United Nations Improvised Explosive Device Threat Mitigation Handbook

Second edition
2025

United Nations

United Nations Improvised Explosive Device Threat Mitigation Handbook

Second edition
2025

United Nations

Produced by:
Office of Military Affairs
Department of Peace Operations
United Nations
405 E. 42nd St., New York, NY 10017
Tel. (917) 367-2487

Approved by:
Major General Cheryl Pearce
Acting Military Adviser
Office of Military Affairs
Department of Peace Operations

May 2025

Contact: PDT/OMA/DPO
Review date: 2 May 2029 (or as needed)
Reference number: 2025.11
Printed at United Nations, New York
Illustrations: Helena Ohlsson, Aoife Hamilton

Contents

page

page

page

page

Foreword

It is with great pride and a profound sense of responsibility that I introduce this *United Nations Improvised Explosive Device Threat Mitigation Handbook*. Developed in close collaboration with the Mine Action Service of the United Nations (UNMAS), United Nations police and United Nations peacekeeping missions, this *Handbook* represents a milestone in our collective efforts to address one of the most pressing challenges facing personnel deployed in conflict zones worldwide.

The scourge of improvised explosive devices (IEDs) knows no boundaries, indiscriminately targeting military forces, civilian staff and innocent bystanders alike. Therefore, the importance of equipping ourselves with the knowledge and resources to counter this threat cannot be overstated. This *Handbook* stands as a testament to our unwavering commitment to safeguarding lives and promoting stability in the most volatile of environments.

What sets this *Handbook* apart is its accessibility. Recognizing the diverse backgrounds and expertise of our audience, we have strived to create a resource that is both comprehensive and user-friendly. Through a wealth of supporting illustrations and graphics, we aim to demystify the complexities of IED threat mitigation, empowering individuals at all levels to navigate these challenges with confidence and proficiency.

As we embark on this journey together, let us not lose sight of the human cost of our endeavours. Behind every statistic lies a story of resilience, courage and sacrifice. It is incumbent upon us to honour the sacrifices of those who have gone before us by arming ourselves with the knowledge and tools necessary to confront this menace head-on.

In closing, I extend my deepest gratitude to all those who have contributed to the development of this *Handbook*, from the dedicated personnel in the field to the experts who have lent their expertise and insights. May this *Handbook* serve as a beacon of hope and a guiding light in our ongoing quest for peace and security in a world fraught with uncertainty.

CPearce

Major General Cheryl Pearce
Acting Military Adviser
Office of Military Affairs
Department of Peace Operations

Writing workshop for the *Handbook*

No.	Rank	First name	Surname	Country/department/ organization
1.	Warr. Off. 1	David	SMYTHE	Australia
2.	Col.	Thomas	ENENKEL	Austria
3.	Mr.	Orkhan	TALIBOV	Azerbaijan
4.	Mr.	Dmitri	ALECHKEVITCH	DPO OROLSI PD
5.	Sen. Capt.	Nounagnon Ruben Cyrano	TESSI	Benin
6.	Warr. Off.	Dann	BORK	Denmark
7.	Cdr.	Samuel	THUILIER	France
8.	Cdr.	Christian	DUERR	DPO OMA PDT
9.	Maj.	Andreas	BERGMANN	Germany
10.	Warr. Off.	Zoltan	MÉSZÁROS	Hungary
11.	Lt. Col.	Ridwan	ABDUL	DPO OMA MPS
12.	Maj.	Brian	CLANCY	Ireland
13.	Lt. Col.	Marco	APPODIA	Italy
14.	Maj.	Habert	NJAGI	Kenya
15.	First Serg.	Elvijs	ERNESTS	Latvia
16.	Comm. Insp.	Romas	DIDZIULIS	Lithuania
17.	Capt.	James	GAUCI	Malta

No.	Rank	First name	Surname	Country/department/ organization
18.	Lt. Col.	Sergio	VALENCIA SICAIOS	Mexico
19.	Maj.	Thomas	SHANAHAN	NATO Centres of Excellence – Counter-Improvised Explosive Devices
20.	Capt.	Erik-Paul	DE JONGE	Netherlands (Kingdom of the)
21.	Maj.	Joseph	ENYIA	Nigeria
22.	Lt. Col.	Muhammad	SAFDAR	Pakistan
23.	Capt.	Michal	ADAMIAK	Poland
24.	Lt. Col.	Jean Emmanuel	BADIANE	Senegal
25.	Maj.	Oumar	BA	Senegal
26.	Mr.	Rowan	BURROWS	UNMAS Mali
27.	Warr. Off. 1	Kevin	WRIGHT	United Kingdom
28.	Capt.	David	OWLES	United Kingdom
29.	Mr.	Judson	STROM	SETAF
30.	Mr.	Chris	LEE	AFRICOM
31.	Maj.	Benjamin	HOWARD	UNMAS

Not in the picture

32.	Mr.	Ruslan	BILOUS	DPO OROLSI PD
33.	Lt. Col.	Mohammad Shahed	CHOWDHURY	DPO DPET ITS
34.	Mr.	Decio	LEAO	UNDSS DPSS
35.	Mr.	Ralf Alexander	RIEBL	UNDSS DPSS
36.	Mrs.	Sophie	VAN ROYEN	UNMAS MINUSMA
37.	Mr.	Mark	FLOOD	UNMAS MINUSMA
38.	Capt.	Austin	GALLAIS	Canada
39.	Gp. Capt.	Paulinus	OKONKWO	DPO OMA PDT

Rationale

United Nations peacekeeping operations are often deployed into complex and volatile environments that may include unresolved violent conflict between non-State and State armed groups. Operations in those missions are further complicated by the threat of improvised explosive devices (IEDs). IEDs are comparatively cheap to produce and present an ever-growing threat to peacekeepers and the local population. Within a United Nations-led peace operation, the military is usually not alone and is always working alongside United Nations police and civilian personnel from various United Nations entities. Owing to the nature of the threat posed by IEDs, a comprehensive and coordinated approach is needed to achieve mandated tasks, mitigate its impact and minimize the risk to personnel and property.

Accordingly, based on the Secretary-General's Action for Peacekeeping initiative, the Declaration of Shared Commitments on Peacekeeping Operations and Security Council resolution 2436 (2018), as well as the recommendations of the Special Committee on Peacekeeping Operations, this *Handbook* is provided to improve the safety of peacekeepers within the continuously evolving peacekeeping environment.

Purpose

The purpose of the *Handbook* is to provide United Nations military commanders, police supervisors and planning staff officers with a coherent conceptual framework and operational vocabulary to address IED threats.

This *Handbook* also aims to be a reference for everyone involved in United Nations peacekeeping operations, regardless of whether they are uniformed personnel or civil servants, who are required to contribute in the best possible way to mitigate the threat.

Adoption of the terminology and definitions provided in this *Handbook*, annex A, is imperative to improving the reporting, collection and exploitation of IED information at the tactical and operational levels and will assist in:

- Improving database content management.
- IED threat mitigation-related education and training.
- Development and understanding in support of IED threat mitigation policy and doctrine.

Scope

This guidance applies to all those involved with IED threat mitigation activities in the protection of civilians, safety and security of United Nations personnel and other responsibilities in pursuit of United Nations mandates.

Hierarchy

The present *Handbook* is the principal guidance document for IED threat mitigation at the operational and tactical levels of United Nations peacekeeping. It is subordinate to the Department of Peace Operations Counter-IED (C-IED) Strategy.[1] It should be read alongside other guidance relating to force protection, explosive ordnance disposal (EOD) and protection of civilians.

This *Handbook* replaces the first edition of the *IED Threat Mitigation Military and Police Handbook* from December 2017, as well as the Mine Action Service of the United Nations (UNMAS) IED Lexicon (2017).

Reference

All United Nations guidance documents referenced in the present *Handbook* are available at

The Policy and Practice Database (for personnel in the United Nations system):

- ○ https://unitednations.sharepoint.com/sites/PPDB

The Peacekeeping Resource Hub:

- ○ https://peacekeepingresourcehub.un.org

[1] Strategy on Counter Improvised Explosive Device (C-IED) for Peacekeeping Operations. Available at https://resourcehub01.blob.core.windows.net/$web/Policy%20and%20Guidance/corepeacekeepingguidance/Thematic%20Operational%20Activities/Mine%20Action/Counter%20Improvised%20Explosive%20Device%20for%20Peacekeeping%20Operations%20(Strategy)%20(2024).pdf.

Posters

The posters contained in this *Handbook* are available online on the Peacekeeping Resource Hub, under the Training section, Functional Training, Military Explosive Ordnance Disposal (EOD) Unit:

https://peacekeepingresourcehub.un.org/en/training/stm/eod

It is encouraged to use these posters in national or in-mission training for continuous sensitization in United Nations peacekeeping missions (e.g. by placing them in buildings), but also for risk education, for example.

1. IED threat

The term improvised explosive device (IED) threat mitigation is used to denote the scope of activities undertaken in United Nations missions where IEDs impact mandate delivery.

An IED is “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”.[1] IEDs fall within the scope of the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-personnel Mines and on Their Destruction, if and when they constitute anti-personnel mines as per the definition in article 2.[2]

The use of IEDs is not new in warfare. They may be simple in design or sophisticated, incorporating modern electronic components. IEDs are a subset of several forms of asymmetric physical attack, which enable adversaries to strike without being decisively engaged – an extremely effective weapon of choice. IED proliferation is so widespread that it has become a global threat.

IED attacks[3] do not target only armed forces, security forces or parties engaged in conflict, but also civilians, government and local officials, and members of humanitarian organizations. It may also cause collateral damage if the attack is indiscriminate.

There are many reasons a person or group may use IEDs. In this *Handbook* the person or group is referred to as the perpetrator.[4]

IEDs may be used to initiate complex attacks that include a direct assault or an ambush to inflict lethal damage or to demonstrate the target’s vulnerability. The motivation of perpetrators varies widely and may extend from a radical ideology to financial reward.

The perpetrator’s intended outcome can include long-term strategic, political, ideological or psychological effects, as well as immediate tactical effects. Primarily, IEDs are intended to kill people. In addition, it could be used to:

- Damage, destroy or penetrate armoured vehicles.
- Damage or destroy physical infrastructure, aircraft and their payloads and watercrafts.
- Kill or wound first responders, such as exploded ordnance disposal teams, medics and firefighters.
- Obtain knowledge of peacekeepers tactics, techniques and procedures (TTPs).
- Harass, disrupt or extort, as criminal activity.

[1] International Mine Action Standard, IMAS 04.10 second edition, amendment 11, January 2023.

[2] See www.unmas.org/sites/default/files/documents/apmbc.pdf.

[3] An aggressive and violent action by an IED perpetrator designed to destroy, incapacitate, harass or distract an intended target.

[4] In this *Handbook* an IED perpetrator is considered any person or group of persons or organization that has the intent and/or capacity to inflict or threaten physical violence through the use or threatened use of IEDs. The affected person is the victim.

- Experiment to improve IED lethality or create an obstacle to channel movement.

Those who manufacture IEDs continuously alter the characteristics, the functioning or the delivery method of the device.

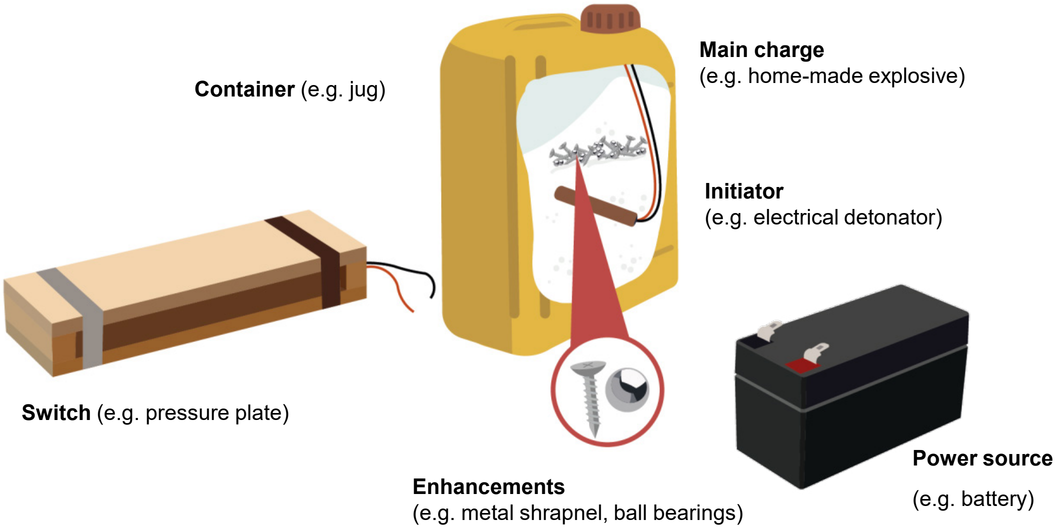
IEDs generally consist of a:

- Switch
- Initiator
- Main charge
- Power source
- Container

And they may contain:

- Enhancements.

Figure 1.1
Components of an IED


Container (e.g. jug)
Main charge
(e.g. home-made explosive)
Initiator
(e.g. electrical detonator)
Switch (e.g. pressure plate)
Power source
(e.g. battery)
Enhancements
(e.g. metal shrapnel, ball bearings)

All IEDs can be classified in one of the following categories:

- Timed
- Command
- Victim-operated

There are, by definition, no manufacturing standards for IED construction, although new trends may appear and change over time, and there may be attempts to achieve commonality between IED components.

Figure 1.2
Timed IED

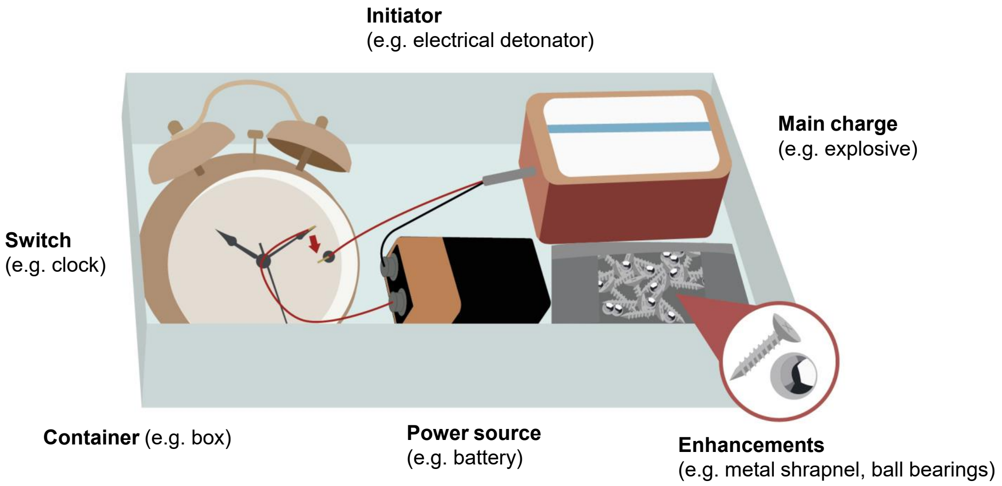


Figure 1.3
Command wire IED

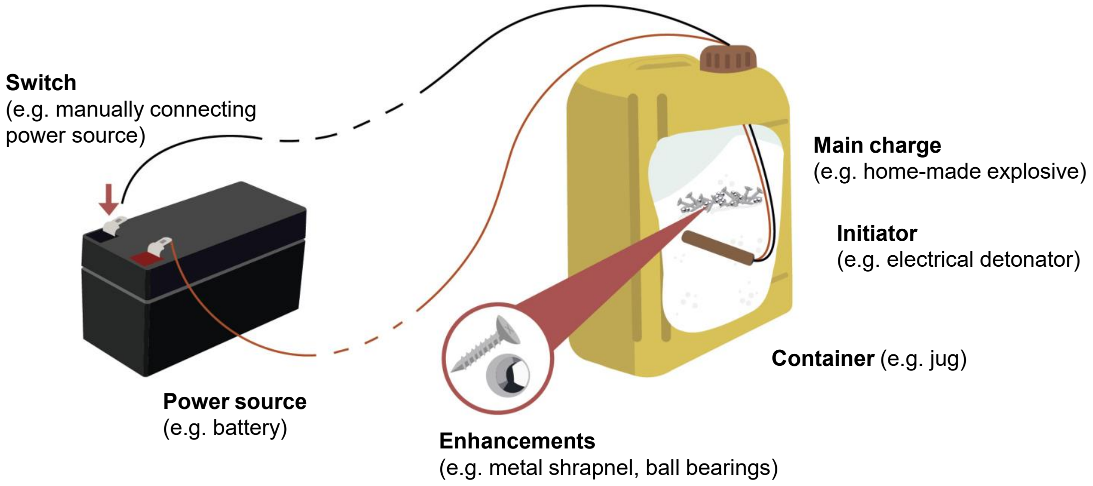
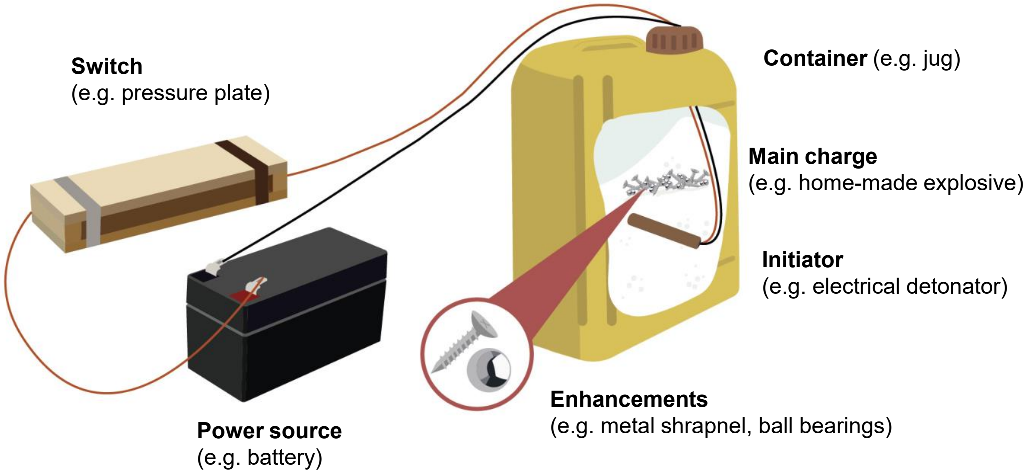


Figure 1.4
Victim-operated IED



IED attacks take a toll both in terms of human casualties and psychological impact, as well as causing damage to vehicles, infrastructure and resources and supplies. IEDs are often indiscriminate killers, hampering reconstruction efforts, stabilization tasks and the delivery of humanitarian aid in conflict and post-conflict environments. The clearance of IEDs, along with explosive remnants of war (ERW), which can be used to manufacture IEDs, is an essential prerequisite for the safe and unimpeded delivery of humanitarian assistance and the return of life to normal in a post-conflict environment.

Perpetrators attack civilian targets to create an environment of insecurity and fear. There are no patterns, but places with large crowds are particularly targeted for attacks owing to the possible high number of victims, such as

- Public meetings and political rallies
- Return of displaced persons
- Government buildings, courts and community centres
- Gathering places of security forces, especially recruitment locations

IEDs are tactical weapons, but they can have effects up to the strategic level. They create a profound psychological and destabilizing effect, leading to widespread fear and demoralization on the local population by creating the impression of insecurity, thereby damaging the cohesion between the population and the legitimate government. This contributes to political instability, diminishing the legitimacy of the ruling government, as well as impeding socioeconomic life and host nation service delivery. The impact can also be felt beyond immediate borders and on a regional level.

Operating in areas with an IED threat can also have a significant psychological and physical impact on host nation security forces, United Nations peacekeepers and civilian staff.

Media and political attention given to the actions of IED perpetrators can reach far beyond the borders of the country in which an attack occurs and affect domestic and international support for a United Nations peacekeeping mission.

IED manufacturers continually adapt their designs to circumvent effective IED threat mitigation measures.[5] Furthermore, perpetrators spread/share their knowledge using numerous communication technologies available.

Thus, addressing the issue of IEDs requires:

- The entire hierarchy of peacekeepers to be informed, trained, equipped and supported to be capable of understanding, identifying and planning against the threat of IEDs.
- All mobility units[6] to be appropriately trained and equipped to conduct an all arms search.
- Explosive ordnance disposal (EOD) units[7] to be appropriately trained and equipped to enable the safe conduct and disposal of IEDs.

[5] IED threat mitigation measures focus on the application of physical, procedural and training responses which can be applied collectively to mitigate the threats posed and consequences of IED attacks.

[6] Mobility units are defined in this *Handbook* as units moving outside the secured perimeter of a United Nations installation to execute any given task.

[7] Improvised explosive device disposal (IEDD) operators may be generated either from government, military, police, commercial or non-governmental entities.

In-depth knowledge of IEDs enables the efficient identification of the resources, training, equipment and capabilities required to effectively mitigate the threat. Considering the safety of peacekeepers and civilians is a priority, these improvised devices must be studied to determine their components, functioning and methods of employment within the context of the local and regional environment.[8] This technical and operational information must be recorded and shared with all actors engaged in IED threat mitigation to enable a recognized IED threat picture to be developed and to adapt the most appropriate IED threat mitigation tactics and methods.

1.1. IED system

The IED system adopted by perpetrators or non-State actors may or may not be structured. It involves multiple actions, from the collection and procurement of material for IED manufacturing to the placement of the IED at the point of attack. It requires elaborate planning and resources, including personnel, technical expertise and IED-making material. The actual IED attack is just one part of the whole system.

A perpetrator must conduct many activities supported by personnel and resources for an IED event to be executed. Collectively, these activities are linked by networks and are described as the IED system.[9]

An IED event is only a single activity within the overall IED system, which is made up of networks of links and nodes. An IED system:

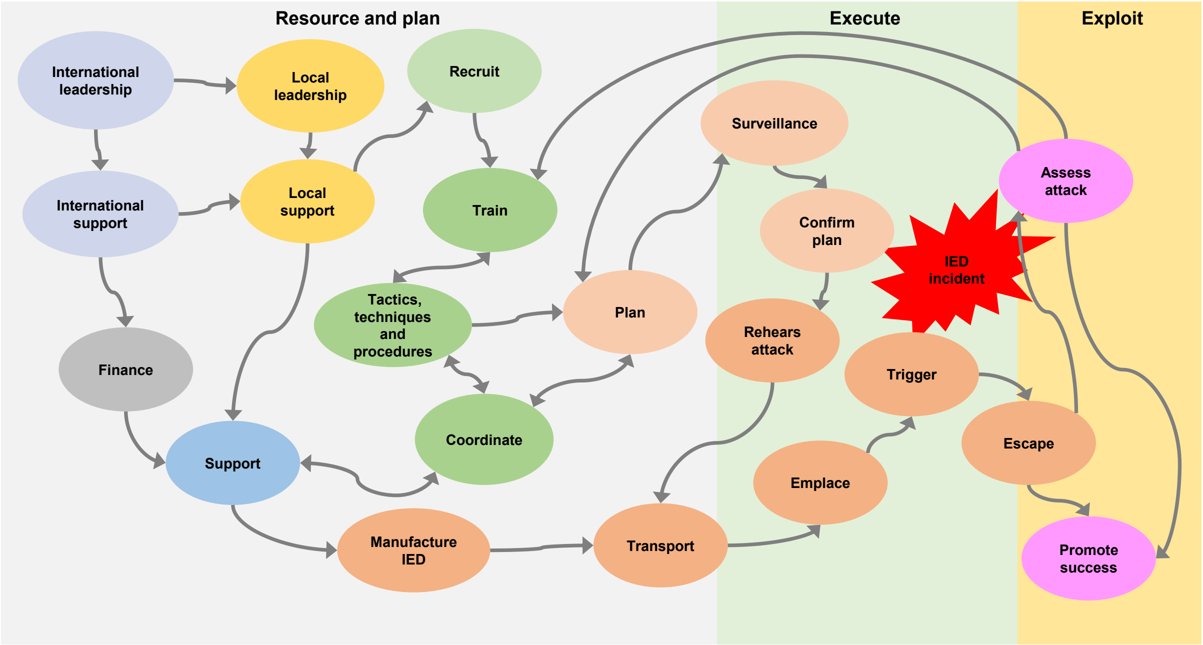
- typically comprises multiple activities executed by different elements but could just as easily consist of a few individuals filling multiple roles.
- requires multiple actions and resources to stage an IED event.
- may be either hierarchical or non-hierarchical, but it will contain critical capabilities, such as personnel, resources and actions that are linked.
- may incorporate international leadership, financing and procurement and support from outside of the mission area.
- may be part of large, international threat networks; some may be State-sponsored while others may work completely independently and may extend from the global down to the lowest level.

All those activities can be further categorized into three areas: resource and plan, execute, and exploit (see figure 1.5). Ideally these activities take place sequentially for a single IED event but are likely to occur concurrently or simultaneously. Separate perpetrator activities are often conducted by cells within the network whose members may be unaware who is in the other cells conducting other activities.

[8] Security Council document S/2021/1042, “The United Nations Response to Explosive Ordnance Threats: A more coherent approach is needed”, 23 November 2021; see also the Strategy on Counter Improvised Explosive Device (C-IED) for Peacekeeping Operations.

[9] Networks are considered a subset of the concept of the IED system.

Figure 1.5
IED system activities



Resource and plan involve obtaining financial and technical support, recruiting and training, material collection and manufacturing of the IED. Usually, an IED is made at a remote location to prevent premature detection. After preparation of the IED, a specific plan for its placement is prepared and local support is critical.

In the **Execute** phase, prepared IEDs are transported near the anticipated target location. After carrying out reconnaissance of the targets, the precise attack plan is prepared (time and point of attack) and rehearsals are sometimes carried out. At a suitable time, the IED is emplaced at the target location, usually at night or early in the morning to avoid detection. The emplacement of IEDs is usually guided by the following principles:

- Achieving maximum effect
- Avoiding detection
- Defying neutralization

Exploit usually consists of two subphases: assessing the results and projecting success. Success or failure of the IED attack is ascertained by observation. It is measured through its consequences, which may be in casualties, in the fear created within the general population, by the reaction of security forces or by the response at the national and international levels. Observations of the attack and of the responses of victims and locals also provide lessons learned to the perpetrators to overcome any mistakes made and to consider an increase in the lethality of future IED attacks.

IED attacks are essential elements of the perpetrator's information strategy. Images and other details of successful IED attacks are usually recorded and released to the targeted population, either directly or via the media. This is to boost support; lower the morale of peacekeepers, security forces and locals; and create an image of security failure.

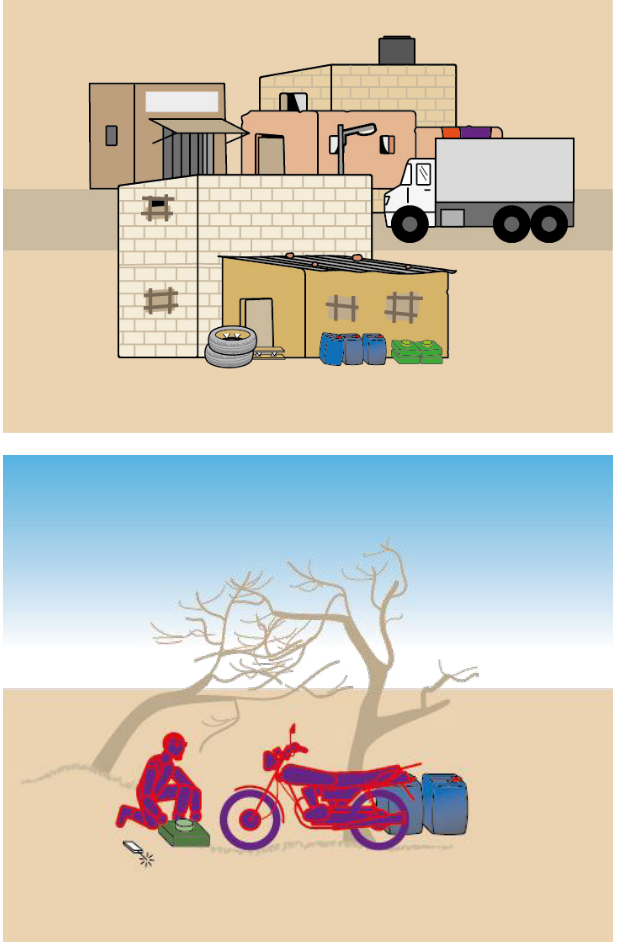
Within IED systems, network members may exchange information using low-cost global communications, and they have the ability to operate part-time and blend into civil society when actions are completed. That is why these systems are survivable, extremely resilient and invariably hard to target. Accurate analysis and evaluation must define the critical vulnerabilities of an IED system. This is a continuous and evolutionary process, reflecting the dynamic nature of the threat and essential for effective IED threat mitigation execution.

1.2. IED system key perpetrators

To employ an IED, different actors are required, whose involvement is usually linked to one of the three areas: resource and plan, execute, and exploit.

To mitigate the threat of IEDs it is not always necessary to find and neutralize the device itself. The engagement of political leadership of a United Nations peacekeeping operation with local authorities or even perpetrators themselves might lead to the identification and neutralization of one of the actors thereby degrading the network.

Figure 1.6
IED building place hidden in village and IED emplacer



The distribution of tasks is not always strictly separated and can overlap. For example, one person performs several activities that follow each other or at various times in the process.

The perpetrators do not all have to belong to a particular group or social class. Nor do they all have to be located in the same region or country. It is possible that the perpetrators come from different social environments, act from various places and cannot be found locally at all but are connected only by the same goal. It is also possible that not even this fact is given, as they carry out their activities independently of each other without knowing what purpose or goal their contribution serves. In that case it can be assumed that there is at least one person or group that coordinates the different activities.

In this respect, any information can contribute to mitigating the threat, and efforts should not focus exclusively on the IED itself; understanding and analysing all activities of the network are necessary to have a solid foundation for minimizing the threat.

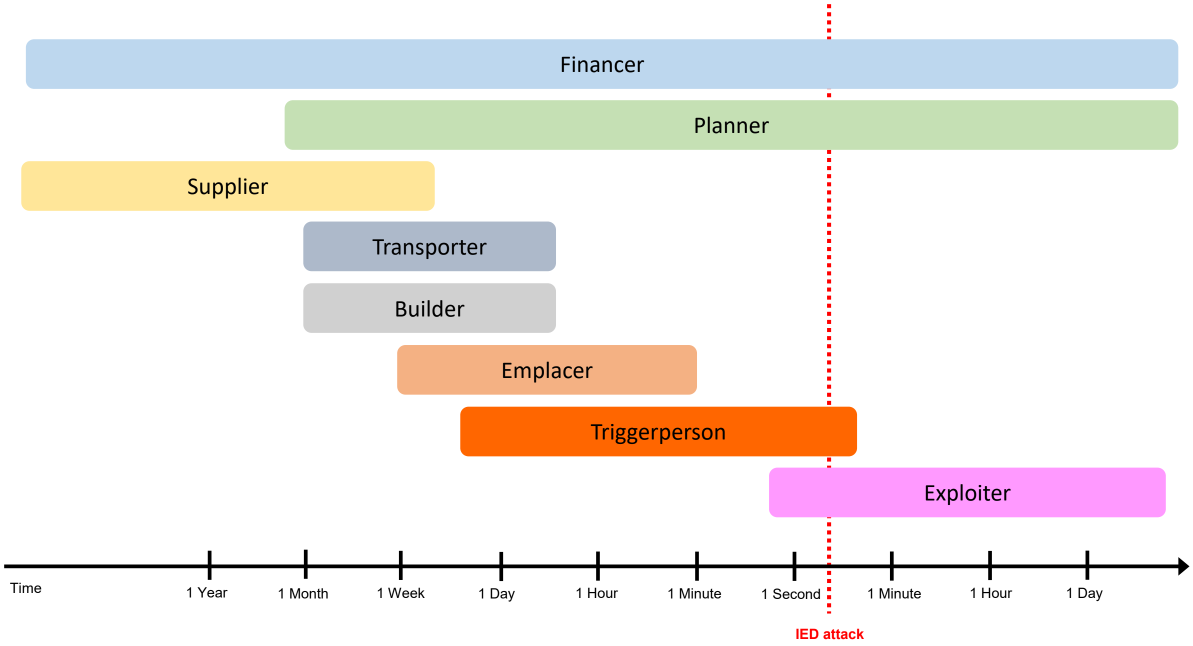
A network may include the following:

- Financer, who organizes funding or funds by own means for the activities.

- Planner, who plans, organizes and synchronizes all efforts.
- Supplier, who provides the parts and associated components to build the device.
- Builder, who builds the device.
- Transporter, who transports the IED to the place of use.
- Emplacer, who places the IED at the place of intended attack.
- Triggerperson,[10] who observes the movements of the peacekeepers and operates the trigger of an IED.
- Exploiter, who monitors and evaluates the effectiveness of the attack.

Figure 1.7

IED system key perpetrators



1.3. Perpetrators' TTPs

An understanding of the IED threat environment is enhanced by knowing the current trends in IED manufacture and use. To build that understanding, a continuous threat assessment for any United Nations peacekeeping operation is mandatory and must be conducted to identify emerging threats and current operational realities.

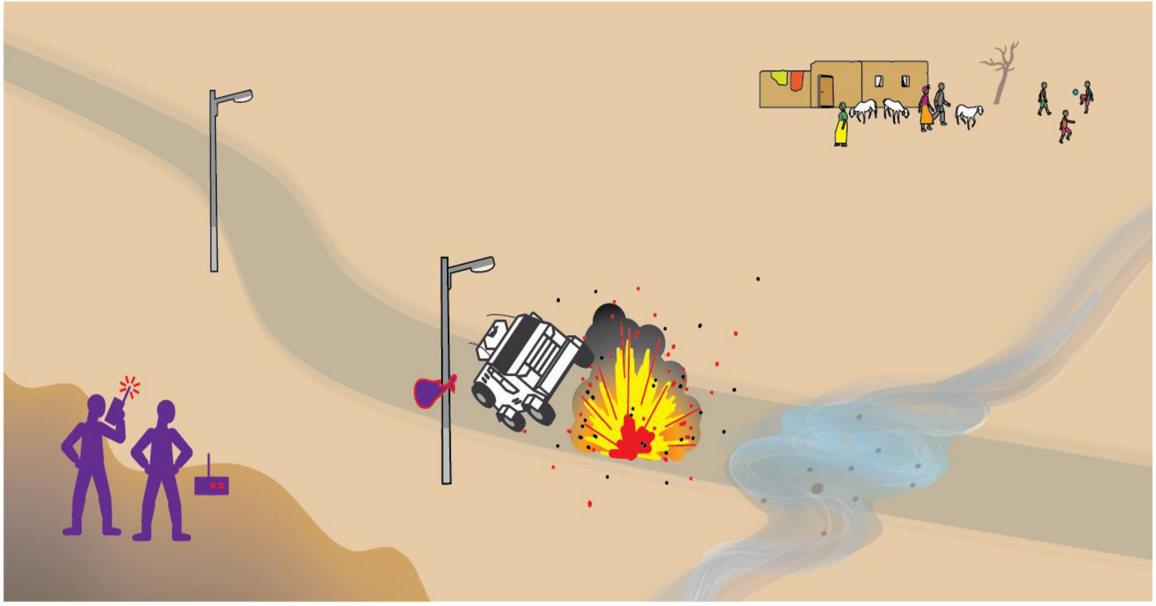
The inexpensive nature of precursor material (e.g. containers, gun powder, home-made explosives, ball bearings, nails, wires, wooden pieces) has made IEDs easy to manufacture. Information on how to make IEDs can be found and shared quickly via the Internet. Technical knowledge of electronic circuits is also utilized for the preparation of remotely operated and timed IEDs.

[10] A person who will manually close the electric circuit at a chosen time to make the IED explode is also referred to as the triggerperson.

The IED threat is transnational in nature. Porous borders facilitate movement and transportation of IEDs and associated components from one country to another such that the IED threat is similar in countries within a geographic region. Similarities can be found in the perpetrators' TTPs of IED attacks. As a result, the response to the IED threat must also be transnational, through cooperation with neighbouring States.

The IED is an evolutionary threat. It retains its relevance using ingenuity in manufacturing and deployment methods. Moreover, due to easy access to IED-making methods (mainly through the Internet), low-tech IEDs can become high-tech. The perpetrator can modify TTPs to counter the IED threat mitigation capabilities of United Nations military and police personnel.[11] In view of these trends, there is a need to continuously monitor the IED threat once a peacekeeping mission is deployed, both inside and outside the mission area.

Figure 1.8
Perpetrator TTPs



Perpetrators continuously observes United Nations peacekeeping operations best practices to exploit patterns. From one rotation to another they evaluate the capacity of the contingent and they use new practices or they reuse old practices to target United Nations peacekeeping operations.

In the recent past, some trends, listed below, have been observed. However, this list should be viewed critically, because trends can change very quickly owing to the transfer of knowledge, the availability of new technical equipment and construction materials and so on, as well as the assessment of the TTPs applied by United Nations entities to mitigate the threat.

[11] A hoax is an IED incident that involves a device fabricated to look like an IED and that is intended to simulate one to elicit a response. A hoax IED can be placed to observe peacekeepers' TTPs. Hoax devices are also used to draw troops onto the grounds for subsequent attack and to divert an intended action.

At the start of a United Nations peacekeeping operation any available source, for example, local authorities, non-governmental organizations (NGOs), the Mine Action Service of the United Nations (UNMAS) and so on, might be able to provide information regarding the existing threat.

Once the United Nations peacekeeping operation is established, the IED threat mitigation working group, U2 (intelligence), the Joint Mission Analysis Centre or crime intelligence units will be able to provide continuously updated information on the latest trends.

Trends in IED attacks in various conflict areas are as follows:

- Several types of IEDs, including person-borne IED, vehicle-borne IED, command wire IED, radio-controlled IED, victim-operated IED and other uncategorized IEDs, are confronting United Nations peacekeepers in mission areas.
- IEDs are usually planted on roadsides and in the middle of rough tracks.
- IEDs formed out of artillery projectiles, rockets and missiles are often used to create maximum destruction.
- Vehicle-borne IEDs are used to attack United Nations convoys, buildings and infrastructure.
- Suicide bombers wearing suicide vests filled with explosives and metal shrapnel target check posts, community meetings, marketplaces and congregations.
- IEDs can be activated using a wide range of switches, including remote detonation by cell phone and other wireless devices, or activated through contact with a pressure plate and so on.
- Uncrewed systems (land, air and sea) are used to either deliver an IED or be directly employed as an IED.
- Complex attacks using a remote-controlled device, a pressure plate with large amounts of explosives or multiple command and victim-operated IEDs with large explosive charges, in conjunction with a direct fire small arms attack.

IEDs are generally situated:

- Near inhabited zones
- At a vulnerable point
- In vulnerable areas

Figure 1.9

Example of command wire IED emplacement and initiation

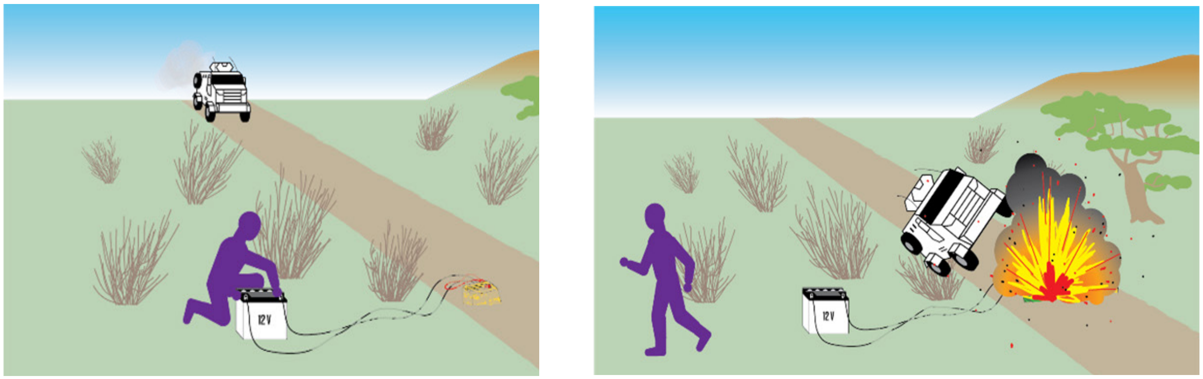
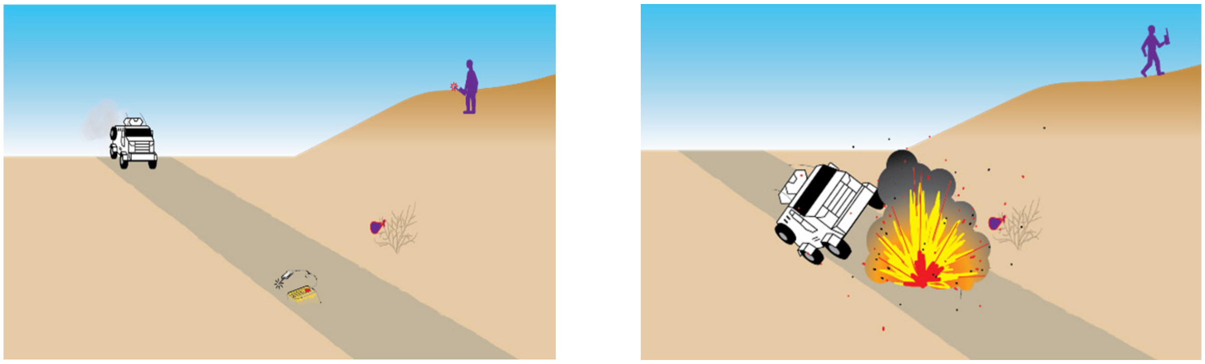


Figure 1.10
Example of remote-controlled IED emplacement and initiation

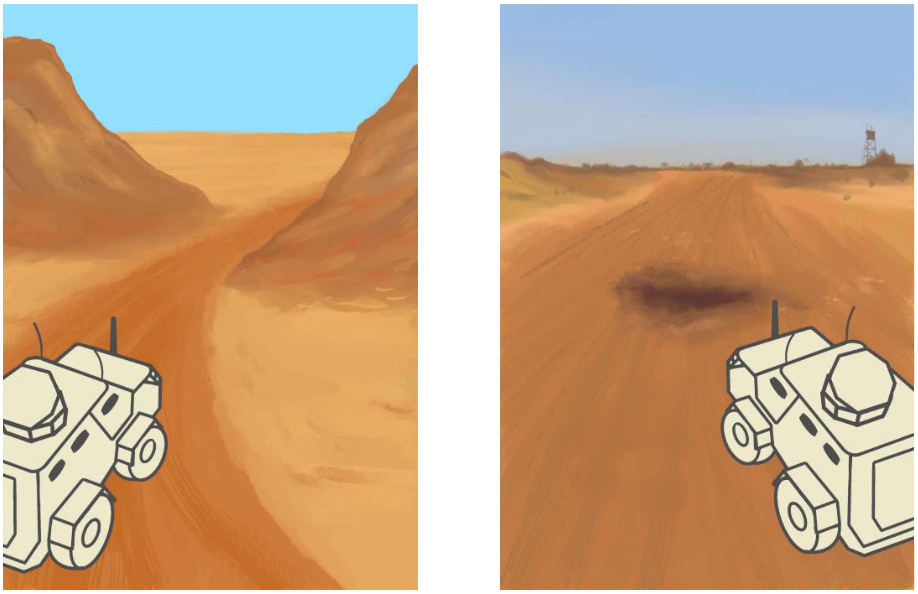


A **vulnerable point** is a specific point where it is particularly advantageous to target-friendly forces with an IED and/or small arms and light weapons, ambush or both. They are typically characterized by prominent or restrictive features, such as limitation of speed, movement or visibility due to terrain or choke point on the ground. They could also be based on patterns established by peacekeepers, using the same entry to camps, patrolling the same roads and villages, using the same lookout and so on.

Several factors pertaining to perpetrators capability, intent and ground use will contribute to the vulnerability of a specific point.

The assessment of vulnerable points must be continuously and dynamically conducted by all peacekeepers, factoring terrain, environmental considerations, patterns of life, atmospherics and so on.[12]

Figure 1.11
Examples of vulnerable points

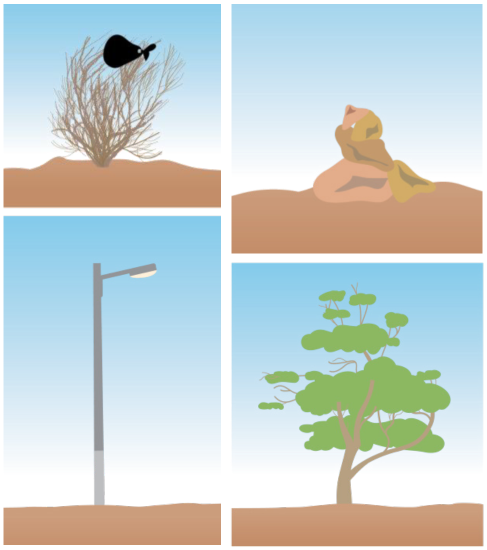


Channelling – caused by natural terrain

Channelling

[12] See www.gichd.org/fileadmin/uploads/gichd/Media/GICHD-resources/rec-documents/IED_indicators_and_grounds_sign_awareness_handbook__EN.pdf.

Bridges and culverts

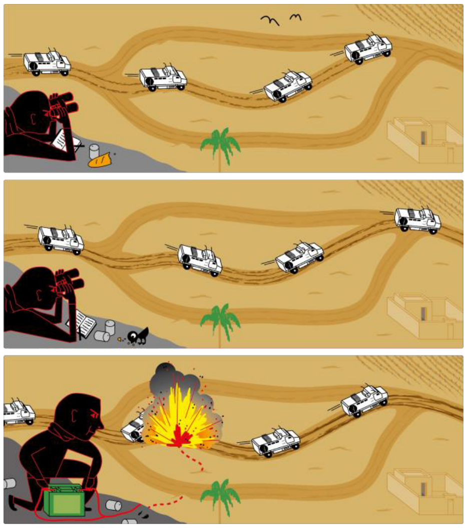


Markers

Predictability – avoid using same routes

Slow down point/junction

Previous attack locations and rest areas



Pattern setting

Vulnerable areas are those areas where the ground lends itself to an IED or small arms and light weapons attack. Common characteristics of vulnerable areas include the following (note the mnemonic POLICE THESE):

- **P**reviously used tracks and patrol routes
- **O**ften-used positions
- **L**inear features
- **I**nterior of buildings
- **C**analized routes
- **E**xtended long stretches of road

- **T**actically important areas
- **H**igh ground dominated areas
- **E**scape routes into and out of areas
- **S**uccessive vulnerable points in close proximity
- **E**xit or entry of areas of urban/rural interfaces

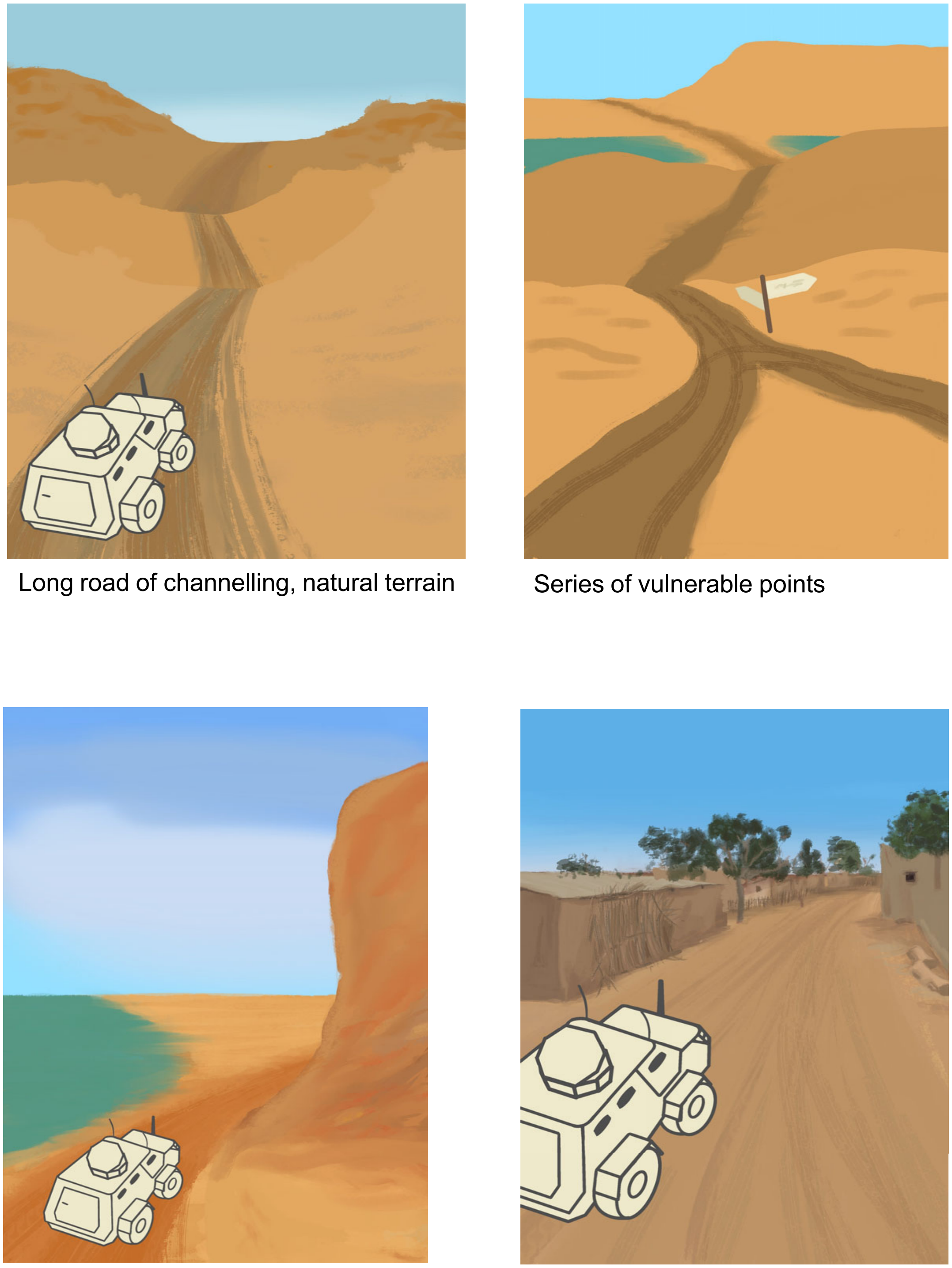
IEDs may be placed anywhere, especially when peacekeepers are the target of an attack. From the perpetrator's point of view, terrain sections with the following characteristics are suitable, where:

- Military and police forces have set regular patterns during moves.
- Terrain has a channelization effect.
- Terrain slows down the velocity of a movement/choke points.
- Terrain supports a follow-on ambush.

Common areas of IED emplacement include, but are not limited to:

- By the shoulder or buried under the surface of the road.
- Inside the culverts or concealed in the walls of culverts.
- On the trees alongside the road.
- Potholes in paved roads; additionally, the perpetrators may make their own "potholes" to emplace IEDs.
- Unpaved roads – in tyre ruts of likely movement areas.
- In areas with built-up and/or restrictive terrain that provide ample cover and concealment.
- Inside, beside or buried under heaps of any type of material or packaging.
- Concealed in cars, trucks, motorcycles, bicycles, dead animals and human carcasses.
- As secondary IEDs near the main IED, especially designed to target first responders.
- Placement in a manner that directs the blast into the pre-planned ambush area (e.g. placed along roadside or against rock piles, sand/dirt piles).
- Areas that slow, stop or canalize vehicles of military and police within the IED's blast radius.
- Where they can be combined with follow-on small-arms and rocket-propelled grenade fire.
- In previously used IED sites, for example, potholes that are covered with dirt or sand. Frequently multiple IEDs are daisy-chained together.
- Abandoned huts.

Figure 1.12
Examples of vulnerable areas



Long road of channelling, natural terrain

Series of vulnerable points

Large ground features

Urban/rural interfaces

The IED emplacer benefits from the support of observers who inform them about routes used by the peacekeepers and the approximate timelines of their arrival. They can place the IED a few minutes before the convoys pass. Mixed into the population and observing continuously, the perpetrator attacks when peacekeepers are predictable (e.g. routine movements in and out, or canalizing terrain). The perpetrator may continue to observe the spot where an IED has been placed to prevent civilian casualties. If the attack does not reach its target, the perpetrator may remove the IED or remove only the switch or the power source. In some cases, the IED can be kept permanently activated, if the intention is to target everyone.

Figure 1.13
"CAGE" scheme

CAGE is a simple tool that can be used by all soldiers to identify vulnerable areas and vulnerable points:

C

CHANNELLED

- Is your movement restricted to a specific route?
- Can you choose a less obvious route?
- Are there human-made or natural obstacles in your path?
- Your enemy will place IEDs at points where they are most likely to be channelized.

A

AIMING MARKERS

- Are there human-made or natural features that could be used as aiming markers for a command-initiated IED attack?
- An aiming marker must be visible from the firing point.
- Consider whether there are lines of sight and whether or not the ground lends itself to an attack.

