background**. Provide relevant description of the context of the event including near, middle and far terrain assessment.

4. **Basic Information**. Provide relevant details: DTG, associated reports, location, intended target, detainees (photos with evidence).

5. **Device Construction and Method of Operation**. Provide details on:

a. Delivery method (use of vehicle, person, object and how it was employed).

b. Emplacement.

c. Main charge (what is the main charge, type of explosive, estimate weight), power supply (type), container / packaging (description), trigger (type).

d. Method of functioning (how the device functioned).

e. Geography (use of the terrain for facilitating the attack).

f. Atmospherics (local population attitude to inform Information Operations effort).

g. Evidence recovery (detailed list of IED components, UXO, media, clothing, etc).

h. Chain of evidence (all the evidence sent to L2 or not).

6. Enemy TTPs: Provide details on :

a. Enemy mission analysis :

(1) Mission.

(2) Enemy.

(3) Troops.

(4) Time.

(5) Civil considerations from enemy point of view.

b. Enemy terrain analysis:

(1) Observation and fields of fire.

(2) Cover and concealment.

(3) Obstacles.

(4) Key terrain.

(5) Avenues of approach from enemy point of view.

7. **Friendly TTPs:** Provide details on:

a. ECM employment.

b. Immediate area security checks before and after explosion / discovery (5/25 m check, vulnerable point check etc).

c. Frequency of the use of these routes or locations by friendly forces and C-IED drills performed.

8. **History.** Provide details on similar devices used in the area before, with references to previous reports.

9. **Investigators Comments.** Provide details of observations, conclusions, recommendations, assets used (dedicated WIT, EOD,) and contact details of the investigators.

10. Triage comments. Provide relevant details on triage (required, not required, explanations).

11. Annexes. Provide annexes if appropriate for:

a. Immediate report storyboard.

b. Map of location.

c. Historical overlay.

d. Labelled pictures showing direction of travel, cardinal directions, aiming marks, indicators, IED placement, firing point, IED main charge, IED seat of blast, evidence collected etc.

e. Pictures showing the device as it was emplaced, with close-up pictures of components with graduated scales, so that sizes/dimensions are clear.

ANNEX D TO
STANAG 2298
(Edition 1)

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[9].

Ser (a)	Capability (b)	Effect Required (c)	Example (d)	Remarks (e)
1	Personnel Protection Equipment (PPE)	Protect personnel from the contamination of 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,…	
7	Materiel safety equipment	The ability to ensure material is safe to recover and submit for further exploitation	Portable X-ray, voltmeter, etc	
8	Materiel recovery	The ability to recover material safely for further investigation whilst preserving biometric evidence	Evidence bags, forensic gloves, sealing equipment, metal ammo boxes, knife, etc	
9	Energetic sample recovery	The ability to safely recover samples of energetic material	Detonator containment units, sample vials swabs, spatulas, explosive test kits, etc	
10	Biometric recovery capability	The ability to collect biometric identities pre and post mortem	Finger print kit, deoxyribonucleic acid (DNA) kit, etc	
11	Reporting capability	The ability to report incidents	Laptop, database, communications, Reference material, A5 sketch pads, etc	
12	Miscellaneous	The ability to further support and enhance other capabilities	Light, magnifying glass, etc	

[9] 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.

LEXICON

PART 1- ABBREVIATIONS & ACRONYMS

ACO: Allied Command Operations

AEODP: Allied Explosive Ordnance Disposal Publication

AJP: Allied Joint Publication

C-IED: Countering-Improvised Explosive Device

DNA: Deoxyribonucleic Acid

DTG: Date Time Group

EOD: Explosive Ordnance Disposal

ERW: Explosive Remnant of War

ID: Identification Document

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)

L2: Level 2

L3: Level 3

NATO: North Atlantic Treaty Organization

SIM: Subscriber Identify Module

SOP: Standard Operating Procedure

STANAG: Standard NATO 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.

COUNTERING-IMPROVISED EXPLOSIVE DEVICES

The collective efforts at all levels to defeat the IED system by Attacking the Networks, Defeating the Device and Preparing the Force. (AJP 3.15 - Lexicon)

Note: Networks within the context of C-IED describe interconnected people or things and can be identified, isolated and attacked.

FORENSICS

The scientific data and procedures that pathologists, laboratory, technicians, and other scientists work with - in order to solve crimes. (Collins Dictionary)

IED EVENT

An event that involves one or more of the following types of IED related actions or activities in relation to IEDs: an IED explosion ; an attack; an attempted attack; a find; a hoax; a false or a turn-in. (AJP-3.15-Lexicon)

IED SYSTEM

An IED system comprises personnel, resources and activities and the linkages between them that are necessary to resource, plan, execute and exploit an IED event. (AJP 3.15 - Lexicon)

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)

TACTICAL QUESTIONING

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)

TECHINT

Intelligence concerning an adversary’s technological developments and the performance and operational capabilities of adversary materiel, which may have or may eventually, have a practical application for military purposes. (AAP-6)

WEAPONS 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)