Humanitarian IED Disposal – Gathering of IED Technical Information

Technical Note

Contents

SECTION ONE - Introduction

1.1 Background and Scope

IED clearance has many considerations which are distinct from regular ERW clearance procedures. One of the key distinctions is that IEDs are far less uniform in their construction than conventional munitions and an HIEDD operator is unlikely to know the full nature of the device until an RSP (Render Safe Procedure) is complete. Pre-planned RSPs cannot be applied to all devices, so the HIEDD operator must be guided by assessing the information presented to him/her on the task at hand, as well as knowledge of previous device history in the area.

As such, the ability of humanitarian mine action organisations to gather, review and share technical information will be of vital importance to running a safe and effective clearance programme. The aim of this technical note is to offer guidance as to how this can be best achieved, whilst ensuring the safety of individuals and safeguarding neutrality and humanitarian principles. It should be read in conjunction with global and programme IED clearance SOPs.

1.2 HIEDD Operator Safety

Gathering of information is one of four humanitarian IED clearance philosophies which guide all operations. For reference these are repeated below, in priority order:

1. Protection of life
2. Protection of property
3. Returning the situation to normal as soon as possible
4. The gathering and sharing of information where safe to do so

While important, gathering technical information is never prioritised over other philosophies.

HIEDD operators must never endanger themselves, others, property or expend undue time in order to gain additional technical information. Nor must others pressurize them to do so.

However, with some relatively simple observation and record keeping procedures an HIEDD operator should be able to gather useful technical information, while adhering to SOPs.

1.3 Neutrality and Humanitarian Principles

As well as operator safety, gathering information on IEDs in post-conflict situations can be a sensitive topic amongst stakeholders. Law enforcement, intelligence and military agencies often consider IEDs to have particular intelligence value, as detailed knowledge of technical specifications, forensics, etc. can directly assist planning and executing military/security operations. Often these are referred to as counter-IED operations (see SOP 1 for further information)

HALO programmes should never directly support or enable counter-IED or other military operations. To do so may not only jeopardize our wider acceptance within the communities where we work, and could result in active targeting of our HIEDD operators' RSPs

Managing this may be challenging- particularly on programmes where there is necessarily close liaison between local security forces, the community, other conflict actors and operational staff. Some planning consideration and guidance is below:

- If HIEDD operators are collecting technical data in the field then consideration should be given to how this is perceived by other stakeholders. Operations staff should endeavor to keep this a low-key, routine activity and have a clear message on how and why HALO stores and shares such information.
- Transparency of gathered information. Further guidance on IM is below, but in general programmes should be prepared to share technical data across the HMA sector- particularly if new types of device are discovered or useful data on EO/IED contamination patterns emerges. This can be done through TWGs, sharing of technical information reports, IMSMA reports etc.
- Careful use of language. There is often an overlap of military language in HIEDD operations, largely due to the background of many of the personnel involved. While this is perfectly understandable, certain terms can be sensitive; programmes should understand what these sensitivities may be and manage the use of terminology accordingly (in both English and local languages). Some examples are:
    - Intelligence: The term “intelligence” has direct associations with security force operations, and usually implies actionable information that can assist in targeting or other military decision making. Programmes should avoid using the term. Information is suitable alternative that better describes our role.
    - New devices: Describing a device as new can have a variety of different meanings. It could imply a device that has a technical construction that has not been seen before, a device that has been emplaced more recently than others (but a permissive environment still exists) or a device that has been placed after clearance has started. All of these require dramatically different responses from HMA actors and operational staff should ensure that there is absolute clarity when describing such occurrences.

SECTION TWO – Gathering & Managing Technical Information

2.1 Field Collection of Information

HIEDD operators must never place themselves or others at risk in order to gather technical information, but if their RSP allows it then an effort should be made to record some of the below. As a general rule operators should ask themselves "if I didn't need to gather any information, would this be the RSP that I would use?" If the answer is no, then operators should review their actions and re-plan their RSP accordingly. Useful information may be gathered quickly and safely from the below:

- Photos of recovered component parts
- Photos of component parts "in place"- noting the requirement to minimize the time at target[1].
- Assessed distance of device from other devices and photos of general location (building, doorway, ditch etc.)
- Assessed depth and distance between individual component parts and their orientation
- Detectability threshold of recovered component parts with specified detector
- General condition of component parts, including any date stamping (e.g. battery expiry dates)
- Colours of tape, wiring, detcord, containers etc.
- Measurement of battery voltage and output capacity using an multimeter or similar
- Type and condition of any manufactured explosive components (detonators, conventional ordnance main charges etc.)

It is probably unnecessary to gather all of the above for each device found by clearance teams. As it would be impractical and would unnecessarily slow operations where large numbers of devices are being cleared. The level of detail required should be set by the Country Operations Manager, in conjunction with the information management team.

In exceptional cases, a suitably experienced HIEDD operator may consider it appropriate to make minor modifications to an RSP in order to gain clarity on a specific technical matter. In this case a referral to the Operations Manager will always be required, who must be satisfied that there is no credible risk to life or property as a result of the proposed actions.

2.2 Recovery of Components for Free from Explosive (FFE) displays

Any recovery of EO for FFE displays should be conducted with extreme care. This is especially true for improvised devices where detailed technical/reference material will never be available. The following should be considered:

- All collection should be conducted in-line with HALO's FFE Certification Guide (available on Confluence), including keeping of registers, transport etc.
- Only the Country Operations Manager may authorize the collection of improvised components for FFE displays.