G

GROUND

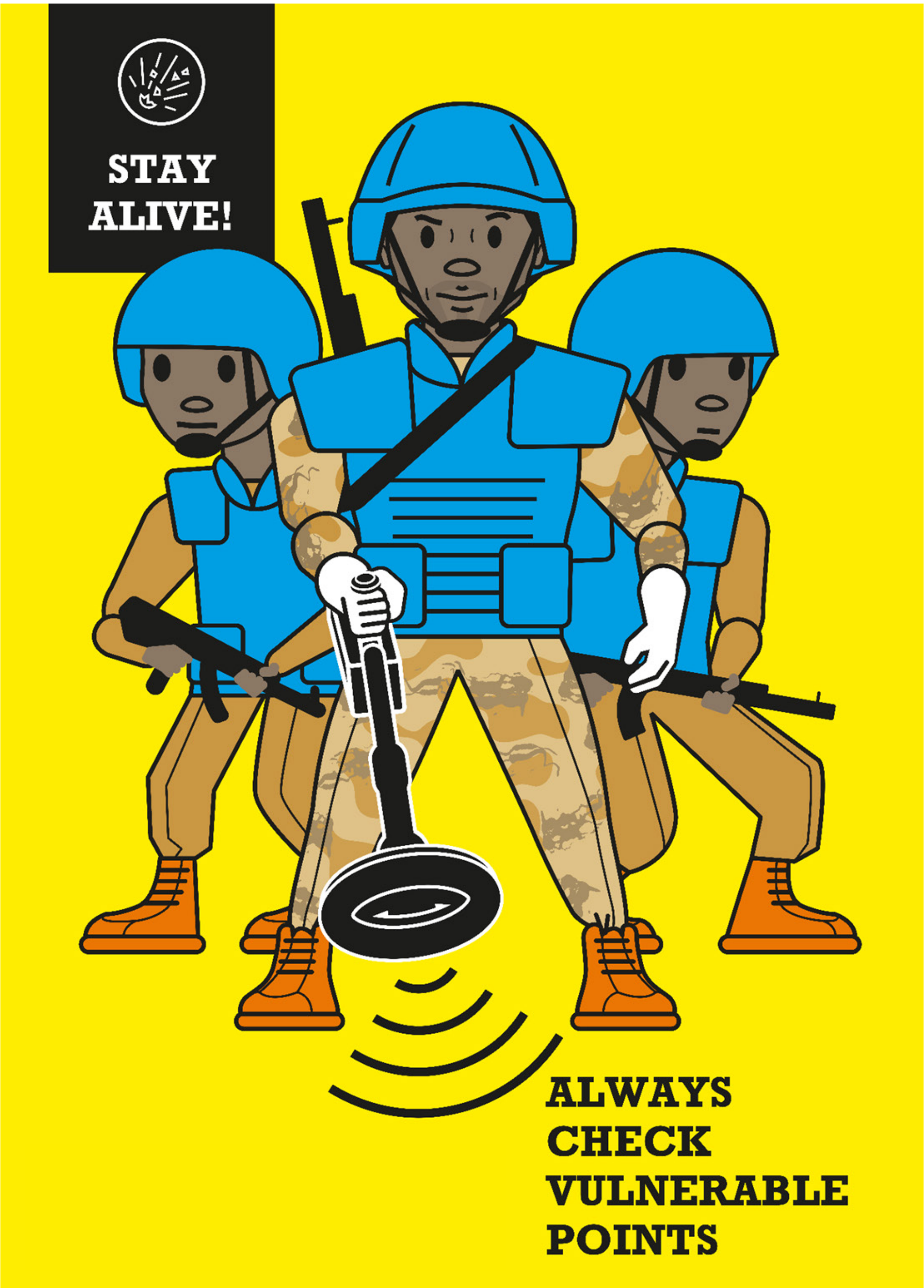
- Is there a ground sign present?
- Does the ground lend itself to an attack?
- Are you forced to slow down/reduce the gap between vehicles or persons.
- Are there good lines of sight (between a possible firing point and a contact point)?
- Are there escape routes for the enemy?
- Have patterns been set here or have friendly forces used the area before?
- Is this a site of tactical importance?
- Have you shown intent to use this ground?
- Does the area provide concealment for an IED emplacer?
- Crossing points, track junctions, bends and slowdown points.
- Urban/rural interfaces.
- Likely approach routes for force base.

E

ENVIRONMENT

- What does the atmosphere tell you?
- Is anything out of the ordinary? Is the market unusually quiet? Is the road less busy than normal? Ask yourself why.
- Look for the absence of the normal and the presence of the abnormal.

Figure 1.14
Sample poster for United Nations peacekeeping missions (1)



2. IED threat mitigation

Mitigating the threat of IEDs requires a comprehensive response and must not be planned or executed in isolation, confined to any single entity or implementation phase. It is cross-functional and must be fully integrated at the operational and tactical levels within the mission as part of the overall United Nations peacekeeping operations effort.

IED threat mitigation needs to be conceptualized for all phases of the mission life cycle, including:

- Assessment and mission planning
- Mission start-up
- Mandate implementation
- Transition or drawdown

Adopting a systematic approach, incorporating all elements, including United Nations military and police, the host Government and local resources, provides direction towards achieving a minimum IED threat level in the host State.

An effective IED threat mitigation approach involves the creation of a core capability through the force generation of IED threat mitigation assets. This capability needs to be formed with a multi-tier approach. Key operational capabilities include essential staff organization at the force headquarters level (both military and police), establishing command and staff responsibilities in the IED threat mitigation domain, the availability of EOD units or teams with the appropriate qualification to handle IEDs in the mission areas, a strong interface between the IED threat mitigation actors and the peacekeeping-intelligence surveillance and reconnaissance component, technical peacekeeping-intelligence, a well-established liaison and coordination mechanism and media support. In addition, essential support structures need to be detailed according to the threat assessment to enhance the potential of the headquarters for all phases of operations.

Capability requirements for peacekeeping will vary from mission to mission, depending on such factors as the mandate, security environment, geography, population distribution and even the climate. Although the spectrum of United Nations peacekeeping operations does employ some common capabilities, the military component and police requirements of each mission are planned with specific capabilities to achieve the desired effect based on the respective mandates. Civilian components, as well as human and technical peacekeeping-intelligence, also contribute to understanding the overall threat picture.

Consideration should be given throughout all mission planning processes to the identification of specific resources (e.g. materiel, personnel) required for effective IED threat mitigation measures. Findings related to threats posed by IEDs, as noted in the strategic, operational or other assessments should lead to development of the overall mission concept. These findings should be incorporated as part of the budget development processes, as well as the military, police and support concepts and plans. Materiel and equipment requirements should be addressed through the Chief of Mission Support and/or Director of Mission Support in relation to budget preparation.

The status of unit requirements/force requirement documents must reflect the findings and include the necessary capabilities for a particular unit.

2.1. Conceptual contours of IED threat mitigation

Primary responsibility for the security and protection of personnel deployed through the United Nations system and organizational property rests with the host Government.[13] The United Nations has a responsibility to reinforce and, where necessary, supplement the capacity of the host Government to fulfil these obligations.

The United Nations has a comprehensive system on safety and security which includes the United Nations Security Management System. United Nations civilian personnel and individually uniformed personnel and military or police are covered by the System.[14]

The security of troops with their contingents is covered by separate force protection mechanisms that encompass the capability of military units to manage risks and protect themselves from prevailing threats and hazards.

Military contingents are responsible for delivering diverse mandated tasks, often carried out in a challenging security environment, including IEDs. This necessitates that military contingents identify the threats, understand appropriate force protection procedures to manage these risks and emplace mitigation measures to minimize loss of United Nations personnel and property.[15]

The force protection guidelines include fundamental principles and operational guidance on measures to minimize the vulnerability of United Nations troops, facilities, equipment, materiel, operations and activities from threats and hazards to preserve freedom of action and operational effectiveness. Force protection is not limited to physical protection of troops, facilities or protection during movement; it also includes actions for mitigating other hazards and threats, such as information security, medical exigencies, fire and explosive ordnance (EO), including mines, IEDs and so on.

Hence for mitigating an IED threat, the force protection considerations and planning procedures are to be applied as described in the Guidelines, Force Protection for Military Components of United Nations Peacekeeping Missions (2021).

Notwithstanding the various responsibilities and procedures, adopting a systematic approach, incorporating all elements in a whole-of-system approach, including United Nations military and police, civilian components, the host Government and local resources, is key to planning, organizing and synchronizing the various capabilities in a United Nations mission to minimize the IED threat level in the host nation.

To this end, all efforts should be planned and sequenced in phases. Prerequisites to all phases are local and government support, integration of all stakeholders and the resolve of leadership at all levels.

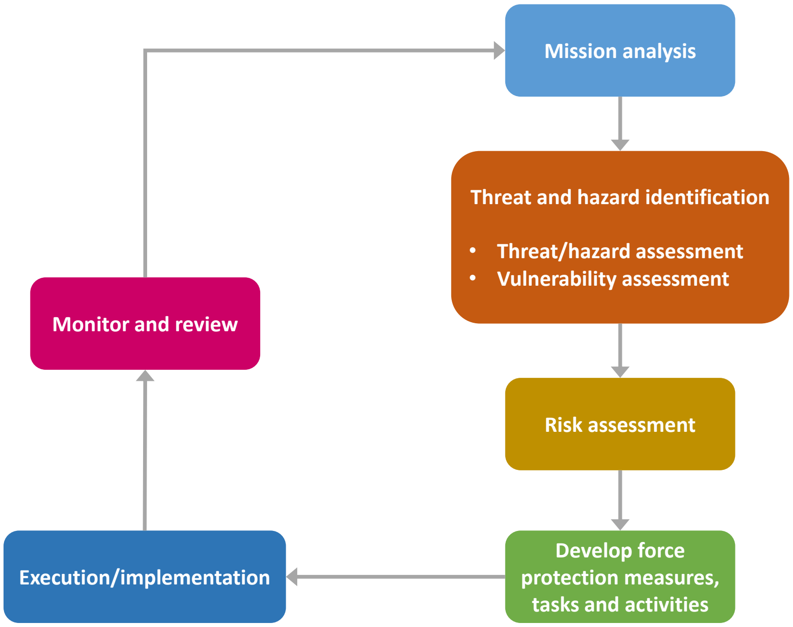
[13] Guidelines, Force Protection for Military Components of United Nations Peacekeeping Missions.

[14] *United Nations Security Management System: Security Policy Manual*, chap. III (25 August 2023):

Persons engaged by a United Nations Security Management System organization to perform services on a non-staff contract, such as a consultancy contract. This includes, but is not limited to, military observers, military staff officers, military liaison officers, individual police officers, independent contractors, international individual contractors, local individual contractors, personnel services agreement and service contract holders.

[15] Guidelines, Force Protection for Military Components of United Nations Peacekeeping Missions.

Figure 2.1
Force protection process[16]


Mission analysis
Threat and hazard identification
• Threat/hazard assessment
• Vulnerability assessment
Risk assessment
Develop force protection measures, tasks and activities
Execution/implementation
Monitor and review

Phase I – IED threat assessment

- Collection of information/peacekeeping-intelligence
- Management of the information
- Analysis of the information and definition of the threat

Phase II – Reduction of the threat level

- Operational planning/applying risk analysis
- Development of a threat mitigation plan
- Exploitation activities

Phase III – Mitigation of the threat

- Geographic containment of the IED threat
- Minimizing the transition of the threat or transfer of IED-making materials and knowledge from neighbouring States

2.2. Mindset/foundation

There are fundamentally different guidelines for mitigating the threat of IEDs within the United Nations as an organization.

For all United Nations personnel who are not military or police or individual unit personnel, the principles set out in the *United Nations Security Management System: Security Policy Manual* apply.

[16] Ibid.

Chapter III of the *Manual* governs applicability, while chapter IV discusses possible actions in detail.[17]

Managing the security risk from IED threat is one of both prevention and mitigation and can include various measures.[18] Active engagement is explicitly not desired.

In contrast, the possibilities for uniformed peacekeepers (military and police) and special entities, such as UNMAS, are much greater and include direct engagement of IEDs.

Regardless, for anyone in an environment where the threat of IEDs is prevalent, there are principles that are basic requirements and do not require any specific knowledge or skills.

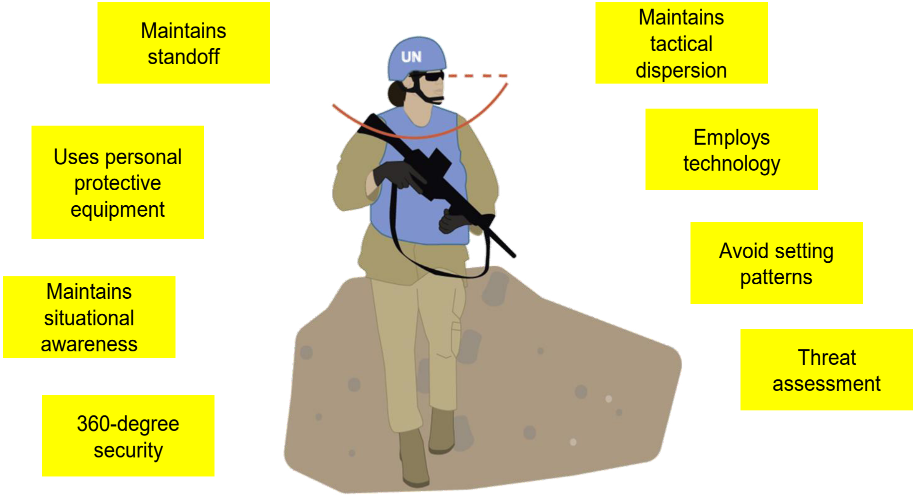
Among these requirements, the most important to successfully prevent and mitigate the threat posed by IEDs is the appropriate attitude – the right mindset.

Mitigation of the threat should not be considered as a task for a few, but rather as a joint effort of the entire United Nations peacekeeping operation.

Every uniformed peacekeeper, as well as United Nations staff, can make a valuable contribution.

To create and maintain the right mindset, commanders are required to give IED threats the appropriate importance and priority in the day-to-day management of tasks.

Figure 2.2
The right mindset



[17] *United Nations Security Management System: Security Policy Manual,* chap. IV, section P.

[18] Prevention entails physical, procedural and training measures intended to lower the likelihood of an IED incident occurring and affecting the United Nations. Prevention measures available to United Nations entities include, but are not limited to, information exchange and management, travel planning, security-awareness programmes and electronic countermeasures.

To maintain the mindset, the commander needs to do the following, among others:

- Request daily information regarding the threat in the mission, capabilities, shortcomings and so on; the provision of appropriate capacities, including personnel, equipment and training and, if necessary, the requesting of further resources.
- Train continuously and thereby improve existing competencies by granting necessary time.

The right mindset is particularly important if there is a comparatively low threat from IEDs within the mission or if the threat has decreased significantly over the past period. Owing to the dynamic nature of conflicts, it is to be expected at any time that such periods may be used by the perpetrators to make appropriate preparations, gather information about their own forces and so on. In this respect, a special effort is required to keep the vigilance of all those involved high to be able to react appropriately to a possible threat from IEDs at any time.

2.3. Protection of personnel and property

Besides having the right mindset, it is necessary to have a basic understanding of what injuries and damage an IED can cause and how to protect against them.

Literature on injury mechanisms from explosions identify four types of blast injuries:[19]

- Primary blast injuries are caused by the blast wave moving through the body. Since only high-order explosives create a blast wave, primary blast injuries are unique to high-order explosions. A blast wave causes damage to more extensively air-filled organs.
- Secondary blast injuries are the most common cause of death in a blast event. These injuries are caused by flying debris generated by the explosion. Terrorists often add screws, nails and other sharp objects to bombs to increase injuries.
- Tertiary blast injuries result from individuals being thrown by the blast. The most common types of tertiary blast injuries are head injuries, skull fractures and bone fractures. Treatment for most tertiary blast injuries follow established protocols for that specific injury.
- Quaternary blast injuries encompass thermal injuries due to the heat of the explosion.

In addition to the listed categories for blast injuries, which are also limited to physical injury patterns, events involving an IED attack almost always cause psychological effects as a result of previous or current injuries, which may affect the victims much later and often have even greater consequences than physical injuries.

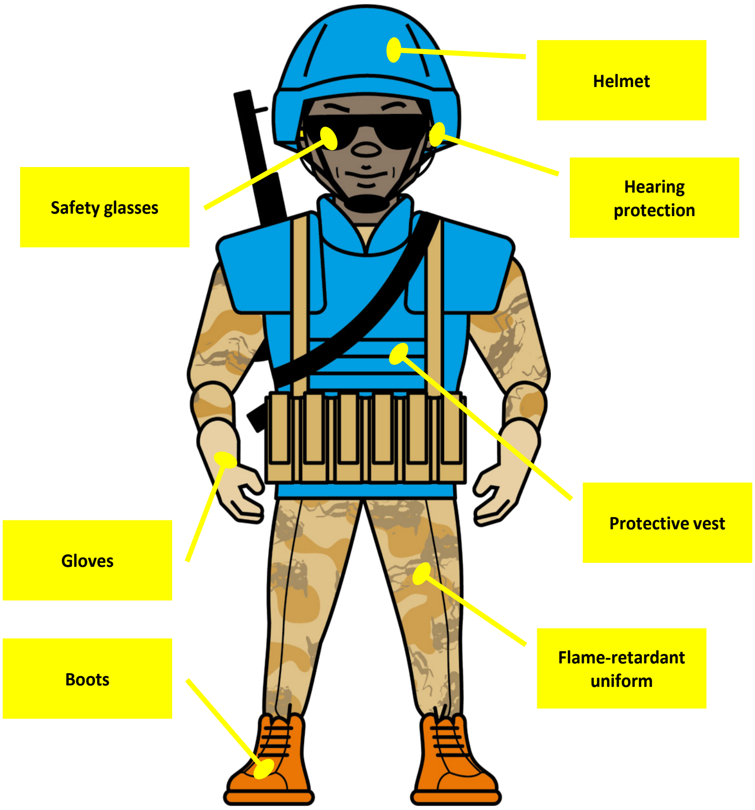
An IED attack may not be preventable. However, it is everyone's responsibility to minimize the risk as much as possible. This can be partially achieved if everyone is aware of what can provide physical protection and thus increase the chance of surviving an attack. However, physical protection is only one component that helps to minimize the risk. It goes hand-in-hand with all other efforts, planning consideration, procedures and so on, listed in the following sections.

[19] Ramasamy, A., and others. Blast mines: physics, injury mechanisms and vehicle protection, *Journal of the Royal Army Medical Corps*, vol. 155, No. 4, pp. 258–264. Available at https://militaryhealth.bmj.com/content/155/4/258.

2.3.1. Personal equipment

To provide immediate protection from the effects of an IED attack, especially heat-generation and fragmentation/explosive effects, it is necessary to wear protective equipment whenever in an environment with an IED threat.

Figure 2.3
Personal equipment



Inside United Nations buildings and facilities, these protective measures can usually be reduced. Depending on the location, it is recommended to continue wearing them in buildings outside United Nations properties if those premises have not been previously searched or assessed for a possible threat.

On patrol, both mounted on vehicles and dismounted, the protective equipment must always be worn, since persons are even more vulnerable without the physical protection of vehicles.

Commanders on the ground take the decision to adjust the level of personal protective equipment according to their assessment and in accordance with the established force protection procedures, including dress and vehicle code.

Among the basic personal protective equipment that should be worn are the following items:

- Helmet
- Protective vest
- Sturdy shoes or boots
- Safety glasses

- Gloves (flame retardant, if possible)
- Clothing made of either flame-retardant fabric or materials that burn without residue, such as cotton[20]
- Hearing protection (this may hamper communication, but is essential to prevent injury to the ears from blast trauma, for example)[21]

If these are not provided or are only partially available, the deficiencies are to be remedied immediately and possibilities are to be identified, to equip the personnel accordingly.

Besides the personal protective equipment, every person should be familiar with and carry the reporting format for an IED incident,[22] as well as the reporting format for medical incident, which requires medical evacuation (9-liner) or for the request of a casualty evacuation (CASEVAC).

Additionally, each peacekeeper should carry a personal kit with medical first aid material that enables the initiation of life-saving measures in the event of an accident (Buddy First Aid Kit or individual first aid kit).

2.3.2. Contingent-owned equipment

The contingent-owned equipment (COE) framework encompasses major equipment, personal protective equipment, ammunition and explosives to enable the troops to protect themselves and carry out their mandated tasks. The equipment is included in the specific or generic United Nations military/police requirement according to the operational tasks assigned to the unit. Troop- and police-contributing countries are obliged to deploy personnel, major equipment and self-sustainment pursuant to the signed memorandum of understanding.

All major equipment to support the IED threat mitigation effort are listed in the COE manual.[23] Equipment not listed in the COE manual but deemed necessary by either party to the COE may be agreed on during the negotiations. In this case reimbursement will follow the special case guidelines as described in the COE manual.

Demining and EOD equipment should perform in compliance with the relevant standards described in the *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual*, and the International Mine Action Standards (IMAS).[24]

2.3.3. United Nations-owned equipment

Equipment can also be procured and provided by the United Nations peacekeeping operations in the mission area. United Nations-owned equipment is issued to mission personnel to perform their daily

[20] Modern synthetic-fibre clothing is comfortable to wear in hot or humid tropical areas, but this clothing also carries the risk that in the event of an IED attack, the garments will burn into the skin and the burns will subsequently require significant medical treatment to enable recovery.

[21] Modern hearing protection has appropriate mechanisms that close in the event of a sudden bang and thus effectively protect the hearing but otherwise allow almost unimpaired communication.

[22] The formats are provided in annex D.

[23] *Manual on Policies and Procedures concerning the Reimbursement and Control of Contingent-Owned Equipment of Troop/Police Contributors Participating in Peacekeeping Missions.* Available at https://digitallibrary.un.org.

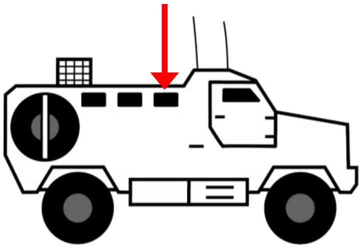
[24] See www.mineactionstandards.org/standards/.

tasks in support of the mission's mandate. Individuals signing for the equipment are responsible for the safekeeping, properly handling and reporting of any inventory discrepancy.

United Nations-owned equipment is handled by every United Nations peacekeeping operation independently and procedures are defined in specific standard operating procedures as per the operational situations. United Nations-owned equipment and related infrastructure may be provided by the mission to the deployed military and police contingents under the terms and conditions agreed upon in memorandums of understanding between the United Nations and the respective contingents. In exceptional cases, when the deployed contingents are unable to deploy full self-sustainment in terms of services and equipment or in cases of delays to replace aged equipment or replenish supplies, support from the respective Mission Support Division may be sought. United Nations-owned equipment is subject to physical verification by the property control and inventory unit/COE unit to ensure the correct status of the mission's inventory.

2.3.4. Vehicles

Figure 2.4
Mine-protected vehicle



The shutters of armoured vehicles must be closed to keep the blast effect out of the vehicle.

Convoys are a common target for IED attacks, as they provide opportunity to disrupt a mission's supply and operations. As such mine-protected vehicles remain a critical requirement in environments with a persistent IED threat, as they can greatly reduce the effects of a detonation. In the context of military-pattern vehicles, mine-protected vehicles are armoured personnel carriers or mine-resistant ambush-protected vehicles.[25]

These vehicles are designed to reduce the blast effect of explosive charges detonated under the wheels or under the vehicle's body. Design elements may include:

- High ground clearance to reduce blast effectiveness
- V-shaped bottom hull to deflect the blast
- Strong vehicle structure with increased load-bearing ability
- False floors to allow deformation of the outer hull without injuring the crew
- Padded cabin interior to prevent injuries and reduce secondary hazards
- Blast attenuation seats, commonly side or ceiling-mounted with blast cushions, shock absorption system and footrests
- Five-point seat harness for all passengers including the gunner
- Load-securing points, weapon racks and storage compartments to tie down equipment
- Fire-resistant materials
- On-board fire extinguisher/fire suppression system

The overall design of a vehicle defines its protective level, which is expressed in kilograms (TNT equivalent) blast anti-tank mine, either under the wheels or anywhere underneath the vehicle. For mission

[25] *Manual on Policies and Procedures concerning the Reimbursement and Control of Contingent-Owned Equipment of Troop/Police Contributors Participating in Peacekeeping Missions*, chap. 3, annex A, appendix 2.

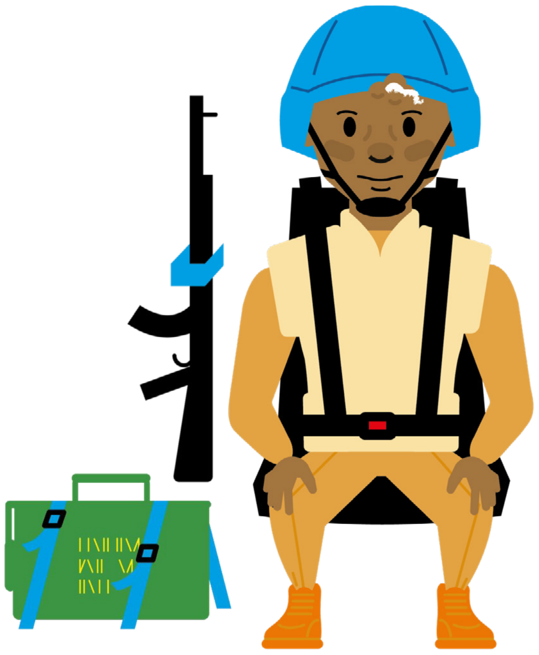
environments with prevalent explosive threats, a blast protection level of at least 10 kilograms (TNT equivalent) blast anti-tank mine, both underneath the belly and the wheels, is recommended.

While the listed items of personal protective equipment are recommended to be carried at all times, there may be different national rules and regulations for vehicle-mounted patrols. Nevertheless, it is recommended that:

- Helmets should be worn at all times to reduce risk of traumatic brain injuries.
- Personal protective equipment should be worn to reduce risk of injury from flying fragments.

It is equally imperative to ensure that inside the vehicles the use the personal restraint system and a proper seat position is maintained at all times. This ensures that in the event of a blast, a person does not suffer secondary damage from colliding with sharp objects in the vehicle and sustaining penetrating or blunt trauma as a pattern of injury. The use of this safety device may significantly reduce flexibility, especially on long journeys and may also hinder quick reaction to dismount. On the other hand, the correct application of these safety measures significantly increases a person's chances of survival. In this respect, safety must be given priority over operational flexibility.

Figure 2.5
Code of conduct in the vehicle



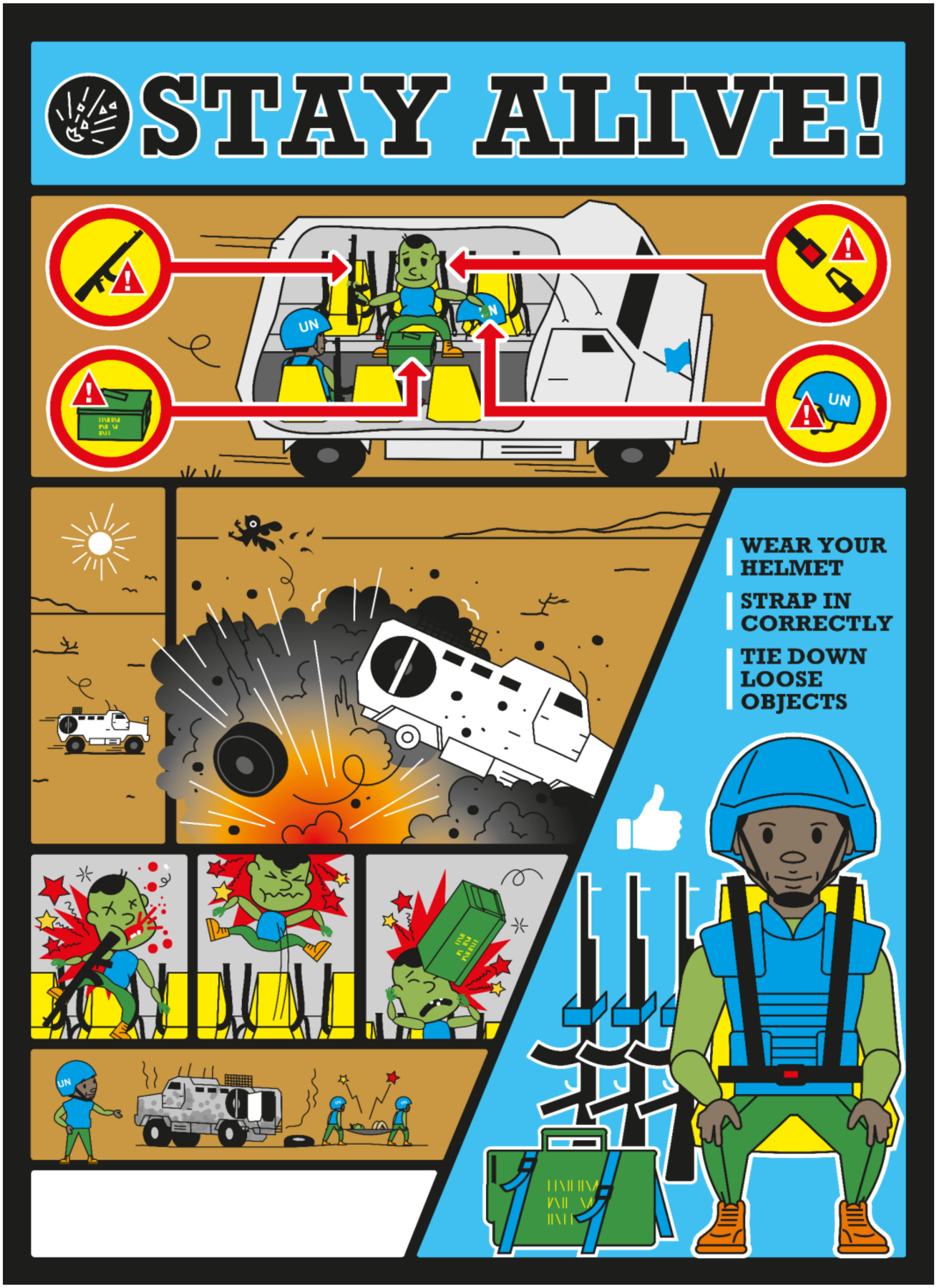
The inside of the cabin must be kept free of debris, including rocks/mud from shoes and trash, such as empty cans, water bottles, ammunition casings and so on that can turn into a secondary hazard.

Aside from the physical characteristics of the mine-protected vehicles, crews need to take personal preventive measures to reduce injuries following detonation of an IED. Even if the vehicle design reduces the blast's shockwave travelling through the vehicle, it is enough to accelerate loose items in the cabin, turning them into secondary hazards. Therefore, it must be ensured that all equipment in a vehicle is stowed in such a way that it cannot become detached in the event of an IED explosion, accelerated by the movement of the vehicle or the blast and turned into secondary projectiles that ultimately injure or even kill the peacekeepers inside the protected vehicle. This includes personal and crew weapons. Storage compartments must be closed and secured while driving.

Operations in challenging environments cause material to experience higher wear and tear requiring shorter maintenance intervals than specified by the manufacturer. Vehicle maintenance should therefore give special attention to components that provide protection such as shock-absorbing systems. Special care should also be given to mine and blast protection systems.

Figure 2.6

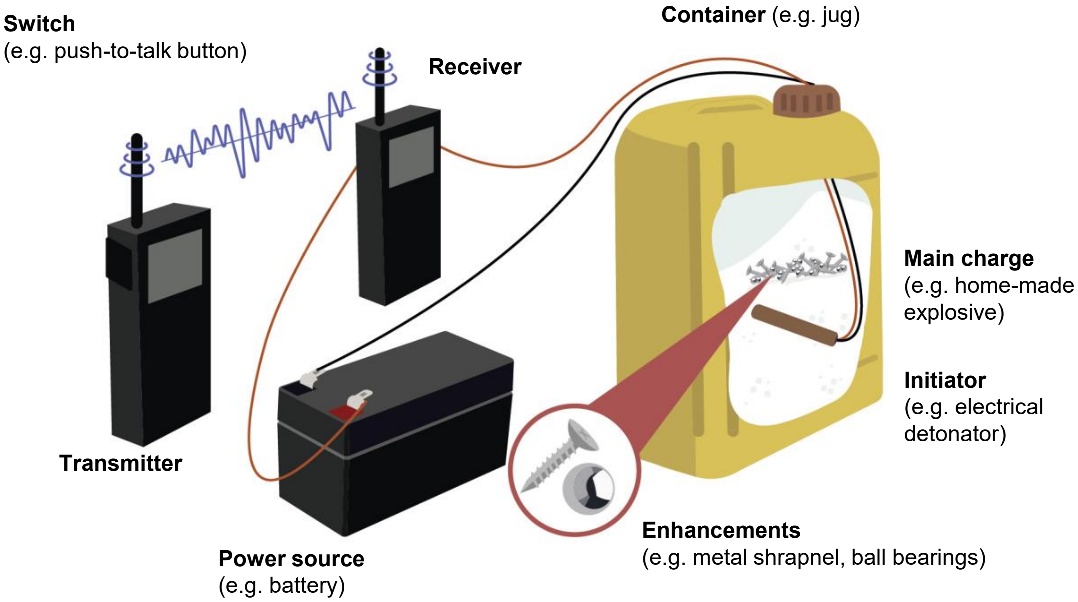
Sample poster for United Nations peacekeeping missions (2)



2.3.5. Electronic countermeasure equipment (jammers)

Electronic countermeasures (ECM) use the electromagnetic spectrum to support force protection by mitigating the risk from radio-controlled IEDs. IED jamming systems provide a degree of protection against radio-controlled IEDs. Effective ECM can mitigate a perpetrator's effective use of the electromagnetic spectrum through using electromagnetic energy. However, it is only a supporting measure to mitigate the threat and does not guarantee protection against an IED threat in general and only to a limited extent against radio-controlled IEDs.

Figure 2.7
Radio-controlled IED (1)



National policies and equipment will dictate the level of assured protection required for differing areas of the electromagnetic spectrum. TTPs will dictate the mix of equipment and composition of patrols/ vehicle packets and their spacing to ensure appropriate levels of assured protection for movement.

Familiarity with ECM systems in relation to force protection and the associated radio-controlled IEDs is required across the force and does not routinely require deploying ECM expertise with each movement. ECM can be used both to provide en route protection during movements and to protect vulnerable points in facilities.

Deconfliction between ECM systems and tactical communications is imperative to avoid interferences in the use of the electromagnetic spectrum. Deconfliction is subject to the spectrum manager.[26]

[26] See the *United Nations Deployed Military Field Headquarters Handbook* and the *United Nations Peacekeeping Missions Military Signals Unit Manual.*

Key ECM considerations are as follows:

- Troop- and police-contributing countries are encouraged to deploy/employ portable ECM equipment to support dismounted search and other dismounted tasks.
- ECM can affect friendly use of the electromagnetic spectrum and so require a dedicated focal point to deconflict with other users of the electromagnetic spectrum.[27]
- The IED threat is usually based on commercial off-the-shelf technology and thus the frequencies and communications technologies used can change rapidly. To counter this agility, ECM equipment uses programmable software, for which configuration management of ECM software is critical.
- Critical friendly force frequencies are programmed into ECM equipment so that they can be detected, identified and not jammed by ECM or protected by other technical means.
- To ensure the troop- and police-contributing countries deploy the right equipment to support ECM, the capability and frequency requirements are included in the status of unit requirements or conveyed during initial discussions with a troop- or police-contributing country on the deployment of a new unit or deployment of troop- and police-contributing countries equipment for an existing unit. The Office of Military Affairs should obtain this information from the field mission. If the troop- or police-contributing country is unable to bring force protection ECM capability as part of its COE, then consideration should be given to:

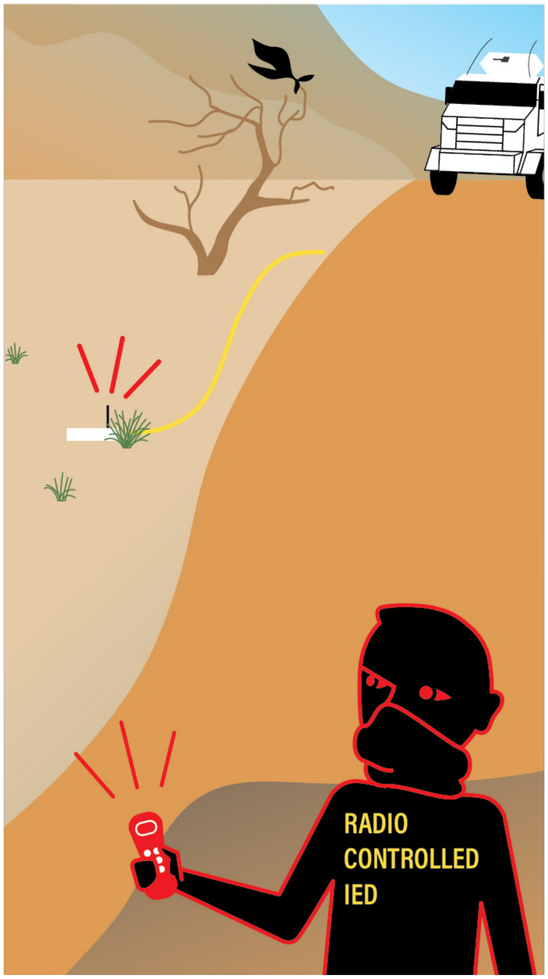
  a) Deploy another unit if it is a new deployment.

  b) Liaise with the light coordination mechanism to find support from another Member State.

  c) Use a United Nations commercial contract, if available, to provide the necessary equipment.

  For options b) and c), care should be taken to provide appropriate training in the use of ECM and its maintenance.

Figure 2.8
Radio-controlled IED (2)



[27] The frequencies are usually managed by U6 (communications).

2.3.6. Infrastructure

The United Nations requires blast protection for all buildings and compounds occupied by United Nations staff in areas with specific threat events related to explosives, such as IEDs[28] and EO attacks. For premises protection assessment, the term blast is understood as an explosion which includes impacts from explosion-related shockwaves, heat waves, shrapnel and backdraught phenomena.[29]

For facilities used by United Nations civilian entities, the Department of Safety and Security is responsible for ensuring that appropriate protection is provided through assessments, consultations and implementation of measures.

For military facilities, the respective commander is responsible.

Nevertheless, the approach and expertise of the Department provide a good reference point for implementing infrastructure protection.

The Department of Safety and Security is responsible for identifying and assessing all blast-related events related to United Nations infrastructure. For every area,[30] the Department develops and periodically updates a security risk management document, based on changes in the security environment.[31]

The security risk management documents are restricted to United Nations official use only. To obtain the latest version of the document of a specific area, the local Department office should be contacted.

The United Nations defines blast protection as the combination of all resources, strategies and procedures to protect United Nations premises from a blast incident, including:[32]

- Blast prevention, which entails all security risk management measures and procedures, including physical security, access control procedures and training, intended to lower the likelihood of a blast incident occurring and affecting the United Nations.
- Blast mitigation, which entails all security risk management measures and procedures, intended to lower the impact of a blast incident once it occurs.

The *Security Management Operations Manual* defines in chapter XV "Guidelines for Blast Protection on UN Buildings", the blast protection for United Nations premises.[33]

The guidelines state that inhabited United Nations buildings at risk of explosive threats should present at least the level of protection III-MEDIUM features.[34]

[28] The different types of IEDs demand different protection systems in physical security. For example, vehicle-borne IEDs require hardening the perimeter; person-borne IEDs require access control procedures and hardening the pedestrian access; mortar/rockets need overhead/side protection, etc.

[29] United Nations Security Management System, *Security Management Operations Manual*, chap. XV "Guidelines for Blast Protection on UN Buildings", 30 September 2020.

[30] The area is a region with similar threat and risk characteristics. It can be an entire country or regions in a country. Currently there is over 360 areas of security designated by the Department of Safety and Security.

[31] To learn more about the security risk management process, see the *United Nations Security Policy Manual on Security Risk Management*. Available at www.un.org/en/pdfs/undss-unsms_policy_ebook.pdf.

[32] United Nations Security Management System, *Security Management Operations Manual*, chap. XV "Guidelines for Blast Protection on UN Buildings", 30 September 2020.

[33] United Nations Security Management System, *Security Management Operations Manual*, January 2023.

[34] The level-of-protection method adopted by the United Nations is based on the manual "UFC 4-010-01 DoD Minimum Antiterrorism Standards for Buildings", from the United States Department of Defense, 2020.

Level of protection is the degree to which an asset (e.g. person, equipment, object) is protected against injury or damage from a blast incident. Each level of protection has an equivalent damage category level.[35] These equivalent systems allow for a consistent analysis of the damage estimation in a United Nations premises.

The following table presents a summary of the levels of protection:[36]

Level of protection	Damage category	Short description	Building collapse	United Nations acceptability
Below antiterrorism standards	A	Severe damage and/or collapse of structure	100% to 75%	Unacceptable
I - Very low	B	Heavy structural damage, requires demolition	75% to 25%	Unacceptable
II - Low	Cb	Moderate damage, unable to be repaired economically	25% to 0%	Acceptable if unlikely
III - Medium	Ca	Minor damage, able to be repaired economically	0%	Acceptable
IV - High	D	Minimal damage, no permanent deformation	0%	Ideal and desirable

There are no "minimum standoff" distances or specific characteristics for a United Nations building. It is necessary to consider the variables of an explosive attack, such as the expected likely point of detonation, the estimated explosive charge weight and the type of protected structure.

The level of protection should be determined by a blast expert, after having performed the blast vulnerability assessment of a United Nations premises, which is a comprehensive and scientific methodology to determine the potential vulnerability of premises to an explosion as identified in the security risk management area, using an explosion consequence analysis and structural vulnerability assessment procedures.[37]

The purpose of the blast vulnerability assessment is to offer comprehensive technical information to United Nations managers[38] to make informed decisions about the appropriate security risk management measures and procedures based on the level of assessed vulnerability of the United Nations to the possible explosive scenarios identified in the security risk management area. In this way, the blast

[35] The damage category was developed by Jarrett (1968) and revised by Gilbert, Lees and Scilly (1994), and the category system is accepted worldwide by the scientific community, as presented in the document "IATG 01.80 Formulae for Ammunition Management". Available at https://unsaferguard.org/.

[36] *United Nations Security Management System*, *Security Management Operations Manual*, chap. XV "Guidelines for Blast Protection on UN Buildings", 30 September 2020.

[37] Explosion consequence analysis is a structured process, utilizing explosives science and explosives engineering, to provide scientific evidence of the potential effect on individuals and property from blast effects and fragmentation in the event of a deliberate explosive event. Structural vulnerability assessment is a systematic approach to identify vulnerable elements of a structure exposed to blast effects.

[38] The blast vulnerability assessment is requested by an interested United Nations entity to analyse a specific premises. The United Nations managers are understood to be the authorities related to a particular premises and is charged with making decisions about the use of the premises, as well as improvements in the recommended mitigation measures. Managers include heads of agencies, resident coordinators, designated officials, Special Representatives of the Secretary-General and so on.

vulnerability assessment helps United Nations managers determine the amount of investment required for each location in relation to the value of potential losses.

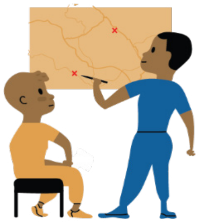
The blast vulnerability assessment, which is conducted by a blast expert from the Department of Safety and Security or a qualified professional contracted by the United Nations Safety Management System, is conducted on a regular basis and updated accordingly by Department of Safety and Security personnel.

2.4. Personal preparation

2.4.1. Explosive Hazard Awareness Training

IED awareness, currently delivered as part of Explosive Hazard Awareness Training, is mandatory for all personnel from troop- or police-contributing countries as part of their core predeployment training.

IED awareness refers to a comprehensive set of IED theoretical and practical lessons, which may include a written and/or practical assessment, with the intent to provide or increase the knowledge of recipients in relation to IEDs, their threat and basic IED threat mitigation measures.



This basic training helps to mitigate the IED threat and the consequences of IED attacks by enhancing personnel safety and to improve the survivability of personnel required to operate in such IED threat environments. At a minimum, and tailored to the local environment, these skills include the ability to:

- Understand the tactics and methods of IED emplacement and deployment.
- Understand the technical characteristics and make-up of an IED and what to look out for. This may include ground sign awareness and understanding the need to be aware of typical local conditions and how to react when a change in normal atmospheric character is noted.
- Understand the importance of not setting patterns in their activities.
- Effectively plan for deployments into, to and through IED threat environments.
- React effectively when an IED is identified, understanding what initial evacuation requirements are required.
- React effectively to an IED attack.
- Report an IED find to the appropriate authority and record event details.

The training is to be included in all initial, predeployment, refresher and continuation training. No live or inert EO shall be handled during awareness training to avoid any unsafe behaviour or action by non-improvised explosive device disposal (IEDD) qualified personnel. Failure to properly train personnel could cause injuries or death.

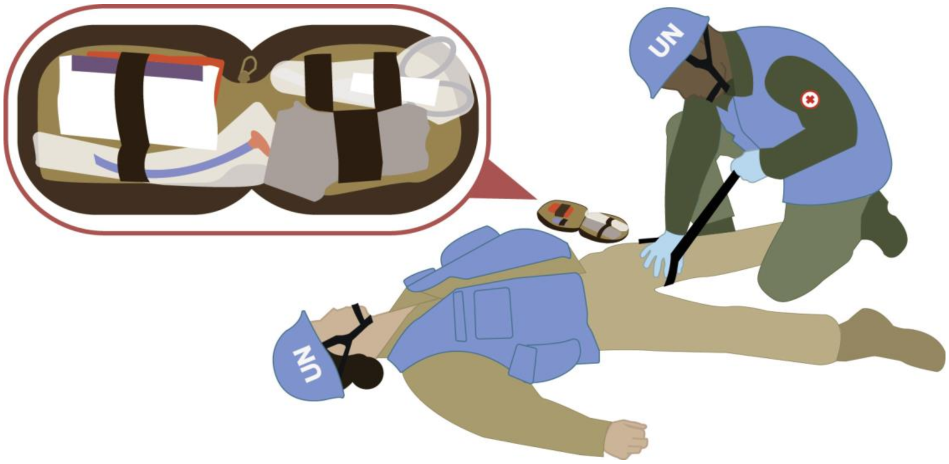
2.4.2. First aid/first responder training

Personnel who provide first aid play a crucial role in the treatment of trauma casualty, given their proximity and rapid access to the victim. The ability of a person to administer first aid and to send an adequate alert message, control bleeding, keep a victim breathing and keep them warm within the "platinum 10 minutes" makes the difference between life and death. This contributes to reducing the casualty mortality rate by up to 30 per cent. In a tactical setting, the treatment of the victim or the ability to coach the victim to provide self-aid is therefore mission-critical for the operation's success.

Treatments provided by one who administers first aid also weighs against the need for rapid transport to a medical treatment facility. Ideally, it is essential to ensure access to a surgical capability and blood products within two hours.

The Buddy First Aid Course is a mandatory part of the predeployment training of all troop- and police-contributing countries to acquire basic first aid knowledge and skills before deployment.[39] For further information, see section 7.1 (Predeployment training).

Figure 2.9
Buddy First Aid Kit



2.5. IED risk education and capacity-building

Against the background of the threat posed by IEDs to the civilian population, but also with a view to greater efficiency in long-term approach, appropriate IED risk education and capacity-building are required in addition to the preparation of uniformed peacekeepers.

The term "improvised explosive device risk education" refers to activities that seek to reduce the risk of death and injury from IEDs by raising awareness and promoting safe behaviour. These activities include information exchange with at-risk communities, communication of safety messages to target groups and support for community risk management.

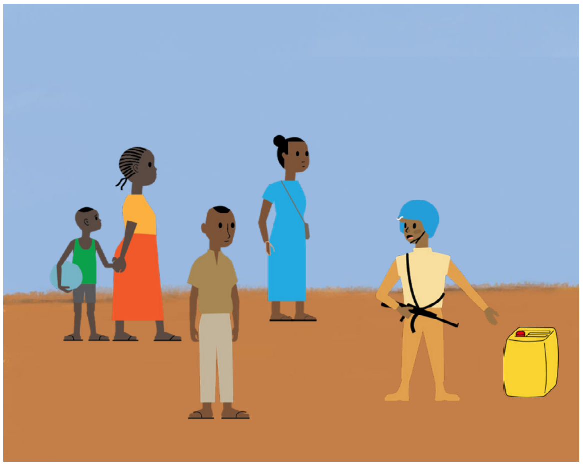
An IED threat may be static or dynamic. Mitigating IED threat in each situation requires a specific approach, and risk education messaging may vary from situation to situation.

The dynamic nature of the IED threat is a key characteristic differentiating IED risk education from traditional mine risk education. The diversity of construction, emplacement of devices and their use in asymmetric contexts render traditional risk education methods insufficient. It can be very difficult to define and educate people on specific IEDs in a similar fashion to landmines. This is because IEDs can be made to look like anything, including innocuous household items. IED risk education should therefore ensure that the local population in the affected communities are aware of the risks posed

[39] *Medical Support Manual for United Nations Field Missions*, fourth edition.

by IEDs and are encouraged to behave in a way that reduces the risk to people, property and the environment. The objective is to reduce the risk to a level where people can live safely and to recreate an environment where economic and social development can occur without being hindered or constrained by IED contamination and associated threats.

Figure 2.10
IED risk education



IED risk education should be preceded by a risk assessment and a gender and diversity context analysis and should be treated as an integral part of operational- and task-level planning and implementation. It may be a stand-alone activity, but, where possible, should be implemented in support of and in conjunction with other IED threat mitigation and mine action-related activities. Programmes and projects may be implemented in situations of emergency, transition or development. If done correctly, successful IED risk education campaigns may discourage the future use of IEDs by branding their use as indiscriminate weapons. However, IED risk education messages should not be perceived as being politically motivated or lead to the perception that the IED risk education entity is part of the conflict. IED risk education can also support information-gathering and contribute to assessing the technical and tactical categorization of the impact of an IED threat, which may vary depending on location and type of device(s).

In cases where IEDD is not possible or has not begun, IED risk education may form part of a school curriculum. It may be managed and monitored independently by educational authorities.

Uniformed peacekeepers in cooperation with other United Nations entities that have appropriate outreach into the respective populations must take advantage of existing opportunities to inform the population of existing IED threat and conduct risk education sequentially or in a coordinated manner. The topics to be covered are the following:

- Danger posed by IEDs.
- How IEDs can be identified.
- How to identify persons of the IED system.
- Precautions and behaviour to mitigate the threat.
- Necessary measures in case of possible wounding.
- Reporting of relevant incidents/accessibility of the United Nations.
- Available assistance from the United Nations.

Risk education should always be combined with the offer to pass on the existing knowledge and to advertise the measure to achieve the greatest possible impact.

In addition to the civilian population, all local authorities and agencies should be involved in potential capacity-building. An appropriate plan for the phased design should include an analysis of which regions are particularly affected and which actors have the greatest need and can serve as the best possible multipliers.

Capacity-building is the best long-term guarantee of the sustainability of the United Nations IED threat mitigation effort in the mission area. All mission components shall work to establish and/or strengthen the host State capability to respond to and investigate IED incidents.

In peacekeeping environments with a high IED threat, the building of the local capabilities and capacities in the counter-IED area should be identified as a priority in discussions with the host State authorities on the defence and police reform. Further, this capacity-building effort should be included in the development/reform plans to foster a sense of local ownership and attract funding both from the State budget and bilateral/multilateral assistance.

A full IED threat mitigation is unlikely to be achieved from the outset since it requires a comprehensive approach as the United Nations counter-IED strategy describes.[40] However, host Government capability will need some structures in place to replicate the IED threat mitigation lines of effort, which may have a mix of military and civilian agencies. Commanders must therefore be prepared to ensure that local forces are organized, trained and, if possible, equipped to operate in an IED threat environment and that they have the capacity to train others.

IED threat mitigation capacity-building of the host Government's security forces should be planned from the outset, in compliance with the United Nations human rights due diligence policy,[41] which includes the development of risk assessment that can further inform the United Nations support to the host Government's security forces, including mentoring, training and technological support.

The long-term goal of capacity-building efforts should be to develop a critical mass of local experts to assume responsibility in combating IED threats. This can include the education and training of appropriate EO personnel and police officers to collect evidence, conduct analysis and reach conclusions about EO incidents. Additionally, the capacity-building efforts should facilitate the investigation and prosecution, and support in developing national counter-IED strategy standard operating procedures, formulating a legal framework and training of legislative institutions. This normative and regulatory framework should be developed in conformity with human rights and humanitarian law standards, best practices in law enforcement operations and the application of human rights in counter-terrorism, and international and non-international armed conflict.

2.6. Support host Government

The host Government's participation in IED threat mitigation may range from a full operational capability to an extremely limited operational capability. In the first case, the host Government may exert full responsibilities while in the second case the United Nations will need to provide the appropriate support.

The IED threat mitigation approach must be established in accordance with the legal arrangements of the host Government, especially regarding the requirements for collecting physical and digital evidence that can be used in court and recording statements.

[40] Strategy on Counter Improvised Explosive Device (C-IED) for Peacekeeping Operations.

[41] Human rights due diligence policy on United Nations support to non-United Nations security forces.

Host Government security forces may be invaluable for both peacekeeping-intelligence and understanding the operating environment. They may have their own counter-IED capability already in place. Their involvement within IED threat mitigation activities is essential and can be especially useful to degrade the network's activities. A variety of modalities for cooperation between the peacekeeping operations and the host Government can be explored within the mission's mandate and in compliance with the United Nations human rights due diligence policy. Risk must be assessed to avoid exposing United Nations peacekeepers to unnecessary risk with regard to host Government involvement in "defeat the device" and IED network disruption activities. The participation of the host Government's forces in IED threat mitigation activities may have a stabilizing impact on the population.

In accordance with host Government laws, the United Nations IED exploitation process can potentially assist host Government's prosecution efforts thereby legitimizing their judicial process.

The United Nations peacekeeping mission must understand the operational and strategic goals of the host Government. They must also consider the economic impact of the IED threat mitigation as well as the activities of NGOs.

3. IED threat mitigation organization (roles and responsibilities)

This chapter focuses primarily on the organization of the military and police components within a peacekeeping mission. The organization of the military headquarters is provided in the *United Nations Deployed Military Field Headquarters Handbook*, while the structure of the police component within a United Nations peacekeeping operations is based on the arrangement in the Department of Peace Operations policy on United Nations police. In a generic way, the responsibilities of U1 (personnel) and U4 (logistics) can be assumed by the administrative pillar, while all other responsibilities can be performed by the operational pillar.

3.1. Commanders

Commanders at all levels play a critical role in IED threat mitigation. They are to ensure that appropriate priority is given to IED threat mitigation efforts. Additionally, they must ensure high standards of predeployment training, in-mission training and reporting, to equip subordinates with the right mindset to support IED threat mitigation activities. All commanders must note that IED threat mitigation is one of the most challenging tasks in the operational area, because the danger is difficult to identify and to fight.

Commanders should also facilitate the involvement of other stakeholders in the area of operation to implement a systematic and whole-of-system approach.[42] They are key figures in communication with host nation and other United Nations entities, as well as with their counterparts in the police or the military component.

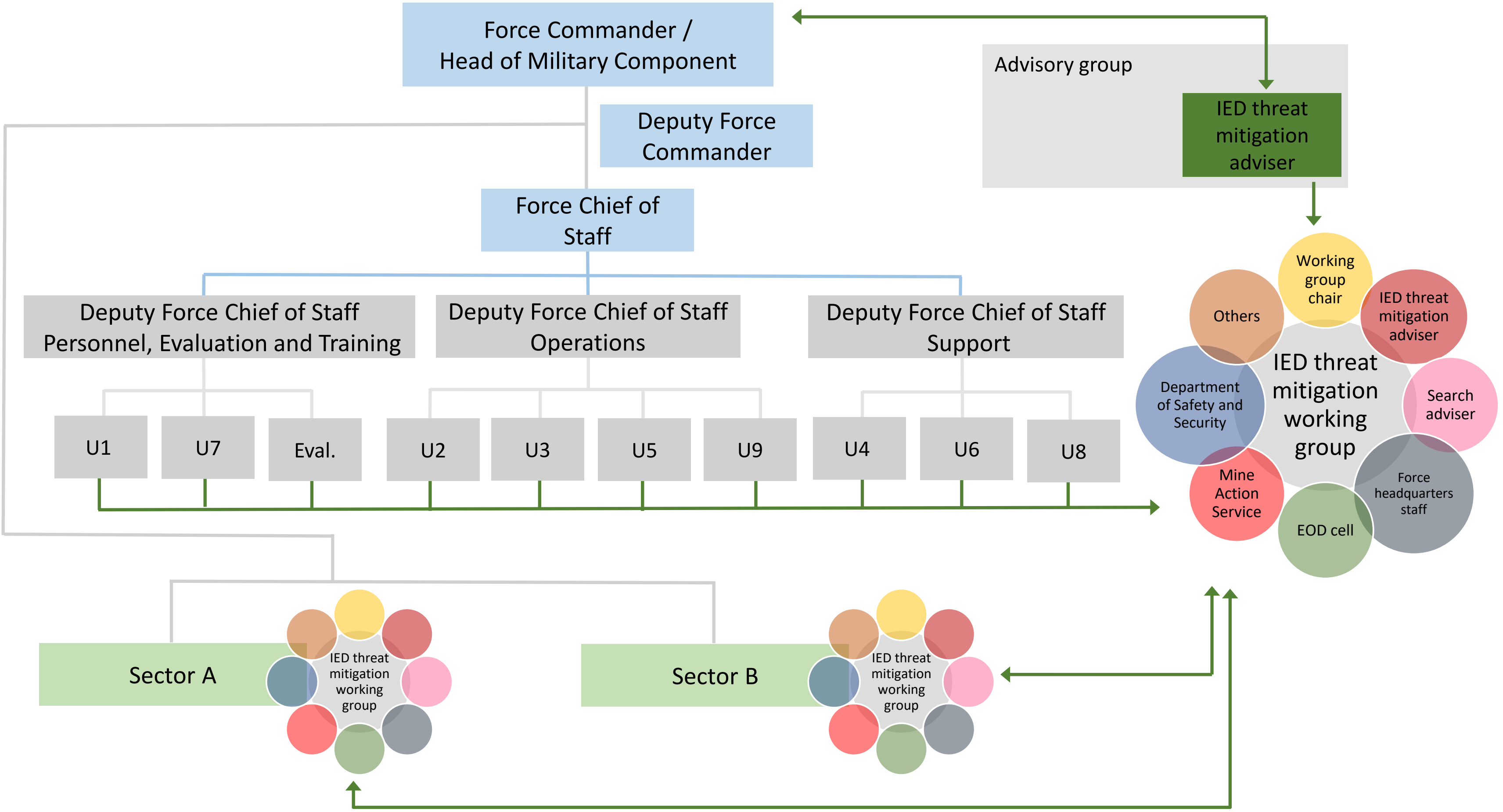
3.2. IED threat mitigation officer/adviser

The IED threat mitigation officer/adviser (military and police) is a staff function at the force headquarters and sector headquarters levels. The IED threat mitigation officer/adviser is sourced from a subject matter expert with appropriate training in IED threat mitigation. Ideally, the IED threat mitigation officer/adviser should have been trained as a search adviser, EO disposer or as an IEDD operator. Within the police component, the IED threat mitigation officer/adviser shall report to the Deputy Police Commissioner for Operations.

The task of the IED threat mitigation officer/adviser, who can be either an individual or an advisory and planning cell, depends on the size of the mission and the threat. Ideally an IED threat mitigation adviser should be sourced for all levels, starting from unit level up to force headquarters to facilitate a coordinated approach throughout. Where the availability of suitable personnel and other limitations does not allow this, the function could be delegated to the EOD cell.

[42] Strategy on Counter Improvised Explosive Device (C-IED) for Peacekeeping Operations.

Figure 3.1
IED threat mitigation organization


Force Commander /
Head of Military Component
Deputy Force Commander
Force Chief of Staff
Advisory group
IED threat mitigation adviser
Deputy Force Chief of Staff Personnel, Evaluation and Training
Deputy Force Chief of Staff Operations
Deputy Force Chief of Staff Support
U1
U7
Eval.
U2
U3
U5
U9
U4
U6
U8
Working group chair
Others
IED threat mitigation adviser
IED threat mitigation working group
Department of Safety and Security
Search adviser
Mine Action Service
Force headquarters staff
EOD cell
Sector A
IED threat mitigation working group
Sector B
IED threat mitigation working group

The role of the IED threat mitigation officers/advisers is to coordinate all efforts regarding IED threat mitigation. The designated officer is to advise the Commander, coordinate with the IED threat mitigation working group, the staff, the force and the police as effectively as possible in this role.

The IED threat mitigation officer/adviser links the planning and implementation of IED threat mitigation measures in the mission area within the military and the police component and liaises with other United Nations entities and actors in the area of operation.

In close coordination with the subject matter experts, the IED threat mitigation adviser's tasks include:

- Advise and assist the commander on all IED threat mitigation matters.
- Control and coordinate IEDD operations in the mission area.
- Advise on the appropriate physical field protection measures to be taken.
- Advise on force protection ECM matters.
- Control proper reporting of incidents and, if necessary, provide additional training to ensure all contributors will meet the standards.
- Support to reduce possible duplication of reports to contribute in the best possible manner to a common operational picture.
- Provide advice on the development of mission-specific guidance documents on IED threat mitigation, for example standard operating procedures.
- Liaise with all units and commanding officers of individual uniformed personnel to understand their level of training, support efforts in maintaining or adjusting their training to the current operational needs and assist in the evaluation of performance.
- Update the IED and explosives hazard information.
- Assist leadership of other headquarters in the mission area in IED threat mitigation planning, if tasked.
- Advise on appropriate technical exploitation procedures.

3.3. Search adviser

Search is a key operational capability, which is interrelated heavily with EOD as well as force protection; however, search has utility across the full spectrum of United Nations operations and can facilitate delivery of strategic mission effects.

Military search capabilities are developed to locate and detect concealed threats using systematic procedures and appropriate detection techniques. Search capability is delivered through a multilayered response that is utilized depending on the threat and type of target. A basic understanding of such search capability should be held by all troop-contributing countries within all United Nations units.

Search is a capability that can be utilized across all operational environments. Search capabilities can be directed based on the outcome of the decision-making process, both in general planning and a wider search planning and fitted to the specific needs of the operation. Search is limited not only to direct support to United Nations operations. It may also support:

- Protection of civilians in humanitarian assistance operations (including disaster relief).
- Force protection (including patrol and convoy operations).
- Threat reduction.
- Host State security force support.

Search advisers are specialist staff at all levels of command, who provide advice and assist in planning of search-related activities. The search adviser must be current on all relevant policies and doctrines to ensure that they provide the right advice to the Force Commander, Sector or Unit Commander they report to, as well as their staff on all search-related matters.

Where possible, the role of the search adviser should be dedicated within a United Nations mission. This consideration is required during the force generation phase of a mission or if there is a change in the mission threat assessment requiring a reconfiguration to include dedicated search adviser roles.

At a minimum there should be a search adviser at the force headquarters level. Under certain circumstances, the role can be double-headed: performing the tasks of the IED threat mitigation adviser and the search adviser.

A search adviser must be qualified for specialist search and have appropriate experience in providing search advice on the staff level.

A search adviser works within the planning sphere to determine the effect required, threat faced and insert key search planning data into the operational planning cycle to establish the best solution to achieve a given mission. A search adviser is responsible for:

- Advice to force engineers or Unit Commanders on search capacity and deployment, depending on the level they are operating at.
- Prioritizing and coordinating search matters with supporting host State and NGOs, where appropriate.
- Synchronizing and aligning available search capabilities and responses across the area of operation.
- Supporting the intelligence and exploitation cycle through search-specific threat assessments and the identification of adversary TTPs.
- Determining which search assets are most appropriate for a task by understanding the capabilities, responsibilities and support requirements of search assets.
- Conducting an estimate and planning for search, based on threats, perpetrator intent and capability before preparing orders for a search commander and/or search teams.[43]
- Providing support and advice to the search team commander conducting search activities.
- In large, complex search operations, the search officer/adviser may be responsible for the coordination of multiple search teams.
- Conduct debriefings to staff and search teams as required.
- Evaluate and adjust search operations and TTPs based on a lessons identified analysis.

[43] See annex B for detailed information on search teams and search commanders.

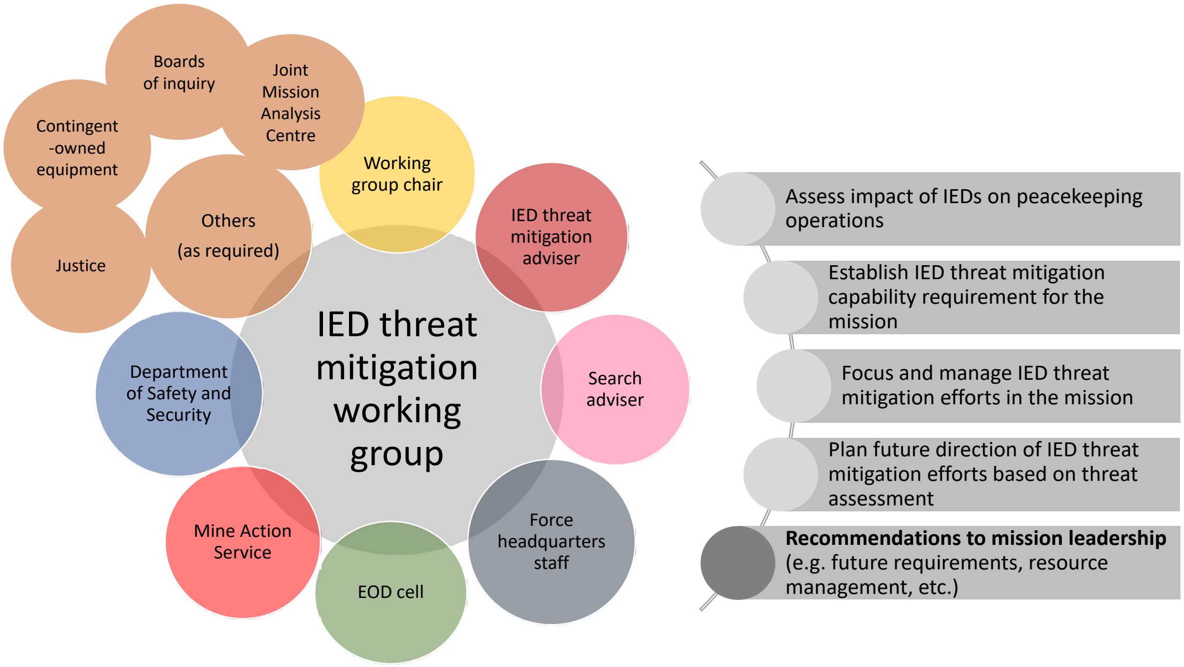
3.4. IED threat mitigation working group

Regardless of the prevailing threat, Force Commanders should establish an IED threat mitigation working group, comprising senior mission management to develop IED threat mitigation measures in accordance with the mission mandate. The strategy should be used to direct, focus and manage IED threat mitigation efforts within the mission.

The IED threat mitigation working group supports decision-making, oversight and good governance, ensuring a mission-wide approach. It supports effective information-sharing between various mission entities and relevant national and international stakeholders. Furthermore, the IED threat mitigation working group provides a framework through which findings and recommendations (e.g. assessments, results of investigations, independent reviews and lessons learned) can be evaluated and prioritized, developed into IED threat mitigation outputs and submitted for decision to the mission leadership. On approval, the recommendations should be disseminated and implemented across the mission.

The composition of the IED threat mitigation working group may vary, depending on the mission size, available resources and level of threat within the mission environment. If the threat is low, the work of the IED threat mitigation working group can be kept to a minimum. However, it is essential to monitor all developments in the field of IEDs, as well as EO or weapons management, to identify possible trends at an early stage. For example, the deterioration of the general security situation in an area of operation can lead to the fact that ammunition and/or weapons depots are no longer guarded and the situation is exploited by groups to acquire material to produce IEDs. Therefore, incidents must be monitored continuously to identify trends at an early stage.

Figure 3.2
IED threat mitigation working group


Boards of inquiry
Joint Mission Analysis Centre
Contingent -owned equipment
Working group chair
Others (as required)
IED threat mitigation adviser
Justice
IED threat mitigation working group
Search adviser
Department of Safety and Security
Force headquarters staff
Mine Action Service
EOD cell
Assess impact of IEDs on peacekeeping operations
Establish IED threat mitigation capability requirement for the mission
Focus and manage IED threat mitigation efforts in the mission
Plan future direction of IED threat mitigation efforts based on threat assessment
Recommendations to mission leadership (e.g. future requirements, resource management, etc.)

Depending on the situation on the ground, the IED threat mitigation working group may be expanded to better manage the tasks at the different levels:

- Counter-IED steering committee (strategic-level decision-making by senior mission leadership).
- Counter-IED working group (operational level designated forum to coordinate and develop proposals for strategies, policies and activities pertaining to counter-IED and prepare decision-making of the steering committee).
- Counter-IED task force (tactical/technical level responsible for current incident analysis, EO coverage planning and so on).

The IED threat mitigation working group may be replicated at the regional level and/or complemented by other tactical or technical level entities (e.g. an exploitation working group), feeding into the IED threat mitigation working group. However, the IED threat mitigation working group may consist of persons or entities shown in the circles in figure 3.2. A regular exchange, which could be virtual if not otherwise possible, is to be scheduled to support the emergence of an appropriate culture or mindset.

3.5. EOD cell

The EOD cell is the designated entity that provides operational control, planning and administrative services related to EOD operations to assigned EOD units in a designated geographical area of responsibility. It is the force tasking authority for all EOD and IEDD tasks, receiving notification of an EOD incident from units and completed incident reports from EOD units, as well as providing scheduling and control of disposal operations in the area of responsibility.

An EOD cell should be established at the force headquarters and sector headquarters levels. Depending on the size of the mission, this could be either one person or a team of EOD qualified personnel.[44]

While the EOD cell coordinates and documents the day-to-day operations of explosive EOD teams, the IED threat mitigation working group focuses more on the exchange of information regarding trends, TTPs (own and the perpetrator's) and so on. To a certain extent the EOD cell assumes the role of the U3 (operations), whereas the IED threat mitigation working group performs the functions of the U5/U7 (planning/training). The findings of the EOD cell must therefore be considered accordingly in the IED threat mitigation working group and, conversely, the recommendations of the IED threat mitigation working group must be implemented by the EOD cell.

3.6. Peacekeeping-intelligence

Understanding and peacekeeping-intelligence are essential to comprehend the operating environment and to enabling IED threat mitigation. To understand the IED threat environment, each mission should employ the full architecture of its EOD entities,[45] as well as other personnel and assets to identify the information needs; acquire, collate and analyse the information; and disseminate relevant peacekeeping-intelligence products to relevant stakeholders.

[44] See the *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual* for further information (e.g. structure, roles and responsibilities).

[45] Joint Mission Analysis Centre, Force U2, police component crime intelligence unit, Department of Safety and Security, Joint Operations Centre.

The Mission Peacekeeping-Intelligence Coordination Mechanism is the entity responsible for managing peacekeeping-intelligence products in missions by overseeing and directing the peacekeeping-intelligence products cycle. The Mechanism comprises the participating mission entities responsible for the acquisition, collation, analysis and dissemination of peacekeeping-intelligence products activities within the mission. This includes Joint Mission Analysis Centres, relevant functions in the military and police component, the Department of Safety and Security and civilian components, including human rights.[46]

The purpose of the Mechanism is to operationalize the central control and direction of the mission's peacekeeping-intelligence system by aligning the acquisition and analysis activities of all participating mission entities with the requirements of senior mission leadership. The Mechanism is to also operationalize appropriate oversight and accountability in the management of the mission's peacekeeping-intelligence processes. The functions of the Mechanism shall preferably be coordinated by the missions' chiefs of staff in their role as the chair[47] of the Mechanism. In some missions, the Joint Mission Analysis Centre fulfils an important leading role in the Mechanism that directs and oversees the peacekeeping-intelligence cycle within the mission. The Centre manages the peacekeeping-intelligence requirements of the Head of Mission and the mission leadership team through the development of a mission-level information acquisition plan. The plan is developed by collating and analysing all source information and by identifying threats and other challenges to the mandate. The Centre acquires and analyses multi-source information to prepare medium- to long-term integrated analysis and assessments for strategic, operational and contingency planning, decision-making and crisis management.

Technical peacekeeping-intelligence,[48] a subset of peacekeeping-intelligence, is a very technical and specialized acquisition method which often requires expert acquisition knowledge and technical and scientific exploitation and analysis. Technical peacekeeping-intelligence exploitation activities include acquisition; collation; and analysis of technical, tactical and forensic information. The United Nations does not utilize technical peacekeeping-intelligence or any associated process to support the operations of individuals or groups outside the United Nations unless this is explicitly mentioned and tasked in the mission mandate. It is important that exploitation activities are conducted persistently and iteratively to provide accurate peacekeeping-intelligence, develop effective countermeasures and contribute to effective prosecutions, including as called for in Security Council resolution 2589 (2021) on promoting accountability for the killings of and acts of violence against United Nations peacekeeping personnel.

Weapons technical peacekeeping-intelligence is defined as peacekeeping-intelligence derived from the processes and capabilities that collect, exploit and analyse asymmetric threat weapons systems to enable force protection, support to prosecution and degrade threat networks.[49]

[46] *Military Peacekeeping Intelligence Handbook*.

[47] Peacekeeping intelligence policy (2019.08) and *Military Peacekeeping Intelligence Handbook*. The Head of Mission shall designate a civilian chair of the Mission Peacekeeping-Intelligence Coordination Mechanism, preferably the mission chief of staff, to serve as the primary link between senior mission leadership decision-making processes and the mission's peacekeeping-intelligence cycle. If the function of the Mechanism is played by the Joint Mission Analysis Centre, the chief of the Centre shall chair the Mechanism.

[48] Technical peacekeeping-intelligence (TPKI) guideline (under development).

[49] Ibid.

3.7. Staff

As part of the systematic and whole-of-system approach to mitigating the threat of IEDs, all staff branches are required to contribute. Successful implementation can be achieved only if activities are not limited to peacekeeping-intelligence (U2) and/or operations (U3).

The principles outlined in this section shall apply, mutatis mutandis, to the personnel of the police component. Within the police component, the Deputy Police Commissioner for Operations shall oversee the IED threat mitigation workstream, assisted by the police planning cell, formed police unit coordinator, IED threat mitigation officer/adviser, police policy and best practices officer/focal point and training focal point. In environments where United Nations police are engaged in the counter-IED capacity-building and development of the host State police, the Deputy Police Commissioner for capacity-building and development shall be responsible for the delivery of such police assistance.

In the following paragraphs, examples of tasks specifically related to IED threat mitigation are listed by staff branches.[50] However, the selection of possibilities should not be limited to the examples given. In the spirit of the IED threat mitigation, just as much creativity is permitted and even desired as is applied by the perpetrators. Usually, unconventional ideas and approaches can often be more successful than known measures. This is because in most missions the TTPs, as well as the pattern of the military and the police, are assessed by the perpetrators, so it must be assumed that most of the mitigation measures are well known.

U1 - Personnel and administration

- Check and ensure that all personnel prior to in-processing attended the mandatory predeployment training, especially explosive hazards awareness training and first aid training.
- Ensure that critical posts for a successful IED threat mitigation are sourced and, if possible, a handover-takeover is conducted in person.
- Ensure mission-critical personnel is sourced in close coordination with United Nations Headquarters.

U2 - Military peacekeeping-intelligence

- Support defining priority peacekeeping-intelligence requirements and other peacekeeping-intelligence requirements regarding IED threat mitigation.
- Ensure that information acquisition activities are conducted in support of mission and force requirements regarding IED threat mitigation.
- Manage the military peacekeeping-intelligence cycle, in line with United Nations Department of Peace Operations peacekeeping-intelligence policy and the *United Nations Deployed Military Field Headquarters Handbook*, through the direction, acquisition, analysis and dissemination phases. This is to ensure that the Force Commander's decision-making process is fully supported with timely, succinct and relevant peacekeeping-intelligence products regarding IED threat mitigation.
- Prepare and update of the information acquisition plan and the analysis of the operating environment.

[50] *United Nations Deployed Military Field Headquarters Handbook.*

- Provide valuable and timely information and technical peacekeeping-intelligence from exploitation tasks following IED incidents.
- Ensure that information regarding adversaries' TTPs and IED employment in general fed into the lessons-learned process is used to adjust training requirements to maintain unit readiness and minimize risks to the force.

U3 - Operations

- Ensure that all force protection planning adequately considers IED threats.
- Ensure that all troop movements in a mid-to-high threat environment are either conducted with an organic EOD capability or are supported by an EOD unit.
- Ensure to maintain an EOD unit as operational reserve to be employed in high-threat operations or in an emergency, if possible, employed with air assets.
- Ensure the availability of CASEVAC capability when operations with an assessed mid to high threat are executed.
- Ensure the availability of quick reaction force capability when operating with an assessed mid to high threat.
- Ensure that all duty/watch officers are familiar with the reporting formats.
- Ensure proper information and knowledge management regarding the current IED threat.
- Ensure that all staff products (e.g. operational order (OPORD) or concept of operations (CONOPS)) contain IED threat mitigation and are regularly updated.
- If it is not an independent branch, synchronize air operations (Air Ops) with the operations staff branch and coordinate with U2 or the information and communication centre to operate the reconnaissance and surveillance assets, obtain information on routes, vulnerable points and support patrols from the air and so on.
- Coordinate with information operations (Info Ops) to support IED threat mitigation efforts.
- Coordinate IED activities with the police component and other entities, as required.
- Coordinate with the disarmament, demobilization and reintegration team, if it is part of the mission, to share information about activities in that area with other components, since the collection of weapon and ammunition poses a potential source for IED construction.
- Coordinate with the human rights component on casualty recording and any explosive weapons-related information collected during investigations.
- Provide input to the training cell on operational needs to determine areas of focus for IED training.
- Plan the resources required for IED training specific to the mission mandate without adversely affecting operational readiness.
- Coordinate training facilities, ranges, ammunition and equipment management and other resources used to deliver in-mission training.
- Provide input on tactical and technical aspects of IED TTPs.
- Coordinate ECM aspects of force protection.

U4 - Logistics

- Ensure, in close coordination with the Department of Operational Support, that required equipment is available.
- Ensure that damaged or destroyed material/vehicles are replaced at the earliest possible date.
- Plan alternative transport routes.
- Plan alternative transport assets (e.g. air assets).
- Supply by alternative methods (e.g. parachute drop or use of unmanned aircraft systems (UAS)), if necessary.
- Make sure that all personnel are equipped with a Buddy First Aid Kit or individual first aid kit.

The senior ammunition technical officer or the ammunition technical officer is responsible to the chief weapons and ammunition management unit for the registration, verification and reporting of ammunition and ammunition storage areas in the mission, and is the primary source of technical advice on ammunition safety issues.[51] The senior ammunition technical officer or the ammunition technical officer supports the storage of devices that have been rendered safe. Hence, they should not be employed, for example, on secondary duty, as IED threat mitigation adviser, or conduct training and so on.

U5 - Planning

- Develop a medium- to long-term plan on how to effectively mitigate the IED threat in the area of operation by coordination efforts. Explore the modalities of mitigating the flow of associated material into the area of operation used to construct IEDs and coordinating with neighbouring States and United Nations agencies.
- Coordinate with Strategic Command on a comprehensive approach on how to support physical efforts by proper messaging, including contingency planning for IED incidents with all kinds of consequences, especially for the existing and identified deficits to contribute effectively to the best possible credibility of the United Nations.

U6 - Communications

- Support collection efforts with regard to IED incidents and other relevant data.
- Ensure an updated frequency management, including ECM, according to the latest trends and analysis regarding especially radio-controlled IEDs.
- Develop and distribute no-comms procedures instructions, which can be applied in case-use communication status is not possible or not recommended.

U7 - Training

The U7 branch plays a critical role within the force headquarters in implementing the Commander's directions and intent. Working closely with the operations branch and peacekeeping-intelligence cells, it is responsible for:

[51] *United Nations Deployed Military Field Headquarters Handbook.*

- Developing and managing an effective in-mission training programme and standards, providing tailored training for all levels of expertise and frequently taking into consideration the latest trends in IED threats to adequately keep the level of training as updated as possible.
- Prepare training plans, guidelines and organization of IED training.
- Organizing IED threat mitigation training, including train-the-trainers courses for, for example, recurrency training conducted under contingent arrangements.
- Providing guidance and support to sector headquarters and IED threat mitigation units in development of training packages and upgrading of TTPs.
- Conducting in-mission IEDD training evaluation.
- Evaluating continuous IEDD force operational readiness.
- Preparing training evaluation reports of IED units to provide feedback to the Force Commander on the level of training achieved by units and identifying shortfalls.
- Developing and managing effective evaluation and lessons-learned process, incorporating TTPs, equipment; and other related change proposals to include reach-back capabilities to analyse and identify capability gaps that support the preparation of future rotations.
- Defining and updating in-mission IED training standards based on results from the lessons-learned process and from the threat assessment.

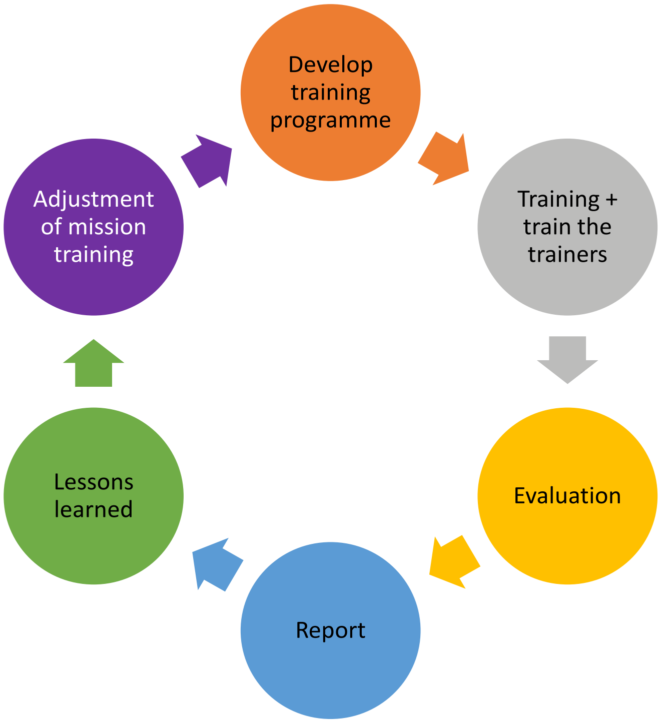
Best practice officer

The best practice officer has a special role to play in actively contributing to mitigation within a peacekeeping operation, but also in exchange with other United Nations missions in the region and in cooperation with United Nations Headquarters.[52] Among the important tasks are:

- Actively liaising with appropriate units on a regular basis (e.g. monthly) to obtain information and collect best practices regarding successfully implemented mitigation measures, procedures and information regarding new trends (e.g. composition of IEDs, materials used).
- Recording and documenting the collected information.
- Writing best practice reports with supporting graphics and/or photos to be shared with all individual uniformed personnel and contingents, other peacekeeping missions in the region and the Office of Military Affairs.
- Publish the reports on a mission-wide, but mission-restricted, accessible online platform.
- Communicate the collected best practices with other staff, especially U7, so as to adjust the in-mission training.

[52] Knowledge Management and Organizational Learning Policy (DPO 2020.11/DPPA 2020.2).

Figure 3.3
Best practice cycle


Develop training programme
Training + train the trainers
Evaluation
Report
Lessons learned
Adjustment of mission training

3.8. Liaison

Regardless of the command structure and arrangements, effective liaison is vital. Liaison officers foster knowledge-sharing and understanding and enhance mutual trust and teamwork.

To be able to conduct this coordination efficiently, missions should establish liaison elements at least at the force headquarters level (and preferably at the section headquarters level). Depending on the mandate, it might also be necessary to have other liaison elements at headquarters, such as liaison officers from signatory groups of ceasefire agreements or from regional organizations that are operating in the same area. These liaison elements are usually organized by a liaison officer under the guidance of a chief liaison officer.

Depending upon the level of the IED threat, consideration should be given to establishing liaison officers within key organizations, including:

- Mission partner, national counter-IED organizations.
- Military and police headquarters.
- Mission component headquarters.
- Troop- and police-contributing countries headquarters.
- Host nation security forces.
- United Nations funds and programmes.
- Other actors in the mission area with capacity and knowledge on IED threat mitigation.

3.9. Sectors

Every peacekeeping operation might develop its own detailed guidelines and standard operating procedures on how to establish their IED threat mitigation organization. To facilitate the development of those guidelines, some of the responsibilities of sector headquarters staff are described below.

Sector Commander

- Control the IED threat mitigation effort in the sector.
- Nominate a focal point to coordinate IED activities in support of commanders' intent.

Sector headquarters staff

- Synchronize and coordinate the IED threat mitigation effort in the sector under a designated IED focal point.
- Plan and control the employment of the IEDD unit or teams against the IED threat.
- Analyse the IED threat in the area and provide input to headquarters.
- Disseminate IED threat reports and alerts to under command units and the police component.
- Organize training of units and teams and facilitate training evaluation by the force/police headquarters.
- Coordinate evidence collection and its secure transportation for exploitation.
- Plan and organize IED awareness training for all command units and United Nations personnel in the sector.
- Initiate regular peacekeeping-intelligence operational reports and returns.

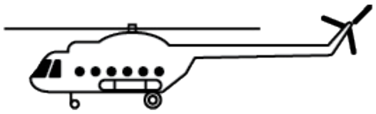
4. IED threat mitigation assets

Depending on the mandate and the area of operation, a variety of assets are usually available to contribute to IED threat mitigation. If possible, these should be planned in such a way that all units and tasks can be equally supported.

In the initial stages, there will be a strong demand for certain limited resources, but this will stabilize over time as a shared operational picture develops. Gaining a clearer understanding of the environment, potential threats and daily activity patterns will help to implement chain management measures. This approach will enable the analysis of specific areas, roads and other locations for anomalies that might suggest the presence of an IED.

At all times, reserves must be built up so that the mission command can react flexibly to any emerging situation. This applies in particular for EOD units to neutralize IEDs, conduct technical exploitations or post-blast investigation, but is equally important to CASEVAC, quick reaction force, fire support and other specialized personnel.

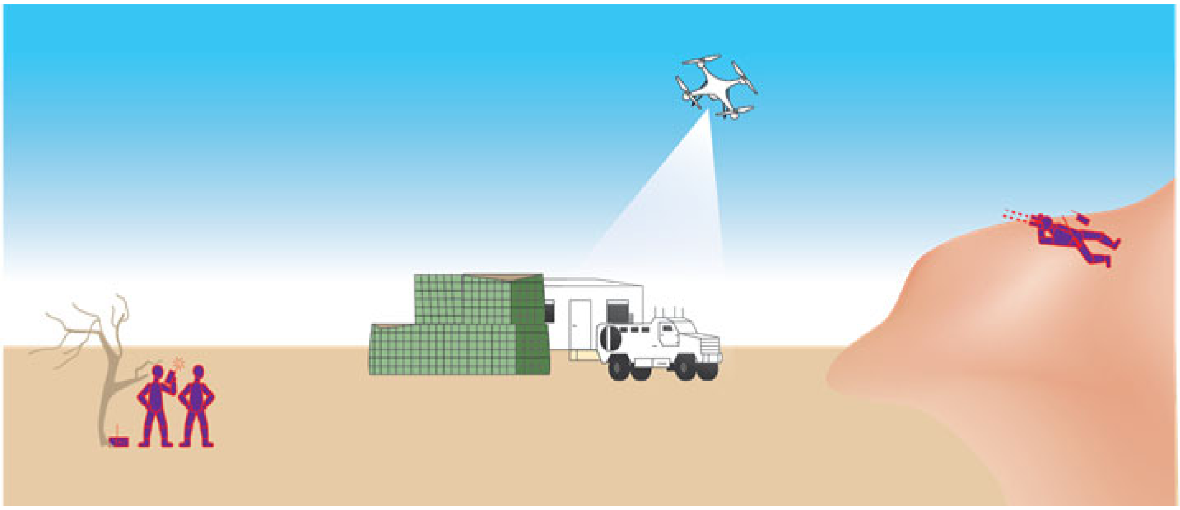
4.1. Air support/peacekeeping-intelligence, surveillance and reconnaissance



Depending on the specific assets available within each mission, the force may have access to a variety of air platforms that have potential to assist with the overall mitigation of IED threats by improving situational awareness of peacekeepers. These platforms could comprise both crewed aircraft (rotary-wing and/or fixed-wing), as well as manned aircraft systems of varying sizes. These may be specifically equipped to carry out peacekeeping-intelligence, surveillance and reconnaissance for other purposes, but still be capable of providing information that may contribute to the overall counter-IED effort. How each air asset can best contribute depends on various factors, such as the capabilities of the platform, the types of sensors it carries, the nature of the IED threat and the needs of the supported ground forces. The peacekeeping-intelligence, surveillance and reconnaissance and/or UAS team within the Force U2 should always be the first point of contact for personnel wishing to fully understand the options available in each mission. Some generic planning considerations are presented below.

It is critical to note from the outset that air assets alone are highly unlikely to be able to consistently and reliably detect emplaced IEDs. They can contribute to general situational awareness and may, under certain conditions, be able to cue ground forces onto areas for further investigation, but they cannot replace ground-based mitigation measures.

Figure 4.1
Air support/peacekeeping-intelligence, surveillance and reconnaissance (1)



Platforms

Each category of air asset has inherent strengths/weaknesses regardless of the sensors it carries, and the relevant air unit, through the Force U2, will be best placed to advise on the appropriate asset for a specific scenario. As a general rule, fixed-wing aircraft will be faster than rotary-wing aircraft, have greater operating ranges, can fly at higher altitudes to reduce their vulnerability to threats from the ground and (depending on size) are likely to be able to carry larger and more capable sensors. Conversely, they always require some form of prepared runway to operate from and are unable to remain static over a location in the way that rotary-wing aircraft can.

UAS assets vary considerably in size, from class I systems that can be carried by one person and operated from almost any location, up to class II and class III systems that can be a similar size (and have similar support requirements) as a crewed aircraft. The lack of a human occupant may make a UAS the preferred asset to employ in situations where a high threat of surface-to-air fire exists or in other situations where the risk to a human crew is deemed unacceptably high. Smaller UAS will also be less visible and much quieter than fixed-wing or rotary-wing aircraft, making them potentially better able to conduct observation of the ground without alerting hostile actors to their presence. However, UAS may be more vulnerable to severe weather conditions than crewed aircraft are.

While not technically an air asset, satellites can provide overhead imagery in a similar manner to aircraft. Missions may have arrangements in place to purchase imagery from commercial satellites, which may be useful in certain circumstances. However, satellites will not be under the direct control authority of a mission and (depending on the specifics of the contract in place with the commercial operator) it may take several days for imagery to be available, making them ill-suited to provide time-sensitive information in a counter-IED context.

Sensors

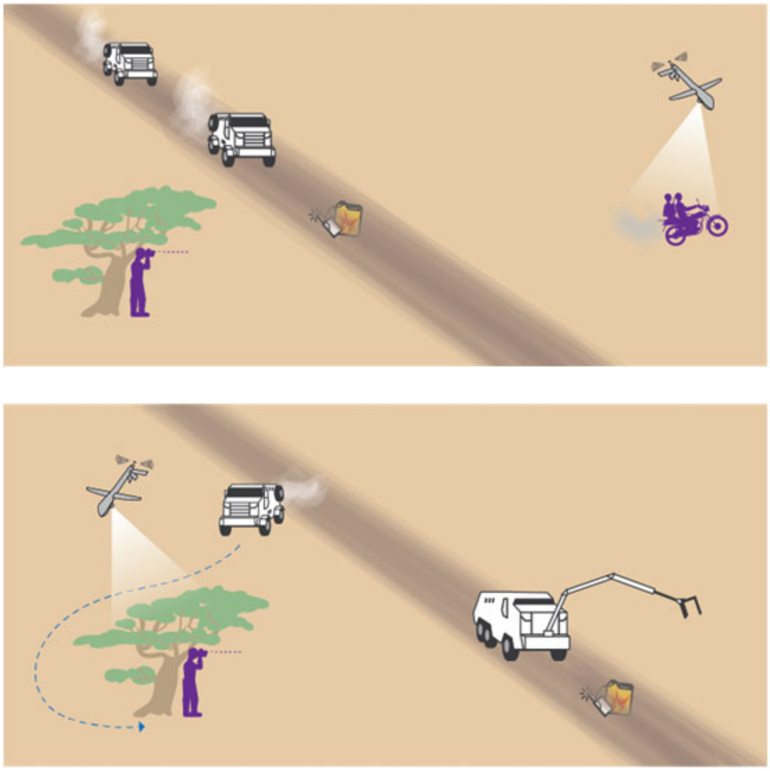
The development of sensors is a continuous process, and it is expected that the capabilities will significantly change over time. Nevertheless, the following paragraphs list the most common current sensors to allow better planning of available resources.

Both crewed aircraft and UAS can carry a variety of sensors, which (like the platforms themselves) have specific strengths and weaknesses regarding IED threat mitigation. In all cases, consideration must be given to how the information that is acquired will be analysed, in what time frame it is required and how it will be of greatest use to the relevant decision maker.

The most common sensor found on United Nations air assets is an electro-optical/infrared camera, often colloquially referred to as a day/night camera. This sensor type offers full-motion video/still imagery capture and is the most flexible sensor type to employ owing to the relative ease of interpretation. If compatible viewing terminals are available, the full-motion video feed from such a sensor will be available to ground forces in near real time, providing an excellent tool for enhancing situational awareness without exposing personnel to direct threat. Electro-optical/infrared sensors could assist ground forces in identifying a variety of potential IED indicators such as ground signs (e.g. disturbed earth, command wires, roadside markers), suspicious behaviour (such as covert observation of United Nations personnel or apparent prepared ambushes) or simply potentially vulnerable points along a route (e.g. blind corners, bridges, culverts, chokepoints).

Synthetic aperture radar sensors offer the ability to detect changes or disturbances to ground surfaces, which has the potential to provide indications of IED-related activity. However, synthetic aperture radar sensors require specialized equipment and highly trained analysts to properly interpret and exploit, and will still require ground forces to investigate suspicious sites to confirm or deny the presence of an IED.

Figure 4.2
Air support/peacekeeping-intelligence, surveillance and reconnaissance (2)



Air support/peacekeeping-intelligence, surveillance and reconnaissance can provide support if there is a threat to a convoy, and it can provide support while the threat is neutralized.

Multispectral/hyperspectral imaging sensors can detect specific substances if they are visible from the air, to potentially include traces of explosives. However, extensive pre-mission planning and supporting data are required before a multispectral/hyperspectral imaging mission can be flown. Additionally, the information collected requires specialized skills to interpret. Moreover, since explosives are much more likely to be visible from the air at the site of IED manufacture rather than at the site of an intended attack, these sensors have very limited application in detecting emplaced devices.

Signal sensors capable of intercepting hostile actors' radio communications would offer the ability to listen for indications of IED emplacement or planned IED attacks. However, the employment of such sensors in a United Nations context is extremely sensitive and requires the full consent of the host nation. As a result, no United Nations air assets (crewed or uncrewed) are fitted with such sensors at this time.

Additional considerations

Regardless of the combination of aircraft platform and sensor type, the contribution of an air asset to the mitigation of an IED threat will always rely on a high-quality, specific, task description being provided to the air unit. It is therefore critical that any airborne information acquisition for counter-IED purposes is planned in advance with inputs from, at a minimum, the air unit; the Force U2; peacekeeping-intelligence surveillance, and reconnaissance/unmanned air system planners; and a subject matter expert in the specific IED threat in the mission area.

4.2. Search teams

Figure 4.3
Search team

In the United Nations mission setting the success of the IED threat mitigation effort is largely dependent on information-based operations against IEDs and associated components. All mobility units are to deploy with all arms search teams that comprise trained searchers, equipped with precision search equipment and ECM, capable of conducting basic search procedures. All arms search team members deploying to the mission should undergo predeployment training on the following:

- IEDs and their threats and methods of attack.
- Ground sign awareness.
- Conduct of vulnerability point/vulnerability area.
- Conduct of person and vehicle search drills and procedures.
- Applying physical force protection measures.
- Applying reporting responsibility.
- Supporting technical exploitation (e.g. collection of evidence)
- Conducting "actions on" drills (action on IED strike/ incident management) (e.g. contact explosion, casualty).
- Operation of search equipment.
- Understanding and employing ECM.

In complex situations, only specialized search teams, usually provided by military engineers, are to be employed.

Annex B provides further details on search in general and in detail on the planning and execution of search procedures, mainly focused on all arms search.

Specialist search is a capability employed by advanced search personnel trained, equipped and qualified to do so. Information regarding specialist search is contained in the *United Nations Military Engineer Unit & CET Search and Detect Manual.*

Figure 4.4
Person search, men

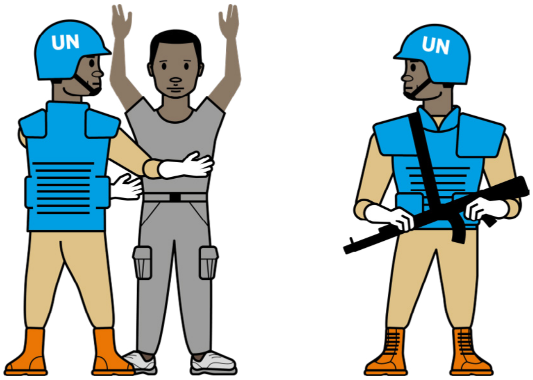


Figure 4.5
Person search, women

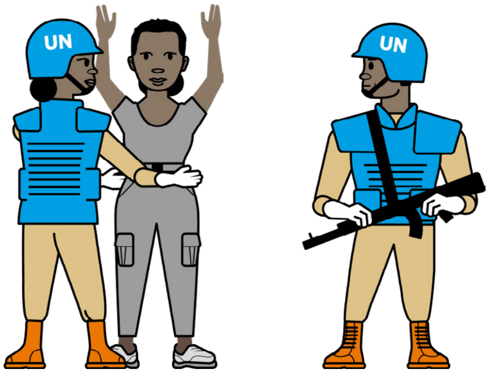
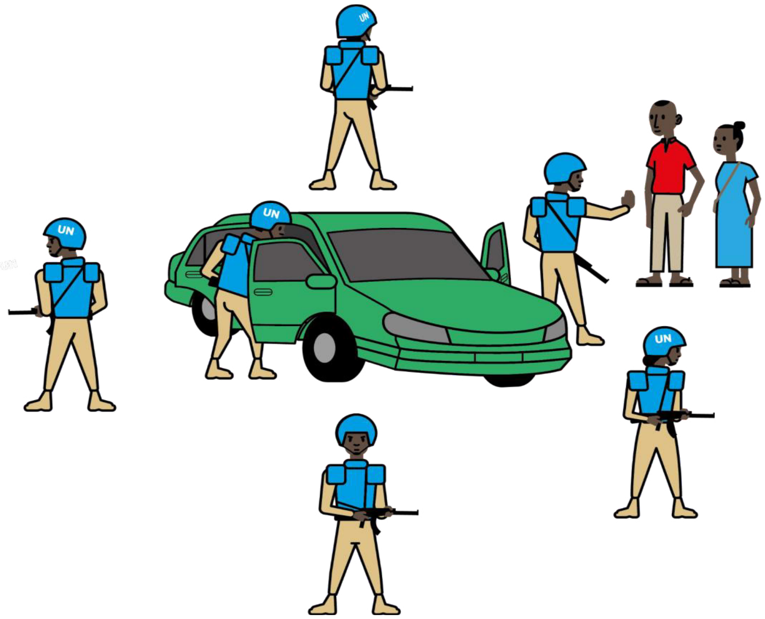


Figure 4.6
Vehicle search



4.3. EOD units

EOD units are enabling forces designed to support the Force and Sector Commander's ability to fulfil their mandates as safely as possible. EOD units can contain separate capabilities, depending on deployment configuration, conventional munitions disposal and IEDD components.[53] The IEDD capability is additional advanced training that implies an existing foundation of conventional munitions disposal.

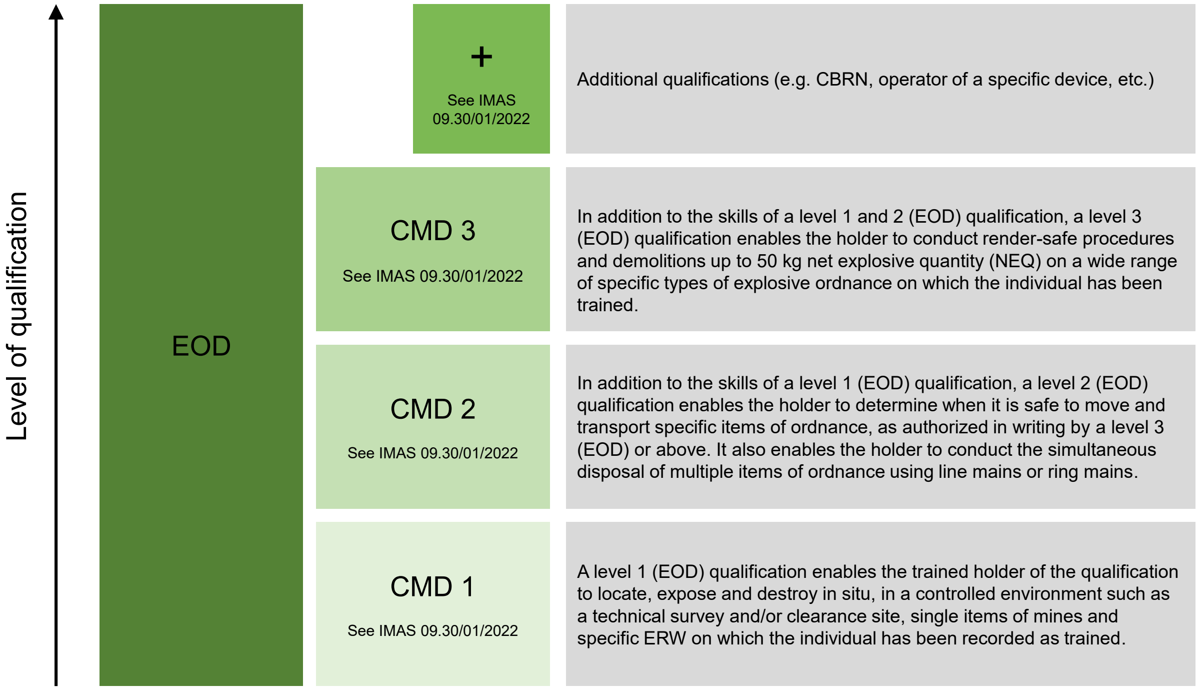
EOD teams are capable of conventional munitions disposal, which refers to any EOD operation conducted on ammunition that is used as a conventional weapon. Conventional munitions disposal activities may be taken as follows:

1. As part of mine-clearance operations, upon discovery of ERW.

2. To dispose of ERW discovered outside hazardous areas (this may be a single item of ERW or a larger number inside a specified area).

3. To dispose of items of conventional ordnance which have become hazardous by deterioration, damage or attempted destruction.

Figure 4.7
EOD/CMD qualifications and capabilities



+ See IMAS 09.30/01/2022	Additional qualifications (e.g. CBRN, operator of a specific device, etc.)
CMD 3 See IMAS 09.30/01/2022	In addition to the skills of a level 1 and 2 (EOD) qualification, a level 3 (EOD) qualification enables the holder to conduct render-safe procedures and demolitions up to 50 kg net explosive quantity (NEQ) on a wide range of specific types of explosive ordnance on which the individual has been trained.
CMD 2 See IMAS 09.30/01/2022	In addition to the skills of a level 1 (EOD) qualification, a level 2 (EOD) qualification enables the holder to determine when it is safe to move and transport specific items of ordnance, as authorized in writing by a level 3 (EOD) or above. It also enables the holder to conduct the simultaneous disposal of multiple items of ordnance using line mains or ring mains.
CMD 1 See IMAS 09.30/01/2022	A level 1 (EOD) qualification enables the trained holder of the qualification to locate, expose and destroy in situ, in a controlled environment such as a technical survey and/or clearance site, single items of mines and specific ERW on which the individual has been recorded as trained.

[53] In the *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual*, IEDD is defined as the location, identification, rendering safe and final disposal of IEDs. Final disposal refers to the final elimination of EO hazards by EOD personnel. This may include demolition, neutralization, burning or other proper means. In some cases, the render-safe procedure is the final disposal.

IEDD teams are EOD (conventional munitions disposal) teams that have additional advanced training. IEDD is the collective term referring to the following EOD procedures, intended to result in the final elimination of an IED, including detection, location, access, identification, evaluation, hazard mitigation, rendering safe, component recording and recovery, and final disposal.

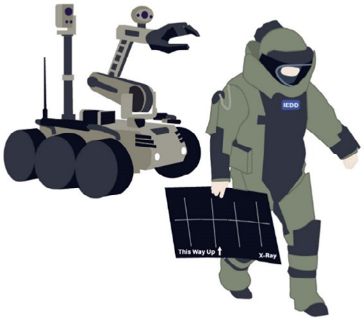
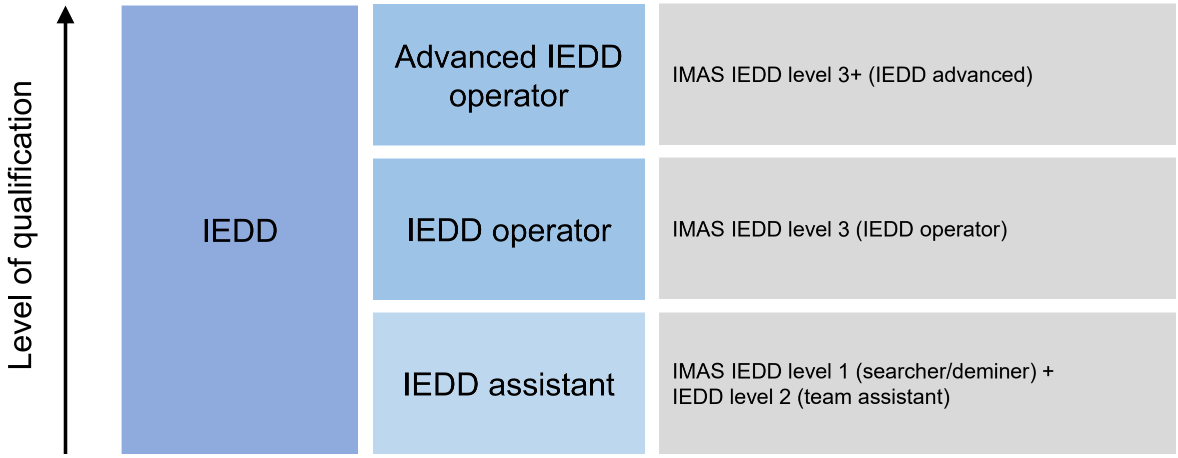


Figure 4.8
EOD/IEDD qualifications and capabilities



IEDD	Advanced IEDD operator	IMAS IEDD level 3+ (IEDD advanced)
	IEDD operator	IMAS IEDD level 3 (IEDD operator)
	IEDD assistant	IMAS IEDD level 1 (searcher/deminer) + IEDD level 2 (team assistant)

EOD units can deploy as an individual unit and be tasked by the force headquarters to serve as general area support or dedicated unit or mission-specific support.

EOD teams may also deploy as a dedicated and organic enabler to a larger force, such as an infantry or engineer company or battalion. Generally, these EOD forces will be solely dedicated to that contingent, supporting only their specific missions.

EOD forces may also be an organic part of other units or contingents, for example, combat transport units to serve as route reconnaissance/route clearance for logistic convoys.

EOD forces are best used in two separate methods: quick response force held at forward operating bases waiting for units in an area (e.g. sector) to locate an explosive hazard, or embedded within their parental units (e.g. infantry, transport) to enable faster response times and reducing the time on scene of an explosive hazard.

Infantry battalions are to employ own EOD teams embedded in sufficient strength to be able to support all given tasks by own means.

EOD units are also sources of advice in the following areas and should be relied upon by the sector and force leadership; route planning (historic targeting information); force protection (base perimeter security and blast mitigation); electronic warfare/ECM support within a radio-controlled IED threat environment; IED evidence collection and exploitation; host nation capacity development; force unit hazard awareness training; and civilian populace risk education.

4.4. Explosive detection dogs

The term explosive detection dog refers to a dog specifically trained to locate and correctly indicate the presence of vapourized molecules of defined explosive substances. Explosive detection dogs are used in many different roles within security risk-mitigating operations and thus complement an existing security framework. Explosive detection dogs are well suited for activities such as entry control point deployment (e.g. vehicle and luggage/cargo verification), facility security verification, open area verification and IED incident response.

The sense most used by detection dogs is smell. The availability of odour to dogs varies in complex ways with the environment in which the explosives occur. Influences include soil types, soil moisture, activity of microorganisms and climatic variables.

Explosive detection dogs are an excellent asset to assist with search in particular, not only in open spaces, but especially in closed spaces. In addition, they can also make a significant contribution to preventing, for example, IEDs from entering United Nations facilities by vehicles, people or mail, when used in access control.

As versatile as the use of dogs is, it can also be challenging. The dog's operational effectiveness depends on the relationship with its handler, and normally each specialist dog has a single handler. A well-skilled dog requires several years of training. It also requires special handling when in the field:

- Special accommodation, including a kennel with sufficient space, shade and so on.
- Appropriate medical supervision and care by a trained veterinarian is to be provided.
- In addition, the vehicle used to transport the dog must be designed in such a way that the vehicle is protected as much as possible from climatic influences.
- There must be appropriate dog food available.
- The dog needs appropriate protective equipment.
- Cultural aspects – some countries/cultures may have negative attitudes towards dogs and mitigation measures need to be considered.

Regarding deployment, it is important to bear in mind that explosive detection dogs can be used for only a limited period of time, after which it must be exchanged/replaced, and their use requires certain logistics, among other issues.

4.5. Technical exploitation

Technical exploitation is the task of EOD teams, if appropriately trained, or other trained personnel to collect, analyse and assess collected evidence in coordination with the IED threat mitigation adviser and to provide information to the work of the IED threat mitigation working group.

Explosive site investigation or post-blast investigation[54] are tasks for which highly skilled and experienced subject matter experts properly analyse captured materiel and put forward results. Exploitation activities

[54] Explosive site investigation or post-blast investigation both quantify on-site investigation within the technical peacekeeping-intelligence process and are often used in an interchangeable manner. This *Handbook* aims to use explosive site investigation as the broader term for a level-1 exploitation, as it includes post-blast investigation, which is the term used for investigations conducted where EO has detonated.

will include collecting and analysing technical, tactical and forensic information. They should not work separately and should closely cooperate with other cells, especially peacekeeping-intelligence.

With the outputs from exploitation/investigation, peacekeeping-intelligence analysts can then further assess the networks, perpetrator personnel, roles and relationships and IED network capabilities, to include associated IED components and materiel. Exploitation activities should be persistent and iterative to provide accurate peacekeeping-intelligence, develop effective countermeasures and contribute to degrading the network. These activities will assist some or all of the following:

- Build understanding of an IED system's centre of gravity, particularly to identify its critical vulnerabilities.
- Identify, confirm, analyse and assess perpetrator TTPs to assess trends and patterns, as well as identifying weaknesses and ascertaining advantages.
- Develop and refine friendly TTPs and contribute to hazard threat awareness training, IED training for EOD units and force protection to develop friendly force advantage.
- Develop detailed technical peacekeeping-intelligence to facilitate countermeasures for IEDs.
- Contribute to the lessons-learned process, leading to more effective operations and improved force protection.
- Provide inputs to the operating framework for the peacekeeping-intelligence cycle.
- Provide evidence for legal action that may lead to prosecutions and/or other government agency action, for example, diplomacy, economic coercion or commercial pressure.