[1] Note, in some circumstances components can be replaced in their original position post-RSP and when explosively safe (an obvious requirement would be the removal of detonators). However, given the possibility for misinterpretation by field staff it is suggested that such actions are only conducted by senior/specified HIEDD operators.

- Recovery should only be conducted once the RSP is complete (i.e. the entire device has been removed and declared explosively safe). No SOP deviations shall be authorized in order to facilitate component recovery
- FFE declarations should only be conducted by a small number nominated senior HIEDD staff. A written record of nominated staff should be approved by the Country Operations Manager.
- Components that contained explosives should never be recovered (e.g. main charge containers, detonators etc.)
- Programmes must understand any relevant local legislation that may prohibit or limit the recovery and storage of IED components.
- Recovered components should be free of voids, air gaps, or other spaces that cannot be visually inspected, as there is a risk of explosive content being present. If there is any doubt the components must not be recovered[2].

2.3 Information Management

As with all HMA data gathering, in order for technical information to be useful and shareable it needs to be subject to quality assurance and good data management practices. Some guidance and potential risks are outlined below:

- It may be appropriate to separate/compartmentalize IED technical information from the main operational database. The amount of data fields required can be extensive, or programmes may prefer to produce individual technical information reports for devices that are of interest.
- Other operators will often share technical information, these should be recorded and shared as widely as necessary within a programme.
- Confluence will be used as a central repository for IED technical information, it will be maintained by the CTA IEDD/Capability Group
- Programmes and individuals must manage the sharing of information carefully. As mentioned formal sharing of technical information is highly encouraged through appropriate channels, but extreme care must be taken following formal or informal requests for data. A well-meaning email to a colleague in the military, containing information about HALO's activity, could jeopardize HALO's neutrality or contractual agreements with donors. As a general rule, the decision to share any information externally should be authorised by the PM, with guidance from the DHoR/HoR

2.4 Other Agencies

IEDs generally attract more interest from other agencies than conventional munitions. This is usually due to their connection with non-state groups and their perceived intelligence value. It is likely that programmes will receive requests, if not pressure, to hand over data or physical components. This may be from host-nation entities, representatives of international governments, international military forces, multi-lateral agencies etc. This can risk both HALO's acceptance in the communities where we work and

2 The use of an X-ray by suitably trained personnel may mitigate this risk

the support of governments on who we rely. Programmes will have to handle such matters with extreme care and almost certainly with guidance from HALO global HQ, but some general principles are:

- Sharing information should be authorised by the PM; bilaterally handing over components must be discussed at Head of Region level, at least.
- Information or physical components should not be handed over where there is not a pre-existing formal agreement in place.
- Information or physical components should not be handed over where there is a likelihood that it will support military or security operations.
- Widely sharing appropriate information may help mitigate any perceptions of impartiality, however this is clearly not possible with physical components.
- Destroying physical components on-site may prevent the issue from being raised (either as part of the RSP or as a post-RSP logistical process). Although this should always be done in accordance with HALO SOPs and any relevant national standards or laws.
- Programmes should be aware that the receiver may not be the final destination. Consideration should be given to where any information or component is likely to end up.

2.5 Component Recovery from Non-HALO Sources

Conversely, there may be occasions when HALO staff are requested to collect component parts from other stakeholders- either for disposal or safety purposes. As the exact nature, state and location from which the components come from may be unknown, extreme caution should be exercised. Technical information need not be collected from these items, unless for example the item(s) are new to the programme, in which case advice should be sought from the senior member of operational staff on the programme.

Components should only be recovered if the purpose is for future disposal by HALO. It should not be for reasons of technical investigation, training aids, or administrative convenience of another party

Examples of the risks of recovering IED components include inadvertent initiation of unfamiliar/improvised components, secondary explosive hazards, or legal/neutrality issues with handling IED components that may be part of ongoing conflicts.

In order to mitigate these risks, the following guidance should be considered:

- If possible, programmes should avoid recovering components from other sources at all, but it is appreciated that this will not always be practical.
- IED components should only be recovered, stored, or disposed of by personnel who are qualified as HIEDD operators
- The authorization and actual recovery of components should be conducted by a small, clearly defined number of personnel (i.e. a list of named personnel, numbering no more than is absolutely necessary to conduct recovery)
- IED Components should only be accepted by HALO personnel if accompanied by an itemised receipt from the organisation that is handing over the components.
- The following should never be recovered:

- Improvised initiators/detonators
- Any components that cannot be positively identified or are considered suspect
- Any components that cannot be confirmed to have been moved from the original emplaced location
- Any components that have not been stored for at least 24 hours by the organization that is handing over the components
- Components should only be recovered if they have been completely separated from other components. HALO personnel should never be pressured into conducting this separation themselves

- All stored IED components must be stored and transported in accordance with HALO explosive storage and transport SOPs.
- Recovered components must be destroyed as soon as possible, usually within 7 days of recovery, unless specifically authorised by the Country Operations Manager.

2.6 Additional Information Sources

- HALO Global IED SOPs
- IMAS 4.10 Glossary of mine action terms, definitions and abbreviations
- IMAS 9.31 Improvised Explosive Device Disposal
- HALO Global FFE Certification Guide