The current United Nations system has three exploitation levels. The relationship between these levels and the information flow between them and the peacekeeping-intelligence functions are shown in figure 4.9.

Flows of information should be both bottom-up and top-down, and they need to be coordinated by the IED threat mitigation adviser, in close cooperation with U2 and the IED threat mitigation working group. Each level of exploitation requires feedback from the all-sources analysis cell, focusing on the priority peacekeeping-intelligence requirements, as well as from the upper exploitation levels, to provide guidance on technical procedures on evidence.

The three IED exploitation levels are:

- **Level 1 exploitation** refers to tactical collection and exploitation. Tactical units may have dedicated teams to perform an initial forensic analysis to develop actionable information while providing expertise and materiel to preserve and collect materials of interest for exploitation. These teams may have specialized training on forensic-enhanced, site exploitation techniques and be equipped with automated technologies to provide forensic analyses.
- **Level 2 exploitation** refers to in-country operational exploitation and analysis. The operational environment includes a modular and scalable deployed forensic capability that may augment the tactical-level capability in support of the Force Commander. Material from an objective is collected, preserved and shipped to forensic facilities (i.e. centres/laboratories) with advanced equipment and technology for exploitation by trained and qualified forensic examiners/technicians. The analysis is documented in a forensic report that is shared with user communities. A forensic analysis may result in identifying, sourcing and tracking materials used to create IEDs and contribute to force protection.
- **Level 3 exploitation** refers to out-of-country exploitation and analysis. International laboratories and centres have leading scientific and technical experts who, collectively, encompass all the

forensic fields, to provide the most comprehensive analyses of collected materials. Some national-level expertise may be provided in support of in-mission centres and laboratories.

Technical exploitation can and should be conducted without limitations since the findings will contribute to understanding patterns and trends. Careful consideration must be made to separating exploitation of device components, which will contribute to force protection measures, and the exploitation of biometrics for prosecutorial purposes.

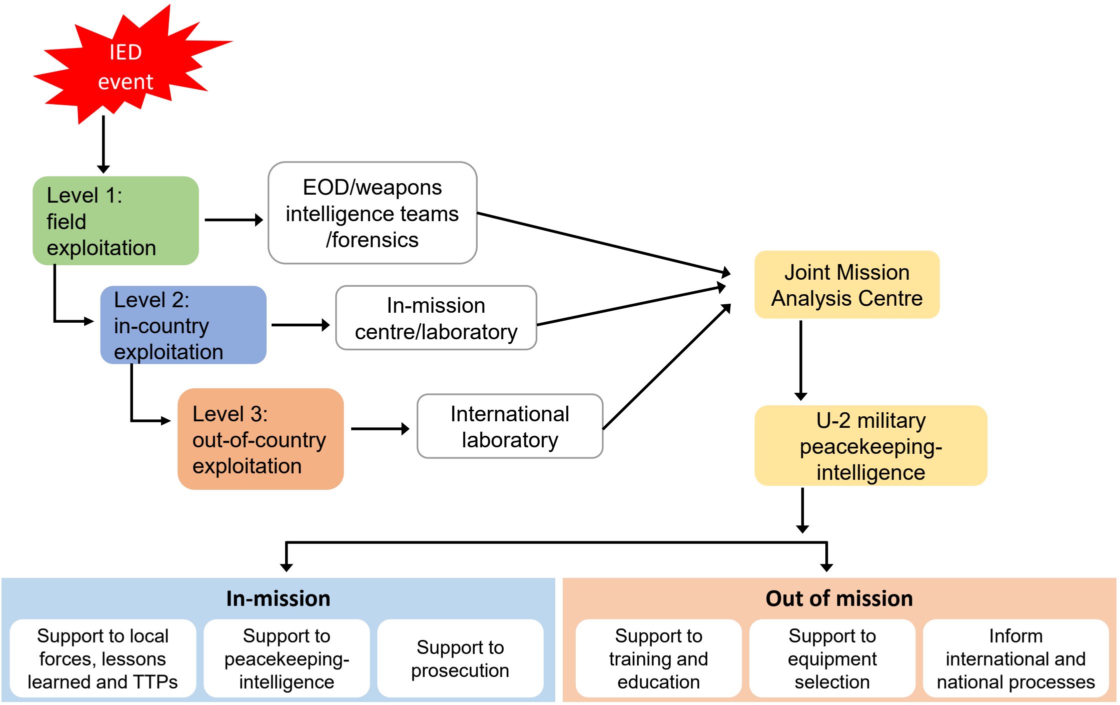
Exploitation of biometrics will be mission-specific and dependent upon several factors, such as the rule of law, capacity of police forces and so on. The collection, custody, use and responsible sharing of forensics and biometrics exploitation are considered ad hoc, to be implemented in concerned United Nations peacekeeping operations where the threat exists.

The common investigative entities within the military component to conduct level 1 exploitation are the military EOD experts and weapons intelligence teams, military police or gendarmerie and any mission military personnel qualified and trained to this effect. A weapons intelligence team refers to a small unit that deploys and undertakes technical exploitation in support of wider EOD efforts in an area of operation.

Execution of levels 2 and 3 technical exploitation depends on mission layout, mandate and availability of this highly technical expertise from troop-contributing countries, which usually consists of appropriately trained personnel and technical installations, such as laboratories and so on.

Planning during the force generation phase for an IED-affected United Nations mission must consider where such capabilities will lie. This phase should also establish how IED components and other related evidence that is recovered are handled to support judicial prosecution of the adversaries involved, including both physical and digital evidence.

Figure 4.9
Levels of exploitation, responsibilities and effects


IED event
Level 1: field exploitation
EOD/weapons intelligence teams /forensics
Level 2: in-country exploitation
In-mission centre/laboratory
Level 3: out-of-country exploitation
International laboratory
Joint Mission Analysis Centre
U-2 military peacekeeping-intelligence
In-mission
Support to local forces, lessons learned and TTPs
Support to peacekeeping-intelligence
Support to prosecution
Out of mission
Support to training and education
Support to equipment selection
Inform international and national processes

Options where such capabilities can reside are within EOD teams, within military police units or as stand-alone dedicated weapons intelligence teams. The decision depends on the IED activity level in the mission and the ability of those tasked to undertake weapons technical peacekeeping-intelligence to have the required time necessary to devote to this role in support of counter-IED operations.

4.6. Military engineers

The core capabilities of the United Nations Military Engineer Unit include combat engineering, construction engineering EOD and support to mission partners. A detailed list of tasks, conditions and standards can be found in the *United Nations Military Engineer Unit and CET & Search and Detect Manual*.

Combat engineers are expected to provide obstacle crossing (including gap and river), route clearance capability and limited capacity to repair roads, airfields and landing zones in direct support of military operations, potentially under hostile conditions. To effectively defeat or mitigate threats posed by EO, these units must be capable of conducting counter-explosive threat activities including but not limited to EOD and demining operations.

Construction engineers provide enhanced capabilities in the construction of physical protection measures for United Nations installations and have the capability to provide their own force protection.

In addition, military engineers can provide technical training and assistance to supported units by demining and EOD support before and during search operations. If demining is done in support of humanitarian mine action, IMAS applies.

Military engineers are also able to support road clearance with their vehicles and equipment, but they usually do not provide a deployable EOD capability to support mounted or dismounted patrols against an IED threat.

4.7. Civil-military cooperation/engagement platoon

The Head of Military Component/Force Commander and police headquarters are responsible for conducting outreach and engagement with the local population. Interaction with local leaders, influential actors in civil society and vulnerable sections of the population is part of the overall force and mission communications strategy. Securing local and host nation support is an essential element of force and mission success and is a key strength of the United Nations in mitigating IED threat. Civil-military cooperation (CIMIC) also requires interaction with United Nations civilian partners, United Nations agencies and NGOs.

Effective CIMIC systems will enhance force protection. CIMIC is necessary to develop a robust interface with the local population and build trust and respect for the military force. This interface with the local population will assist in the generation of a safer environment for the military force.[55]

One of the core principles of United Nations Civil-Military Coordination is to facilitate integration of efforts; provide a key link to the civilian components of a mission, and mission partners such as humanitarian and development actors, host nation military and local populations; and produce analysis

[55] Civil-military coordination in United Nations integrated peacekeeping missions.

in conjunction with military operations and in support of achieving the mission mandate. For that purpose, United Nations Civil-Military Coordination personnel must develop a comprehensive common operational picture and the analysis of such to support planning and the conduct of military operations in the mission. Data collection is achieved through observation of and engagement with the human terrain and physical environment. Observation and engagement can improve force protection and protection of civilians through better situational awareness, allowing risks, threats and violations of United Nations policy or international law to be recognized and reported. Monitoring these risks can identify hotspots that can be targeted by an increased military presence to prevent escalation of violence. Enhanced situational awareness includes identification of security vulnerabilities, identifying vulnerable demographic groups and potential security threats to these individuals/groups.[56]

The engagement platoon is to specifically gain information from the entire population and bridge an identified gap. The aim is to provide infantry battalion commanders further means with specially trained male and female peacekeepers to interact with men, women, boys and girls in the mission area.

Therefore, CIMIC units and engagement platoons are two other assets that can effectively contribute to IED threat mitigation by informing the local population about known threats and potential risk areas, but at the same time gaining information about potential networks, activities or hotspots, which contributes to the overall threat awareness, trend analysis and support for building a common operational picture.

4.8. Maritime IED threat mitigation assets

An IED threat may also be found underwater in shore and riverine operations (e.g. in harbours, on ship's hull, on a bridge pillar, on river submerged banks) or on water surface (e.g. waterborne IED). Depending on the mission mandate, area and source capabilities the following assets may be employed to mitigate an underwater IED threat:

- Air scuba divers are qualified for underwater clearance search and investigation in force protection operations.
- EOD divers are qualified for underwater clearance search, investigation and ordnance disposal[57]
- Autonomous underwater vehicles for sonar bottom search and possible visual identification.
- Remote-operated vehicles for visual search and identification.

Underwater operations are highly environment dependent (underwater visibility, current, pollution), and they require a considerable amount of time, as well as small boats to operate as safety for the divers or the autonomous underwater vehicles/remote-operated vehicles.

For a suspected waterborne IED investigation, UAS support, when available, is a helpful primary means and may be used, as shown in section 4.1.

[56] *United Nations Engagement Platoon Handbook.*

[57] Generally, air scuba divers are an army/navy/police capacity, while EOD divers are usually a navy/police asset.

5. IED threat mitigation plan

In designing an IED threat mitigation plan, six fundamental actions – predict, prevent, detect, dispose, mitigate and exploit – form the basis for developing an integrated, holistic approach.

The output from these six activities provides the capability needed by the mission to predict the perpetrator's actions, prevent the perpetrator from executing plans, detect IED material and devices, neutralize emplaced devices, mitigate the effects of an IED event and exploit IEDs and/or IED events.

Predict

Predict comprises the analytical actions necessary to develop and maintain a comprehensive understanding of the operational IED environment. It exploits peacekeeping-intelligence and in so doing, contributes to a more concise understanding of the perpetrator's cell structures, systems, networks, training, equipment, infrastructure, TTPs, support mechanisms (e.g. IED material) and other actions which forecast the IED operations.

Prevent

Prevent comprises proactive actions associated with the degradation the perpetrator's capability through detection of IED and associated components prior to emplacement, to prevent an attack. Prevent includes:

- Identifying and arresting key actors of an IED network in line with the United Nations rules and regulations.
- Disrupting the IED chain of events prior to emplacement, including through regional cooperation with neighbouring States and international organizations.
- Deterring public support for the perpetrator's use of IEDs.

Actions, in conformity with the United Nations peacekeeping operations rules of engagement, may lead to arrest and detention of key perpetrator personnel, searches of infrastructure and confiscation of logistic capabilities, which are used for IEDs and pose a threat to United Nations personnel or the civilian population.

Detect

Detect occurs after an IED has been emplaced and is a crucial counter-IED element. It includes activities designed to identify and locate personnel, activities, explosive devices (and their component parts), equipment, caches of IED components, weapons and infrastructure.

Dispose

To prevent uncontrolled detonation, IEDs must be disposed of safely through a deliberate detonation, disruption or neutralization. Disposal enables peacekeepers and the local populace to operate safely in and around the emplacement site.

Mitigate

In the event that predict, prevent and detect fail, minimizing the effects of an IED event is an essential preparation activity (see section 5.6 on vulnerability assessment). This includes procedures, countermeasures, equipment and fortification.

Exploit

Exploit is the process through which events and associated physical materials are recorded and analysed. The objective is to understand the perpetrator's methods of operation and relationships and the device's capabilities. Exploitation activities can yield valuable information on the perpetrator's TTPs and provide a starting point to track down the perpetrator's supply chain. Exploitation takes place at any stage within the IED system, although every effort must be made to conduct exploitation as early as possible to restrict the perpetrator's IED activities.

5.1. Information management/exchange

One of the essential prerequisites for successfully mitigating the threat in the medium to long term is to manage all available information appropriately from the outset. Further, information management/exchange ensures that all actors contribute to building up a clear common operational picture of the situation, as possible, through standardized reporting, which in turn enables planners and operators to respond to the threat in the first place.

Any IED threat mitigation organization must consider "the need to share" principle and the sensitivity of the information. In-depth knowledge of the IED threat picture[58] enables efficient identification of the resources, training, equipment and capabilities required to effectively mitigate the threat.

In IED threat mitigation, the "need to share" principle refers to the requirement for all stakeholders in the IED threat mitigation organization in a given locality to share information on IEDs, perpetrators TTPs and so on with other organizations operating in the same area or region. Information-sharing is essential in IED threat mitigation to maintain an accurate IED threat picture, which is a basic requirement for safe, effective and efficient IED threat mitigation. Information-sharing with non-United Nations partners must be in conformity with United Nations rules and regulations and cleared at the appropriate level.

Unite Aware

Unite Aware is a software suite for United Nations peacekeeping operations to centrally collect, secure, retrieve and share critical incident/event data and then present that information to uniformed and other substantive decision makers via analysis, visualization and reporting applications to support tactical, operational and strategic decision-making.

The two main objectives of Unite Aware are to provide a comprehensive and integrated approach to situational awareness and to support United Nations field missions to manage critical information-management processes. The suite aims to create a cohesive solution that enables United Nations

[58] An assessment of the potential use of IEDs in a defined geographical area by a stated IED perpetrator or perpetrators against a stated entity in terms of the technical complexity and tactical sophistication, along with the perpetrators' intent, capabilities and opportunities as well as local factors.

mission staff to access and view near real-time data from a variety of sources, displayed in a clear and intuitive format.

As part of the Unite Aware suite, SAGE (situational awareness geospatial enterprise) is a simple and intuitive web application that offers an integrated field operational and situational awareness information management system. SAGE enables mission components to collect, share and retrieve geo-coded and categorized data related to incidents, violations, events and activities.[59]

All United Nations entities are to use Unite Aware SAGE to report any kind of incident including IED attacks.

To prevent multiple entities from reporting the same incident, which would result in an unrealistic picture, dedicated personnel should be assigned to check and reconcile all entries to ensure that the information is consistent and complementary rather than contradictory or reiterative.

The advantage of unified reporting is that it enables information to be collated in a designated place, shared and made available to all participants for their various analysis.

In a comprehensive approach, the software suite also provides the possibility to identify the transfer of certain threats (e.g. IED and illegal weaponry, ammunition and explosive precursor trafficking) across countries and to warn accordingly of a new or emerging trend in time.

To compare, validate or complement information in SAGE, coexisting information management and reporting systems from relevant entities, for example, UNMAS or the Department of Safety and Security, can be used. Information related to casualty recording and weapon/explosive use within the area of operation can also be provided by the mission's human rights component and Office of the United Nations High Commissioner for Human Rights through their mandated monitoring and investigations capacity.

Global Information Management System

UNMAS programmes, whether in a peacekeeping mission, in a special political mission or in a non-mission setting, report on EO and IED information through the Global Information Management System (Global IMS). Each programme collates, enters and validates data independently using the information on their own products. The United Nations Office for Project Services, Peace and Security Cluster, Information Management and Analytics Team regularly and automatically connects to the various programmes databases and integrates the resulting data sets into a single source of truth. This harmonized data set is then used for internal global products (Global IED Dashboard, Global EO Dashboard, IED QA Report) and shared with partners such as SAGE and Unite Aware.

More information about the data flow and data availability is illustrated in annex C.

Each UNMAS programme has its own sources and media to collate information related to EO and IEDs. For the sake of data quality, programmes are asked to follow the minimum data requirement on their workflows, specified by UNMAS.

[59] The other components of the Unite Aware suite are UA Maps for mapped visualization of incidents/events overlaid with other map layers providing thematic and operational information geographically; UA Patrol Plans for the planning and approval of patrols; and UA Business Intelligence for data visualization of data collected in SAGE and UA Patrol Plans apps.

To ensure the accuracy of the information, data collected follow a minimum two-step validation process before being accessible on the various products.

Data can be saved on different media owned by the programmes, but it will ultimately be stored on secure databases and managed by the United Nations Office for Project Services, Peace and Security Cluster, Information Management and Analytics Team.

Each programme is responsible for creating and maintaining products (e.g. reports and visualizations). The United Nations Office for Project Services, Peace and Security Cluster, Information Management and Analytics Team collates relevant information from the programmes' databases into a single database (via an automated script), and this collated database is shared with external partners.

Safety and Security Incident Recording System

The United Nations Department of Safety and Security's Safety and Security Incident Recording System (SSIRS)[60] is used by all organizations of the United Nations Security Management System as a tool to input and store (record) data regarding safety and security incidents that harmed or had the potential to harm United Nations personnel, programmes, premises and assets.

SSIRS is not limited to IED incidents. SSIRS is intended to record incidents that directly target and indirectly impact the United Nations, including accidental fire, road accidents and other transportation accidents and natural events, such as earthquakes and floods. All incident types are included in the SSIRS incident taxonomy, which is intended to be paired with the SSIRS weapons taxonomy to develop threat events that include tactics and weapons.

Recording incident using SSIRS is intended to improve situational awareness and provide specific information about the types of weapons and tactics that are used against the United Nations in an area of operation. Having this information will assist security managers at the local and national levels to make knowledgeable decisions regarding the most appropriate security risk management measures, given existing threats and risks. This information can also be used strategically, at the headquarters level, through the analysis of well-substantiated data sets to compare threats and risks to the United Nations around the world.

Information on SSIRS includes incident location (e.g. region, country, designated area), time of incident (including duration if the incident takes place over time), description of the incidents and a listing of the impacts on premises, personnel and programmes.

The access is restricted to United Nations staff with the United Nations Security Management System credentials. Depending on the security credentials, the United Nations staff can add incidents or only search incidents or statistics. Access for certain personnel in the military and police component can be granted under special circumstances through the Department of Safety and Security staff (Principal Security Adviser or Chief Security Adviser) in the area.

Specific events searching and reports can be provided through the Department of Safety and Security staff. The standard reports provided by SSIRS include:

- Daily incident list.
- Overview of security incidents that have occurred on a particular date.
- Comprehensive incident report by region/event (with or without impact).

[60] SSIRS is available in the United Nations Security Managers Information Network at https://unsmin.dss.un.org/.

- Comprehensive report listing all events and their description, with impact details (names of staff are not listed).
- Filter by region, designated area, event or impact.
- SSIRS database filtering by incident impact.
- SSIRS incident by date and designated area and impacted agency.
- Arrest and detention and hostage-taking and abduction.

Annex C shows examples of information recorded in Global IMS and SSIRS. Information from both systems can be obtained via the respective representative from UNMAS and the Department of Safety and Security in the specific United Nations peacekeeping operations and can be part of the agenda for the IED threat mitigation working group.

Furthermore, according to the standard operating procedure on integrated reporting from peacekeeping operations to United Nations Headquarters and the policy and the guideline on Joint Operations Centres,[61] the Head of Mission is responsible for reporting regularly to United Nations Headquarters, through the Under-Secretary-General of the Department of Peace Operations, on developments concerning the activities of peacekeeping missions and the implementation of each mission's mandate.[62] Those reports include but are not limited to significant incident reports (e.g. flash report), notification of casualties[63] and hostile act report regarding any hostile act against peacekeepers.[64]

5.2. Reporting

The uninterrupted flow of information is essential for the safe and effective conduct of operations. Staff, troops and units under an IED threat need to communicate timely, clearly and concisely so that IED threat mitigation measures can be planned and executed successfully. Reporting contributes significantly to enhanced situational awareness. This enables headquarters – regardless of the level – to make informed decision and adjust ongoing operations based on the response and impromptu situations that may arise.[65]

The reporting of explosive incidents should include, where possible, and at the earliest stage, technical and tactical information to understand the TTPs of the perpetrators. The primary tool to record and maintain data regarding all explosive incidents is the Unite Aware and relevant entity's respective SAGE to allow continuity and exchange within and across United Nations peacekeeping operations and with United Nations Headquarters.

United Nations peacekeeping operations are to provide unified reporting formats, which can be used using mobile communication means (radios). Standardized report and message formats enable easier

[61] Joint Operations Centre guidelines (2019.21).

[62] Guidelines on the Role of the Head of the Military Component in a United Nations Peacekeeping Operation (2023.04).

[63] Those incidents are reflected in the NOTICAS database. NOTICAS is an automated, web-based application which allows missions to input their data directly into the system. Data are stored securely and archived when appropriate. The tool includes simple aggregated reporting and automated notifications making information readily available for decision-making and communication purposes.

[64] Hostile act reports apply only for hostilities against military and do not include other entities, for example United Nations police. Those reports are collected by the Office of Military Affairs, Current Military Operations Service.

[65] *United Nations Deployed Military Field Headquarters Handbook* (2023.08).

interpretation and efficient exchange of information. Standardized forms are particularly important in combined operations, as they reduce the impact of different operating languages and ease the collation and transmission of complex information. Standardized specimens of the following IED/EO reporting forms are included in annex D.

The reporting templates are designed to be used in any explosive-related event, ranging from all IED-related events (e.g. explosion, find, cache, false, hoax) to indirect fire including complex attack and unexploded ordnance/ERW events.

To be fully effective and ensure the maximum benefit, reporting must be:

- **Accurate** Timings, locations, events and so on must be precise.
- **Complete** All available information relating to an incident must be gathered and all incidents must be reported.
- **Linked** Any links to individuals, geographic areas and conditions should be readily identified and understood.
- **Timely** Dissemination of peacekeeping-intelligence and lessons learned to the right recipient at the right time.

All commanders are responsible for ensuring that their personnel are familiar with the reporting format and can use these even under stress.

Figure 5.1
Reporting scheme

Time	From	To	When	Format	Means
Immediate	Unit/individual uniformed personnel	Headquarters	IED incident	**Explosive ordnance/IED incident report**	Radio/mail
Immediate	Headquarters	EOD	Receiving explosive ordnance/IED incident report (and unit)	**EOD task order** (consist of validated explosive ordnance/IED incident report)	Radio/mail
ASAP-3h (return to base)	EOD team	Headquarters	Initial situational overview and first assessment	**EOD Quick Look**	Mail
Depending on the incident: • **Red** • **Amber** • **Green**	EOD	Headquarters/ database	EOD task order completed	**EOD report**	Mail
No later than 24h	Level 1 technical exploitation (weapons intelligence team, post-blast investigation)	Headquarters	(If there is no weapons intelligence team or post-blast investigation team available, the technical exploitation-1 report will be substituted by the EOD report)	Technical exploitation-1 report	Mail
ASAP	Level 2 technical exploitation		Detailed assessment of all collected evidence with detailed analysis	Technical exploitation-2 report	Mail
ASAP	Headquarters/ IED threat mitigation working group	All units/individual uniformed personnel		**EOD/IED awareness report**	Mail

5.3. Threat assessment

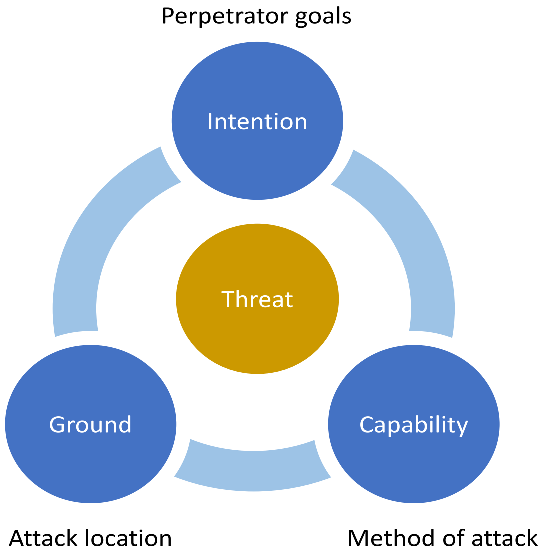
The nature of IEDD operations is inherently more complex than traditional mine action. The introduction of human perpetrators and their unlimited inventiveness into the equation results in a considerably more complex, dynamic and evolving threat. Organizations conducting IEDD must understand that the threat, both from the IEDs and the way they are employed, can and will change rapidly. In developing an understanding of current and probable future perpetrators, it is likely that IEDD organizations will be considered a valuable target. Thus, there is a chance that IEDD personnel will be observed by perpetrator networks who are attempting to identify patterns, capability gaps and weaknesses that can be exploited.

Ideally troop- and police-contributing countries are to be informed of IED threats within the mission area before and during reconnaissance visits, in line with the Department of Peace Operations policy on contributing country reconnaissance visits.[66]

Information on existing IED threats can aid troop- and police-contributing countries to prepare relevant threat mitigation measures. The process of assessing IED threat mitigation preparedness should also be continuous. United Nations Headquarters should ascertain the troop- and police-contributing countries preparedness during predeployment visits in advance of each contingent's induction, in line with the policy on operational readiness preparation (ref. 2024.06). UNMAS currently maintains the technical expertise required to assess the threat and potential impact of IEDs and other explosive hazards. Until a dedicated IED threat mitigation organization (military and police) is developed in a mission, this expertise is available at United Nations Headquarters and should be called upon to participate, support or advise during the assessment and planning processes. This may include the conduct of an assessment mission and/or technical survey.

The IEDD organization is required to constantly evaluate the appropriateness of their troop- and police-contributing countries. To stay ahead of the threat and mitigate the risk to the greatest extent possible, all actors in the IED threat mitigation organization must work together to collect, assess and disseminate tactical and technical observations.

Figure 5.2
Threat analysis



[66] Policy on reconnaissance visits by troop- and police-contributing countries.

A threat assessment determines the targets, perpetrators and capabilities, most likely and most dangerous courses of action and overall intentions of identified threats to help to identify the complete spectrum of capability that will be required to counter the IED threat. IEDD planning is a multidisciplinary activity and needs to be conducted at every level by robust and detailed threat assessments, but at its very heart must have suitably qualified and experienced IEDD operators to properly interpret the threat and inform the technical requirement at every level.

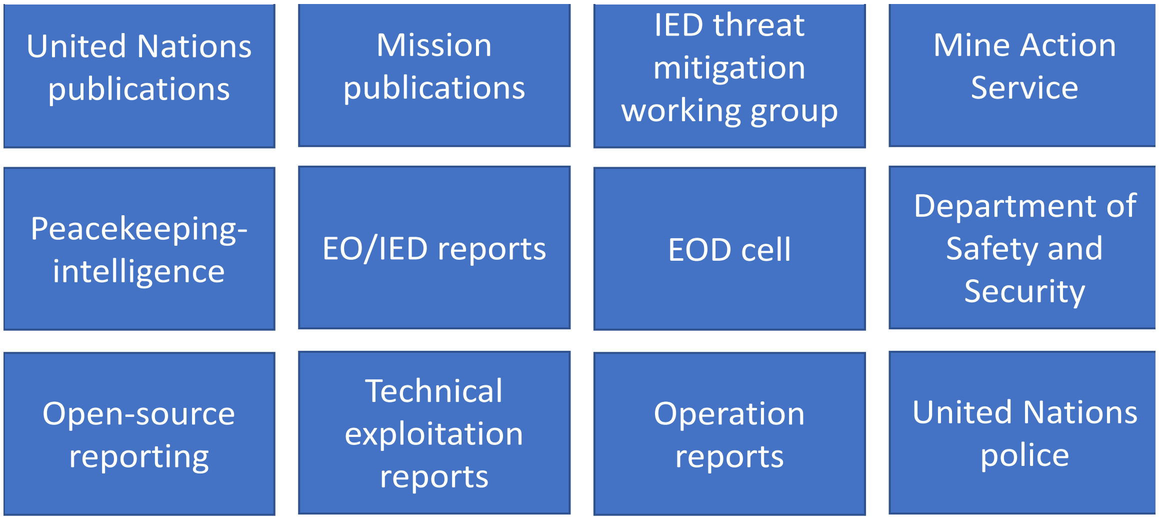
The threat from IEDs can be broken down into "technical" and "tactical" which, when combined, will give the overarching threat picture to IEDD operators and organizations. The "technical" threat refers to the analysis of the perpetrator's likely ability to use complex components and switches, particularly radio command, along with their ability to source those components. The "tactical" threat refers to the TTPs, as well as myriads of subjective factors, based on the perpetrator's intent and history, to understand the likely method of employment of a device.

Planning and threat assessment will take place at three levels:

- Area of operation/peacekeeping operation/regional and neighbouring State analysis
- Sector within a peacekeeping operation
- Scene

The area of operations level may be considered strategic, the sector level operational, and the scene level tactical.

Figure 5.3
Sources of information for planning and analysis



United Nations publications

Mission publications

IED threat mitigation working group

Mine Action Service

Peacekeeping-intelligence

EO/IED reports

EOD cell

Department of Safety and Security

Open-source reporting

Technical exploitation reports

Operation reports

United Nations police

To enable a comprehensive assessment, the assessment of the environment should not focus solely on the period immediately prior to deployment, but should, where possible, consider a longer period. The assessment should be based on the following indicators:

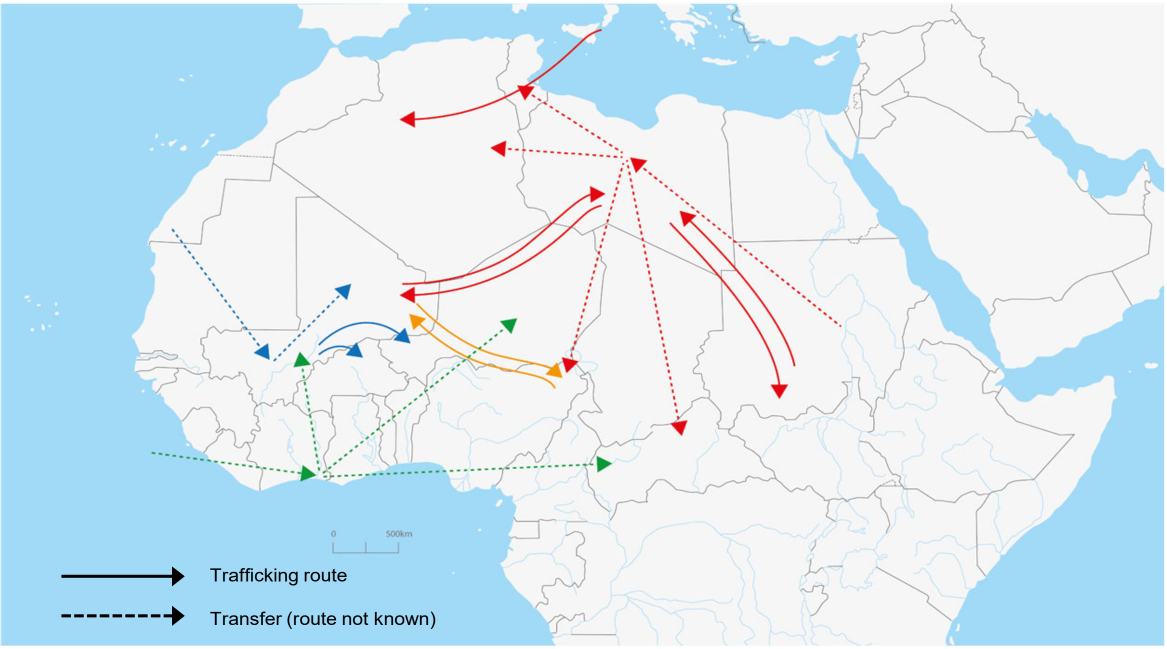
- Local IED capabilities of attackers or non-State actors in the host country.
- Existing level of IED threat in the country through peacekeeping-intelligence collection, assessment and information management.

- Availability of IED manufacturing material in the host country, along with the required expertise to manufacture IEDs.
- Existence of IED manufacturing capabilities in neighbouring States that may result in the transfer of IED capability to the host country after the United Nations mission is deployed.
- Intensity of the use of IEDs in the conflict situation, which may indicate the use of IEDs against United Nations personnel or facilities after deployment.

In this context, weapon trafficking should be analysed not only within the country of the peacekeeping operation, but also trans-border weapon trafficking within a region or even the whole continent. Figure 5.4 shows schematically how far weapon trafficking can have an influence on the IED threat in a specific country.

Figure 5.4
Weapon trafficking[67]

In the Sahara, conflicts are interrelated, and weapons and armed people are moving from one area to another.



5.3.1. Area of operation level

Area of operation level planning and threat assessment relate to higher-level planning to assess the present and potential future explosive hazard threats in a wider geographical region or country. Area of operation planning and threat assessment is an essential first step in determining the safe, effective and efficient IEDD capabilities to be deployed to the IED threat environment and will be instrumental in

[67] See United Nations Office on Drugs and Crime. Firearms Trafficking in the Sahel, Transnational Organized Crime Threat Assessment – Sahel, New York, 2022. Available at www.unodc.org/documents/data-and-analysis/tocta_sahel/TOCTA_Sahel_firearms_2023.pdf. See also RHIPTO, Norwegian Center for Global Analyses, A UN-Collaborating Rapid Response Center on Environment, Development, Peace and Security, Maps and Graphics. Available at www.rhipto.org/maps-and-graphics.

determining the detail of the statement of requirements to be communicated to prospective capability providers.

It is impossible to be completely prescriptive about who exactly will be involved in this area of operations level planning and threat assessment, but it will typically be led by the United Nations Headquarters and United Nations peacekeeping operations mission leadership and include host nation security forces and other organizations, as required and appropriate.

Once complete, the area of operations planning and threat assessment process will be the basis against which capability requirements are put forward for tender and against which detailed terms of reference are agreed. However, the process is never complete and is a continual cycle informed by a constant flow and exchange of information between all three levels.

Planning at the area of operations level will encompass the spectrum of IED threat and cover the complete requirement from traditional mine action activity through to those additional measures required to mitigate the specific IED threat.

The area of operations level must include regional and neighbouring State analysis to understand all external influences which might affect the IED threat. Due to the restrictions on the mandate area, direct influence on regional factors or neighbouring States is only possible to a limited extent. In this respect, creative solutions need to be found, for example consider partnering with and financing research organizations that can collaborate with neighbouring States to carry out some of the required research to achieve a more comprehensive understanding of the situation.

5.3.2. Sector level

Sector-level planning and threat assessment will be conducted by the sector headquarters looking to respond to a statement of requirements developed at the area of operations level. It involves a specialized IEDD operator at the heart of the threat assessment and draw on the expertise of the IEDD organization in determining threat through both technical and non-technical surveys. Informed by the area of operations threat assessment, the process should aim to draw down the threat to an operational picture that will further refine the threat for a more defined geographical location.

The completion and submission of a sector-level threat assessment must be a requirement within the statement of work and without which IEDD clearance operations should not commence.

The sector-level threat assessment must describe, in full technical detail, the known or established threats by device type. During a sector analysis, strong community relationships are essential to building the necessary trust required for a thorough understanding of the IED threat. The use of community liaisons should be strongly considered by IEDD organizations.

The sector-level planning and threat assessment should prioritize clearance operations within the designated area of operations and allocate adequate and appropriate resources. The threat assessment should also detail the freedoms and constraints that will be placed on the clearance teams by detailing the reporting requirements and understanding what situational changes[68] will result in re-evaluation of the IED threat assessment.

The sector threat assessment should be subject to frequent review based on the developing understanding of threat which will come from information from the national-level IED threat assessment, as well as

[68] Situational changes refer to changes in any of the following: IED technical complexity, IED tactical sophistication, perpetrator intent, perpetrator capability and perpetrator opportunity.

from ongoing clearance operations. A robust information knowledge management system, into which IEDD teams submit reports and from which the IEDD organization collates data for analysis and trends prior to dissemination to IEDD teams and to the designated IEDD authority, will underpin the threat assessment and allow managers to react appropriately to a changing threat picture.

5.3.3. Scene level

Scene-level planning and threat assessment commences once the national and area level threat assessments have been completed and clearance teams have been allocated to tasks. These clearance teams will include personnel trained to the appropriate level as determined by the planning and threat assessments and risk analysis. It is the direct responsibility of the supervising IEDD operator to draw down the national and sector threat assessments and then conduct a threat assessment for the specific scene or site where they are operating. This scene-level threat assessment will be an incident appreciation[69] of the immediate site and must be used to confirm the accuracy and validity of the area threat assessment and that the personnel allocated to the task are adequately trained for the assessed threat. This is the most dynamic threat assessment, and it is essential that anything at the scene level which changes the assumptions of the sector or area of operation threat assessments is immediately communicated across the organization and up to the designated IEDD authority, where appropriate.

5.4. IED pattern analysis

Pattern analysis is a planning process used to evaluate the data collected to identify recurring patterns. It is not limited to perpetrators but also examines own patterns.

Regarding the perpetrator, it is important to examine in terms of the type of IEDs, attack locations, times, distance to certain localities, which can, for example, indicate the mobility of the opponent. This can be in terms of the type of IEDs, but also in terms of attack locations, times, distance to certain localities, which can, for example, indicate the mobility of the opponent. It is advisable to process all the data collected in such a way that they are available either in tabular or in graphical form, so that they can be interpreted more easily. Various applications, such as Power BI, are available for this purpose and should be used accordingly.

Perpetrators' attacks should be evaluated at the technical level and also on the tactical side. These patterns can be used to predict future attacks or incidents and plan peacekeeping-intelligence, surveillance and reconnaissance activities and training.

Pattern analysis also includes own pattern, how the respective unit or contingent reacts to the IED threat from the perpetrator. It should always be assumed that perpetrators are continuously observing peacekeepers procedures and best practices to exploit patterns, be it during a patrol in general, during the investigation of a suspected IED or in the case of an IED find.

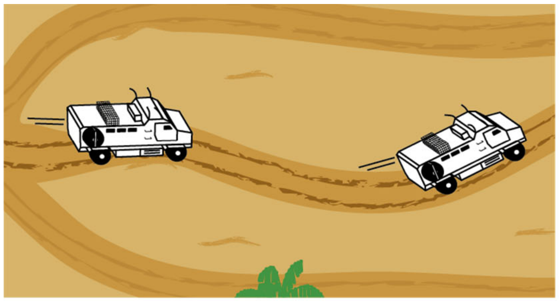
From one rotation to another, the perpetrators will evaluate the capacity of the contingent, if they use new practices or if they reuse old practices. This provides perpetrators with important information on whether their own procedures are still successful or whether they may have to change their measures.

[69] An assessment of an EOD/IED incident from information gathered through observation, map analysis, witnesses, surveys and all other means allowing an area evaluation in support of a threat assessment leading to threat integration from which possible courses of action are identified as part of a safe, effective and efficient EOD plan.

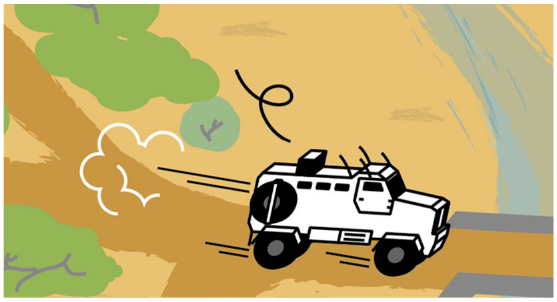
Each contingent therefore should adapt its own best practices to the terrain, mission and perpetrators' capacity.

However, it is important to analyse very critically whether certain own patterns are conducive to attacks with IEDs and must be adjusted or modified, if necessary.

Figure 5.5
Examples of pattern setting



Example: Don't always use the same routes.



Because most people drive on the right-hand side, most vehicles hit an IED with the right wheel. Don't drive on the side of the road. Rather stay in the middle.

5.5. Trends

Trend analysis is closely related to pattern analysis. The aim here is to identify certain changes, so-called trends, at an early stage and to react to them accordingly. A trend can be, for example, that a new type of switch or type of IED appears in the area of operation or that, contrary to previous patterns, attacks suddenly take place on a different day or in a different place. Such anomalies must be paid particular attention to be able to recognize new trends at an early stage.

A corresponding trend analysis also includes not only looking at the country of operation, but also trying to identify regional or even global trends at an early stage. Owing to modern media, the new development of a certain type of attack can spread very quickly and be adapted by perpetrators within the area of operation accordingly. Those trends can, for example, be analysed in other conflicts around the world where peacekeepers are not deployed, but where IEDs are also used by the parties to the conflict.

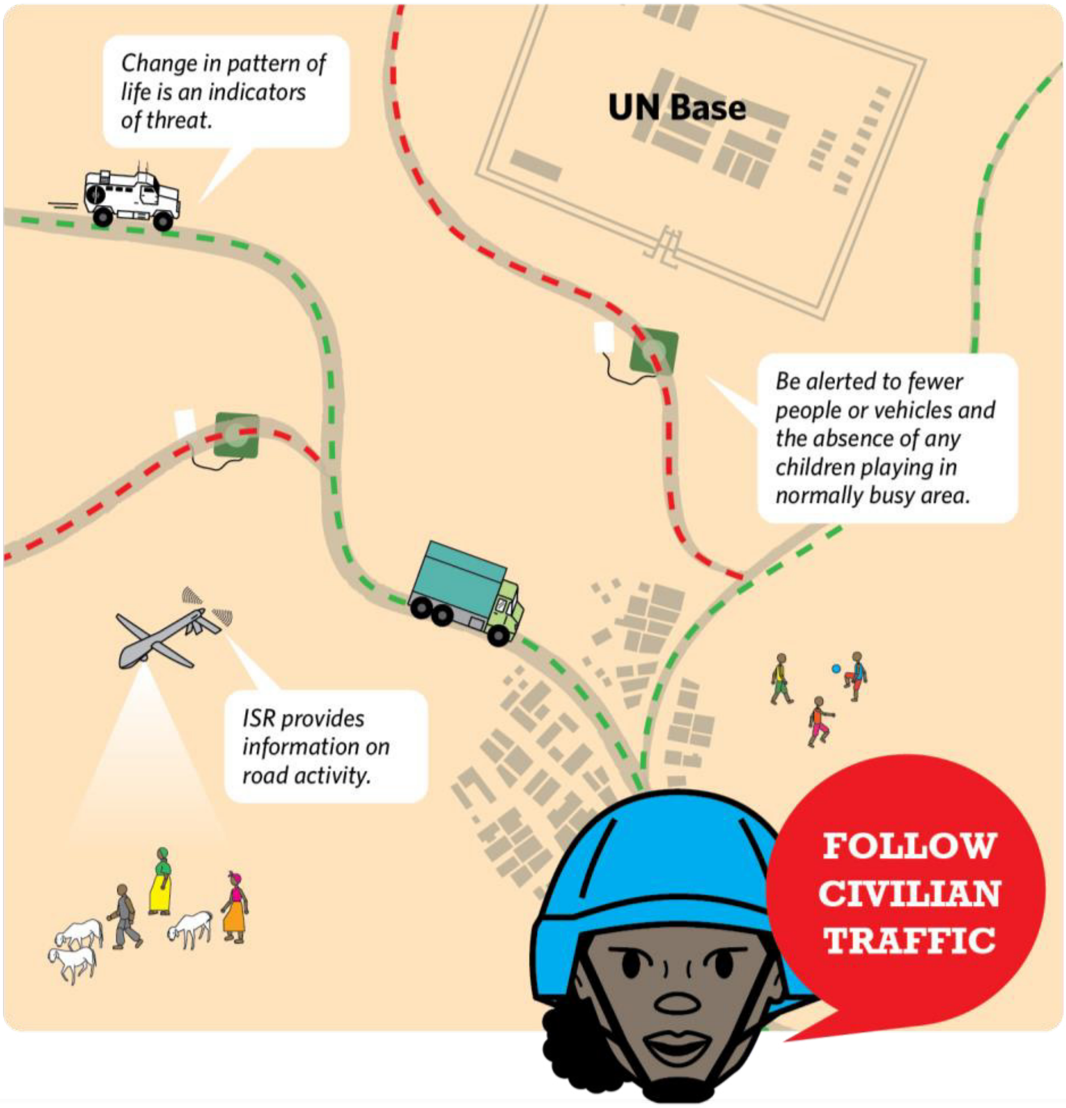
The Comprehensive Planning and Assessment System (CPAS)[70] can be used to conduct trend analysis based on indicators established by the mission. Using CPAS methodology and platform and taking into consideration relevant data already collected by UNMAS, the force and other mission components, the mission can formulate indicators to be collected against IED patterns in the area of operation,

[70] The aim of CPAS is to support the collection of data to help missions to plan and assess performance and impact. CPAS assists missions to regularly revise and update operations to adjust strategies and activities in an evolving environment to increase overall effectiveness. Data to be collected are selected by the mission and for the mission. Currently, only mission personnel and the CPAS team in headquarters have access to the full set of data collected and the accompanying analysis generated by the missions. This is to ensure missions are able to frankly assess mandate implementation. The CPAS team in headquarters is tasked with assisting missions with this process and does not share the data discussed, again to support candid internal critique. In short, the CPAS process is mission-owned and led. See https://iseek.un.org/DPO/CPAS or https://peacekeeping.un.org/en/cpas.

disaggregated as needed (e.g. by perpetrator, victim, type of IED, exploded/detected/defused). Over time, this will allow planners to identify trends and patterns related to IED use within the mission area and the wider region. The data and its analysis can be used to inform IED threat assessments and the development of recommendations on how to mitigate the threat posed by IEDs.

Figure 5.6
Observing changes in civilian traffic patterns

A dedicated map can be realized, marking the routes used by civilians. The threat is higher on routes not used by civilians. During patrols, it is a permanent task to watch routes used by civilians. It is also possible to notice the particular points avoided by civil vehicles. In case of a remote-controlled IED threat, all this is less true. Perpetrators can select the target.


UN Base
Change in pattern of life is an indicators of threat.
Be alerted to fewer people or vehicles and the absence of any children playing in normally busy area.
ISR provides information on road activity.
FOLLOW CIVILIAN TRAFFIC

5.6. Vulnerability assessment

A vulnerability assessment enables planners to determine the susceptibility of personnel, assets or facilities to attack or degradation due to hazards.

In this context, the factors listed in section 2.3 (Protection of personnel and property) are decisive. A vulnerability assessment gives planners a clear indication of which components are exposed to a particular higher risk due to their vulnerability.

In addition to the physical factors, however, there are other aspects to consider. The sociocultural imprints of police, military and civilians vary widely. There are also differences in terms of geographic origin and, sometimes, historical events. A good knowledge of the different troops and contingents is therefore just as important as the purely factual parameters of protection classes of personal equipment, vehicles and infrastructure. Moreover, some units may be more vulnerable than others because of their exposure, mission or mentality, even though they may have better protective equipment. Planners shall therefore assess vulnerabilities to identify deficiencies and/or weaknesses that render their personnel, material, infrastructure or mission vulnerable to a range of known or possible threats or hazards.

5.7. Risk assessment

The threat of IEDs may not be the only threat peacekeepers face. There may be other types of threats that are far greater and more immediate. This can be informed by other relevant actors through their analysis and assessment, including, for example, a human rights due diligence policy risk assessment. To that extent, in terms of force protection, commanders must prioritize which threat is the highest to respond accordingly.

This process of prioritizing threats is facilitated, in accordance with the guidelines for force protection,[71] by a risk assessment that determines the following:

- The likelihood that a threat will occur; and
- The impact that the threat would have if it occurs.

The combination of these two factors enables commanders and staff to determine the risk associated with each identified threat, including IEDs.

The willingness to take a risk depends on a variety of factors: a key aspect is the attitude of the respective commander to assume the risk that peacekeepers might be killed or injured during an operation.

Another aspect is the implementation of the mandate and how far the credibility of the mission will be affected if appropriate measures are not implemented immediately or otherwise.

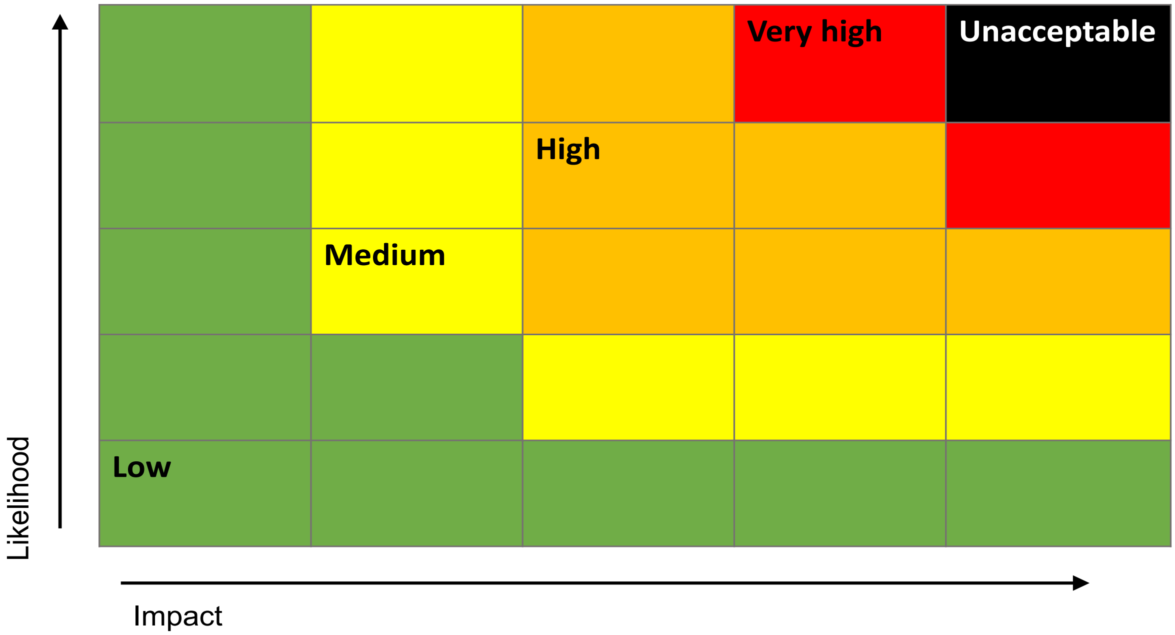
In this respect, each assessment has its own unique situation. The force's risk tolerance or threshold is determined by the Force Commander and/or unit commanders according to force capacity, unit capacity, operational plans or other agreements.

Risks posed by IED threats, for example, must be continually reassessed, as the situation may vary somewhat each time, to ensure that appropriate mitigation measures are always taken. Although it is not possible to protect every asset against every threat all the time, assets that are classified as "critical to the mission" should be protected as a priority. The goal is to reduce the likelihood of the risk and severity of the impact.

[71] Guidelines, Force Protection for Military Components of United Nations Peacekeeping Missions (2021.03).

Figure 5.7

Example of risk analysis matrix



The risk assessment should also be presented visually so that it can be analysed over time and shown on tables and maps.

Furthermore, it is recommended that the respective headquarters (force or sector) perform risk analysis with an appropriate table in matrix form, and each unit should coordinate with higher headquarters in preparing its risk assessment.

5.8. Assessment cycle

The assessment cycle, both of threat, vulnerability and risk, must be repeated continuously to ensure that the most recent events are always considered, and the mitigation measures represent the most appropriate response.

This may even be necessary during ongoing operation in the field if the commander determines that the original assessment no longer appropriately addresses all factors, and a dynamic re-assessment is required as the situation changes.

Based on the use of CPAS mentioned in section 5.5, after the trend/pattern analysis is completed, the mission/force IED analysts should be able to perform a data-based assessment regarding the IED threat. Moreover, by adding the data/information about the vulnerabilities and risks regarding IEDs, the analyst can better assess the IED threat and formulate recommendations for the mission leadership to better address the issue regarding risk management and actions to be taken. All data-based analyses and recommendations can also be shared and discussed with other mission components/sections during the CPAS impact assessment sessions to ensure a broader view of the IED threat.[72]

[72] Currently, training on CPAS is provided online for training the CPAS team in the missions. A broader CPAS training curriculum is currently under development for future implementation.

5.9. Monitoring for early warnings

An essential aspect that favours a good assessment is the so-called early warnings. These are indicators that need to be recognized, received and integrated at an early stage. Early warnings can be detected either by the troops themselves or communicated by the local population.

Not all early warnings are necessarily verbal communications. Very often, especially when the local population is also under surveillance and fear reprisals by the perpetrator if they collaborate with own forces, they can also be non-verbal or visual.

The signs of early warnings are very diverse and can range from the destruction of the ground (e.g. marks), which are detected early (e.g. by UAS), to unusual behaviour patterns (e.g. a person on the street on a usual market day) to direct messages. Indicators might be very weak or subtle.

These indicators must be monitored by all troops deployed in the area of operation through continuous exchange with the local authorities and population.

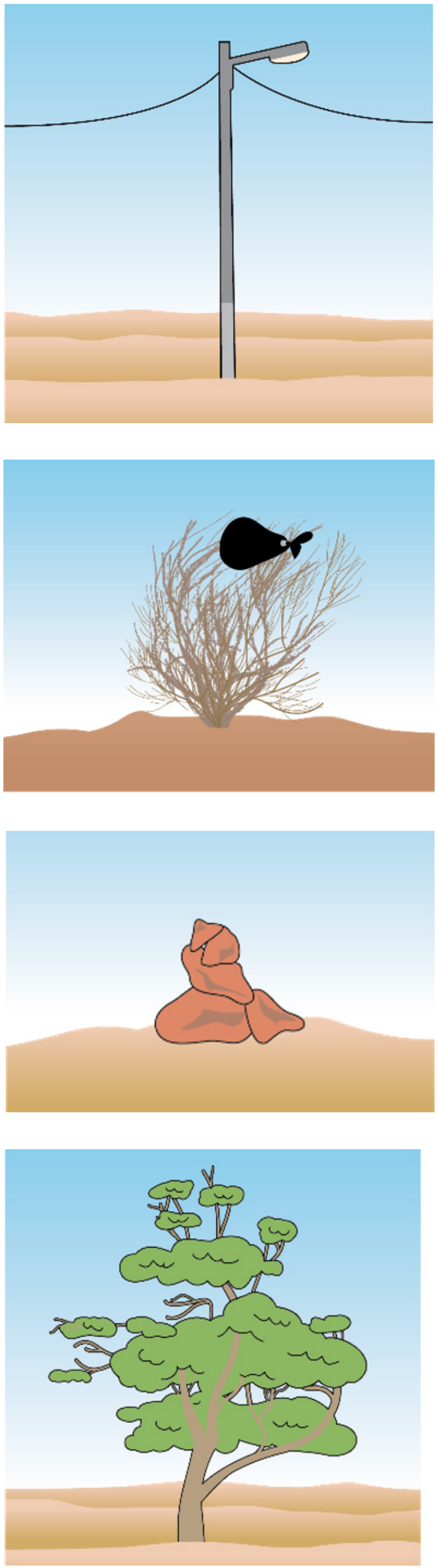
Since early warning depends heavily on the respective situation and differs from community-to-community, area-to-area, no prescriptive list is provided in this *Handbook*. This is to avoid missing out indicators that can be interpreted as early warning. In any case, early warnings should almost always initiate a dynamic and renewed assessment.

5.10. Key indicators or elements of information

Having numerous means of detection can increase the prospects of locating IEDs during the conduct of a mission. Significant information can be drawn from maintaining persistent awareness of the operating environment and contribute to peacekeeping-intelligence efforts. This often represents the best means of detection that can be achieved by any force member while in garrison, during a patrol or any other activity supporting the mission mandate, including interactions with the local population. Indicators could be signs, for example, on the ground, but they could also be the behaviour of persons or groups. The following indicators are examples:

- **Changes in patterns of life**. A sudden absence of playing children, people, normal traffic or other daily activity may indicate an impending IED attack.
- **Colour**. Look for contrasting colours, freshly disturbed earth or concrete that does not match the surrounding areas.
- **Discardable**. Discarded materiel unwittingly or unknowingly left on the scene by the perpetrator provide important clues such as exposed detonating cord, adhesive tape or other parts of the IED.
- **Aiming markers**. Markers are used to trigger the IED at the right time. Look for prominent objects that might be used as a marker and watch for indicators by the side of the road, such as tyres, rock piles, ribbon or tape that may identify an IED location or serve as an aiming reference.
- **Shapes.** Take note of object outlines and unknown devices that seem out of place for the environment that you are in.
- **Graffiti.** Be aware of symbols or writing on buildings and walls that might serve as a warning to locals (interpreters will usually be needed).
- **Signs.** Pay attention to newly erected placards and signs that seem out of place or might serve as warning to locals and messages to perpetrators.

Figure 5.8
Aiming markers



- **Aiming markers/clear line of sight.**
- **Unusual or suspicious individuals.** Repeated, prolonged presence of unknown individuals, personnel on overpasses or in a clearly marked restricted area, deliberate observation or picture taking, video recording (e.g. of ordinary activities, military movements, buildings, landmarks, friendly forces, security practices), map sketching or testing of security measures.
- **Suspicious behaviour.** The following may indicate the perpetrator intent to use IEDs:
  - Questions about security, force capabilities and strength, and so on.
  - Choreographed or timed movements of individual(s) or vehicles.
  - Unusual requests for public documents: blueprints, schedules, maps, routes and so on.
  - Theft or loss of uniforms, military equipment, identification cards, official vehicles, licence plates, explosives or IED associated components.
  - Obvious martial/combat type training occurring in secret. (Bombs are often only a component of an attack and have been used in combination with guns and other weapons and tactics.)
- **Unusual or suspicious vehicles**. Vehicles following or ahead of your convoy for a long distance and then pulling off to the side of the road. Cars parked on the side of the road with flashing lights are indications that something is wrong.
- Other visible IED indicators:
  - Wires laid out in plain sight.
  - Dead animals along the roadways.
  - Freshly dug holes or pavement patching on or along the road that may serve as possible IED emplacement sites.
  - Obstacles and craters in the roadway used to channel the convoy.
  - Signals with flare or city lights (switched off/on) as the convoy approaches.

5.11. Proactive and reactive mitigation measures against IEDs

Based on the findings of the threat assessment, the vulnerability assessment and associated risk assessment, taking into account the available options to protect personnel against a possible attack by an IED (see chap. 2), while making the best possible use of existing assets (see chap. 4), each mission must develop its own threat mitigation plan, define measures that are adapted to the situation on the ground, considering the geographical and climatic conditions that give peacekeepers the confidence to act. These considerations should include possible cooperate with the host nation defence and security forces to take preventive measures against IED networks, can include sharing of peacekeeping-intelligence and even conducting joint operations, if authorized by the mandate and mission leadership. Engagement at a regional level may require political engagement by the mission leadership and United Nations Headquarters, UNMAS, as well as other United Nations entities, funds and programmes (e.g. United Nations Office for Disarmament Affairs, United Nations Office on Drugs and Crime, United Nations Development Programme and United Nations Institute for Disarmament Research).

Peacekeepers must be trained to act according to the applicable situation while under very stressful conditions. Based on the experience of the last few years, several measures have proven successful and have, to a certain extent, become established as standard.

It is the Commander's decision to select the most appropriate mitigation measure depending on the situation. However, every individual is encouraged to contribute as concisely as possible to decisions on how to mitigate the threat.

A distinction is made between proactive and reactive measures:

- Proactive measures are always applied as a preventive measure if an IED threat can be assumed in principle.
- Reactive measures, on the other hand, are for the specific case that an IED has been found or a threat is imminent, and the further aim is to minimize the impact or to neutralize it as best as possible. It is important to balance proactive, reactive and mitigation measure based on an assessment of critical IED system vulnerabilities and an assessment of the military and police capability to degrade those vulnerabilities.

Depending on the time and the available resources, all mitigation measures can be increased or improved to continuously support further mitigation of the threat.

Furthermore, a distinction can be made between static and mobile measures. Static measures refer to situations where peacekeepers are stationary in one place. Mobile measures are for the situation where peacekeepers are moving around in space, for example in the context of a patrol.

Further distinction can be made between static and mobile mitigation measures. Being in a static position generally provides more protection because of the length of the stay, even if it is a temporary operating base or a night position. It is plannable and hence enhanced mitigation measures can be established, whereas mobile units are more exposed to the IED threat and usually expose the protection of their vehicles or personal protective equipment.

The mobile IED threat mitigation (e.g. on patrol outside a United Nations installation) differs from what is feasible within a static position. However, certain measures are always to be applied, regardless of the situation:

- **Be informed** of the EO situation in the theatre of operations.
- **Observe** your surroundings and watch for anything out of the ordinary, such as:
  - Behaviour of the civilian population.
  - Changes made on or at nearby roads, for example, and report your observations!
- Apply the correct **dress and vehicle code.**
- **Warn**

  Warn own forces in the vicinity.

- **Confirm**

  Potential IED finds should be confirmed by search teams/EOD teams.

  Observe them from a distance (using binoculars/optical sights) and from a safe cover. Safety comes prior to confirmation. Compare the suspected object with the EO/IED recognition guide or other EO/IED identification tools.

- **Awareness**

  Beware of ground signs, indicators (e.g. stretched wires or tripwires) and other EO. Keep in mind the IED threat. Do not touch any wires, cables or other parts that appear to be non-hazardous, which could be an element of the IED. Be aware of secondary devices.

- **Chemical, biological, radiological and nuclear threats**

  Give out an immediate chemical, biological, radiological and nuclear threat warning if you observe any leakage of liquids or discharge of vapours.

- **Mark**

  Mark the location of the find at an appropriate distance from the IED.

- **Cordon**

  Cordon off the affected area as required (minimum recommended distance is 300 metres around the suspected IED), stay outside the cordoned area and ensure that nobody enters the area. For suspected IEDs, only EOD personnel shall approach.

- **Report**

  Send an EO/IED incident report (as per orders received from your superior officers). State as well as possible precise coordinates of the EO location and take a picture of the EO.

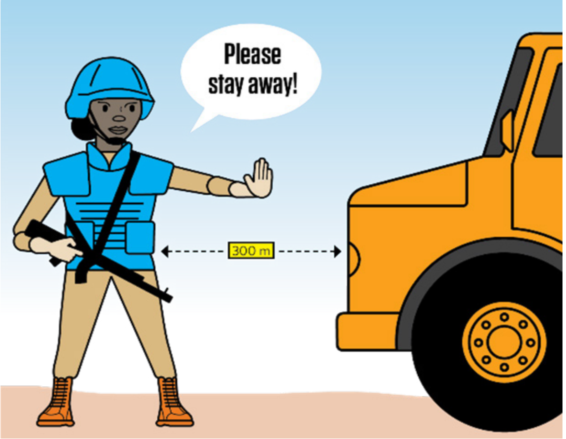
- Do not take unnecessary risks.

Possible mitigation measures are listed in the following section. The list is separated by proactive and reactive measures, both static and mobile. The list is not exhaustive and the examples must be adjusted according to the situation and the threat.

5.11.1. Mitigation measures (static)

Proactive mitigation measures (static)

If peacekeepers are deployed, for example, at an installation or temporary operating space, they can apply the following measures to increase security:



- Post crew-served weapons at all avenues of approach to gates.
- Remain behind protective cover when vehicles approach.
- Ensure that access and entry points are at a safe distance from buildings, roads and so on (at least 300 metres away).
- Post warning signs at the entrance of camps, checkpoints and so on so drivers know where to stop.
- Stop vehicles before reaching the access point to prevent an installation to be overrun.
- Physically control all vehicles with defensive barriers and chicanes that force them to reduce speed.
- Install emergency gates that rise and lower.

In case of a vehicle-borne IED:

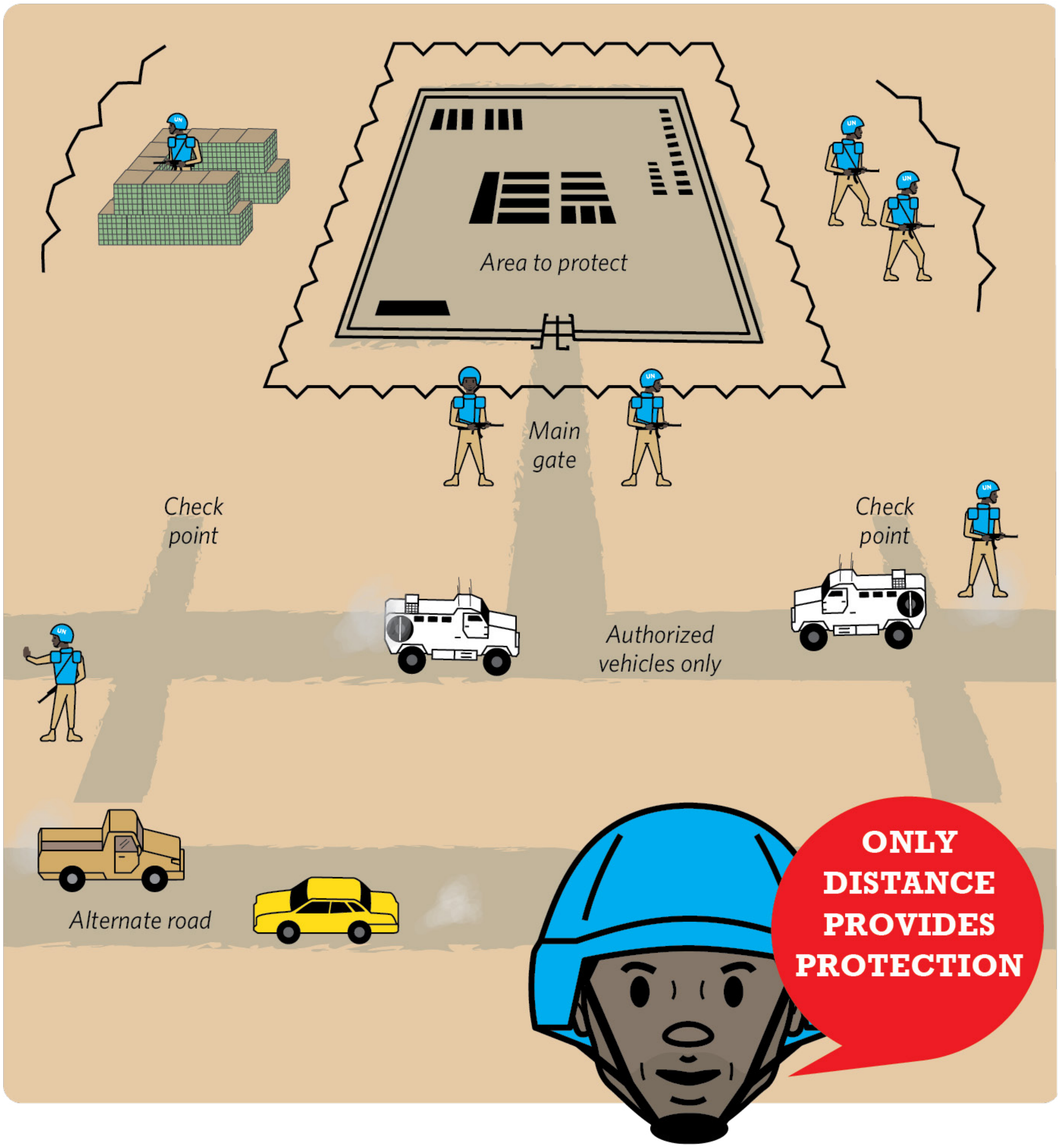
- Vehicle control: use escalation of force.
- Shoot vehicle tyres or engine to slow it down.
- If that does not work, shoot the driver to disable him/her from continuing to conduct the vehicle.

Reactive mitigation measures (static)

In case of an IED find or attack, the peacekeepers are to react in the best possible manner to gain control of the situation and to avoid secondary attacks:

- Enforce all guards.
- Observe surroundings for possible exploitation.
- Close all access points to the camp and so on.
- Watch out for secondary IEDs.
- Inform all personnel, including those currently on patrol outside of the camp.

Figure 5.9
Proactive mitigation measures (static)



It is only by being at a standoff distance that one is protected against a blast. A bastion wall provides security only against direct fire. It is critical to have a base entry that provides standoff for any kind of attack. The main threat is a suicide vehicle-borne IED.

Figure 5.10
Proactive mitigation measures against a suicide vehicle-borne IED (SVBIED)

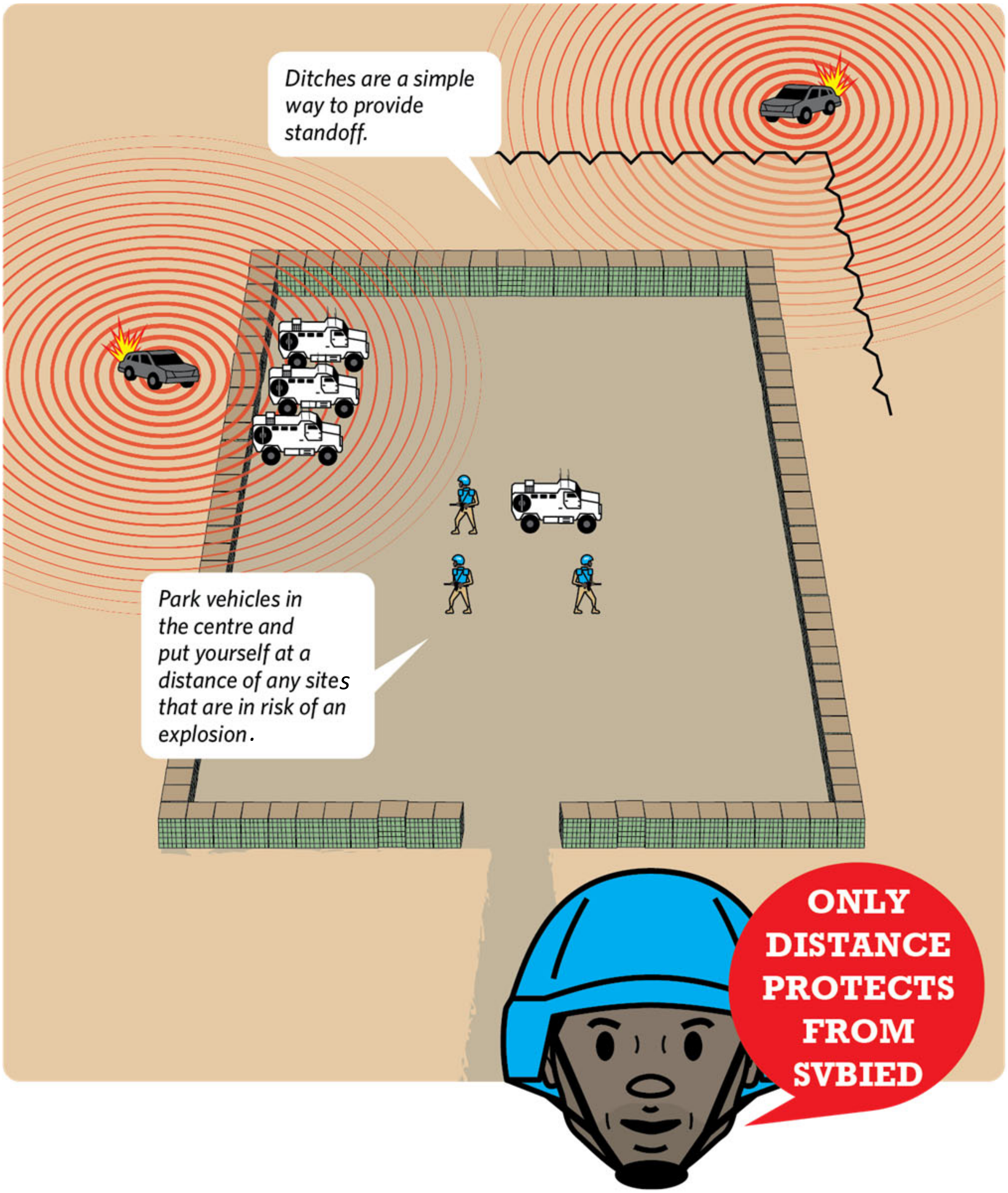
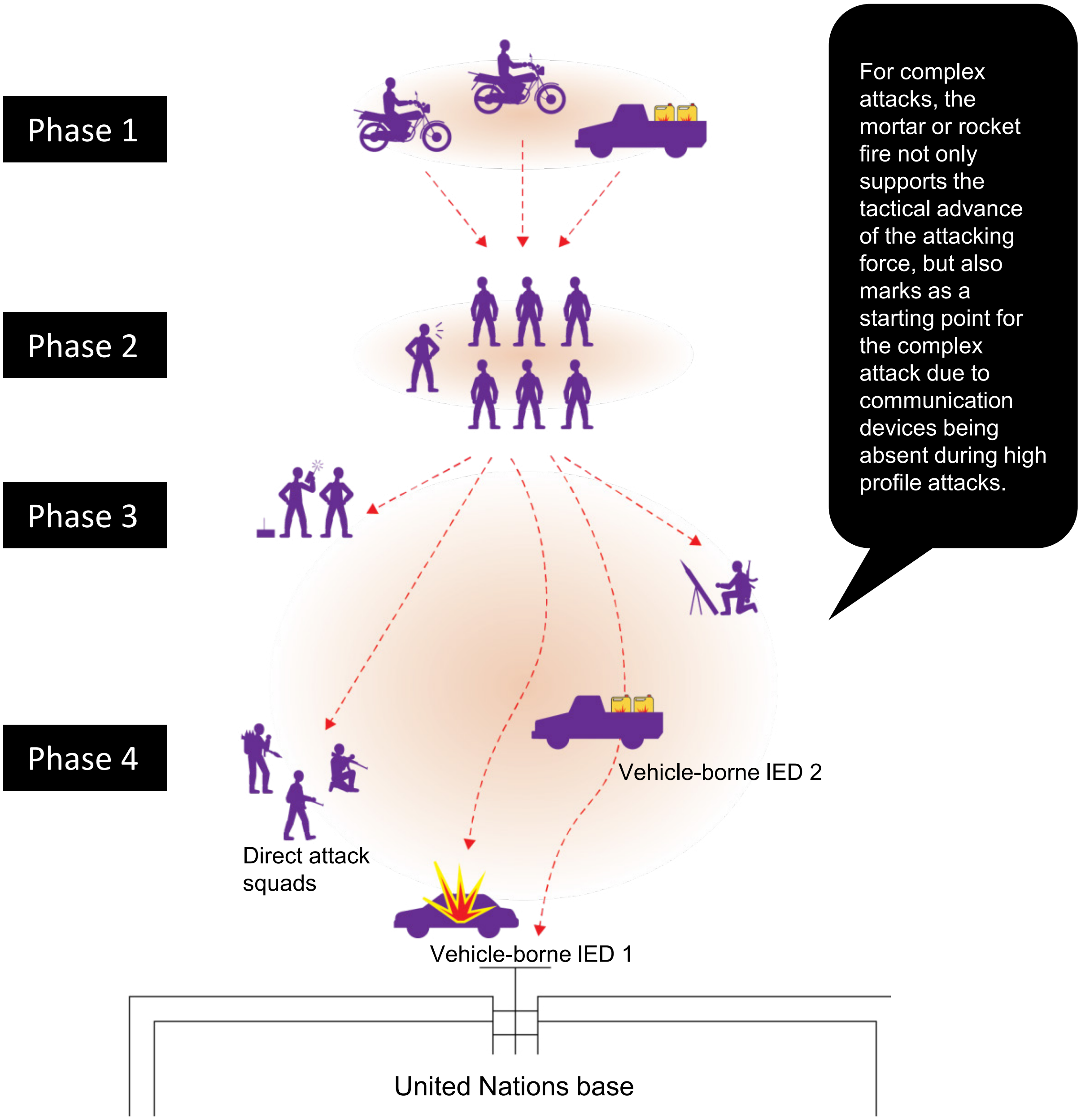

Ditches are a simple way to provide standoff.
Park vehicles in the centre and put yourself at a distance of any sites that are in risk of an explosion.
ONLY DISTANCE PROTECTS FROM SVBIED

Figure 5.11
Complex attack on bases



For complex attacks, the mortar or rocket fire not only supports the tactical advance of the attacking force, but also marks as a starting point for the complex attack due to communication devices being absent during high profile attacks.

5.11.2. Mitigation measures (mobile)

Proactive mitigation measures (mobile)

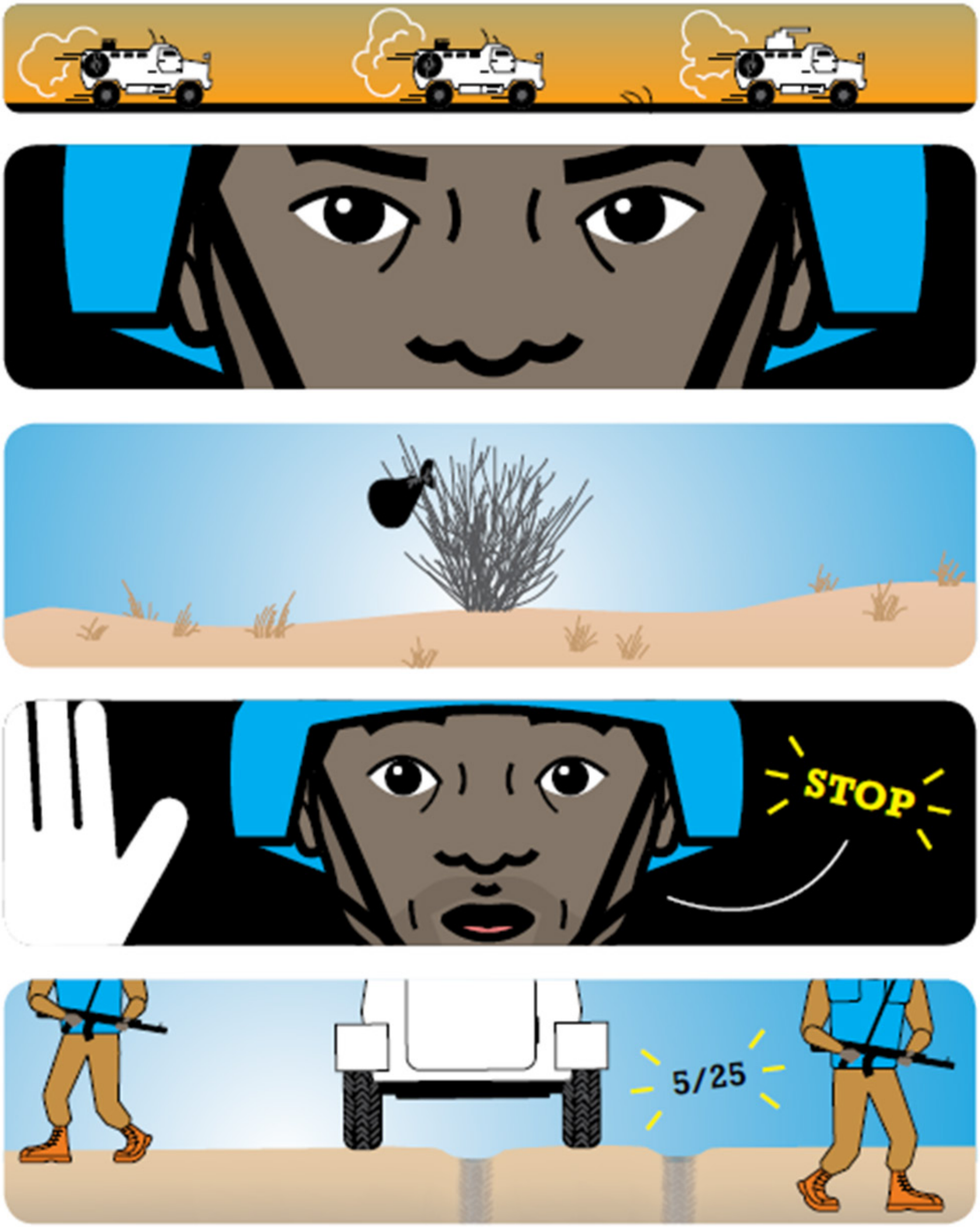
If on patrol or outside of any installation, visual detection becomes the most important detection method to mitigate the threat of IEDs. Therefore, everybody must be alert to signs on the ground which indicate a possible threat (ground sign awareness):

- Establish good communications.
- Do not follow the track in front of you.
- Avoid tops and bottoms of hills; use military crest.
- Conduct visual search under vehicle.
- Conduct 5/25-metre search at each halt before dismount (5-metre check during a short halt) or 5/25-metre check during a longer halt (more than 10 minutes). Use optics to conduct visual checks out to 100 metres.
- Stay within ECM (jammer) range. Know the limitations of your ECM to avoid ECM fratricide.
- Sanitize routes and assembly areas to deny friendly route indicators.

Figure 5.12
Scheme ground sign awareness

Regularity	Straight lines and geometric shapes do not appear in nature. They are often indicators of human interaction with the environment.
Flattening	This is a general levelling or flattening of an area compared with surroundings.
Transfer	Movement of materials from one type of environment to another.
Colour change	Difference in colour or texture from the area that surrounds it.
Disturbance	Any change or rearrangement from the natural state.
Discardables	Perpetrators may intentionally or unintentionally leave behind at the emplacement site of an IED.

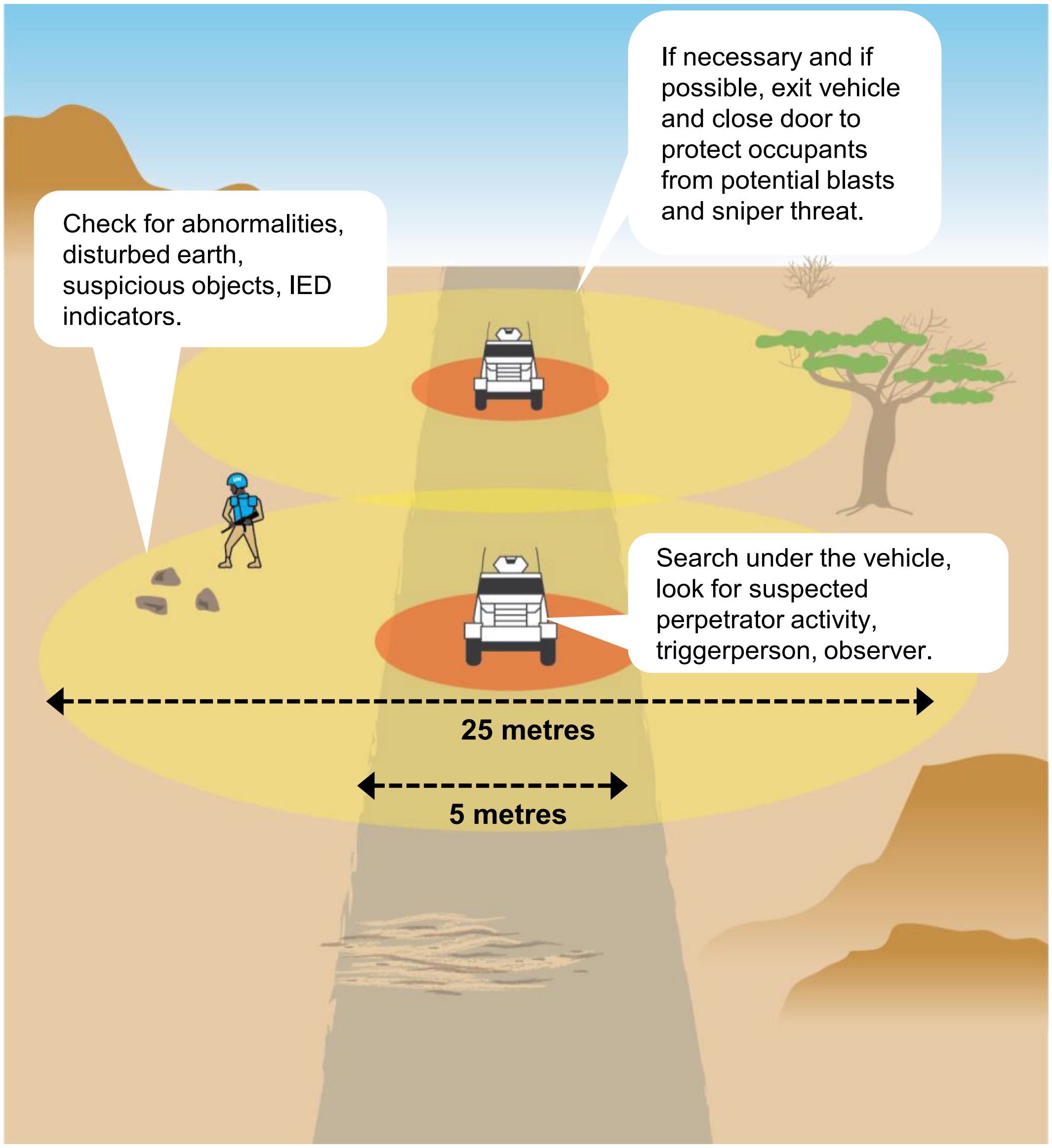
Figure 5.13
Scheme 5/25 check (1)



If you approach an avenue of approach, where traffic is canalized or a vulnerable point, where an IED attack can easily be executed (e.g. bridge, culvert, hill, valley) a dismounted search should be conducted. The following procedures should be applied in that situation:

- Do not walk down the road.
- Search vulnerable areas and vulnerable points.
- Use counter-snipers, if available.
- Control traffic and have ability to allow civilian vehicles to pass, if needed.

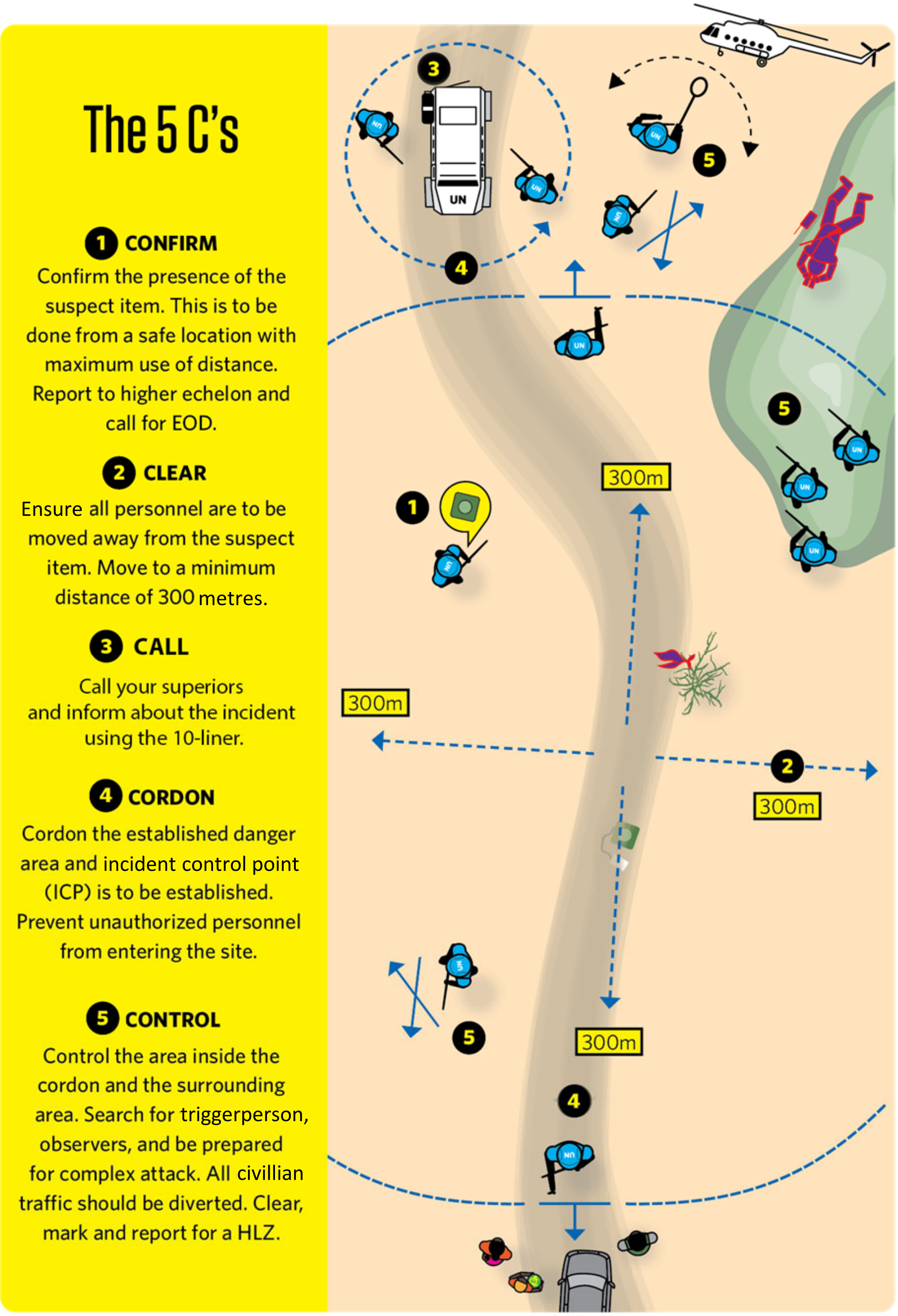
Figure 5.14
Scheme 5/25 check (2)


If necessary and if possible, exit vehicle and close door to protect occupants from potential blasts and sniper threat.
Check for abnormalities, disturbed earth, suspicious objects, IED indicators.
Search under the vehicle, look for suspected perpetrator activity, triggerperson, observer.
25 metres
5 metres

If a convoy or a patrol stops during movement, a 5- and 25-metre check to clear the area around the vehicle is mandatory. Scan outwards continuously at all times. Driver and gunner should remain inside the vehicle for security purposes.

If you approach a site, were you suspect an IED, conduct first the 5/25 check, followed by the five Cs: confirm, clear, call, cordon and control.

Figure 5.15
The five Cs



The 5 C's

1 CONFIRM
Confirm the presence of the suspect item. This is to be done from a safe location with maximum use of distance. Report to higher echelon and call for EOD.

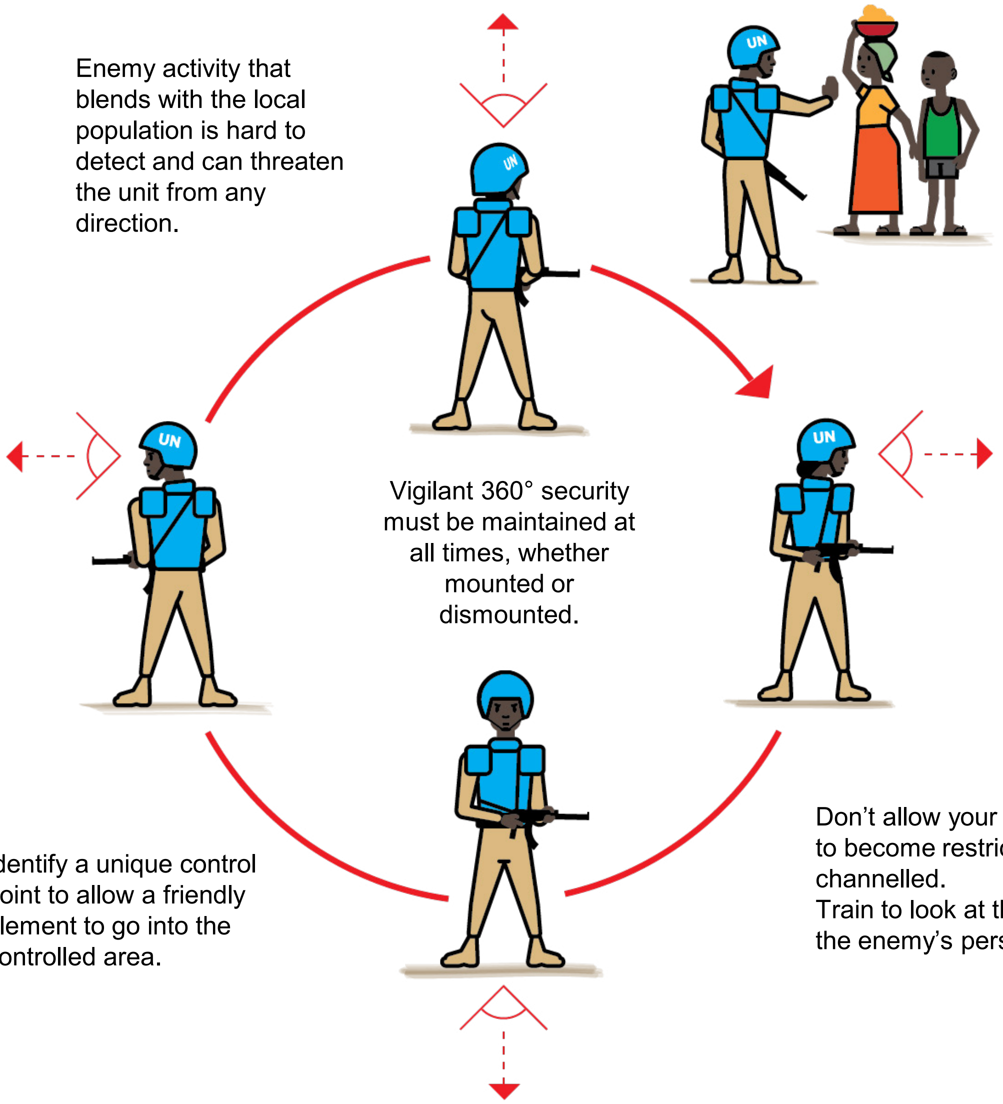
2 CLEAR
Ensure all personnel are to be moved away from the suspect item. Move to a minimum distance of 300 metres.

3 CALL
Call your superiors and inform about the incident using the 10-liner.

4 CORDON
Cordon the established danger area and incident control point (ICP) is to be established. Prevent unauthorized personnel from entering the site.

5 CONTROL
Control the area inside the cordon and the surrounding area. Search for triggerperson, observers, and be prepared for complex attack. All civillian traffic should be diverted. Clear, mark and report for a HLZ.

Figure 5.16
360 degrees of security



Enemy activity that blends with the local population is hard to detect and can threaten the unit from any direction.

Vigilant 360° security must be maintained at all times, whether mounted or dismounted.

Identify a unique control point to allow a friendly element to go into the controlled area.

Don’t allow your focus to become restricted or channelled.
Train to look at the terrain from the enemy’s perspective.

If not searching, be aware of signs indicating an IED ahead on the track. Drive unpredictably in desert or bush and try to use alternative tracks if they are not too obvious. Be aware of spotters, screeners and triggers. If searching is not an option, avoid the IED threat:

- Bypass unpredictably in the bush, vulnerable points or vulnerable areas.
- Mitigate perpetrators’ TTPs.

Figure 5.17

Bypass if not searching

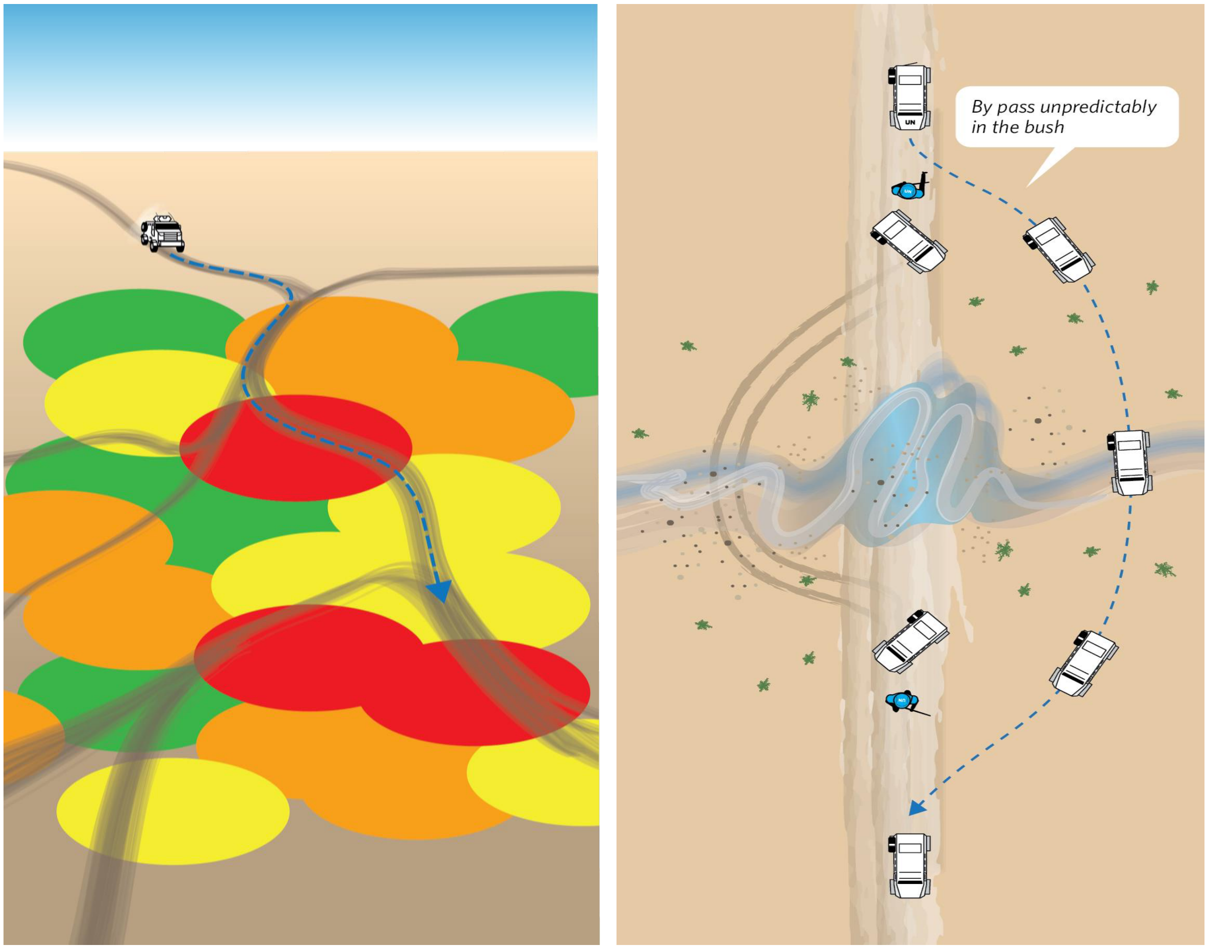
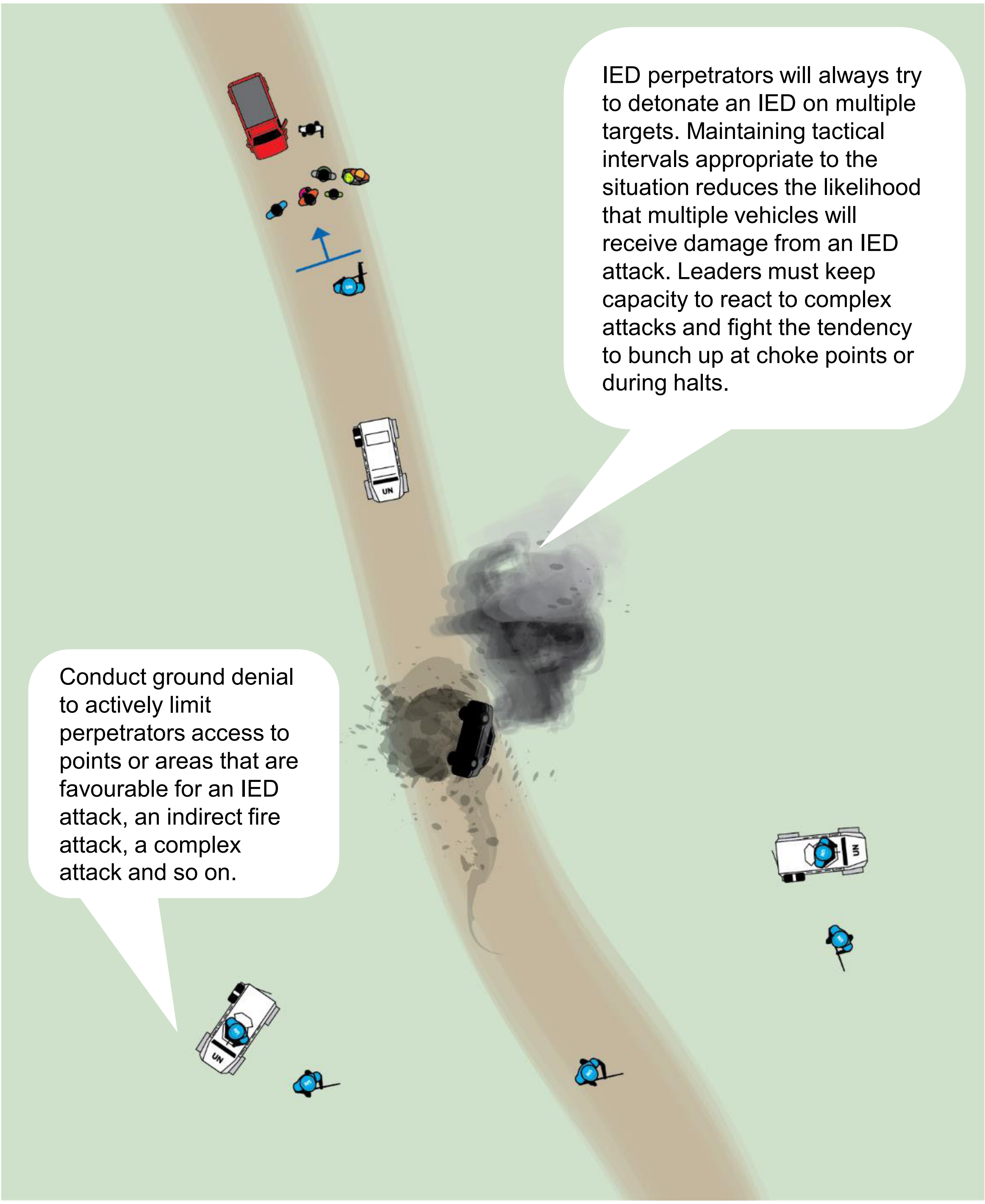
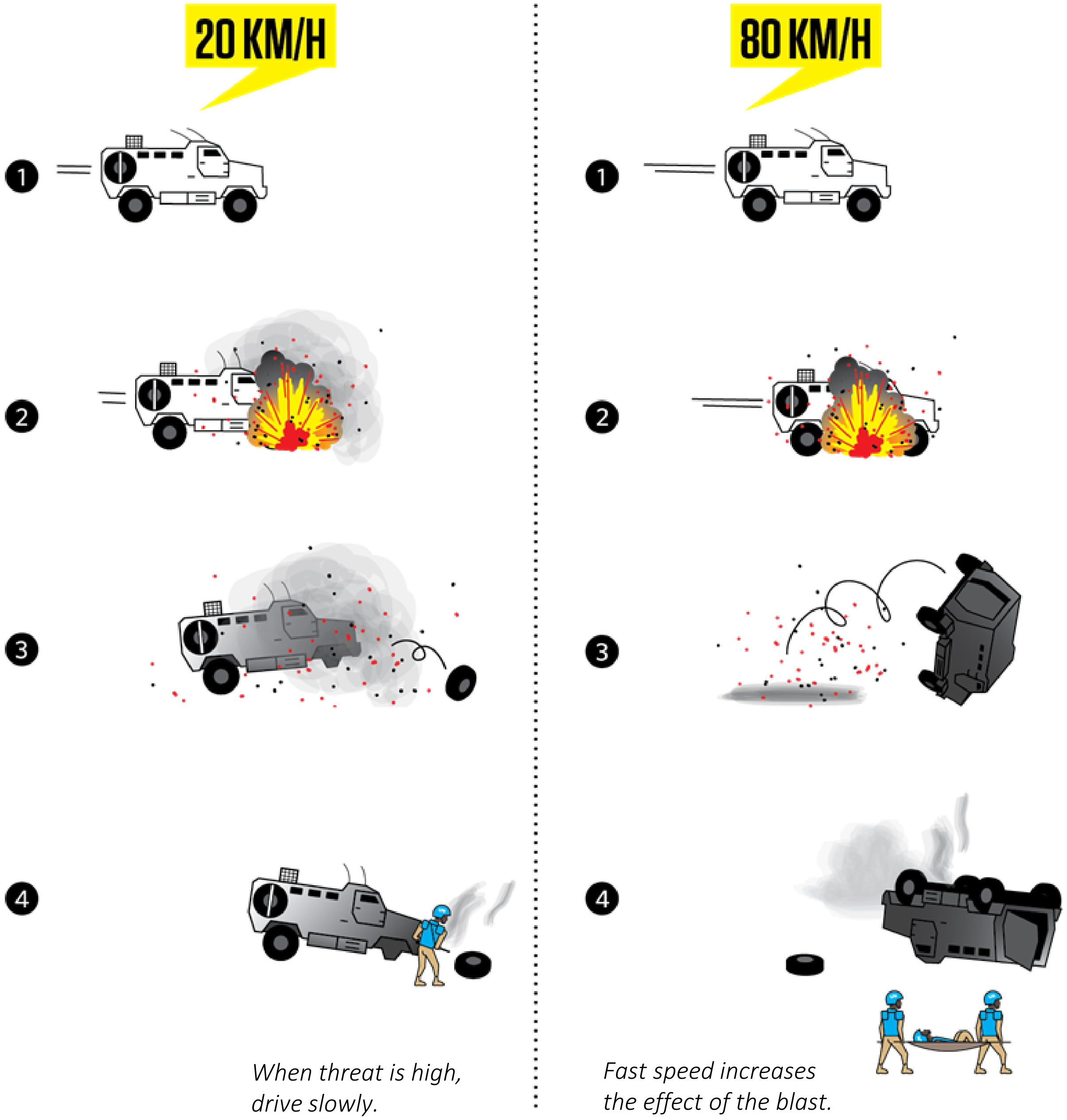


Figure 5.18
Maintain tactical dispersion


IED perpetrators will always try to detonate an IED on multiple targets. Maintaining tactical intervals appropriate to the situation reduces the likelihood that multiple vehicles will receive damage from an IED attack. Leaders must keep capacity to react to complex attacks and fight the tendency to bunch up at choke points or during halts.
Conduct ground denial to actively limit perpetrators access to points or areas that are favourable for an IED attack, an indirect fire attack, a complex attack and so on.
UN
UN
UN
UN

Conduct your patrol at an appropriate speed, which allows you to observe the environment and spot potential threats but minimizes the impact in case of an IED incident.

Figure 5.19
Speed kills



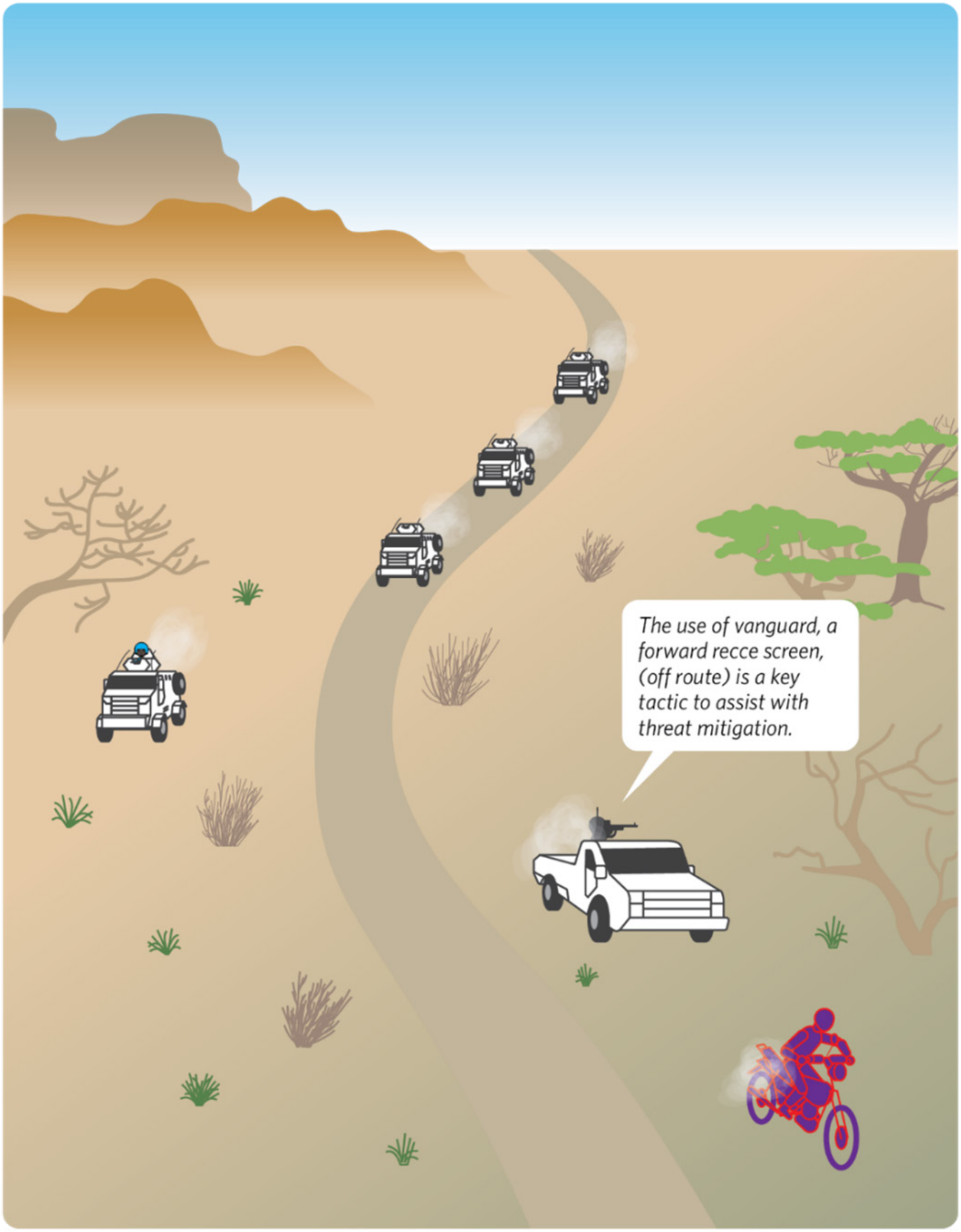
When threat is high, drive slowly.

Fast speed increases the effect of the blast.

If the required assets are available, consider employing an independent vanguard/reconnaissance element as a spearhead unit to identify possible threat ahead of the deployment of the main convoy/ patrol to conduct the following tasks:

- Detect and engage IED triggerpersons, camera operators and lookouts.
- Conduct tactical questioning, search and initial processing of detainees.
- Employ travelling overwatch when contact is likely.
- Lag behind or double-back behind convoy to catch IED reseeding elements.

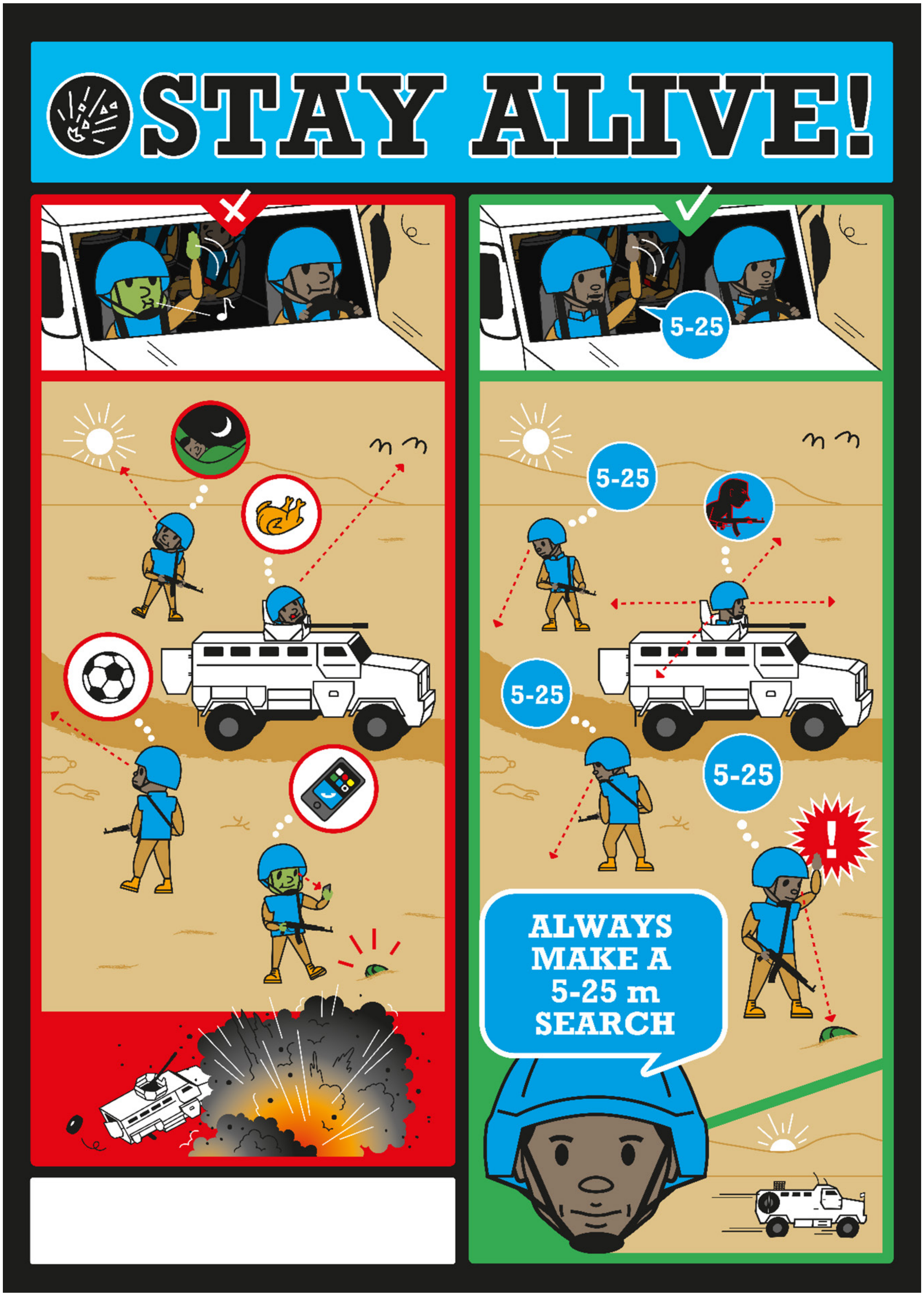
Figure 5.20
Vanguard


The use of vanguard, a forward recce screen, (off route) is a key tactic to assist with threat mitigation.

Returning to base and applying the "honesty trace", reporting truthfully where you have been and what you did, what you searched and what you did not, to support building a realistic threat picture.

Figure 5.21

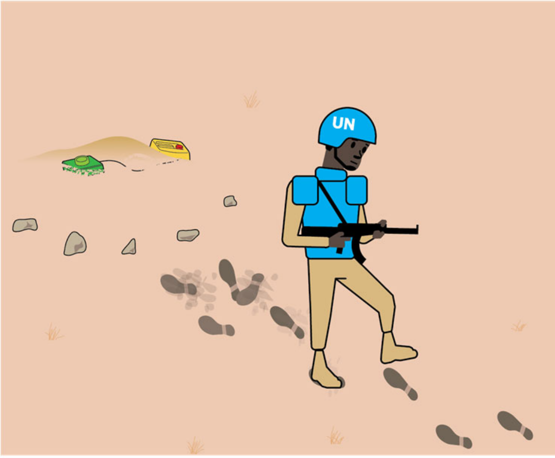
Sample poster for United Nations peacekeeping missions (3)



Reactive mitigation measures (mobile)

Overall safety at IEDD tasks is ensured by the creation of a cordon where personnel, under the oversight of an incident commander or clearance site manager, are positioned at appropriate intervals around the IED to ensure that no persons can inadvertently stray into the danger area. The cordon should remain in place until the IEDD task is completed, all components have been recorded and/or recovered and declared safe by the IEDD team leader. Cordon personnel should be aware that they are sometimes vulnerable to attacks by perpetrators with direct and indirect fire weapons, as well as by suicide IEDs. All cordon personnel should therefore maintain continuous situational awareness. All cordon and evacuation distances need to be based on the tactical situation and the decision of the IEDD operator, grounded on thorough risk assessment.

Figure 5.22
Retrace footsteps



Mark your step path, step into the footprints of the person walking in front of you and keep a minimum distance of 25 metres between each other.

In addition to the above-mentioned proactive measure to stay on paved or well-travelled roads or tracks when operating in areas with an IED threat, the following measures should be applied, when mobile:

- Communicate distance, direction and description of IED.
- When finding IED, inform fellow peacekeepers immediately with an appropriate warning (remember that you might be observed and a loud “HALT!” might alert the triggerperson of your possible find), remain in position and decide according to the situation whether it is safer to continue in the direction you were heading or to return, avoiding the area of the possible find.
- Establish 360-degree security.
- Conduct 5/25-metre search.
- Look for tripwires, unusual objects and anything else that seems out of the ordinary.
- Return fire to perpetrator as needed/counterattack.
- Conduct the five Cs.
- Try to bring some distance between you and the IED.
- Exit through the rear or the roof of the vehicle.
- Be careful when you turn around and try to step in your own footprints or step only in the tracks left by your vehicle as you walk back out. If no footprints are visible, create a marked step path for your own safety.
- Employ tactical casualty care (initiate CASEVAC call) and evacuate casualties.
- If necessary, move to a rally point, consolidate and reorganize.
- If possible, clearly mark the area.
- Record the find location on the map.
- Send the EO/IED incident report.
- Continue mission, if able.

The two most likely ways you will discover that you are in an area with emplaced IEDs are either that there is an explosion or that you see ground signs. If someone has been injured, you should not rush in to help, as you will endanger yourself and others around you. Stay calm and follow these rules.[73]

Figure 5.23
Emergency procedures on foot

M	Movement stops immediately. Stop! Remain still and do not move your feet.
I	Inform and warn the people around you. Call for help but keep others away.
N	Note the area. What else can you see: mines, tripwires, mine signs, for example. Visually locate the nearest safe area, the last place you knew you were on a safe surface, such as a paved road, well-used path, concrete or steel structure.
D	Do not move, if there is no indication of a safe area or you cannot reach it without stepping on unknown ground. Wait for help to arrive.

If you have any reason to believe that you have driven into an area with IEDs (or a mined area) such as another vehicle detonating an IED (or a mine), by seeing a mine or ground signs (mine signs) or if your vehicle has hit an IED (landmine), the following steps should be observed:

Figure 5.24
Emergency procedures in a vehicle

A	Attempt to reverse out of the area and do not move the steering wheel. Be calm and, if possible, stay in the vehicle.
I	Inform and warn people around you. Call for help but keep others away. Use the car horn to summon help.
N	Note the area. What else can you see: mines, tripwires or signs of mines? Visually locate the nearest safe area, the last place you knew you were on a safe surface, such as a paved road or well-used path.
E	Evaluate your course of action. Be prepared to take control.
D	Do not move if there is no indication of a safe area or you cannot reach it without stepping on unknown ground. Wait for help to arrive.

When a vehicle strikes an IED, mine or ERW, the first instinct of survivors may be to rush out of the vehicle. However, unless the vehicle is on fire or has ended up in a life-threatening position, stay in the vehicle. It is very likely that there will be more IEDs, mines, including anti-personnel mines or other

[73] These rules can equally be applied if you are in a mined area. You might then see either mines or signs of mines.

ERW in the area. If you can, give first aid assistance to other passengers in the vehicle who require it. Stay calm.

Marking of a find location

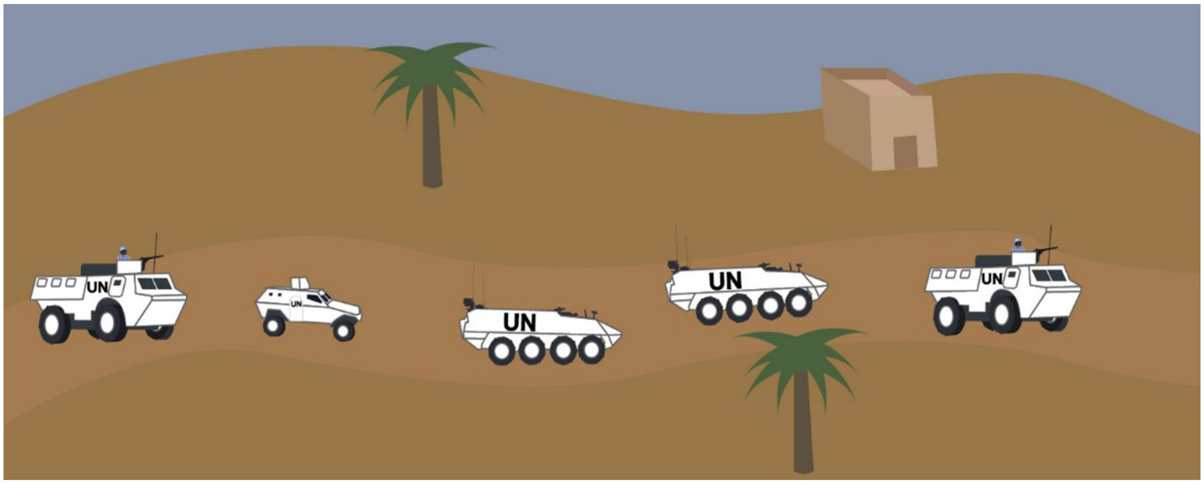
- Use something as a marker that will easily catch the eye (preferably the colour spray from the marking kit).
- When choosing your marking materials, keep in mind that their durability may be considerably affected by rain, snow, wind or sunshine, as well as by exposure to cold and hot temperatures.
- Also, when choosing your marking materials, keep in mind that they may be of use to the local population, such as tin cans, bottles or even pieces of wood.
- If no other materials or no other objects are available, render the objects you intend to use less useful to the population, for example by punching holes in tin cans or by cutting away the bottom ends of plastic bottles. Rather than using pieces of wood (e.g. crossed twigs, roof battens) you should use stones that can be arranged in a way that easily catches the eye and/or that you can paint with colour.
- Be sure to fix the markings in a way that makes them last, because environmental conditions may cause them to deteriorate more quickly.
- If you have to drive sticks or similar objects into the ground for marking purposes, keep in mind that this causes vibrations, which may propagate to the EO, so be sure to put the sticks at a somewhat greater distance from the ordnance.

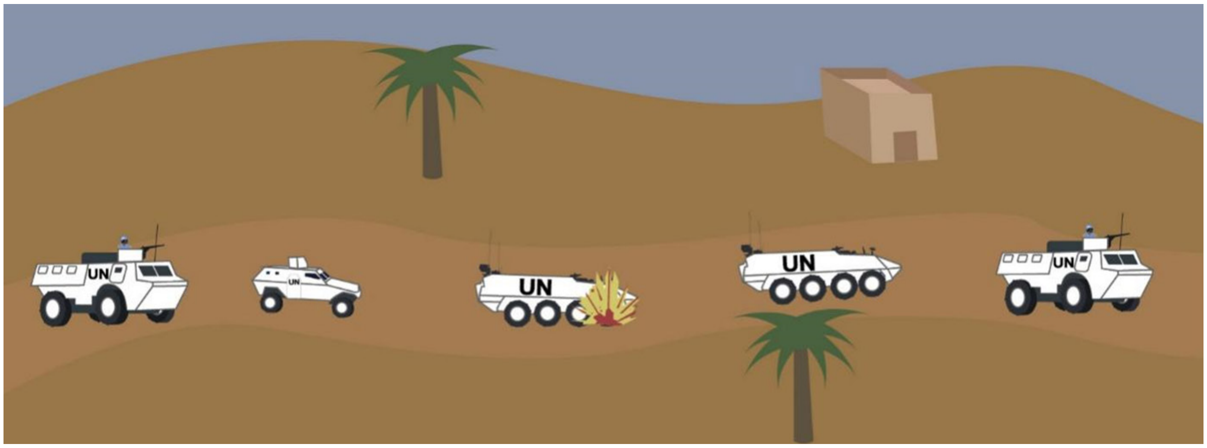
NOTE: Stay around the IED for as little time as possible, because it may have a self-activating feature.

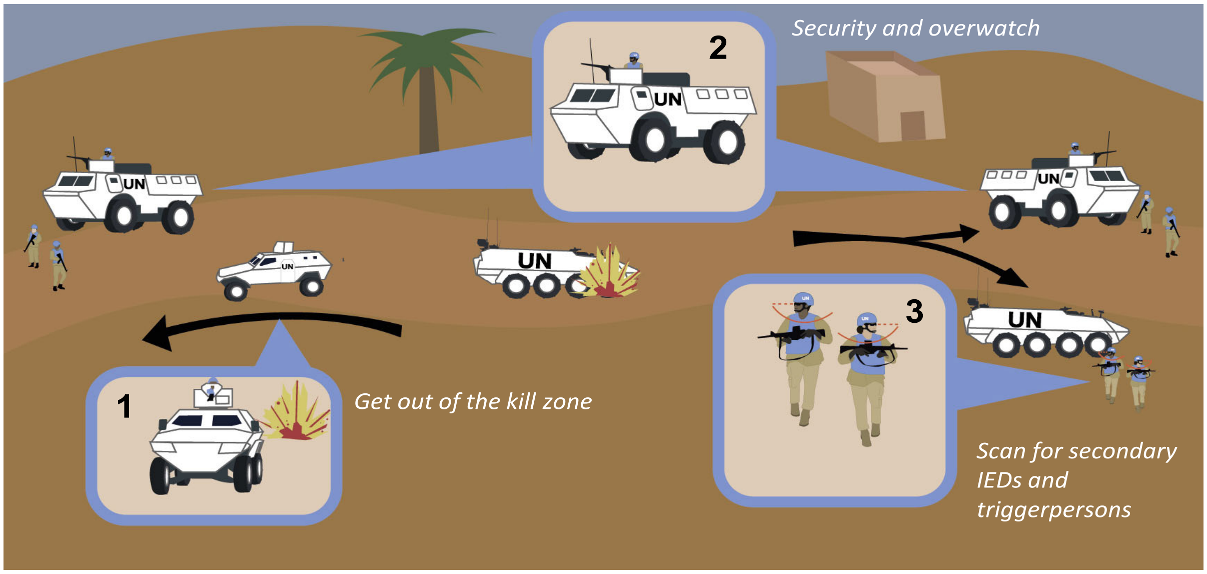
5.11.3. Actions on an IED strike

Figure 5.25 shows examples of possible actions to be taken in the event of an IED strike. The final decision is made by the commander on the ground, taking into account the situation as it presents itself, the mission and the threat.

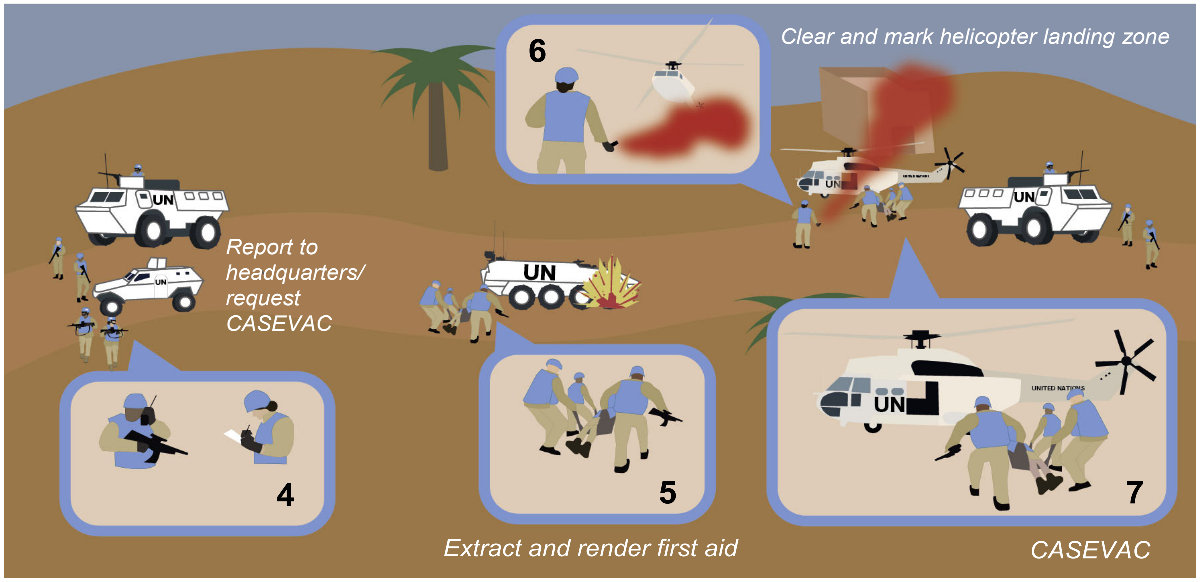
Figure 5.25
Procedures in case of an IED attack (example)







Maximize concurrent activity


6
Clear and mark helicopter landing zone
Report to headquarters/ request CASEVAC
4
5
Extract and render first aid
7
CASEVAC

Maximize concurrent activity

Exit area and continue with mission

5.12. Route search and route clearance

Route search refers to a mobility unit-level, all arms search capability used to check assessed vulnerable points and vulnerable areas along a route of travel for the presence or absence of IEDs. It involves knowledge and skills to assess a vulnerable points and vulnerable areas and determine how best they should be secured and searched to locate and isolate suspected IEDs so they can be identified, marked, confirmed and rendered safe by EOD/IEDD operators or other suitably qualified personnel.

As an example, a logistics convoy moving along a route will use their organic all arms search team to secure and check vulnerable points and vulnerable areas identified in their mission planning for threats. If a suspected IED is found, the convoy would cordon the area and call for EOD support to confirm and dispose of the IED.

In comparison, a **route clearance** refers to a deliberate operation by a dedicated, task organized unit to identify and dispose of IED threats along a specified route to provide freedom of movement to friendly forces and the civilian population. Route clearance searches the entire route with a detailed search of high-risk areas. This operation requires specialized detection, interrogation and proofing equipment to identify and remove IEDs. It may also include engineer construction equipment to eliminate places to conceal IEDs (e.g. potholes, culverts) or reduce cover and concealment along the sides of the route.

Examples of the use of such assets may be to:

- Clear the vegetation and scrub around junctions which are assessed vulnerable points.
- Improve and secure culverts to prevent their use as IED emplacement locations.
- Use such assets to improve the road surface to hinder IED emplacement along it.
- Improve mobility and enhance freedom of movement.

Route clearance is a capability that is usually provided by military engineers only.

Additional force protection elements may also be included to provide overwatch or secure vulnerable areas and vulnerable points to prevent the replacement of cleared IEDs until after a critical convoy has passed.

A **route clearance package** is a combination of protection assets, search and EOD capabilities which are threat aligned and within available resources to clear a defined route to a determined standard.

It is the task organization within the mission of dedicated route clearance assets and associated teams to assist with route management in an explosive threat environment. Such dedicated units within an all-arms grouping can, if large enough, be a stand-alone mission asset or alternatively can be a platoon or larger element within a United Nations engineer unit. A route clearance package can be equipped with a mix of general and specialist vehicles, equipment and personnel integrated to conduct route clearance. Their purpose is to eliminate concealment for IEDs, munitions and caches, as well as providing systematic detection and deterrence sweeps along cleared routes. A route clearance package can be used in general support to maintain main supply routes and in close support providing support to United Nations units on tactical road movements.

As an example: A task organized route clearance package consisting of engineers, EOD and security is tasked to clear a route ahead of a high-value convoy. They search the entire route, identifying, interrogating and disposing of any explosive hazards using their internal EOD assets.

Search capabilities (intermediate and specialized) can contribute to route clearance operations by means of area and route search procedures.

A **temporary composite route clearance packages** is an asset for an operation to establish a cleared route assembling the required assets at the start of a mission or when an IED threat emerges and then standing it down when their assigned task(s) is completed. This would typically involve the forming of a composite unit or route clearance package normally around combat engineering assets. This can be a very efficient use of resources and personnel. However, once stood down it is possible that continual route maintenance will be required to keep the routes in a state that mitigates the threat of IEDs and repair damages caused through the continued use of IEDs along them.

5.13. Routines

It must be assumed that perpetrators are continuously observing United Nations peacekeepers to assess and understand their TTPs and patterns, for example which procedures are applied to find an IED, but also what recurring routines are used in general.

Therefore, it is necessary to continuously assess those patterns to avoid making them a routine. It will be impossible to avoid all routines and patterns, and as such all effort must be made to observe and then mitigate such patterns of route, time and action.

For instance, using different entry and exit gates on camp, patrolling on different days of the week and at different times of the day and night, changing the order of the vehicles in a patrol, to name just a few, are good examples of changing routine to allow the perpetrator not to be assured what peacekeepers are doing. In a larger approach it should be considered, for example, if there are other patrol routes, supply routes, whether the supply of outposts must always be done by land or whether it is possible to organize certain procedures by air, possibly with a parachute drop. Long-term measures, for example, ensuring that outposts need fewer resupplies or are more self-sustaining through solar panels and reduced energy consumption, would help to prevent establishing necessary routines for resupply. The IED threat mitigation working group should provide recommendations on how routines can be avoided to support mitigating the threat of IEDs.

It must be remembered that United Nations peacekeeping missions can be heavily driven by logistic considerations, and it is important for IED threat mitigation advisers and all commanders to understand the dangers of setting patterns and be able to communicate this in an effective way.

The goal is not to give the perpetrator the certainty to base planned attacks on peacekeepers, by avoiding using the same routines repeatedly.

Figure 5.26
Sample poster for United Nations peacekeeping missions (4)

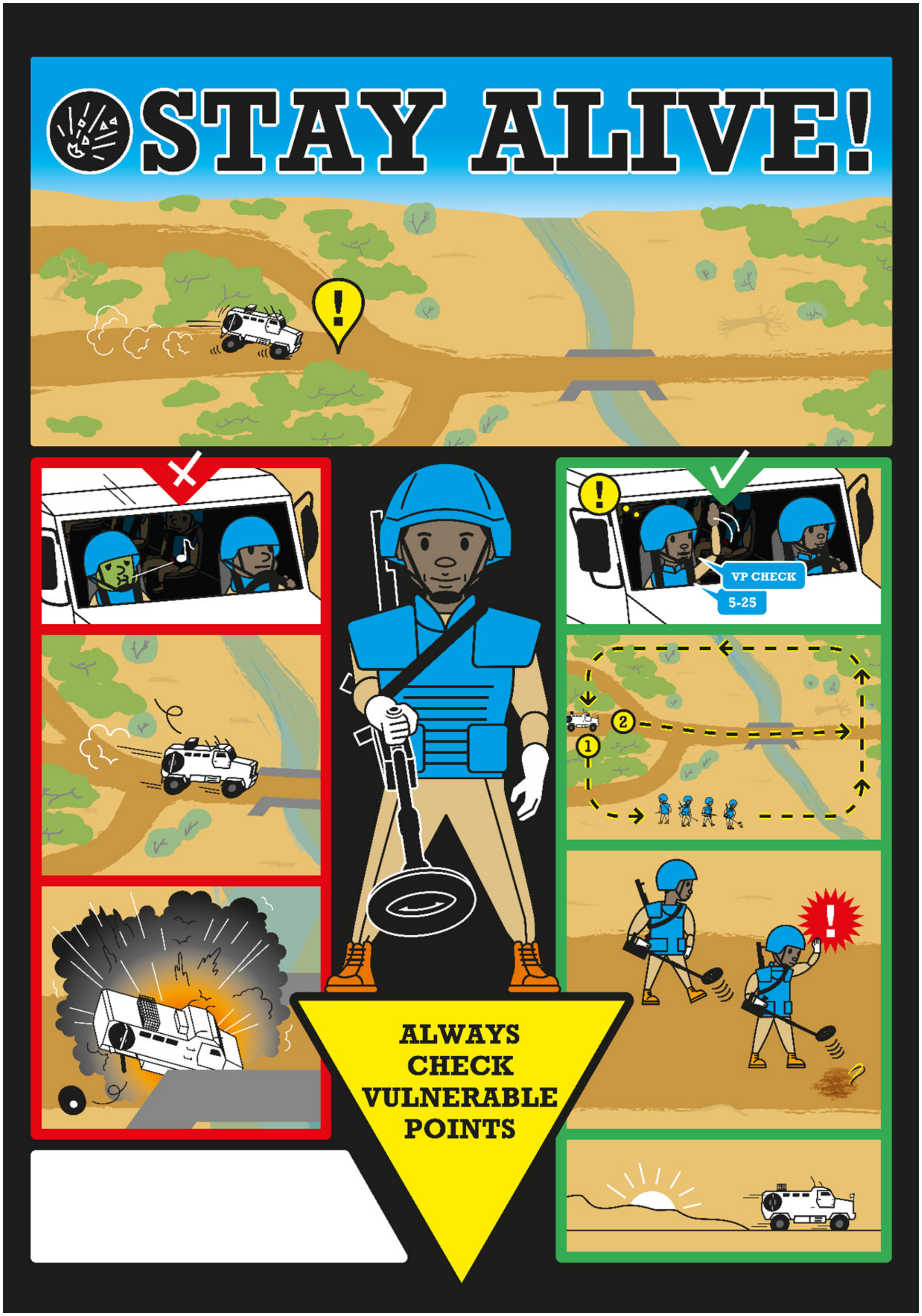


Figure 5.27

Sample poster for United Nations peacekeeping missions (5)

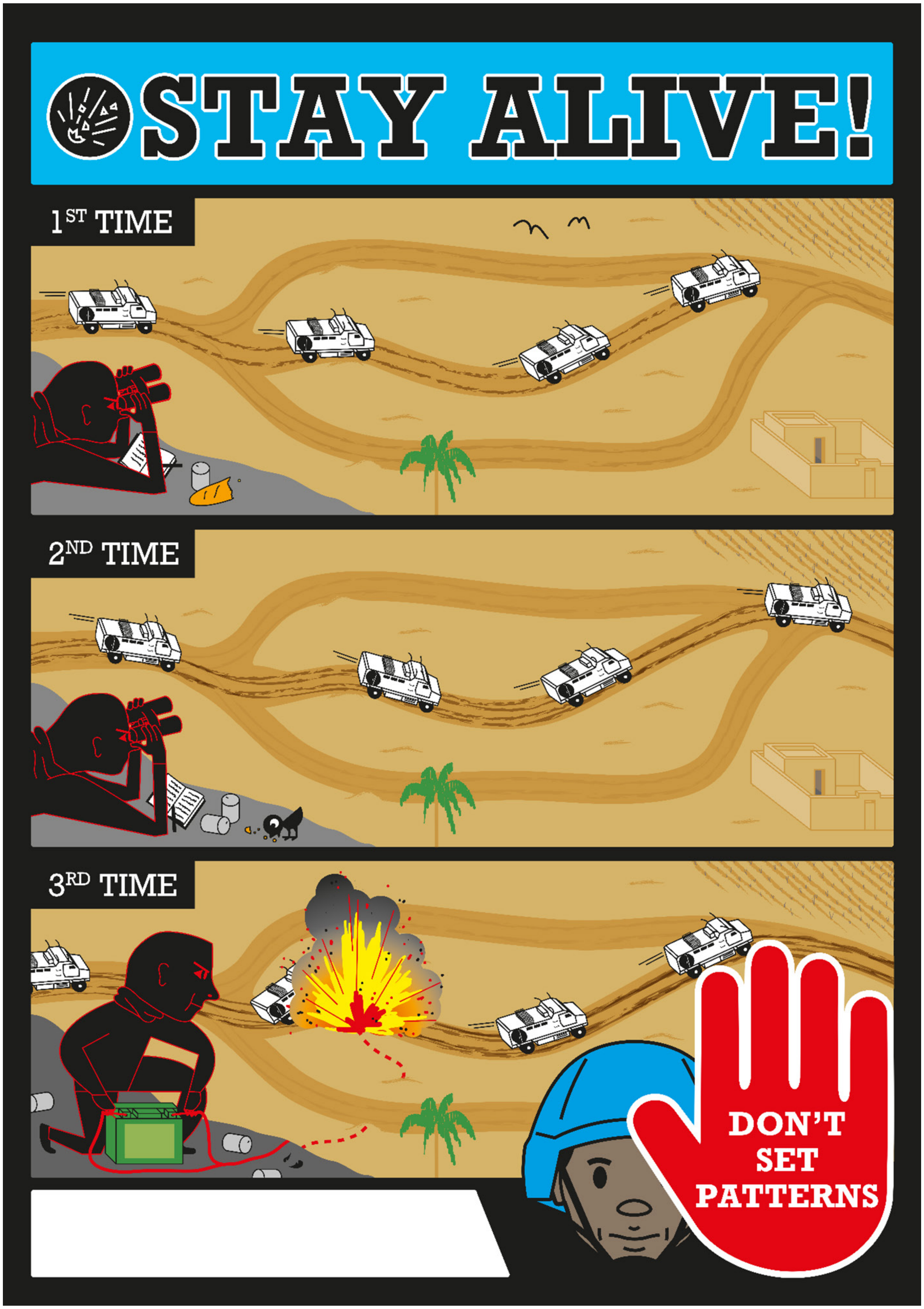
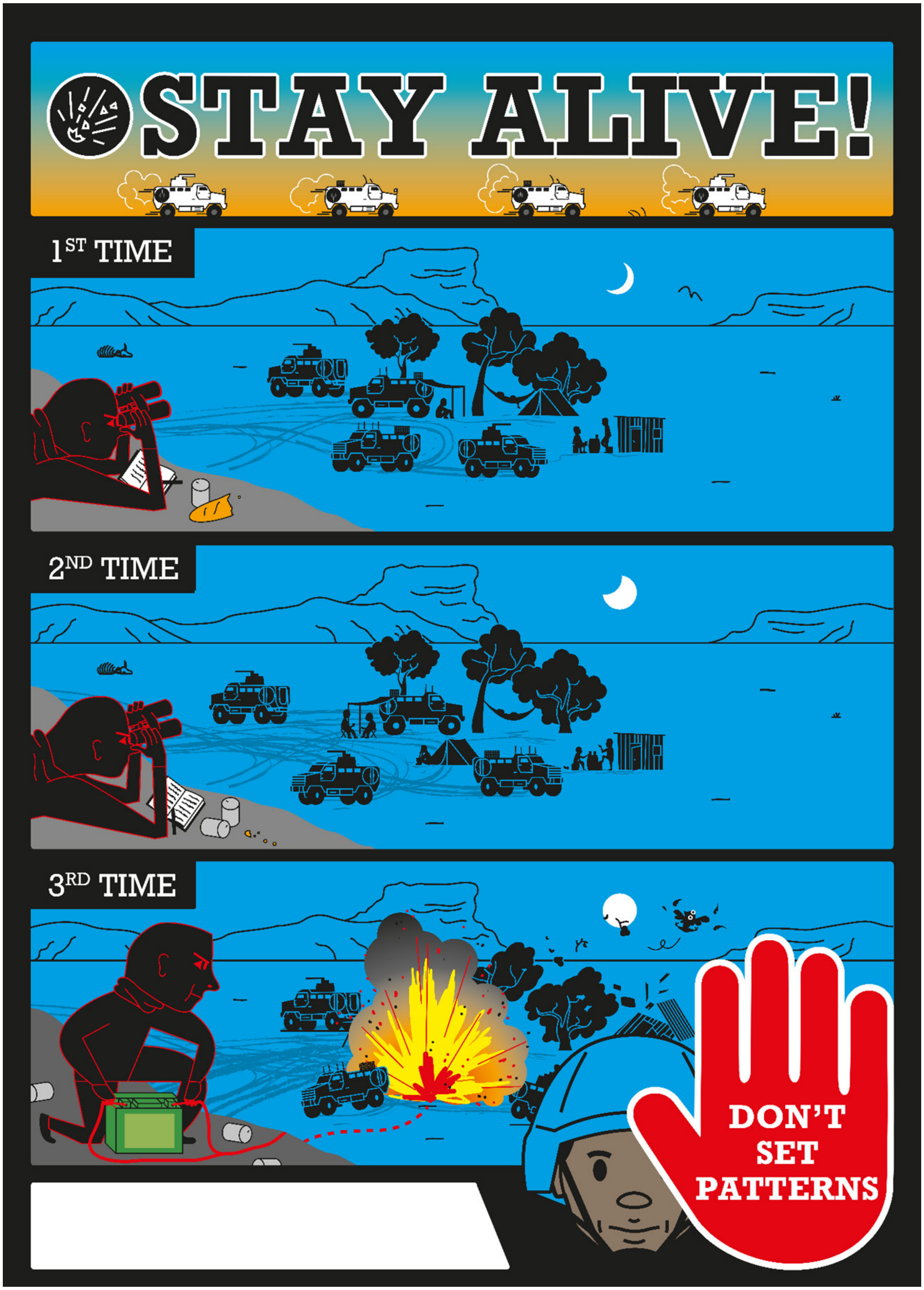


Figure 5.28
Sample poster for United Nations peacekeeping missions (6)



On the other hand, routines are crucial and neglecting or changing them can have fatal consequences. This applies to all pre-mission planning and preparation to ensure that one's own procedures and materials work and can be used at any time, for example ensuring that communications systems between all different elements of the convoy or patrol both air and ground are working effectively.

In long mission deployments and performance of routine tasks, particularly those that are physically strenuous or uncomfortable, individuals and units may become complacent, resulting in lowering of their guard, which can lead to a deviation from the routine and in the end can have a negative impact on the safety of peacekeepers.

5.14. Strategic communication

Besides the assessment and the development of a plan with appropriate procedures against the IED threat, communication is one of the most important means to mitigate the threat. Therefore, a clear distinction must be made between public information and strategic communication.[74]

Communication is of crucial importance because it conveys the capabilities, goals and determination of peacekeeping and it can admit to failures. Communication is perceived by the public, local population and own troops, as well as by perpetrators. It supports exploiting achievements, as it can counter possible criticism and frustration if success does not materialize quickly or to the intended extent.

By communicating efforts in mitigating the IED threat, the population becomes involved in the peacekeeping operation to create a safe environment for the community; it contributes to creating sympathy and support and establishes continued engagement, especially in remote areas where peacekeepers cannot be seen on a daily basis.

Regarding the perpetrators, not only can the unity and strength of peacekeepers be echoed, but it is also that their attacks are unsuccessful or not as effective as believed. Further support can be sought from the population to degrade the network of the perpetrators.

Strategic communication also provides the opportunity to reflect on one's own failures or shortcomings and how the mandate has been achieved. Such self-critical behaviour prevents one from being confronted with too-high expectations of oneself and being exploited, for example, to blame the peacekeeping operation for not living up to its own standards.

Communication is a powerful tool that should be used extensively. The domination of the information domain and a very lively representation of United Nations peacekeeping operations to the public make it more difficult to discredit the mission or the peacekeepers. Further, communication serves as an identity-building criterion, which ultimately also helps the public to immediately recognize whether the information is credible or the perpetrators are using means of misinformation and disinformation to discredit United Nations peacekeeping operations.

To that end, a communication plan that is long term, sustainable and consistent, harmonized and synchronized with the efforts of the IED threat mitigation working group, is an important element of a successful IED threat mitigation plan.

[74] Policy on Strategic Communications and Public Information (2016.11).

5.15. Delineation between military and police

In peacekeeping settings, the primary responsibility for responding to an IED incident is vested in the United Nations force, in contrast to the domestic setting of many United Nations Member States. However, United Nations police plays an important role in IED threat mitigation in several areas, including:

- Cultivation of rapport with local communities as part of the community-oriented policing and collection of information for situation awareness and threat assessment.
- Dissemination of EO risk education materials to community members.
- Securing a crime scene following an IED incident to preserve and, if required, collect evidence.
- Capacity-building and development of the host State police and other law enforcement agencies in the area of IED threat mitigation, investigation, forensic analysis, case management and procurement.
- Information-sharing and liaison with regional police organizations and INTERPOL on counter-IED issues and best practices.

The education and training for military and police personnel is usually very different. Most of the procedures described in this *Handbook* are primarily geared towards the military. However, the essential principles described in this *Handbook* do not require specific training or knowledge. By applying all procedures and recommendations contained in chapter 2, the appropriate mindset and awareness, every person in the mission already contributes significantly to mitigating the IED threat.

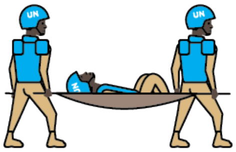
Furthermore, knowing what information is important, everybody can contribute to building a common operational picture, portraying the IED threat in the most accurate way possible, by reporting back what he observed.

Applying some of the mitigation measure, for example the five Cs, individual peacekeepers can protect themselves, other peacekeepers as well as the local population from an IED threat. Additionally, they are enabled to alert appropriately qualified forces to neutralize the threat.

Being aware of the threat and properly analysing own limitations, any individual or unit can further mitigate the IED threat by requesting through the chain of command capabilities that are required but lacking, for example the attachment of search or EOD team and so on.

5.16. Medical support (CASEVAC)

CASEVAC is defined as the evacuation of a casualty[75] from the point of injury or illness to the closest appropriate medical treatment facility, utilizing the most effective means of transportation. It is a continuum of care that supports a resuscitative process from the point of injury or illness, through evacuation, into surgery and on to intensive care where this is required. Responsibility for the mission's CASEVAC system rests with the Head of Mission, though normally



[75] Casualty here is used to mean those suffering a trauma injury and those with sudden onset, acute life-threatening conditions requiring immediate expert medical intervention. See United Nations policy on casualty evacuation in the field (DOS/2020.07).

managed by the Director or Chief of Mission Support and Chief Medical Officer or other officials delegated to fulfil this task. The CASEVAC system must be simple in structure, lean in management and easily understood by those who use it.

CASEVAC takes priority over all other mission activities except actions to counter immediate threats to United Nations personnel. CASEVAC operations will be further prioritized taking into consideration the category and number of patients.

CASEVAC assets, usually aircraft or vehicles, are not an IED threat mitigation asset per se, but it is an essential asset in that it ensures the necessary care of casualties if an IED attack occurs. In this respect, availability, both in terms of time and range, must be considered to ensure that before a mission with a possible IED threat is carried out.

In the case of penetrating trauma, there is no inflection point in time after injury at which death or residual disability rates rise sharply, rather there is a progressive, largely linear, increase.

Consequently, delay in treatment leads to an increased rate of death and disability. For operational health planning purposes, guidelines have emerged that seek to trade-off clinical need against operational risk. The metric adopted in the United Nations system is the “10-1-2” guideline:[76]

10 Immediate life-saving measures are applied by personnel trained in first aid. Bleeding and airway control for the most severely injured casualties is to be achieved within 10 minutes and a casualty alert message transmitted.

1 Advanced resuscitation/treatment is commenced by emergency medical personnel within 1 hour of injury/illness onset.

2 Where required damage control surgery is commenced as soon as practicable, but no later than 2 hours after injury/illness onset.

5.17. UNMAS

UNMAS is the designated centralized service provider to all United Nations Headquarters entities for mine action and the United Nations system-wide coordinator providing expertise to United Nations Member States and system partners, ensuring rapid response to requests for assessments and implementing responsive programmes in peace operations and non-mission settings leading on strategy development, programme design, monitoring and oversight and stakeholder engagement.

UNMAS coordinates the mine action work of the United Nations system as Chair of the Inter-Agency Coordination Group on Mine Action and subsidiary groups, and the Global Protection subcluster Mine Action Area of Responsibility. UNMAS also chairs the IMAS review board and its steering committee and is the United Nations depositary of these standards. In representing the United Nations system in international legislative bodies and other forums, UNMAS represents mine action as a critical enabler of humanitarian, development, human rights and peace and security efforts and as an accelerator of the 2030 Agenda for Sustainable Development. UNMAS is a committed advocate for victim assistance.

[76] The 10-1-2 guideline cumulative; the total time lapse between injury/onset and surgery should be under two hours. See policy on casualty evacuation in the field (DOS/2020.7).

In a mission environment, UNMAS brings a variety of potential resources. These can include advisers, mentors, training and equipment. In peacekeeping operations, UNMAS is ready to assist mission and force leadership with advice regarding unexploded ordnance, IEDs, ammunition and other EO matters. In some mission settings, UNMAS could provide real-time guidance to troop-contributing countries in dangerous IED environments. Although troop-contributing countries are expected to arrive in missions fully trained and with all appropriate equipment, UNMAS is periodically called upon to assist in bridging gaps through predeployment training, in-mission training and specialized EOD equipment.

5.18. International NGOs/civil society

There may be other actors, private companies or organizations in the area of operations that are conducting demining or even counter-IED operations, either on behalf of the host nation, the United Nations or another initiative.

In any case, it is advisable to liaise with these entities to exchange information and experience and, if necessary and feasible, to mutually support with material or machines, if this is the last resort to mitigate an immediate threat at short notice.

6. Organizational learning

The capability of organizational learning is critical to successful IED threat mitigation because it ensures that lessons learned flow directly into training and thus ensure that personnel are better prepared for change. The process should not only focus on which procedures and so on need to be improved, but also which ones have proven successful, to provide positive confirmation that no adaptation is necessary and peacekeepers can be confident in using current best practices.

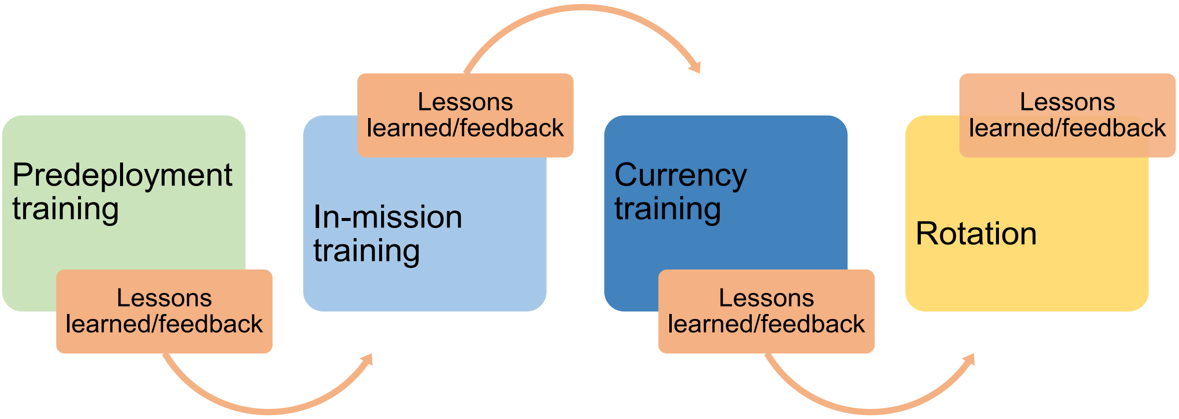
This will require formal and informal reporting methods and the submission of detailed after-action reports. Commanders and staff need to develop a simple and straightforward process that encourages people to share their experiences. Complicated forms and elaborate procedures should be avoided; otherwise, there is a risk that no one will want to participate.

Furthermore, commanders in the field must be forthcoming and candid in the acknowledgement of errors so others may learn, missions may be better accomplished, and injury and loss of life would be avoided.

Modern means, such as online questionnaires or the like, should be used whenever possible. The process should closely involve the best practice officers in the field, and they should play a key role in implementing this process.

The lessons learned are to be shared with all stakeholders in an equally effective manner. This does not only include any contingent or individual in the mission, but also troop- and police-contributing countries, doctrine writers and training teams, to ensure that all are aware of the development. A centrally accessible archive must be provided so that older reports can be compared with new findings at any time.

Figure 6.1
Organizational learning



6.1. After-action review

An after-action review is an analysis of an action, activity or project that allows personnel to reflect on what went well, identify areas of improvement and suggest recommendations to enhance similar actions, activities or projects going forward. An after-action review can be a brief discussion or longer exercise depending on the topic at hand and is most often conducted through a guided group discussion. After-action reviews are not a performance review tool and should be conducted in a spirit of openness, honesty and learning.

After-action reviews differ from lessons-learned studies since the scope and timing of an after-action review is usually more limited and more immediate, following the action, activity or project under review. Lessons-learned studies are in-depth analyses of a specific effort, process, theme or functional area with the objective of drawing lessons to improve relevance, efficiency and effectiveness of subsequent processes or efforts in field missions or at Headquarters.

After-action reviews are part of the United Nations Department of Peace Operations-Department of Political and Peacebuilding Affairs knowledge management toolbox to capture lessons and enhance the effectiveness of the Organization. The conduct and procedure of after-action reviews should be in line with the respective departmental policy.[77]

Coordination and dissemination of after-action reviews should be a function of the EOD cell or nominated person. Should immediate dissemination of information to peacekeepers be required, an incident awareness report (annex D, appendix 4) should be distributed without delay.

In the case of IED threat mitigation, after-action reviews should ideally be initiated within two weeks of the completion of an incident response action to capture best practices while the team of relevant staff members are available and memories are fresh. For reviews of the United Nations crisis response or other events potentially requiring urgent corrective actions, after-action reviews should be initiated immediately following events. The completion of an after-action review should, when possible, be integrated into the planning process of the unit/force.

The IED threat mitigation adviser or the EOD cell, in consultation with U2/best practices officer, should initiate an after-action review reaching out to the unit that has dealt with an IED incident and supporting to provide the required information by guiding them through the necessary questions to answers and information to capture.

Staff should have their commander's endorsement to undertake an after-action review, and higher commands (sector/force headquarters) should be informed of the activity. Any other unit or staff officer at sector/force headquarters who were involved in the IED threat mitigation effort under review (regardless of their rank or status) should be invited to participate in the after-action review. Other United Nations departments and entities as well as external partners may also be involved, when relevant.

6.1.1. Planning and methodology

After-action reviews are designed to be a flexible learning tool whose methodology is adaptable to the context and learning objectives. The duration and methodology of an after-action review may vary,

[77] Knowledge Management and Organizational Learning Policy (DPO 2020.11/DPPA 2020.2).

depending on the scale of the reviewed action. For example, while an after-action review discussion on the search action may take a few hours, an after-action review on an IED incident with injuries or fatalities may require one or more days of workshop as well as other methods such as surveys, one-on-one interviews or a (limited) document review. During one-on-one interviews, participants should be informed that their contributions are protected by the Chatham House Rule,[78] as neither their identity nor affiliation will be revealed in connection to any detail in the report. However, in all cases the objective of an after-action review remains to provide for a light methodology involving a group discussion among key stakeholders whenever possible.

Once it has been agreed to conduct an after-action review, the commander/team leader, in consultation with relevant stakeholders, should agree on the objectives, issues of focus, methodology, participants, length, timing and location of the after-action review discussion and key questions for the exercise. For more comprehensive exercises, for example if multiple stakeholders are involved, it is recommended that a concept note or terms of reference be prepared.

The commander/team leader should identify a facilitator to lead the discussion phase, draw out lessons learned and ensure the maintenance of an open environment throughout the exercise. The facilitator should have sufficient knowledge on IED threat mitigation procedures, but should ideally not have been involved in the actual issue at hand and should be impartial.

The commander/team leader should identify a note-taker who will summarize the discussions and should prepare the after-action review report.

6.1.2. After-action review report

An after-action review report should summarize the learning identified in the discussions. Key documents, such as checklists, planning documents, process maps and any other illustrative flow charts may be attached as annexes. Emphasis should be placed on producing a short succinct report with clear identification of good practices, innovations, gaps and actionable recommendations, within a time frame of no more than four weeks from the inception of the report.

The note-taker or facilitator should share a copy of the after-action review report with all participants for comments and feedback and to ensure that the learning is accurately reflected. As learning documents, after-action review reports do not require clearance by the Sector Commander/Force Commander. However, the overall contents of the report should be agreed upon and validated by the after-action review participants, including the commander/team leader of the unit that initiated the report.

To facilitate organizational learning, teams are encouraged to classify after-action review reports as "Unclassified" whenever possible, in line with the classification scheme outlined in document ST/SGB/2007/6.[79] To allow for the after-action review report to be widely disseminated, it is possible to cover confidential issues in a short addendum to the report, to be shared only with a specific, clearly defined target group and/or senior management.

[78] Under the Chatham House Rule, anyone who comes to a meeting is free to use information from the discussion but is not allowed to reveal who made any particular comment. It is designed to increase openness of discussion. The rule is a system for holding debates and discussion panels on controversial topics, named after the London headquarters of the Royal Institute of International Affairs, where the rule originated in June 1927.

[79] Available at https://digitallibrary.un.org/.

All after-action review reports must include the following disclaimer to ensure that the document is understood as a product of an organizational learning process and not confused with official guidance:

"This report is not an official document and does not necessarily represent the views of the United Nations Department of Peace Operations or the United Nations Department of Political and Peacebuilding Affairs."

6.1.3. Dissemination

Once finalized, the after-action review report should be disseminated to all participants and to relevant Department of Peace Operations divisions/offices at Headquarters and field missions. Peacekeeping operations should send their after-action reviews to the knowledge management and guidance team in the Policy and Best Practices Service in the Department of Peace Operations.[80] The knowledge management and guidance team shall upload after-action review reports to the Policy and Practice Database in accordance with their classification level. The knowledge management and guidance team may also include after-action review reports in newsletters or use other dissemination tools.

Regardless of their classification, in principle after-action review reports are documents internal to the United Nations. Depending on the issue and the field mission, the Department of Peace Operations can exercise flexibility in sharing unclassified after-action review reports with other relevant United Nations departments and entities and with other partners if the after-action review was conducted jointly with them. Similarly, field missions can share unclassified after-action reviews with other relevant United Nations entities within the area of operation or another United Nations entity that deals with the subject matter.

If it is in the interest of the organization, after-action review reports or certain elements can be shared with external partners with external audiences by the directors of the Policy, Evaluation and Training Division or the Policy and Mediation Division in consultation with the Office of the Under-Secretary-General of the Department of Peace Operations and/or the Department of Political and Peacebuilding Affairs where relevant. Certain elements of internal lessons-learned reports may be reused for external products, as agreed by the author and the appropriate offices within the Organization. In consultation with the drafting office or mission, after-action review reports may be uploaded to the Peacekeeping Resource Hub to facilitate joint learning with Member States, in particular troop- and police-contributing countries.[81]

Access to confidential and strictly confidential after-action review reports shall be considered on a case-by-case basis by the knowledge management and guidance team, in consultation with the relevant field mission through the mission's policy and best practices officer/Force Commander where applicable or with the lead office within the Department of Peace Operations and/or the Department of Political and Peacebuilding Affairs. Release of a confidential or strictly confidential report shall be made on a need-to-know basis in accordance with ST/SGB/2007/6.

6.1.4. Follow-up to after-action reviews

The findings of an after-action review should feed into organizational learning and the development of guidance and training. When an after-action review presents significant findings and recommendations

[80] Email: peacekeeping-bestpractices@un.org.

[81] See https://peacekeepingresourcehub.un.org/en/introduction.

with broader implications for field missions, for the United Nations peace and security pillar or for the United Nations at large, these should be tabled for discussion and follow-up by senior management at the appropriate level, either through ad hoc mechanisms or existing bodies such as the Guidance Development and Learning Steering Committee. Where appropriate, senior management should agree on follow-up actions with clearly assigned responsibilities.

7. Training

Responsibilities for ensuring peacekeepers are adequately trained and qualified before their deployment and during their employment on any United Nations peacekeeping mission are shared between troop- and police-contributing countries, command and staff.[82]

Military and police staff of a United Nations mission headquarters directly support the Force Commander/Police Commissioner's intent and vision to deal with IED threats. The staff actions are guided by the operational requirements of force protection and protection of civilians needed to fulfil the mission mandate, in line with the Commander's priorities. The Commander and key staff officers should keep themselves abreast of information analysis and IED threat assessment reports and ECM updates issued by force headquarters.

Effective training is fundamental to successful operations in an IED threat environment. It must be reinforced by strong leadership and a disciplined approach to develop a professional mindset.

Training and education are to ensure that all individuals and units in the Force have a thorough understanding of and are appropriately prepared in IED threat mitigation doctrine and procedures to the level required by their operational role. Such preparation should include IED threat awareness, cultural awareness (as this is often vital when conducting operations in IED environments) and training to employ the correct TTPs – developed as the output of the lessons-learned process. The Commander's training responsibilities include:

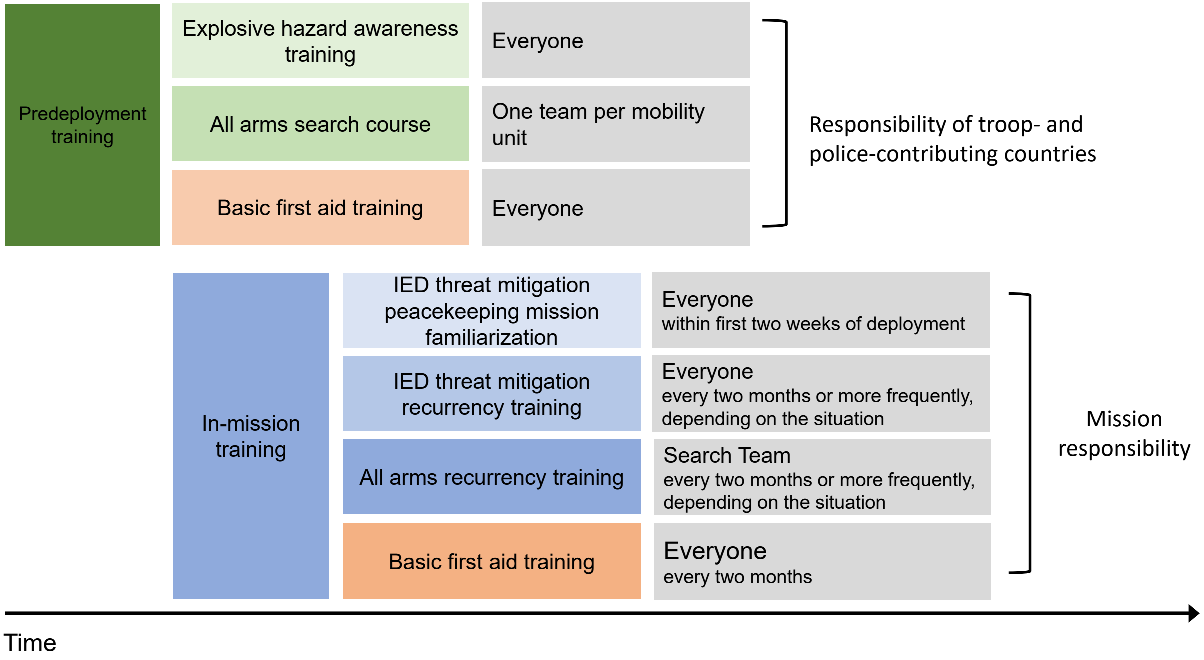
- Ensuring that peacekeeping-intelligence on perpetrators IED TTPs is passed quickly to all peacekeepers in order that friendly TTPs can be modified to be as up-to-date, appropriate and effective as possible.
- Giving special attention to training of IEDD units for their effect-based and threat-based employment to achieve IED threat mitigation in the mission area.
- Ensuring all mobility units are familiar with the appropriate TTPs for detecting IEDs, as well as with the capabilities of units that are available to support them.
- Quickly addressing any deficiencies through the provision of additional resources, and/or by adapting training to the needs of the mission, in response to the evolving threat.

Figure 7.1 shows the required training and timelines. It is the responsibility of the respective troop- or police-contributing countries, commanders and staff to provide the necessary resources to ensure that the appropriate training is conducted. Should a troop- or police-contributing country not be able to meet the requirements, appropriate mechanisms should be put in place to help to meet the responsibility.[83]

[82] Training for all United Nations peacekeeping personnel (2010.20).

[83] Support to military and police predeployment training for United Nations peacekeeping operations (2009.21).

Figure 7.1
Training for IED threat mitigation



Predeployment training	Explosive hazard awareness training	Everyone	Responsibility of troop- and police-contributing countries
	All arms search course	One team per mobility unit	
	Basic first aid training	Everyone	
In-mission training	IED threat mitigation peacekeeping mission familiarization	Everyone within first two weeks of deployment	Mission responsibility
	IED threat mitigation recurrency training	Everyone every two months or more frequently, depending on the situation	
	All arms recurrency training	Search Team every two months or more frequently, depending on the situation	
	Basic first aid training	Everyone every two months	

7.1. Predeployment training

According to General Assembly resolution 49/37, Member States are responsible for the delivery of predeployment training for uniformed personnel deploying to United Nations peacekeeping operations.

Owing to the persistence of IED threat to United Nations peacekeepers, general IED awareness is mandatory for predeployment training, regardless of military or police, contingent or individual uniformed personnel and if the mission is facing an IED threat or not.

For **individual uniformed personnel** the specialized training material for United Nations military observers, available on the Peacekeeping Resource Hub, contains a lesson on IED awareness.[84]

For **military units**, the specialized training material for United Nations infantry battalions, annex E, contains:

- Explosive Hazards Awareness Training.
- IED training materials – block of infantry-specialized training material.[85]

For military commanders and planners, a dedicated IED threat mitigation course, with respective training material, is currently under development.[86]

[84] See https://peacekeepingresourcehub.un.org/en/training/stm/unmo.

[85] Peacekeeping Resource Hub, specialized training material for United Nations infantry battalions, annex E. Available at https://peacekeepingresourcehub.un.org/en/training/functional.

[86] Training materials will be made available at https://peacekeepingresourcehub.un.org.

The specialized training material for United Nations infantry battalions, annex E, also contains the all arms search course.[87] This module is an additional requirement for all units deploying outside of United Nations facilities (e.g. United Nations camp, temporary operating base) as part of their mission, regardless of whether this is on a single occasion or constantly. These units are to identify and train appropriate personnel, to form a search team, and to be employed as an organic asset of that unit to support any movement of the unit outside a United Nations facility.

In addition, every peacekeeper is required to complete the basic first aid course, as well as part of the predeployment training.[88]

The course is also available as a mobile application, "UN Buddy First Aid".[89]

In addition, the Peacekeeping Resource Hub provides specialized training material for formed police units for example (see module 4: First aid training), which complements the individual training.[90]

Common standards, trained on before and applied during deployments, will ensure personnel have the knowledge and the skills necessary to successfully perform the required IED threat mitigation and search tasks.

The national training must meet and should, wherever possible, exceed United Nations standards. Every investment in appropriate training significantly reduces the risk of peacekeepers getting wounded or killed by an IED.

All commanders must attend the mandatory training as well. The information received could be decisive to survive an IED incident when visiting troops in the field or meeting with the local population. It also allows commanders to decide, based on the recommendations provided by the IED threat mitigation adviser or the IED threat mitigation working group, to monitor the situation and adjust the force posture, if required.

For United Nations civilian staff, three IED awareness training modules are available: The modules BSAFE and Safe and Secure Approaches in Field Environments (SSAFE) are provided by the Department of Safety and Security.

- BSAFE is an online training, mandatory for all United Nations staff.[91] There is a module in this course presenting mine and explosive awareness.
- SSAFE is a three-day training, conducted in person, presenting explosive hazards awareness training and IED awareness, including practical exercises to identify mines, IEDs and "booby traps", as well to demonstrate safe response to an incident involving explosives and associated injuries. This course is mandatory for United Nations staff working in high-risk areas.

The third online training is provided by UNMAS via the United Nations internal learning platform INSPIRA. It contains information regarding landmines and ERW.[92] The accompanying *Landmines,*

[87] Peacekeeping Resource Hub, specialized training material for United Nations infantry battalions, annex E. Available at https://peacekeepingresourcehub.un.org/en/training/functional.

[88] *Medical Support Manual for United Nations Field Missions*, fourth edition.

[89] Available from Google Play or Apple App Store.

[90] See https://peacekeepingresourcehub.un.org/en/training/stm/fpu.

[91] See https://training.dss.un.org/thematicarea/category?id=6.

[92] United Nations Inspira platform. Learning Module: Landmines and Explosives Remnants of War (LMS-2356).

Explosives Remnants of War and IED Safety Handbook is available in several languages from the UNMAS website.[93]

7.2. In-mission training

In mission, threat-specific training for IEDs is a continuation of predeployment training. It should begin as early as possible after arrival in the mission area as part of the induction training.

Despite units being trained and qualified before deploying on a peacekeeping mission, they are required to become familiar with the geographic characteristics, procedures established, new equipment and so on in the mission context. Capability integration may then be necessary to align all units. The Force Commander may delegate this responsibility to one or more troop- or police-contributing countries to conduct the required training once deployed.

To ensure operational readiness, the training cell bears with the responsibility to facilitate and conduct training to adjust the existing knowledge and skill of uniformed contingents and individuals to the current situation.

In-mission training should focus on the latest threat assessment and include, but not limited to:

- In-mission IED threat familiarization (perpetrator's TTPs), prevailing IED threat environment in the mission area, understanding of patterns, IED precursors, road signs indicating IED placement, local behaviours and so on.
- Information about available IED threat mitigation assets, including who is conducting technical exploitation, evidence collection and so on.
- Training on available equipment.
- Protective measures for personnel and United Nations installations (dress and vehicle code).
- IED search procedures (e.g. route search, area search, building search) incorporating local IED indicators, characteristics and trends.
- Mitigation measures during convoys.
- Training together with different units to ensure that there are no misunderstandings regarding the application of established procedures.
- Reporting procedures and formats.
- Crisis action planning of post-IED-attack actions including, for example, medical response, personnel evacuation and other immediate actions.
- CASEVAC procedures with available assets to ensure proper knowledge of how to approach the vehicles (e.g. specific helicopters), available material and so on.

Consideration should be given to the use of simulation systems, use of training ranges (e.g. IED lane) and mock exercises to enhance realism for post-IED scenarios and to expose personnel to realistic training while still in a safe and controlled environment.

[93] See www.unmas.org/en/publications.

Apart from the requirements adapted to the specific situation in the mission, the performance evaluation criteria[94] also provide a good benchmark for organizing appropriate training. This ensures that the knowledge and qualifications identified as a minimum can be performed.

Due to the complexity of the situation, a simulated IED threat can be embedded in any tactical training scenario. This ensures that training on essential skills such as battle drills, communication (among each other and with other agencies), coordination of personnel and vehicles, first aid and others are conducted in a way that provides a good basis for all challenges in the field.

United Nations peacekeeping operations are to ensure that the convoy commander course and mobility planning course are offered on a regular basis, and it is mandatory for every contingent training for staff understanding of concepts.

United Nations peacekeeping operations are encouraged to develop a dedicated staff officers training on IED threat mitigation to provide all personnel with the required tool kit to contribute to planning effective IED threat mitigation measures.

In addition, there is the possibility of requesting appropriate training (e.g. from UNMAS), especially for personnel who are particularly exposed to the threat of IEDs.

Organizing joint exercises should always be considered, since joint patrols can be carried out at any time. In this way, all parties involved are aware of each other's capabilities and limitations and can prepare to better manage them. The agreement of clear procedures will in any case contribute to the fact that in the concrete case of an IED threat a higher security prevails.

In addition to the United Nations military and police units, training shall include participation from host nation military and security forces. This is necessary to benefit from the experience of the host nation's security forces, to support the development of their capability and prepare them to take on IED threats as part of capacity-building. Training and education of the host nation security forces, from the outset and within operational security constraints, are provided through mentoring, followed by partnering until the host nation can operate independently.

[94] Military performance evaluation standards.

8. Evaluation

Predeployment training should be oriented to the achievement of the standards required to pass relevant evaluations. There are three types of evaluations, which are conducted at different stages of the preparation and deployed in a mission:

- Self-certification/evaluation.
- Military skill validation during predeployment visit.
- In-mission evaluation by force headquarters and/or sector headquarters.

The evaluation aligns with the United Nations policy on operational readiness preparation, which outlines a framework, including timelines for the evaluation and self-certification of United Nations military units provided by troop-contributing countries in accordance with status of unit requirements, the 2023 COE manual and other United Nations peacekeeping missions military unit manuals.

The purpose of formal evaluation is to assist troop-contributing countries and military contingents in meeting national and United Nations standards of operational performance. In addition, mission evaluations also serve to determine whether the initial training level could be maintained and what adjustments, if any, need to be made for future rotations.

Evaluations may be conducted in a graduated manner by level (from individual soldiers to commanders) and activity (i.e. teams, platoon, company or battalion/task force) in a task-oriented manner to systematically build expertise and integrate capabilities for collective application.

The operational readiness regarding IED threat mitigation is evaluated based on risk assessment for threats of EO, including IEDs, and take appropriate force protection measures during the operational planning. During the operation, the unit is required to carry out appropriate procedures to manage EO/IED risks and emplacing mitigation measures to minimize vulnerability of United Nations forces, facilities, equipment, materiel, operations and activities to threats and hazards from IED and to preserve freedom of action and operational effectiveness.

Evaluation should analyse task-oriented activities at each level within the military contingent to include individuals, groups and commanders.

For the in-mission evaluation by force headquarters and/or sector headquarters, U7 (training), in close cooperation with the IED threat mitigation adviser, the search adviser and the IED threat mitigation working group, should develop a catalogue of criteria which is based on the knowledge and skills units are required to acquire and demonstrate before the start of the deployment. Further, the in-mission evaluation accesses the completion of in-mission training, which is geared to the specific local conditions and challenges.

In all types of the evaluations (e.g. self-certification, military skills validation during predeployment visits and in-mission evaluation), the units are evaluated for their preparedness and readiness for explosive hazards assessment and awareness, individual and collective skills for EO including IED threat mitigation, appropriate conduct of all arms search ability and providing appropriate first aid to the EO/IED casualties.

Annex A. IED lexicon

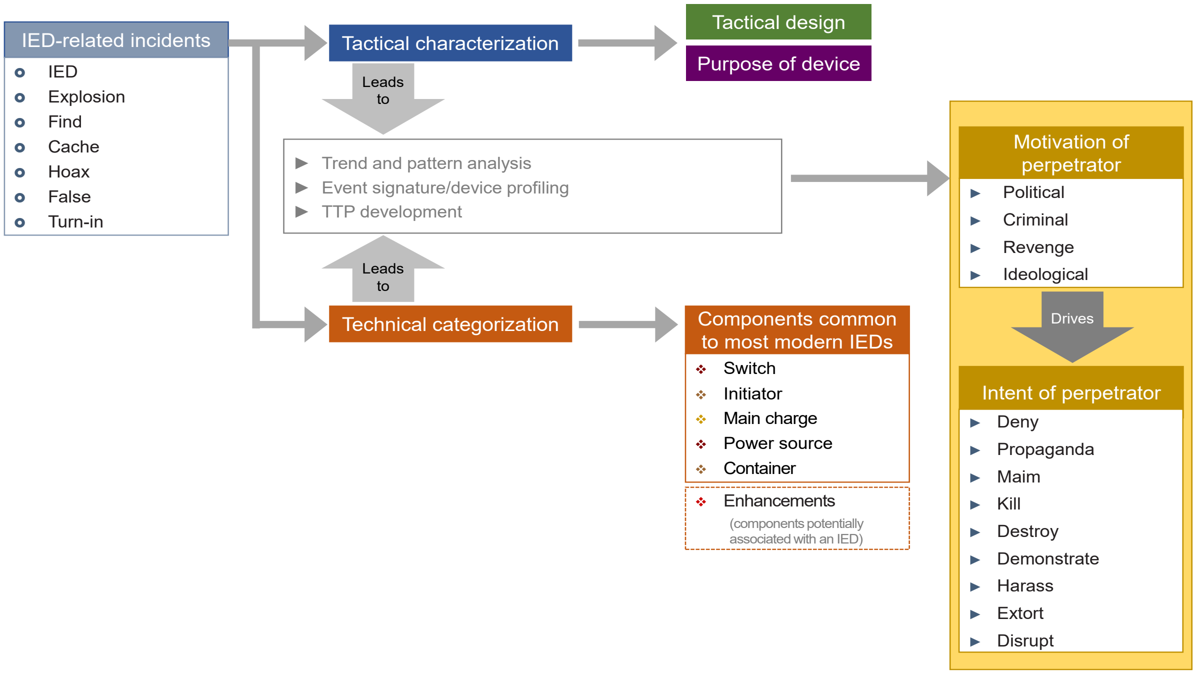
This lexicon is intended to provide the United Nations system with a coherent conceptual framework and operational vocabulary to address the improvised explosive device (IED) threat worldwide. It encompasses the broad spectrum of IED employment scenarios, the variety of IED devices and their critical components.

Adoption of this lexicon will improve the collection, reporting and exploitation of IED information at the tactical, operational and strategic levels. The lexicon will assist in:

- Standardizing terminology across IED reports and improving database content management.
- IED-related education and training.
- Development and understanding in support of IED policy and doctrine.

In order to maintain the ability to effectively communicate and understand the IED using the construct and definitions posed in this lexicon, modification of definitions and diagrams is not recommended.

A.1. IED lexicon construct



IED-related incidents
- IED
- Explosion
- Find
- Cache
- Hoax
- False
- Turn-in

Tactical characterization

Tactical design

Purpose of device

Leads to

- Trend and pattern analysis
- Event signature/device profiling
- TTP development

Leads to

Technical categorization

Components common to most modern IEDs
- Switch
- Initiator
- Main charge
- Power source
- Container

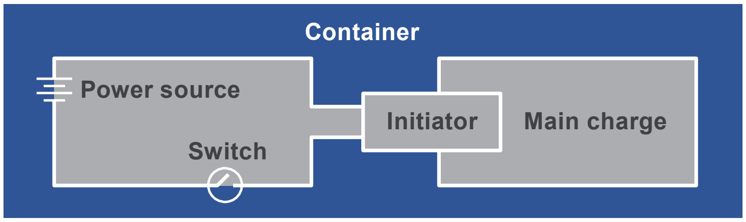
Enhancements
(components potentially associated with an IED)

Motivation of perpetrator
- Political
- Criminal
- Revenge
- Ideological

Drives

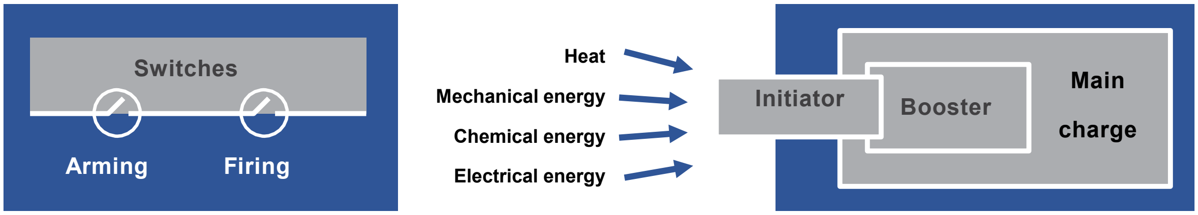
Intent of perpetrator
- Deny
- Propaganda
- Maim
- Kill
- Destroy
- Demonstrate
- Harass
- Extort
- Disrupt

The five components common to most modern IEDs:



Multiple switches are sometimes present and connected together.

A booster is sometimes present in the IED explosive train.



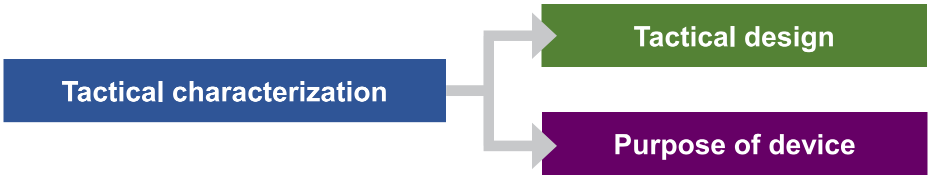
A.2. Categorization

To understand, categorize and analyse an IED incident, two main aspects are to be considered:

- Tactical characterization
- Technical characterization

A.3. Tactical characterization

The way an IED incident is planned and conducted (tactical design) and the intent (purpose of device).



Tactical design

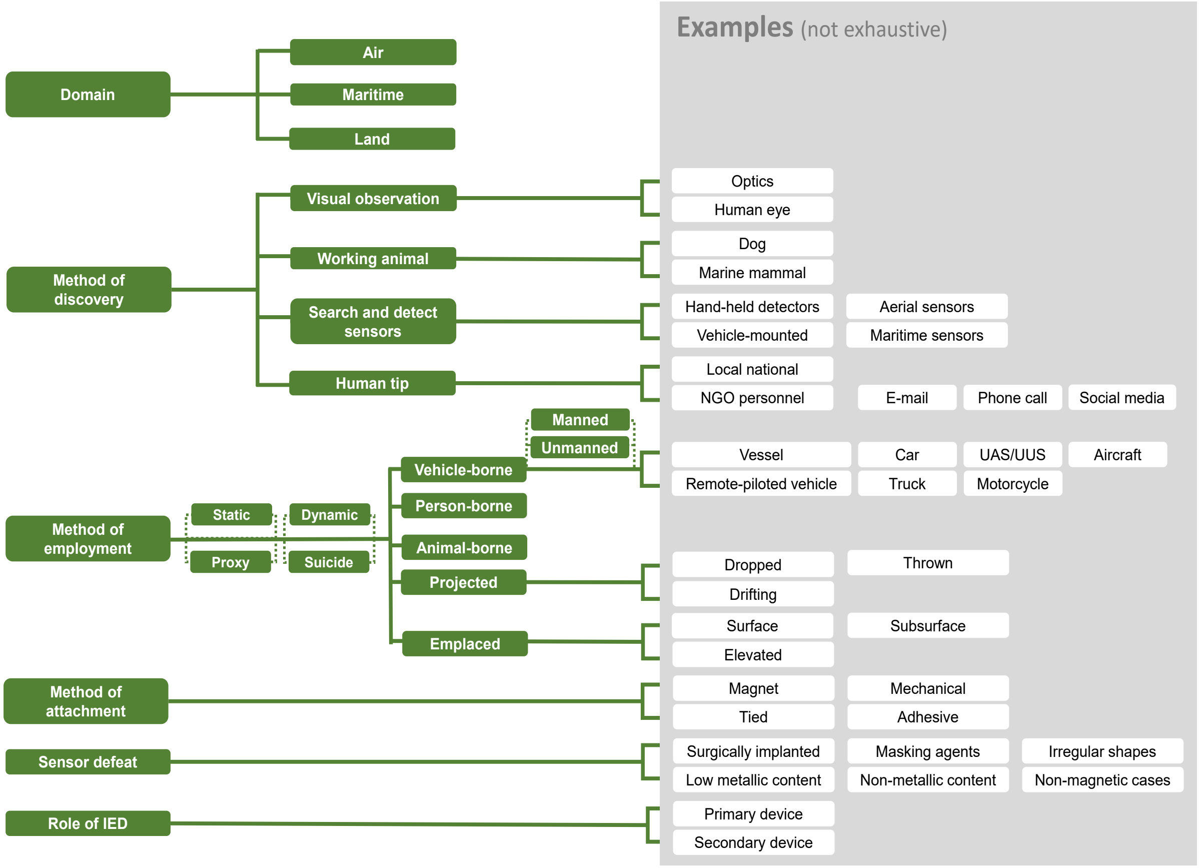
The specific design of an IED attack, including but not limited to position of the IED, the type of IED, type of road segment used, concealment technique, use of secondary devices, the time of day and so on. Tactical design addresses the questions:

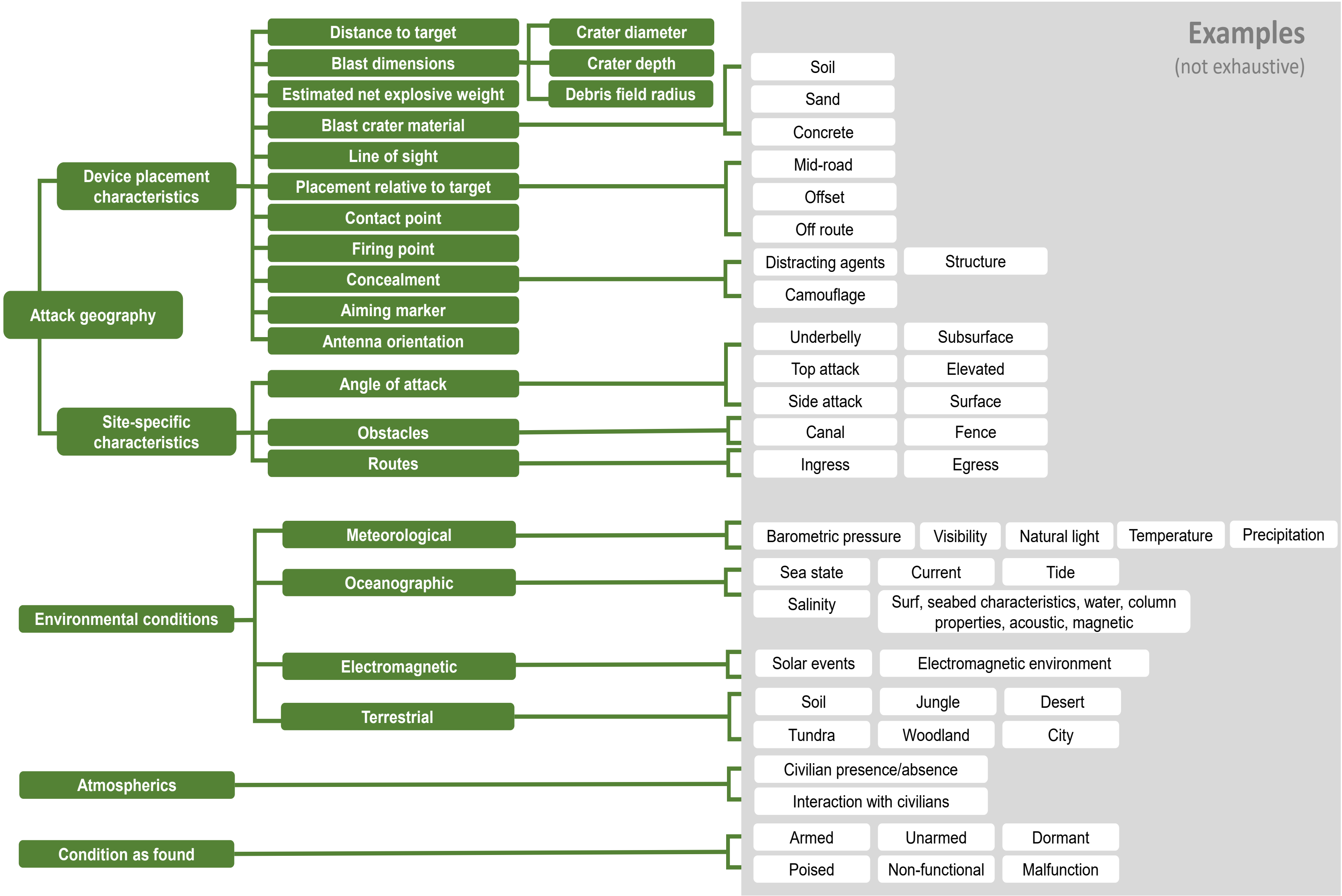
- Why here?

- Why now?
- Why in this way?

Terms used to describe a specific type of device or component of a device (e.g. vehicle-borne IED) are often used to describe all or part of the tactical design.

- Method of identification
- Method of employment
- Method of emplacement
- Method of attachment
- Sensor defeat
- Role of IED
- Attack geography
- Incident environmental conditions
- Incident atmospherics

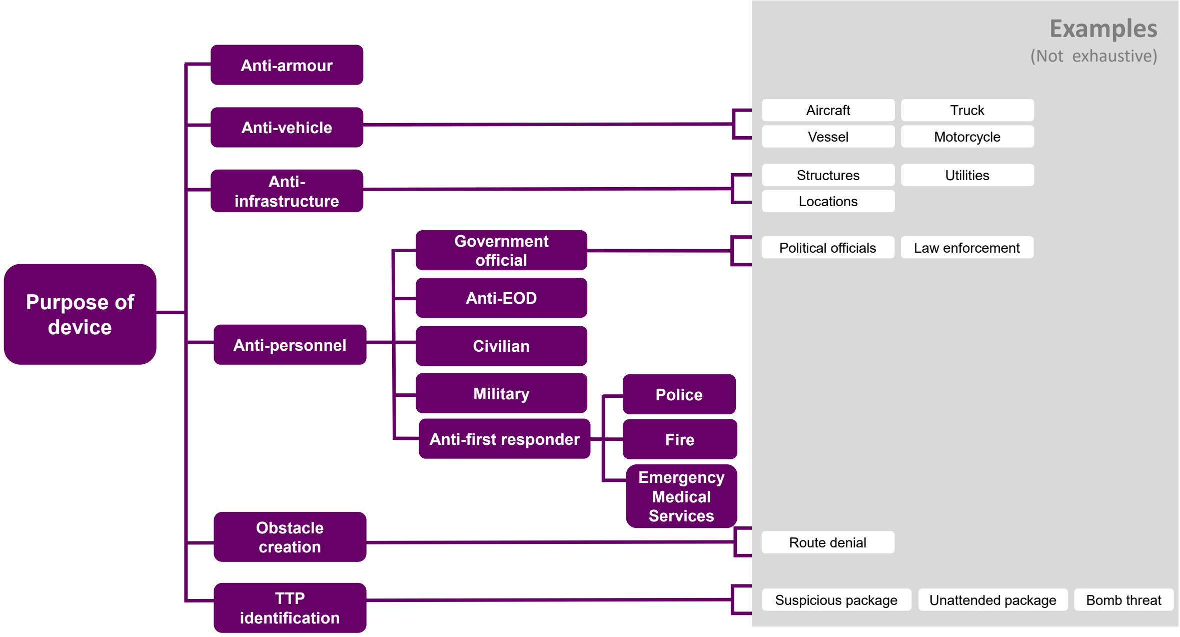




Examples
(not exhaustive)

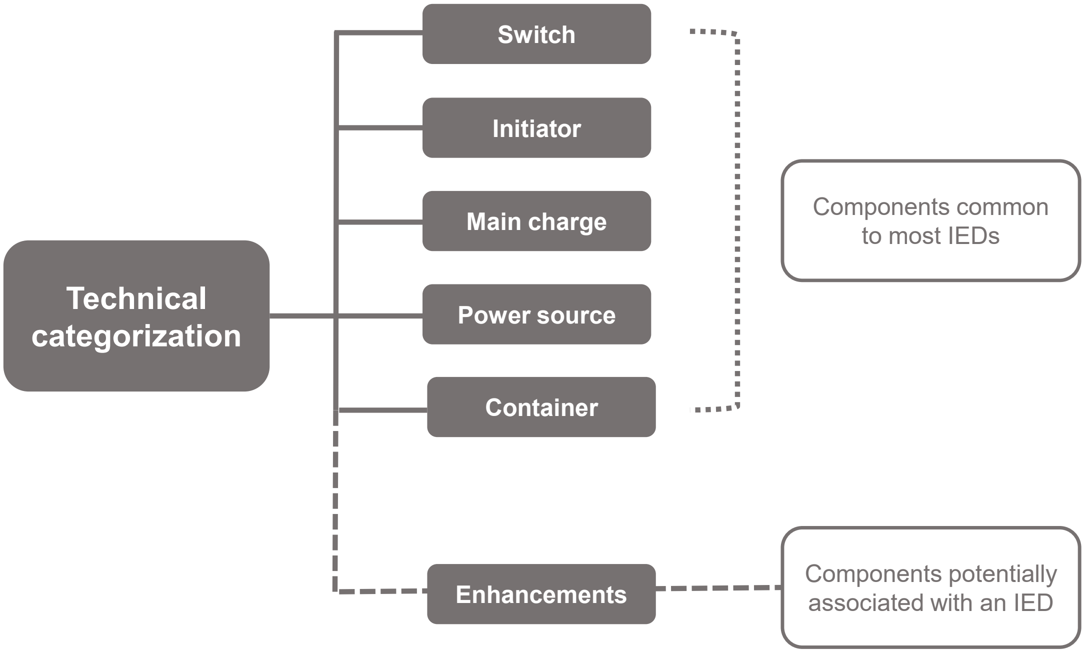
- Attack geography
  - Device placement characteristics
    - Distance to target
    - Blast dimensions
      - Crater diameter
      - Crater depth
      - Debris field radius
    - Estimated net explosive weight
    - Blast crater material
      - Soil
      - Sand
      - Concrete
    - Line of sight
    - Placement relative to target
      - Mid-road
      - Offset
      - Off route
    - Contact point
    - Firing point
    - Concealment
      - Distracting agents
      - Structure
      - Camouflage
    - Aiming marker
    - Antenna orientation
  - Site-specific characteristics
    - Angle of attack
      - Underbelly
      - Subsurface
      - Top attack
      - Elevated
      - Side attack
      - Surface
    - Obstacles
      - Canal
      - Fence
    - Routes
      - Ingress
      - Egress
- Environmental conditions
  - Meteorological
    - Barometric pressure
    - Visibility
    - Natural light
    - Temperature
    - Precipitation
  - Oceanographic
    - Sea state
    - Current
    - Tide
    - Salinity
    - Surf, seabed characteristics, water, column properties, acoustic, magnetic
  - Electromagnetic
    - Solar events
    - Electromagnetic environment
  - Terrestrial
    - Soil
    - Jungle
    - Desert
    - Tundra
    - Woodland
    - City
- Atmospherics
  - Civilian presence/absence
  - Interaction with civilians
- Condition as found
  - Armed
  - Unarmed
  - Dormant
  - Poised
  - Non-functional
  - Malfunction

Purpose of device



A.4. Technical categorization

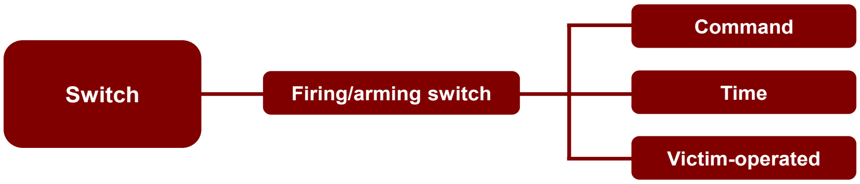
A description of an IED using a hierarchical construct to identify its key components. The components identified in this categorization are the elements from which technical and forensic information is recovered and exploited.



Switch

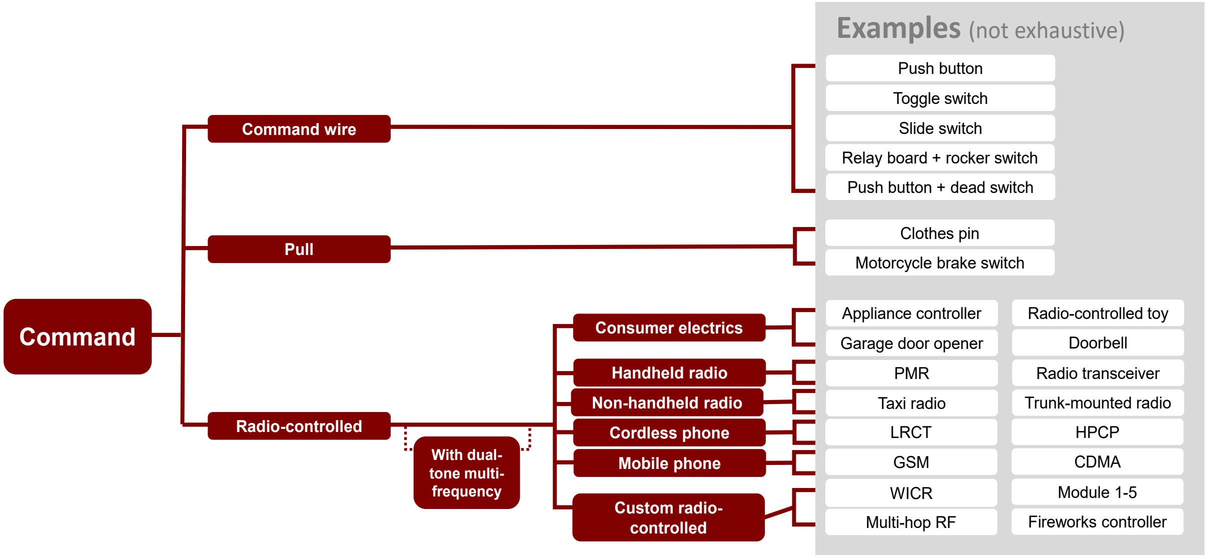
A device for making, breaking or changing a connection in an IED.

A single switch can have multiple functions (i.e. arming and firing).

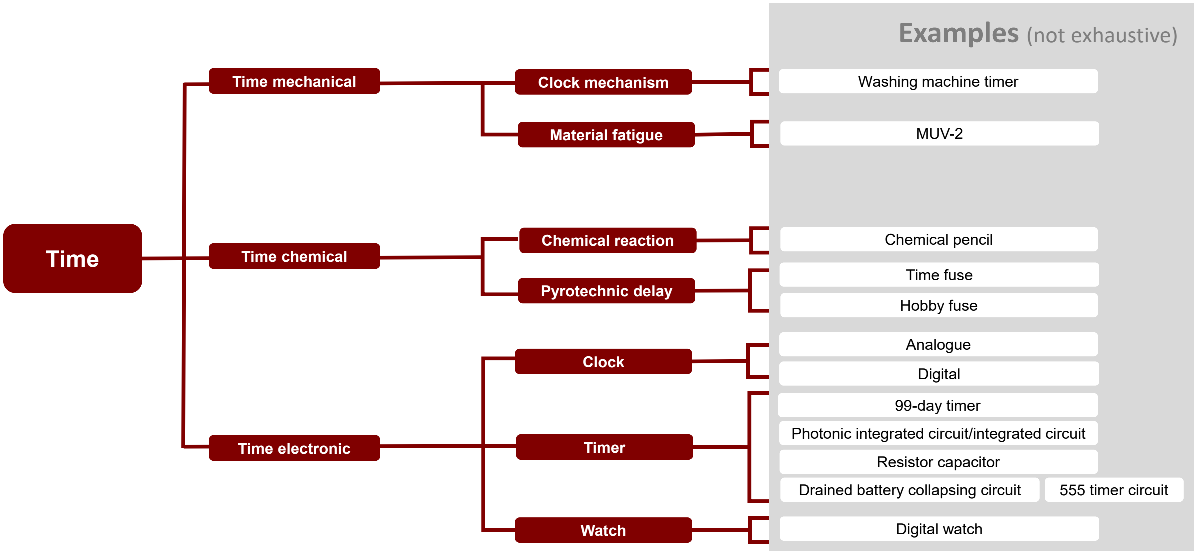


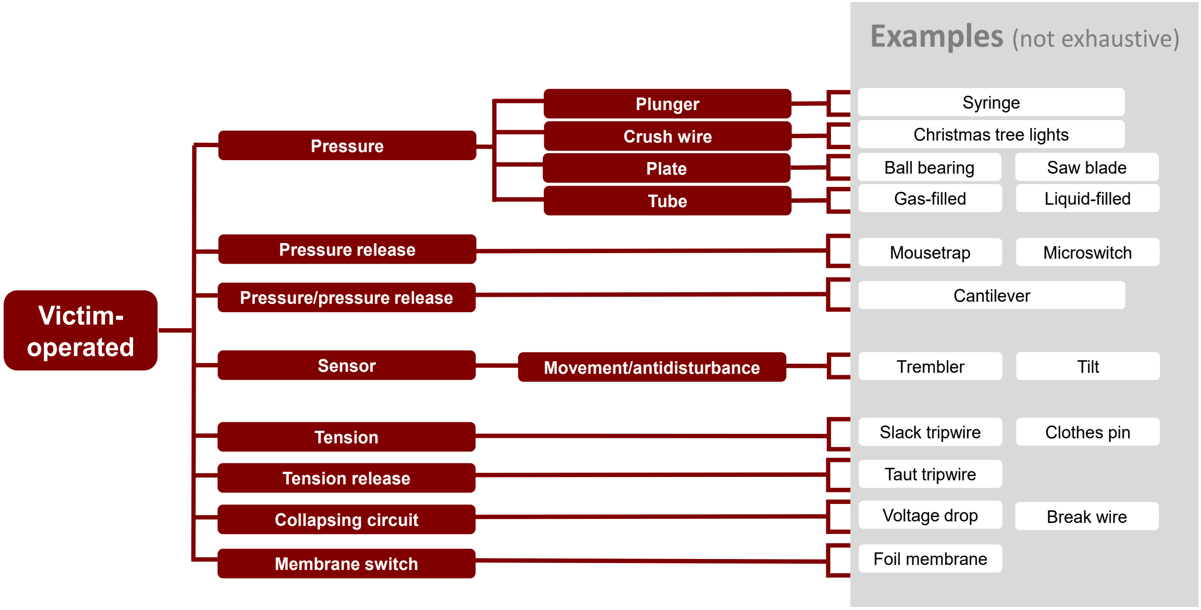
The firing switch that initiates the IED determines the device type by category (e.g. command, time, victim-operated). If present, the arming switch should also be categorized.

When categorizing switches, it is important to understand switches can be configured in a multitude of ways. The observed configuration of the switch should be considered when categorizing the device. Also, the same configuration of components could function in more than one way.



Abbreviations: CDMA, code division multiple access; GSM, global system for mobile communication; HPCP, high-power cordless phone; LRCT, long-range cordless telephone; PMR, personal mobile radio; RF, radio frequency; WICR, Wireless Custom Receiver.



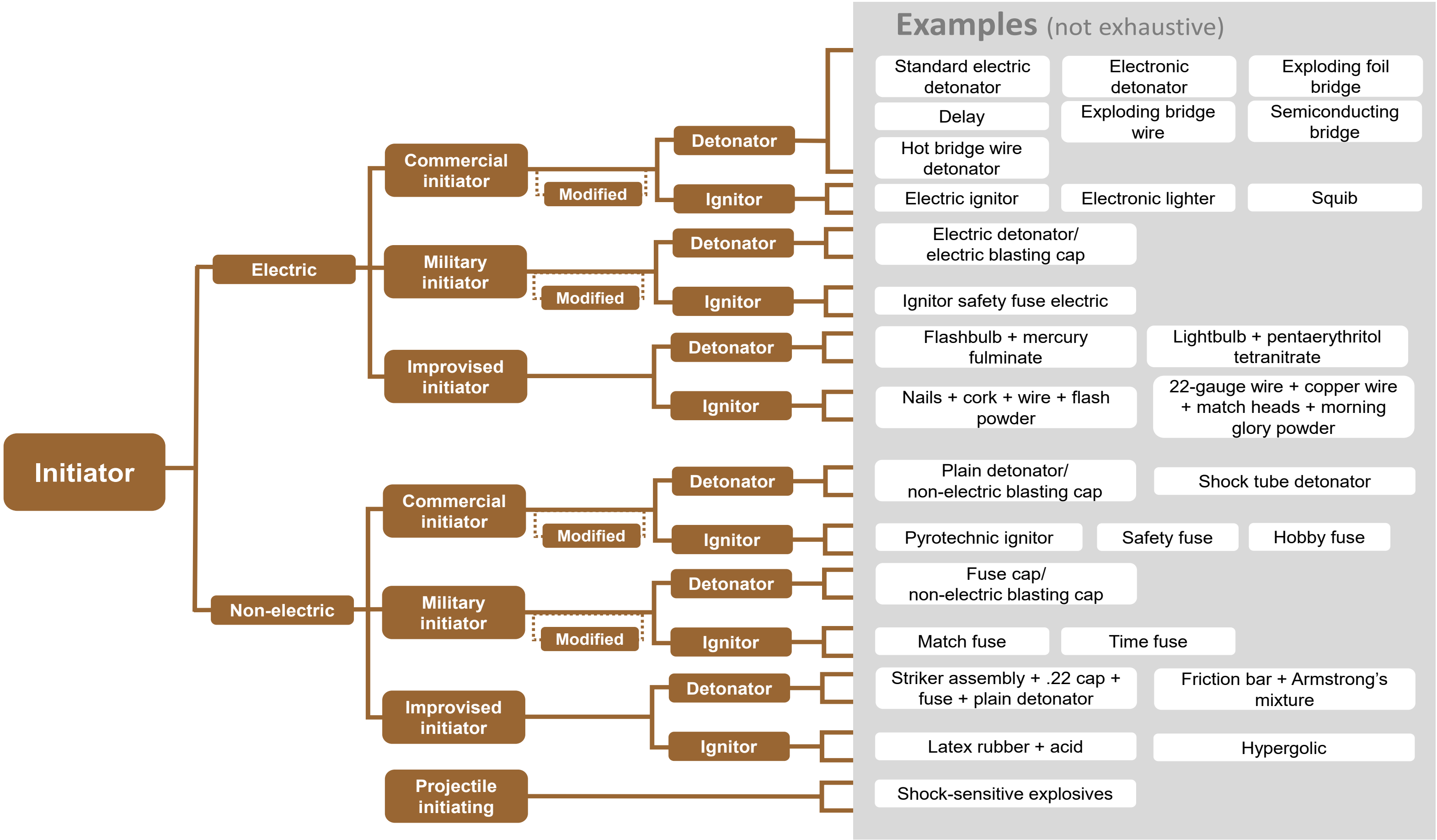


Initiator

Any component that may be used to start a detonation or deflagration.

An initiator will be categorized as either a detonator or an igniter. The initiator can be:

- Electric
- Non-electric


Examples (not exhaustive)
Initiator
Electric
Commercial initiator
Modified
Detonator
Standard electric detonator
Electronic detonator
Exploding foil bridge
Delay
Exploding bridge wire
Semiconducting bridge
Hot bridge wire detonator
Ignitor
Electric ignitor
Electronic lighter
Squib
Military initiator
Modified
Detonator
Electric detonator/ electric blasting cap
Ignitor
Ignitor safety fuse electric
Improvised initiator
Detonator
Flashbulb + mercury fulminate
Lightbulb + pentaerythritol tetranitrate
Ignitor
Nails + cork + wire + flash powder
22-gauge wire + copper wire + match heads + morning glory powder
Non-electric
Commercial initiator
Modified
Detonator
Plain detonator/ non-electric blasting cap
Shock tube detonator
Ignitor
Pyrotechnic ignitor
Safety fuse
Hobby fuse
Military initiator
Modified
Detonator
Fuse cap/ non-electric blasting cap
Ignitor
Match fuse
Time fuse
Improvised initiator
Detonator
Striker assembly + .22 cap + fuse + plain detonator
Friction bar + Armstrong's mixture
Ignitor
Latex rubber + acid
Hypergolic
Projectile initiating
Shock-sensitive explosives

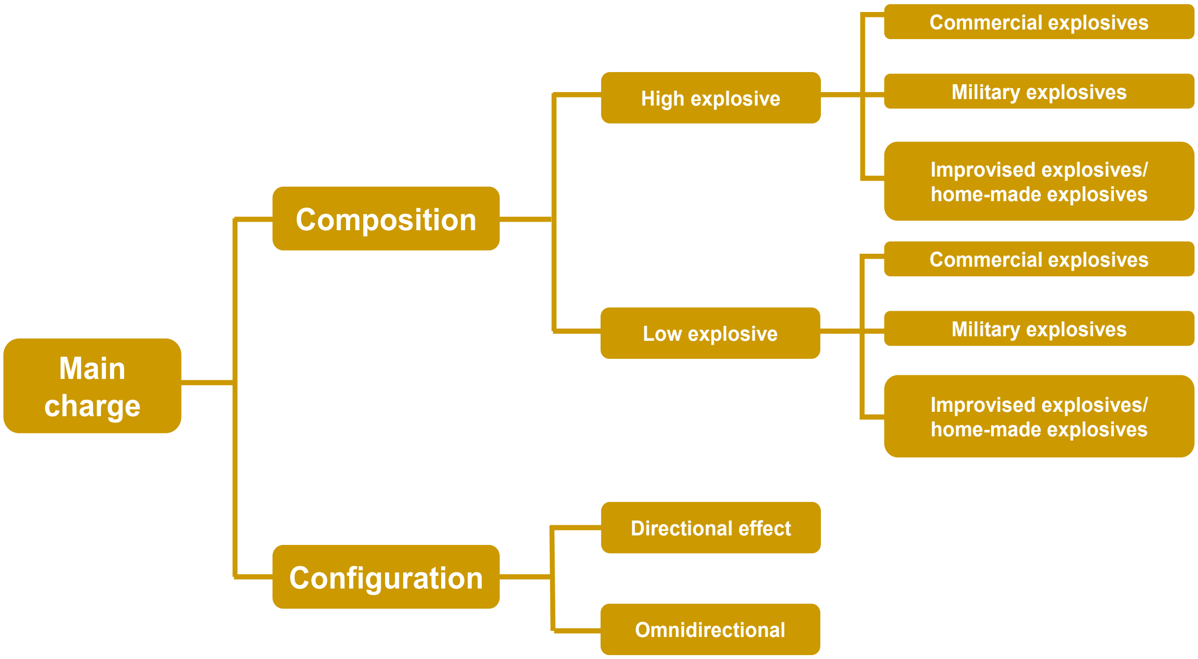
Main charge

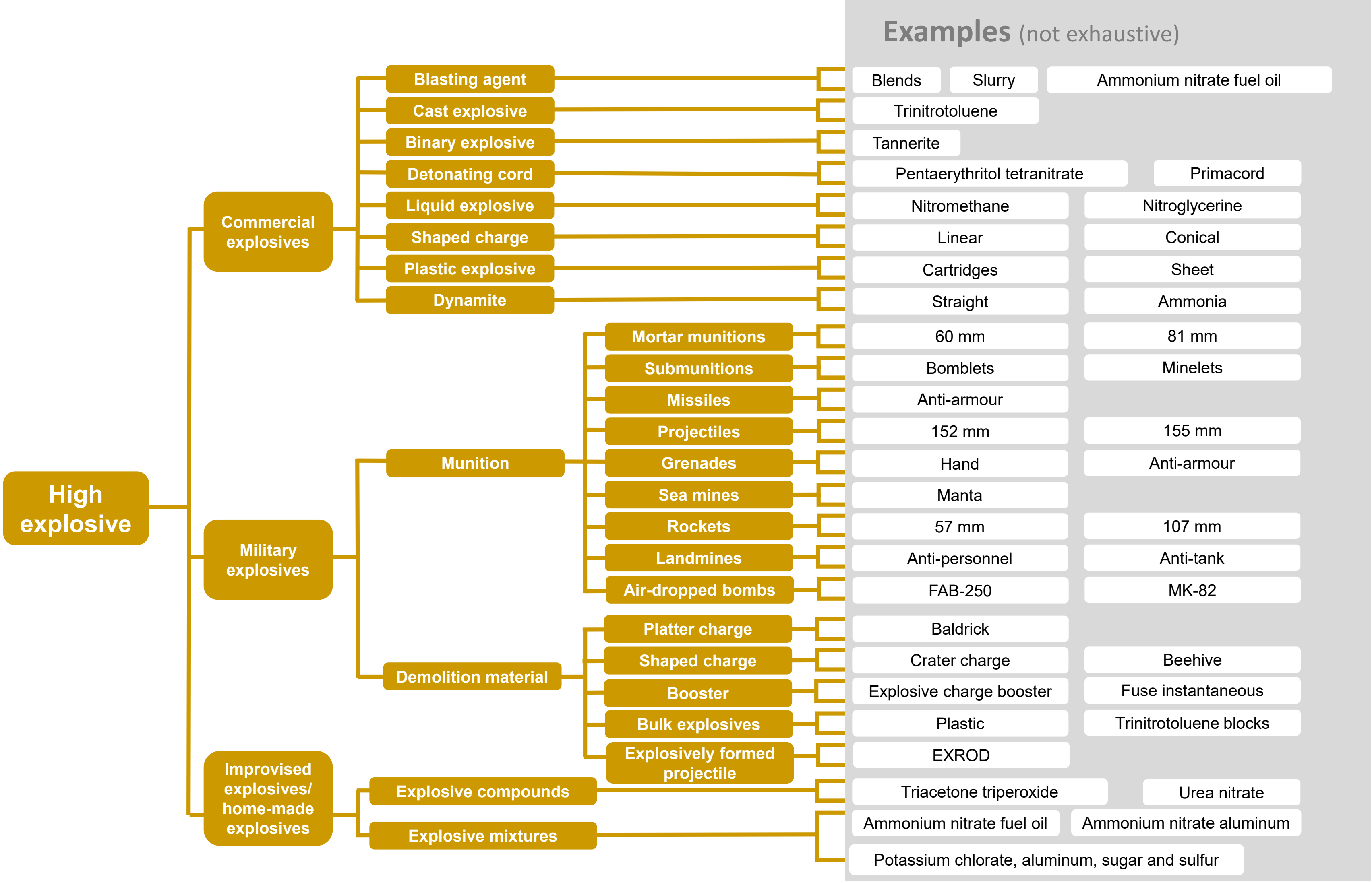
The main charge is the explosive charge which is provided to accomplish the end result in a munition.

Examples for end results are bursting a casing to provide blast and fragmentation, splitting a canister to dispense submunitions or producing other effects for which the charge may be designed.

The main charge can be:

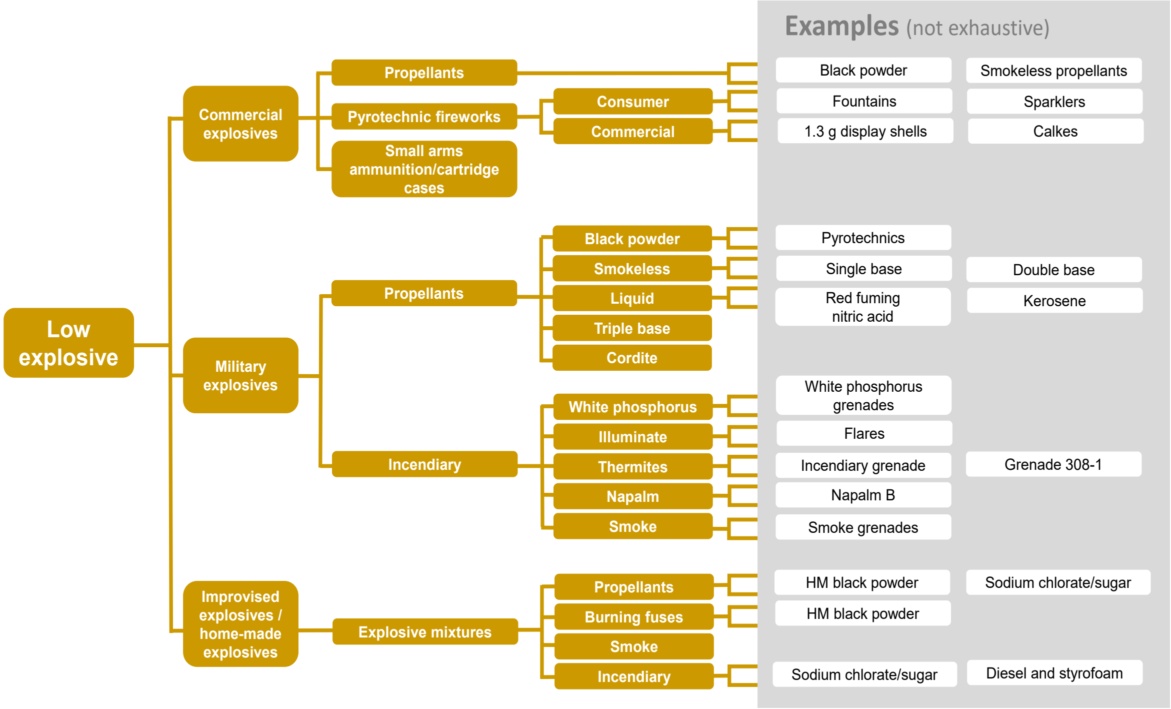
- High explosives
- Low explosives
- Main charge configuration

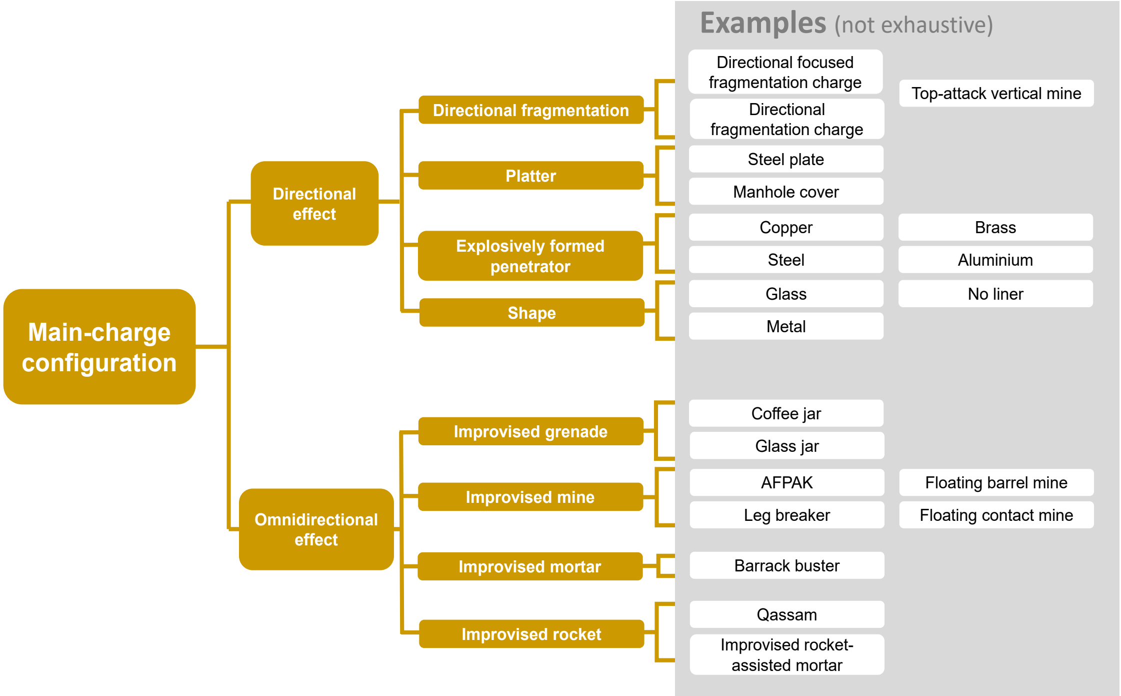




Examples (not exhaustive)

- High explosive
  - Commercial explosives
    - Blasting agent: Blends; Slurry; Ammonium nitrate fuel oil
    - Cast explosive: Trinitrotoluene
    - Binary explosive: Tannerite
    - Detonating cord: Pentaerythritol tetranitrate; Primacord
    - Liquid explosive: Nitromethane; Nitroglycerine
    - Shaped charge: Linear; Conical
    - Plastic explosive: Cartridges; Sheet
    - Dynamite: Straight; Ammonia
  - Military explosives
    - Munition
      - Mortar munitions: 60 mm; 81 mm
      - Submunitions: Bomblets; Minelets
      - Missiles: Anti-armour
      - Projectiles: 152 mm; 155 mm
      - Grenades: Hand; Anti-armour
      - Sea mines: Manta
      - Rockets: 57 mm; 107 mm
      - Landmines: Anti-personnel; Anti-tank
      - Air-dropped bombs: FAB-250; MK-82
    - Demolition material
      - Platter charge: Baldrick
      - Shaped charge: Crater charge; Beehive
      - Booster: Explosive charge booster; Fuse instantaneous
      - Bulk explosives: Plastic; Trinitrotoluene blocks
      - Explosively formed projectile: EXROD
  - Improvised explosives/ home-made explosives
    - Explosive compounds: Triacetone triperoxide; Urea nitrate
    - Explosive mixtures: Ammonium nitrate fuel oil; Ammonium nitrate aluminum; Potassium chlorate, aluminum, sugar and sulfur


Low explosive
Commercial explosives
Propellants
Pyrotechnic fireworks
Consumer
Commercial
Small arms ammunition/cartridge cases
Military explosives
Propellants
Black powder
Smokeless
Liquid
Triple base
Cordite
Incendiary
White phosphorus
Illuminate
Thermites
Napalm
Smoke
Improvised explosives / home-made explosives
Explosive mixtures
Propellants
Burning fuses
Smoke
Incendiary
Examples (not exhaustive)
Black powder
Smokeless propellants
Fountains
Sparklers
1.3 g display shells
Calkes
Pyrotechnics
Single base
Double base
Red fuming nitric acid
Kerosene
White phosphorus grenades
Flares
Incendiary grenade
Grenade 308-1
Napalm B
Smoke grenades
HM black powder
Sodium chlorate/sugar
HM black powder
Sodium chlorate/sugar
Diesel and styrofoam

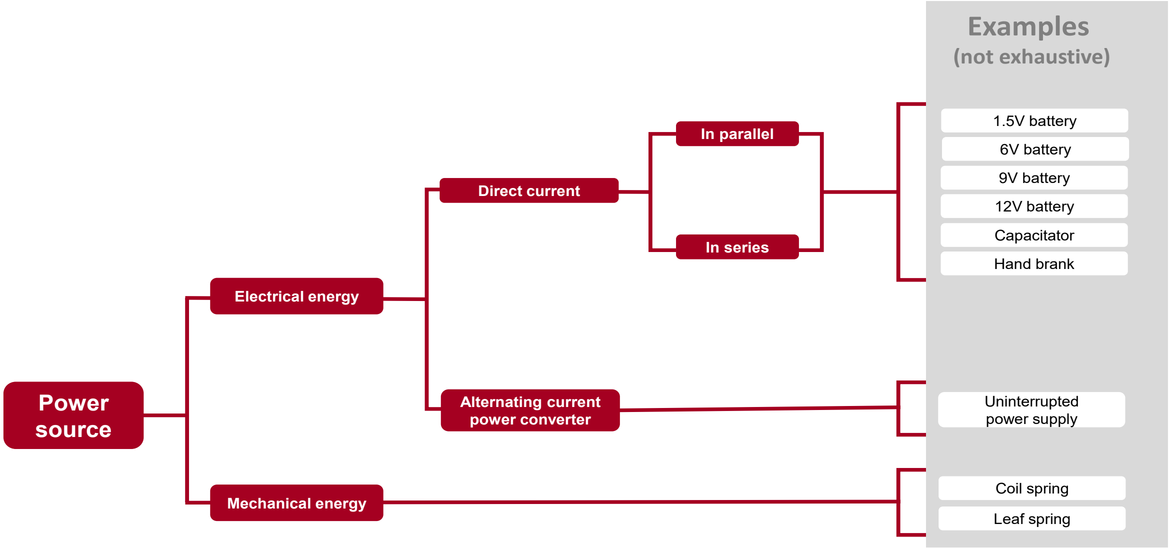

Main-charge configuration
Directional effect
Directional fragmentation
Platter
Explosively formed penetrator
Shape
Omnidirectional effect
Improvised grenade
Improvised mine
Improvised mortar
Improvised rocket
Examples (not exhaustive)
Directional focused fragmentation charge
Top-attack vertical mine
Directional fragmentation charge
Steel plate
Manhole cover
Copper
Brass
Steel
Aluminium
Glass
No liner
Metal
Coffee jar
Glass jar
AFPAK
Floating barrel mine
Leg breaker
Floating contact mine
Barrack buster
Qassam
Improvised rocket-assisted mortar

Power source

A device that stores or releases electrical or mechanical energy. The key elements of information about a power source are its type and source, number of batteries and their configuration (series or parallel), its voltage (if electrical) and how it is connected to close an IED switch.

The power source can be:

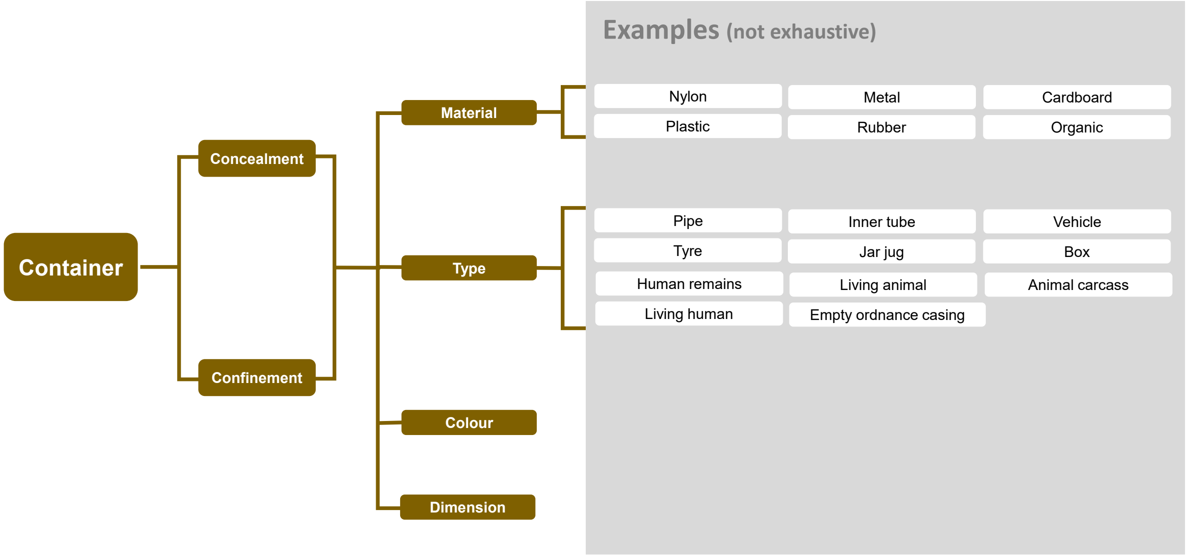
- Electrical energy
- Mechanical energy



Container

A container can be a:

- Concealment
- Confinement



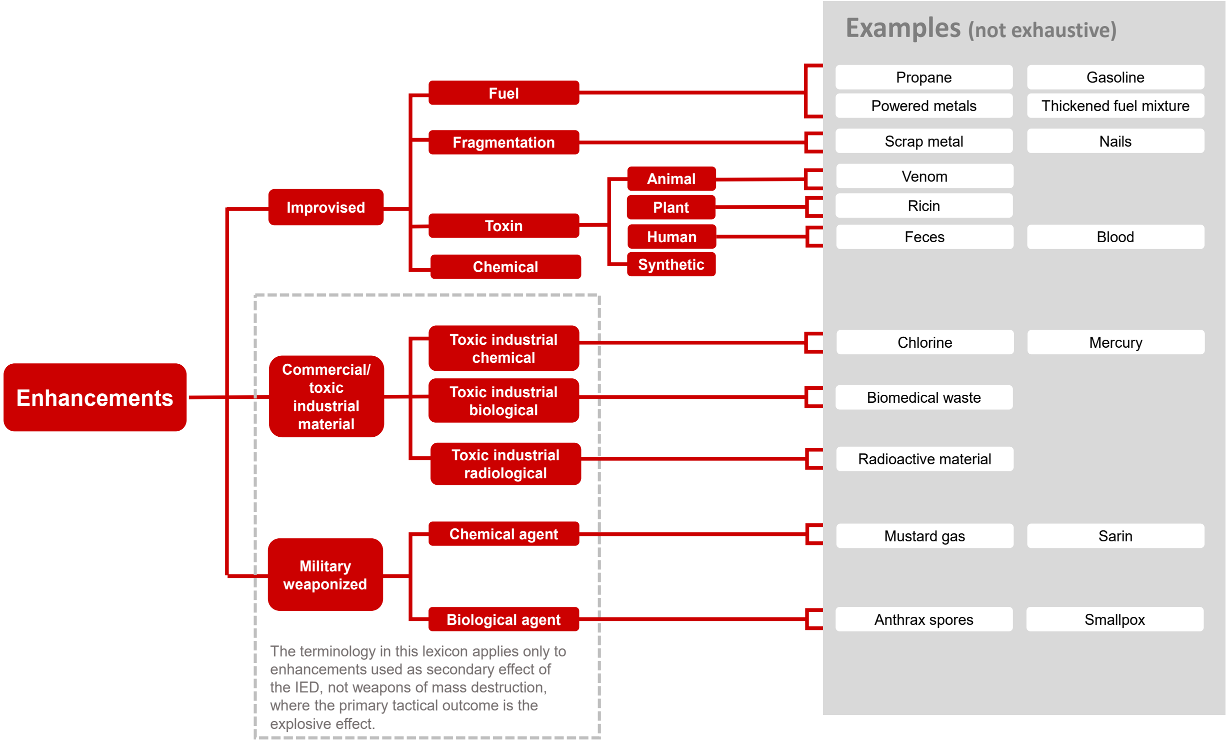
Enhancements

An enhancement is an optional, deliberately added component, as opposed to a secondary hazard which modifies the effects of the IED.

The IED would be effective yet produce a different measurable result if this material were not added. The effect can be additional physical destruction, proliferation of dangerous substances (e.g. radiation, chemicals) or other results to enhance the effect of the IED.

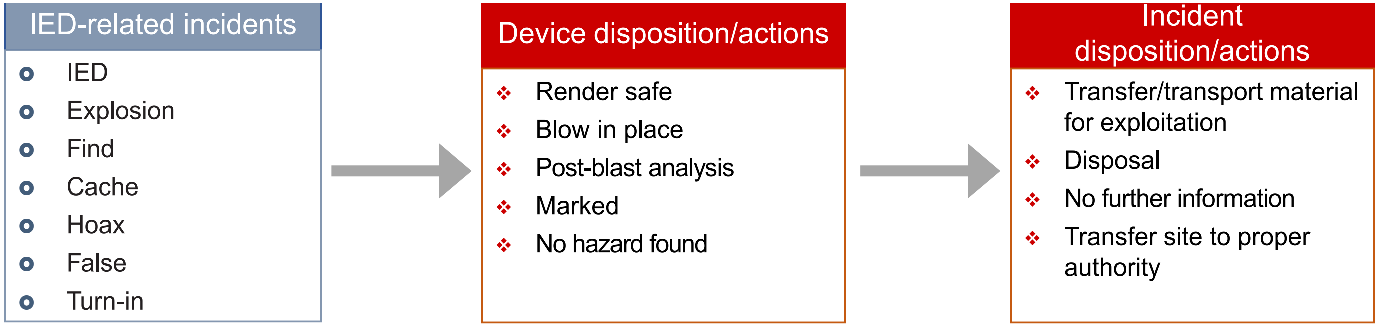
The enhancement can be:

- Improvised
- Commercial/toxic industrial material
- Military weaponized



The terminology in this lexicon applies only to enhancements used as secondary effect of the IED, not weapons of mass destruction, where the primary tactical outcome is the explosive effect.

A.5. Supporting terminology for IED incidents



IED-related incidents

- IED
- Explosion
- Find
- Cache
- Hoax
- False
- Turn-in

Device disposition/actions

- Render safe
- Blow in place
- Post-blast analysis
- Marked
- No hazard found

Incident disposition/actions

- Transfer/transport material for exploitation
- Disposal
- No further information
- Transfer site to proper authority

Site exploitation
A series of activities to recognize, collect, process, preserve and analyse information, personnel and/or materiel found during the conduct of operations.

Technical exploitation
The application of scientific methods to gain further knowledge and insight from materiel and information. It enables commanders and staff to gain fidelity and understanding of the operational environment through the collection of data, information and intelligence.

This includes biometric, forensic and document and media exploitation (DOMEX) capabilities.

A.6. Glossary

Term	Abbreviation	Definition
Air domain		The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible.
Alternating current	**AC**	Electric current that flows through a circuit in both directions with the change in direction occurring with a well-defined and specified frequency.
Anti-aircraft		An IED primarily intended to damage or destroy aircraft and/or their payload.
Anti-armour		An IED that utilizes a directional explosive effect primarily intended to penetrate armoured vehicles.
Anti-explosive ordnance disposal	**Anti-EOD**	An IED primarily intended to kill or wound EOD personnel or to counter render-safe procedures.
Anti-first responder		An IED primarily intended to kill or wound first responders such as police/law enforcement, medics and firefighters.
Anti-infrastructure		An IED primarily intended to damage or destroy physical infrastructure such as pipelines, communications towers, bridges, buildings, utility lines and/or facilities such as electrical transformers or water pump houses.
Anti-personnel		An IED primarily intended to kill or wound people.
Anti-vehicle		An IED primarily intended to damage or destroy vehicles, and is not designed to penetrate a vehicle's armour.
Anti-vessel		An IED primarily intended to damage or destroy maritime vessels and/or their payload.
Armed		In a state of readiness for initiation. Any safety devices have been eliminated but the device has not received a sufficient or proper stimulus to cause it to fire.
Arming switch		A switch that prevents an IED from arming until an acceptable set of criteria has occurred and subsequently effects arming and allows functioning.
Associated components		Components that are: 1) part of an IED or improvised weapon system; 2) the tools required to produce the components; or 3) precursors to the manufacture of IED components to include explosives.
Atmospherics		The environmental mood of an area – how a place looks, sounds, tastes, feels and smells – relative to a baseline. Changes in the atmosphere of a community or individual can indicate imminent hostile action, such as an IED attack. The most obvious indicators are the sudden absence of normal routines, patterns and attitudes of the local populace or the presence of abnormal activity.

Term	Abbreviation	Definition
Attack geography		A description of the road segment, buildings or foliage selected as the site of the attack or explosive device. Understanding the geography will aid in determining how the enemy uses the terrain to channel tactical response, slow friendly movement or prevent pursuit of enemy force.
Binary explosive		An explosive formed by combining two non-explosive materials (an oxidizer and a fuel).
Biological agent		A microorganism that causes disease in personnel, plants or animals or causes the deterioration of materiel.
Blasting accessory		Devices and materials used in blasting. Examples are cap crimpers, tamping bags, blasting machines and blasting galvanometers.
Blasting agent		An explosive material which meets prescribed criteria for insensitivity to initiation. Generally, a non-detonator-sensitive explosive that must be initiated by a booster to detonate. May be configured in cartridge form or as a mass of explosive material prepared for use on site without packaging.
Blasting cap/ detonator		A device containing a sensitive explosive intended to produce a detonation wave. Can be either electric or non-electric.
Bomb threat		A declaration, indication or warning that an explosive device will be used to inflict injury or damage at a specified location or target.
Booster		A high explosive element sufficiently sensitive so as to be actuated by small explosive elements and powerful enough to cause detonation of the main charge filling (initiator > booster > main charge).
Borne		For IEDs, borne is a descriptor that includes a delivery method as an employment component. For example, a vehicle-borne IED is not simply an IED emplaced in a vehicle. It is an IED integrated into a vehicle with an intent to strike external targets. Currently, this condition is used to describe vehicle-, person- and animal-borne IED systems.
Bulk explosives		Manufactured explosive charges in their original packaging or that have been removed from weapons or munitions.
Cache		A space in which resources are concealed. It may be used, before, during or after an incident and may be static or mobile.
Cast explosive		Any explosive poured in liquid form and allowed to harden.
Chemical agent		A chemical substance which is intended for use in military operations to kill, seriously injure or incapacitate mainly through its physiological effects. The term excludes riot control agents when used for law enforcement purposes, herbicides, smoke and flame.

Term	Abbreviation	Definition
Chemical reaction		A switch using the reaction of chemical compounds to provide a delay before starting the initiation train.
Clock mechanism		The internal working parts of a clock used in an improvised manner to function an IED.
Collapsing circuit		A switch which utilizes a circuit designed to detect a failure in an active circuit by monitoring voltage or amperage levels on the target circuit (wire being cut or battery drained).
Command		A type of switch that is activated by the attacker to control the moment of initiation.
Command wire IED	**CWIED**	A switch where the firing point and contact point are separate but joined together by a length of wire. A command wire may contain multiple power sources located near both the firing point and the contact point to overcome the resistance in the length of the wire.
Commercial explosives		Explosives produced and used for commercial, industrial or recreational applications.
Component material sourcing		The process of determining the origin (e.g. production facility, person, geographic location or specific country of origin) of collected material, such as IED components.
Concealment		Materials used to prevent the discovery of an IED by visual inspection. May also be used to add fragmentation.
Condition as found		Refers to the state of readiness of a device to arm, fire or function at the time of discovery.
Confinement		A vessel used to hold the main charge together. May also be used to add fragmentation.
Consumer electronics		Electronic components, readily available in the consumer marketplace and not specifically identified in the schema (not purpose built for telecommunication purposes).
Crush wire		Contact point(s) spanning a length of wire that function an IED when crushed.
Custom radio-controlled		A purpose-built radio-controlled circuit board.
Delay		A mechanical, electric or explosive train component that introduces a controlled time delay in some phase of the arming or functioning of an initiation system.
Detonating cord		A waterproof, flexible fabric tube containing a high explosive designed to transmit the detonation wave.
Direct current	**DC**	Electric current that flows through a circuit in just one direction.
Directional effect		Type of main charge configuration where the explosive effect is channelled to an intended area.

Term	Abbreviation	Definition
Directionally focused fragmentation charge	**DFFC**	Any device designed to explosively propel ball bearings or other fragmentation in an extremely narrow pattern in an aimed direction. Intact DFFCs will always involve fragmentation being held in a concave pattern (using a resin or plaster or similar material).
Directional fragmentation charge	**DFC**	Any device designed to explosively propel ball bearings or other fragmentation in a cone shaped ("shotgun type") pattern.
Domain		A sphere of activity, interest or function. Domains are useful concepts for visualizing and characterizing the physical environment.
Dormant		In mine warfare, the state of a mine during which a time delay feature in a mine prevents it from being actuated.
Dual-tone multi- frequency	**DTMF**	A pairing of transmitter and receiver utilizing dual tones and multiple frequency hardware that allows for precision arming and firing, thus preventing unintended firing.
Dynamite		A high explosive used for blasting, consisting essentially of a mixture of, but not limited to, nitroglycerin, nitrocellulose, ammonium nitrate, sodium nitrate and carbonaceous materials.
Electric		An initiator whose function is initiated by an electrical impulse that creates heat or a spark.
Electromagnetic		The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems and platforms.
Electronic countermeasures	**ECM**	The use of electronic systems to detect, jam or disable radio signals that could trigger remote-controlled explosives, preventing detonation and enhancing operational security.
Electronic initiator		An electric initiator containing an electronic component which only allows the initiator to be used when paired with a blasting machine that is capable of sending a compatible passcode.
Elevated		IED emplaced above the surface: hanging from an overpass, on a roof and so on.
Emplaced		An IED that is statically placed where it is likely to be encountered by the intended target.
Enhancements		An optional, deliberately added component as opposed to a secondary hazard which modifies the effects of the IED. The IED would be effective yet produce a different measurable result if this material were not added. The effect can be additional physical destruction, proliferation of dangerous substances (e.g. radiation, chemicals) or other results to enhance the effect of the IED.

Term	Abbreviation	Definition
Environmental conditions		The ambient meteorological and oceanographic conditions that can affect the functioning and performance of IEDs, the sensors used to detect them and IED countermeasures.
Estimated net explosive weight	**NEW**	A reference to the estimated weight of the main charge which can be derived from observations of the blast effects, crater characteristics or container dimensions.
Event signature development/ device profiling		The process of analysing the tactical and technical identifiers of an IED incident to support force protection, targeting, prosecution and sourcing.
Exploding bridge wire	**EBW**	An initiator or system in which a very high-energy electrical impulse is passed through a bridge wire, literally exploding the bridge wire and releasing thermal and shock energy capable of initiating a relatively insensitive explosive in contact with the bridge wire.
Explosion		A nuclear, chemical or physical process leading to the sudden release of energy.
Explosive compounds		Homogeneous substances whose molecules contain within themselves the oxygen, carbon and hydrogen necessary for combustion.
Explosive ordnance	**EO**	All munitions and improvised or clandestine explosive devices containing explosives, propellants, nuclear fission or fusion materials, and biological and chemical agents.
Explosive ordnance disposal	**EOD**	The process to detect, locate, access, diagnose, render safe/neutralize, recover, exploit and dispose of explosive or improvised explosive threats.
Explosive train		A succession of initiating and igniting elements arranged to cause a charge to function.
Explosively formed projectile	**EFP**	Specially designed main charge configuration incorporating an explosive charge with a concave metal liner which by the force of the charge reshapes the plate into a high velocity metal slug capable of penetrating armour (Misznay-Schardin effect).
False		An IED-related incident that is incorrectly identified though reported as an IED, which is subsequently categorized as a false alarm after positive EOD.
Find		An item of EO, weapons or other terrorist/insurgent or military equipment/resources, found either during a planned search or during other operations.
Firing switch		The component that initiates the explosive train.

Term	Abbreviation	Definition
Force protection	**FP**	The cyclic process of detecting threats and hazards to United Nations personnel, facilities, resources, operations, activities, and assessing their risk in order to apply proactive and reactive risk mitigation measures.
Fragmentation		Small objects designed to be accelerated by explosive forces.
Fuel		An incendiary material designed to enhance the burning and visual effect of the device.
Fuel oxidizer explosive mixture	**FOX**	An explosive mixture of fuel and oxidizer that deflagrates (very rapid burning) or detonates creating a blast wave.
Global system for mobile communication	**GSM**	European standard for digital cellular networks.
Heat		A type of initiator that serves as an igniting element through the application of heat. This may include direct heat to a sensitive explosive.
High explosive		A chemical compound or mixture that is capable of supporting or sustaining a detonation wave. High explosives do not require confinement as they combust instantaneously producing heat, gas, a rapid expansion of matter and a detonation/shock wave.
High-power cordless phone	**HPCP**	High power refers to devices with greater than 1 watt.
Hoax		An incident that involves a device fabricated to resemble and intended to simulate an improvised explosive device or a false warning of the presence of an improvised explosive device, in order to elicit a response.
Hot bridge wire detonator		A detonator that utilizes heat from a bridge-wire to heat an explosive compound to the point of detonation.
Human tip		Information provided by an individual or individuals, usually in advance of an IED-related incident, possibly in a confidential manner regarding an IED, IED-related materials or associated personnel. This information can be received from, but not limited to, the local populace or government, a member of a law enforcement agency, or an inside source.
IED-related incidents		An event that involves one or more of the following IED-related actions/activities: IED, explosion, find/cache, turn-in, hoax or false.
Ignitor		A device designed to produce a flame or a spark to initiate an explosive train.

Term	Abbreviation	Definition
Improvised explosive device	**IED**	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. Refers to a type of IED incident that involves a complete functioning device. (United States Department of Defense definition)
Improvised explosive device disposal	**IEDD**	The process to detect, locate, access, diagnose, render safe/neutralize, recover, exploit and dispose of improvised explosive threats.
Improvised explosive/home-made explosive	**IE/HME**	Non-standard explosive mixtures/compounds which have been formulated/synthesized from available ingredients. Most often utilized in the absence of commercial/military explosives.
Improvised grenade		An improvised weapon, using military or home-made components, designed to explode when a restraint is removed (usually thrown, but can be projected).
Improvised initiator		An initiator which is made from readily available materials. An improvised initiator does not contain any part of a commercially manufactured initiator. Items used in an improvised initiator may include household and mass-produced items which can be local procured. Items used are typically easy to purchase and readily available. Items could include, but are not limited to pens, syringes, metal tubing, light bulbs and so on.
Improvised mortar		An improvised weapon, using military or home-made components, designed to launch an explosive charge to the target.
Improvised rocket		An improvised weapon, using military or home-made components, designed to propel an explosive charge to the target.
Incendiary		Chemical mixtures and flammable liquids that cause fire.
Initiator		Any component that may be used to start a detonation or deflagration. An initiator will be categorized as either a detonator or an igniter.
Land domain		The Earth's land area, including its man-made and natural surface and subsurface features and its interfaces and interactions with the atmosphere and the oceans.
Landmine		In landmine warfare, an explosive munition designed to be placed under, on or near the ground or other surface area and to be actuated by the presence, proximity or contact of a person, land vehicle, aircraft or boat, including landing craft.

Term	Abbreviation	Definition
Light bulb/ flash bulb		Devices used as electric initiators that incorporate an improvised use of the bulb flame to initiate primary or low explosives.
Liquid explosive		An explosive material in a liquid state. Examples include nitric acid esters (e.g. nitroglycerin, nitroglycol) and ethylene glycol.
Long-range cordless telephone	**LRCT**	LRCTs use base stations matched to one or more handsets to connect to or operate independently of regular telephone lines over long ranges. High gain antennas can further boost range and some systems can transmit and receive faxes and connect to the Internet or satellite communications.
Low explosive		A chemical compound or mixture that is designed to deflagrate (burn rapidly) and generally require confinement to explode.
Main charge		The explosive charge which is provided to accomplish the end result in a munition or improvised device. Examples for end results are bursting a casing to provide blast and fragmentation; splitting a canister to dispense submunitions; or producing other effects for which it may be designed.
Main charge configuration		The arrangement or design of the main charge and other materials (usually metal) to create an effective weapon to attack personnel, vehicles or structures.
Malfunction		A failure to function as designed. Would cover partial detonations and low orders.
Maritime domain		The oceans, seas, bays, estuaries, islands and coastal areas, including the littorals.
Mechanical energy		Stored or applied energy that results in physical movement of an IED component.
Meteorological		Conditions involving phenomena of the atmosphere or weather.
Method of discovery		The manner in which a unit located a device, components or improvised weapon (e.g. via visual observation, working animal, sensor or human tip).
Method of employment		A description of how the device and target were brought in proximity of each other.
Military explosives		Explosives manufactured for military use.
Military police	**MP**	A military unit charged with conducting provost duties within the United Nations peacekeeping missions.
Missile		A self-propelled munition whose trajectory or course is controlled while in flight.

Term	Abbreviation	Definition
Misznay-Schardin effect		A characteristic of the detonation of a broad sheet of explosive. The explosive blast expands directly away from (perpendicular to) the surface of an explosive.
Modified initiator		A commercial or military manufactured initiator which has been altered or combined with other items which were not a part of the original manufactured design. Examples include converting a manufactured non-electric initiator into an electric initiator and converting a manufactured electric initiator into a non-electric initiator.
Mortar munition		The complete munition comprises a projectile and propellant system, to be fired from the mortar. The projectile normally comprises fuze, body filled with high explosives or other filling, obturator and a tail assembly.
Movement/ anti-disturbance		A switch designed to complete a circuit as two parts make contact when an IED is physically disturbed (tilt, vibration).
Munition		A complete device charged with explosives; propellants; pyrotechnics; initiating composition; or chemical, biological, radiological or nuclear material, for use in military operations, including demolitions.
Munroe effect		A focusing of blast energy caused by a hollow or void cut into the surface of an explosive.
Non-electric		An initiator that functions by other than electric means (e.g. friction, chemical, impact).
Non-functional		IEDs that were mechanically broken, damaged by an unknown source, incomplete, improperly assembled, and/or with inoperable power sources.
Obstacle creation		An IED primarily intended to create an obstacle to impede movement or channel movement into a desired location.
Omnidirectional effect		An aspect of main charge configuration where the explosion expands in all directions.
Parallel circuit		Multiple batteries or other power sources which have their positive terminals connected to one another and their negative terminals connected to one another which results in an increase in the available current.
Percussion		An initiator that serves as an igniting element when mechanically struck.
Person-borne IED	**PBIED**	An IED worn, carried or housed by a person, either willingly or unwillingly.
Personal mobile radio	**PMR**	A two-way radio system used for communication over short distances used to maintain contact with a central base station.
Plastic explosive		A malleable or flexible explosive at room temperature.

Term	Abbreviation	Definition
Platter charge		The use of an explosive to propel a metal plate towards a target in a manner where the plate remains intact (Misznay-Schardin effect).
Poised		A device in which a counter setting has been run down to "1" and is ready to detonate at the next actuation.
Power source		A device that either stores or releases electrical or mechanical energy. The key elements of information about a power source are its type/source, number of batteries and their configuration (series or parallel), its voltage (if electrical) and how it is connected to close an IED switch.
Pressure		A switch designed to function when pressure is applied in a predetermined direction (e.g. plate, tube, plunger, crush wire).
Pressure and pressure release		A method for activating the device that occurs as a result of either application or reduction of pressure.
Pressure release		A switch for activating the device that occurs as a result of reductions in pressure.
Primary device		The most tactically significant IED within an incident. The primary may not be the first IED encountered.
Projected		Thrown or cast forward by human, mechanical or environmental means (such as tides or river currents).
Projectile		An object, projected by an applied exterior force and continuing in motion by virtue of its own inertia. Projectiles can have a variety of fillers including explosives or chemicals.
Projectile initiating		An initiation method designed to rely solely on the impact of an object, such as a bullet or other fast-moving item, into an explosive component.
Propellant		An explosive material that normally functions by burning to produce a controlled release of gases used for propulsion purposes.
Proxy		A person (unwitting or coerced) who acts as a means of delivery of an IED.
Pull		A switch that functions when a person applies tension to a firing mechanism, such as pulling a spring. The tension causes an action that releases a firing pin or activates an electrical or electronic switch.
Purpose of device		The intended immediate or direct tactical effect of the IED.
Pyrotechnic delay		A pyrotechnic device added to a firing system which transmits the ignition flame after a predetermined delay.
Radio-controlled	**RC**	The use of radio signals to remotely control a device.

Term	Abbreviation	Definition
Radio-controlled IED	**RCIED**	A switch initiated electronically by wireless means consisting of a transmitter/receiver.
Radiological dispersal device	**RDD**	An improvised assembly or process, other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage or injury.
Rocket		Self-propelled ordnance that uses gas pressure from rapidly burning propellant to transport a payload (warhead) to a desired target.
Role of IED		Identifying enemy use of IEDs as a primary, secondary or subsequent form of attack.
Sea mine		An explosive device laid in the water with the intention of damaging or sinking ships or of deterring shipping from entering an area. The term sea mine does not include devices attached to the bottom of ships or to harbour installations by personnel operating underwater.
Search and detect sensors		Equipment which detects, measures and may indicate and/or record objects and activities by means of energy or particles emitted, reflected or modified by objects for the purpose of identifying IED activity.
Secondary device		One or more additional IED used to attack individuals or vehicles after the initial event.
Sensor		A switch used to detect change in heat, light, movement, vibration, electromagnetic frequency, sound or magnetic field.
Sensor defeat		Methods and technologies incorporated into the device construction and employment for the purpose of defeating detection or identification methods and friendly TTPs.
Series circuit		Multiple batteries or other power sources which have one positive terminal connected to the negative terminal of the next power source which results in an increase in the available voltage.
Series-parallel circuit		A combination of one or more series circuits and parallel circuits.
Shaped charge		A main charge configuration incorporating explosives shaped to concentrate explosive force utilizing the Munroe effect in a particular direction in order to cut or penetrate.
Shock tube detonator		A thin, plastic tube of extruded polymer with a layer of powdered high explosive deposited on its interior surface that propagates a detonation wave to the blasting cap.

Term	Abbreviation	Definition
Signature characterization		The process of identifying distinct characteristics of a device or its components. A signature is a distinctive basic characteristic or set of characteristics that consistently recurs and uniquely identifies a piece of equipment, material, activity, individual or event. Signatures also refer to characteristics relating to the manufacture of the device.
Submunition		Any munition that, to perform its task, separates from a parent munition. Submunitions are classified as bomblet, grenades or mines.
Suicide		When an IED is initiated by the attacker at a time of their choosing in which they intentionally kill themselves as part of the attack or possibly to deny capture.
Support to prosecution		The process of associating related people, places, devices or equipment to an individual for evidentiary purposes in a law enforcement investigation or court of law.
Suspect or suspicious package		Any item found under suspicious or unusual circumstances. A suspect or suspicious package necessitates a bomb squad response.
Switch		A device for making, breaking or changing a connection in an IED. A single switch can have multiple functions (e.g. arming and firing).
Tactical characterization		The manner in which an IED incident is planned and conducted (tactical design) and the intent (purpose of device).
Tactical design		The specific design of an IED attack, including but not limited to position of the IED, type of IED, method of actuation, type of road segment used, concealment technique, use of secondary devices, the time of day and so on. Tactical design addresses the questions of "why here, why now and why in this way". Terms used to describe a specific type of device or component of a device (e.g. vehicle-borne IED) are often used to describe all or part of the tactical design.
Tactics, techniques and procedures	**TTPs**	The established methods and practices used by military personnel to carry out operations and accomplish missions.
Targeting		The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.
Technical categorization		A description of an IED using a hierarchical construct to identify its key components. The components identified in this categorization are the elements from which technical and forensic information is recovered and exploited.

Term	Abbreviation	Definition
Technical intelligence	**TECHINT**	Intelligence derived from the collection, processing, analysis and exploitation of data and information pertaining to foreign equipment and materiel for the capabilities and developing countermeasures designed to neutralize an adversary's technological advantages.
Tension		A switch that functions when tension is applied to a firing mechanism, such as pulling a tripwire. The tension causes an action that releases a firing pin or activates an electrical or electronic switch.
Tension release		A switch that functions when tension is released – such as when a taut wire or cord is cut or broken – releases a spring-loaded firing pin or closes electrical contacts initiating the device.
Terrestrial		The Earth's land area, including its man-made and natural surface and subsurface features and its interfaces and interactions with the atmosphere and the oceans.
Tilt		A switch that allows current to flow to the output wires after a conductive material (e.g. mercury or a ball bearing) is moved enough (up/down, left/right) to flow onto the switch contacts, completing the circuit.
Time		A type of switch that functions after a set time.
Time chemical		A chemical timing switch using a corrosive chemical with a known decomposition rate that is designed to destroy a physical restraint on a triggering device to start the initiation train.
Time electronic		A timing switch using a commercial or improvised electric timer or integrated circuit to start the initiation train.
Time fuze/ safety fuze		A pyrotechnic burning at a certain rate used to transmit a flame to the non-electric detonator or a low explosive charge with a predetermined delay.
Time mechanical		A timing switch constructed or modified so that physical contact between two parts of the timing mechanism completes an electrical circuit.
Toxic industrial biological	**TIB**	Any biological material manufactured, used, transported or stored by industrial, medical or commercial processes which could pose an infectious or toxic threat.

Term	Abbreviation	Definition
Toxic industrial chemical	**TIC**	A chemical developed or manufactured for use in industrial operations or research by industry, government or academia, for example, pesticides, petrochemicals, fertilizers, corrosives, poison and so on. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities or areas dangerous for human use. Hydrogen cyanide, cyanogen chloride, phosgene and chloropicrin are industrial chemicals that can also be military chemical agents.
Toxic industrial material	**TIM**	A generic term for toxic or radioactive substances in solid, liquid, aerosolized or gaseous form that may be used or stored for use, for industrial, commercial, medical, military or domestic purposes. Toxic industrial material may be chemical, biological or radioactive and described as toxic industrial chemical, toxic industrial biological or toxic industrial radiological.
Toxic industrial radiological	**TIR**	Any radiological material manufactured, used, transported or stored by industrial, medical or commercial processes, for example, spent fuel rods, medical sources and so on.
Toxin		A toxic substance produced by and derived from plants and animals or created synthetically.
Trend and pattern analysis		The practice of analysing information to discern a pattern, trend or relationship between activities or behaviours, to predict future enemy actions, target threat networks, interdict IED supply chains and plan intelligence surveillance, reconnaissance activities.
TTP development		Using the lessons learned from an IED-related incident to refine and improve the tools and methods used during all missions in which an IED may be encountered (e.g. convoys; tactical suppression efforts; intelligence, surveillance and reconnaissance; counter-IED and so on).
TTP identification		An IED primarily intended to cause a reaction by forces in an effort to learn and understand employed tactics. This knowledge is then used by the attacker to plan new attacks incorporating the lessons learned to inflict additional casualties or to avoid countermeasures. The IED need not function to serve this purpose. A suspicious package can have TTP identification as its intended outcome.
Turn-in		An IED-related incident where an IED or associated component are turned over to the proper authority.

Term	Abbreviation	Definition
Unarmed		A device in which all safety devices and features are present and functioning to prevent the device from starting its arming sequence. It is the condition of an IED when it is safe for handling, storage and transportation.
Unattended package		An unattended package is defined as an item of unknown origin found without suspicious circumstances. A bomb squad response may not be required.
Underbelly		An IED emplacement in which the device is intended to target the underside of a vehicle.
Unmanned aircraft systems	**UAS**	A system whose components include the necessary equipment, network and personnel to control an unmanned aircraft.
Unmanned underwater systems	**UUS**	That system whose components include the necessary equipment, network and personnel to control an unmanned underwater vehicle.
Vehicle		A self-propelled, boosted or towed conveyance for transporting a burden on land, sea or through air or space.
Vehicle-borne IED	**VBIED**	A device placed or fabricated in an improvised manner on or within a vehicle incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract.
Victim-operated IED	**VOIED**	A switch that is activated by an unsuspecting individual. These switches rely on the intended target to carry out some form of action that will cause it to function.
Visual observation		Attained or maintained by sight, done or executed by sight only and relating to or employing visual aids.
Weapons technical intelligence	**WTI**	Intelligence derived from the processes and capabilities that collect, exploit and analyse asymmetric threat weapons systems to enable material sourcing, support to prosecution, force protection, signature characterization and targeting of threat networks.

Annex B. Search

Military search capabilities are developed to locate and detect concealed threats.[1] Although this annex was developed based on military search activities, it is intended that this material is equally applicable to search activities undertaken by military, police or civilians who are employed in a peacekeeping operation with an improvised explosive device (IED) threat.

Search is a capability that is an enabler to explosive ordnance disposal/improvised explosive device disposal (EOD/IEDD). An all arms search team, qualified to conduct route search or even intermediate search, and specialized search teams will often work in concert with an EOD/IEDD team. The ability to locate and detect IEDs is crucial within any counter-explosive threat capability. In order to defeat the device, a proactive rather than reactive approach is required to put pressure on the IED network. A key enabler in these efforts is locating and detecting IEDs and their components before they can achieve their desired effects.

This annex refers to search rather than "military search" or "engineer search", unless in regard to specialized search capabilities. It also focuses on search in the land domain and does not refer to riverine or maritime search activities.[2]

B.1. Tactics, techniques and procedures

Since the tactics, techniques and procedures (TTPs) of search teams are often sensitive security or classified, details of such TTPs are not provided in this annex. Such information can be utilized by those who employ IEDs to counter these techniques and procedures and exploit this knowledge to design IEDs to target search personnel. Troop-contributing countries should not be required to alter/amend their own national search TTPs for United Nations missions unless due to changes of the perpetrator TTPs or based on information gained through theatre-specific training and with concurrence of troop-contributing countries, with the understanding that they must be:

- Effective, efficient and safe, leading to the detection and location of threats.
- In line with the mission mandate.
- In line with search principles (section C).

While search TTPs are a national responsibility, troop-contributing countries providing search capabilities within a United Nations mission are encouraged to share search TTP best practices and related lessons learned to the benefit of all mission search personnel.

[1] Conventional weapon systems, items of explosive remnants of war and improvised explosive threats and components thereof, in particular IEDs.

[2] This annex does include vessel search as a capability under advanced search but refers to the search of vessels which are moored and not under way.

B.2. Search objectives

Search is a key enabler in support of United Nations operations. It provides a means to shape and control the environment in which United Nations capabilities are active or where there are security interests across an operational theatre. Search can be broken down into two distinct types: pre-emptive search and protective search.

Pre-emptive search

The objectives of pre-emptive search are to gather information and material for exploitation, to deprive a perpetrator of resources and to secure material for possible future evidential value. The detailed applications are as follows.

- **Gain intelligence.** Information and material gathered during search operations is often a rich source of intelligence. Alongside intelligence, surveillance and reconnaissance assets, this information allows for the creation of a full intelligence picture and informs of threats in the theatre, especially when it comes to the technical exploitation of explosive threats or hazards.
- **Deny resources and opportunity.** United Nations commanders can gain or maintain the initiative in an operational environment through the reduction of a perpetrator's capability to deliver explosive threats. Through the discovery and interdiction of weapons and explosives, it retains freedom of action for friendly forces, while reducing the extent to which a perpetrator can impose their will through attacks with conventional or IEDs.
- **Secure material for exploitation.**[3] In order to identify perpetrator networks and their key capabilities and vulnerabilities, United Nations forces must be able to collect, exploit and disseminate findings concerning adversarial technology and tactics. United Nations forces engaged in operations must act and be seen to act in accordance with international and national legal frameworks in the collection of forensic evidence.[4] Documentation, material handling and forensic awareness must adhere (where tactically viable) to identified best practices to assist any subsequent exploitation and possible prosecution. The following exploitation philosophy should be applied after assessment by those involved as best suits the situation. The exploitation philosophy involves three parts:
    - Safety
    - Forensic integrity
    - Continuity of evidence

The application of this philosophy requires balancing these against each other to select the most suitable course of action, with safety considerations inevitably carrying more weight than others. The prioritization of the three parts of the exploitation philosophy depends on the key operational actions defined by the commander. In every case, safety is always the priority in all exploitation activities.

Protective search

The objective of protective search is to protect potential search targets, as well as protecting United Nations/unit assets. This is achieved through the following:

[3] Level 1 exploitation, section 4.5.

[4] The use of the word "evidence" in this publication refers to an intent to potentially utilize recovered materiel and information to prepare forces for subsequent operations or legal purposes. The term is used in a general sense, and no attempt is made to define what would constitute evidence in a particular theatre for a nation.

- **Force protection.** Protective measures taken to mitigate hostile actions against friendly personnel, resources, facilities and critical information. Search should be considered a key element of United Nations force protection. Protective search provides means of reducing risk to United Nations personnel and enables freedom of action/movement.
- **Protection of pre-planned events**. Protective search provides advanced security to protect potential targets during pre-planned events, according to the level of threat and the estimated consequence of failure. By executing a pre-emptive search, United Nations forces can mitigate explosive threats in the target area, route or building.
- **Protection of critical infrastructure**. Search can be utilized to protect critical military, governmental, industrial and civil infrastructure within the theatre of operation, providing vital protection to the economy and well-being of the host nation.

B.3. Search principles

Success of search as a capability is largely due to the procedures founded on four basic principles that can be adapted to suit the operational tempo and tactical situation. The procedures and techniques involved in all search activities should be based on the following principles, regardless of the exact details of the actions to be taken. The level of assurance provided varies on the level of training and equipment available. The search principles are:

- **Systematic.** All search activities regardless of the level at which they are conducted are systematic in their nature, which is achieved by the approach being careful, deliberate, detailed and methodical. The systematic search principle applies equally to the planning, coordination and execution of all search operations.
- **Flexible.** TTPs, as well as equipment, must be adapted to an evolving operational/tactical environment where the perpetrator constantly changes his methods of operation in an attempt to either trap, deceive, mislead or misdirect search capabilities. All procedures should be flexible but consistent in their application without compromising safety.
- **Focused.** All planned search operations should be targeted and have clearly defined objectives that contribute to the mission. The political, cultural, social and economic impact of any intended search operation should be addressed when considering the objectives.
- **Safe.** Search activities are conducted within the margin of acceptable level of risk for the operation and the assessment associated with it as determined by the commander.

B.4. Search effects

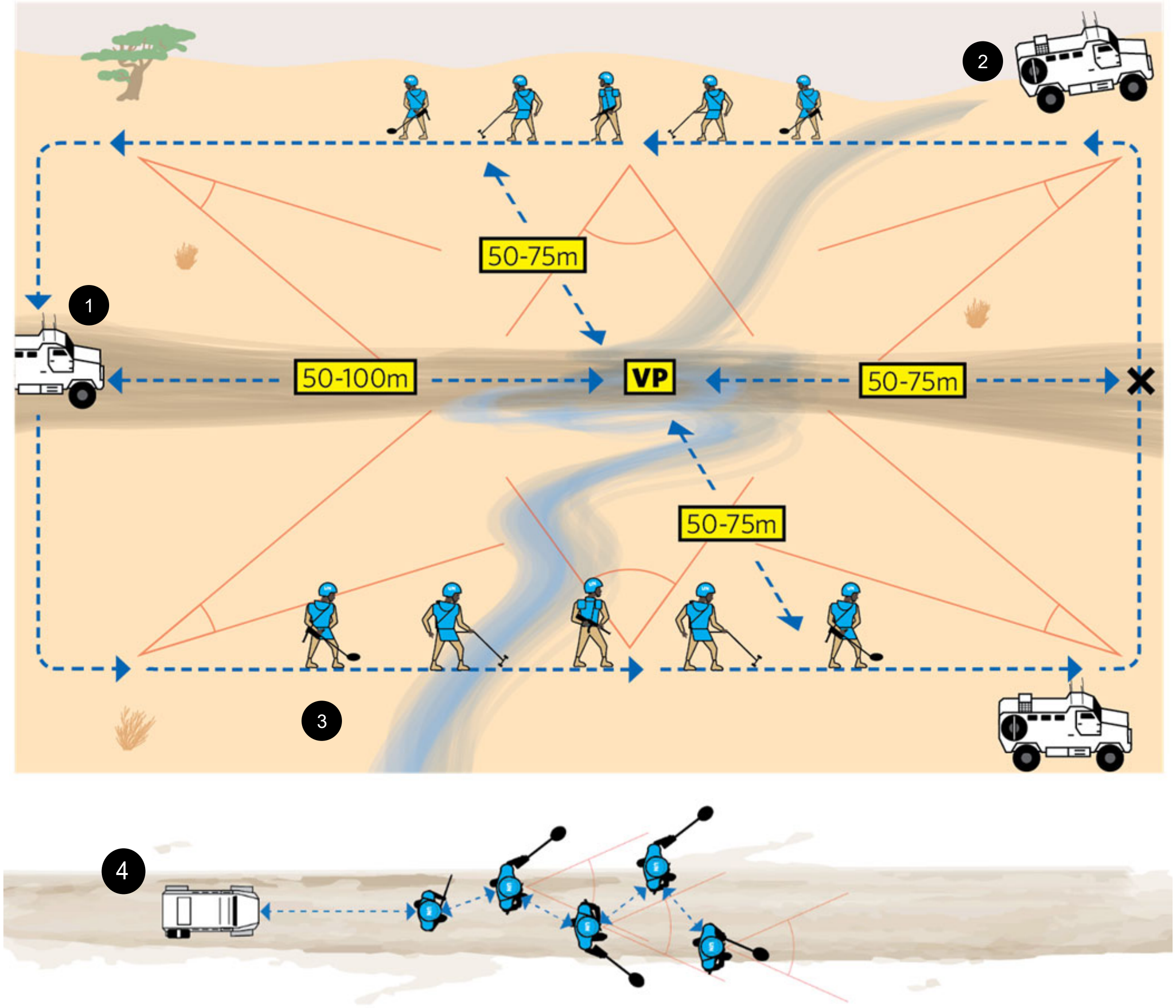
Search can support and deliver effects to reinforce a United Nations commander's intent in protective and pre-emptive operations from the tactical to the strategic level. This is supported through the following effects:

- **Shape** the conditions for future operations.
- **Deter** adversaries.
- **Deny** resources and freedom of action for the perpetrators.
- **Protect** United Nations or supported forces and secure freedom of action and movement.
- **Exploit** technical and tactical intelligence gained through search operations.

B.5. Framework for search operations

All search operations can be planned and executed using a four-stage framework.

Figure B.1
Four stages of search operations



1. **Arrival and short stop point**. Lead vehicle stops in an unpredictable and assessed safe area 75–100 m from the vulnerable point (short stop point). Top gunner conducts 360-degree visual search. 5/25 m checks conducted.
2. **Dominate the ground** around the vulnerable point. Deploy flanking patrols in vehicles or on foot to likely firing points. Conduct 5/25 m checks at over watch positions.
3. **Isolation.** A physical 360-degree search out to a distance of 50–75 m around the vulnerable point is conducted to locate any command wires or other physical links (command pull) running into the vulnerable point.
4. **Search through.** Under the direction of the commander, search the route in a “V” formation from the halt location through the assessed vulnerable point to locate the presence of any IEDs. Overlap of detector search heads must be maintained to avoid gaps within the searched area.

Secure the incident control point

Any search operation must have an incident control point that has been previously secured and searched. It is where the incident control point is established and the resources and means for the search mission are centralized and controlled.[5]

Isolate and dominate the target

Before the target is searched, it must be isolated from outside influences by dominating the surrounding terrain. Persons and vehicles should be directed to a segregated area to be searched away from others and outside interference. Routes and buildings must be searched under the protection of a security cordon, so that nobody gets in or out when the search is taking place. Isolating the target means also isolating the effects of an explosion. For example, surrounding a person or vehicle search area with protective works.

Execute the search

Search procedures are being applied and all findings documented.

Secure and hand over your search target

If the mission requires it, a searched target can be handed over to appropriate authorities for further activities. Therefore, a searched person is allowed to enter a controlled area and must remain supervised to be considered "searched". A searched building must have its access points controlled to be deemed "searched and secure". A searched route must be under continuous surveillance to be deemed "searched and secure". If a target has been searched and after that is no longer under control it must be considered "unsearched and unsecured".

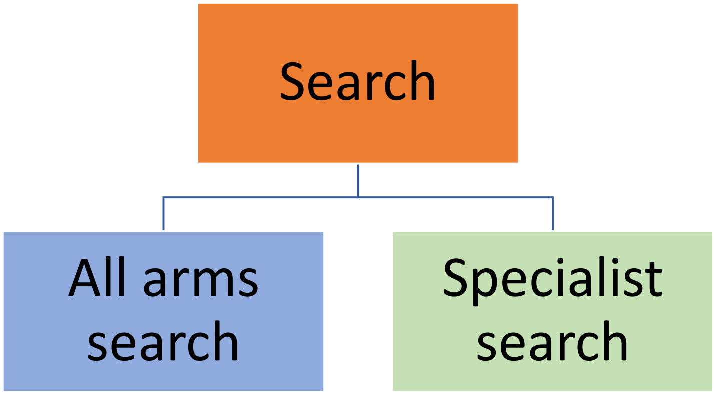
B.6. Defining search capabilities

Search is the capability to locate specific targets using intelligence assessments, systematic procedures and appropriate detection techniques. Specified targets may include people, vehicles, routes, areas, locations, buildings and material resources employed by a perpetrator or to be used by friendly forces. Search involves the planning, management and application of systematic procedures and appropriate techniques to confirm the presence or absence of concealed threats such as conventional weapon systems, items of explosive remnants of war and IEDs and components thereof. Search can be employed in support of the full spectrum of operations.

For the purpose of this annex the search capabilities are outlined in the following organization chart to provide an overview of the full spectrum of search capabilities that the United Nations may employ.

[5] See *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual*.

Figure B.2
Search capabilities (1)

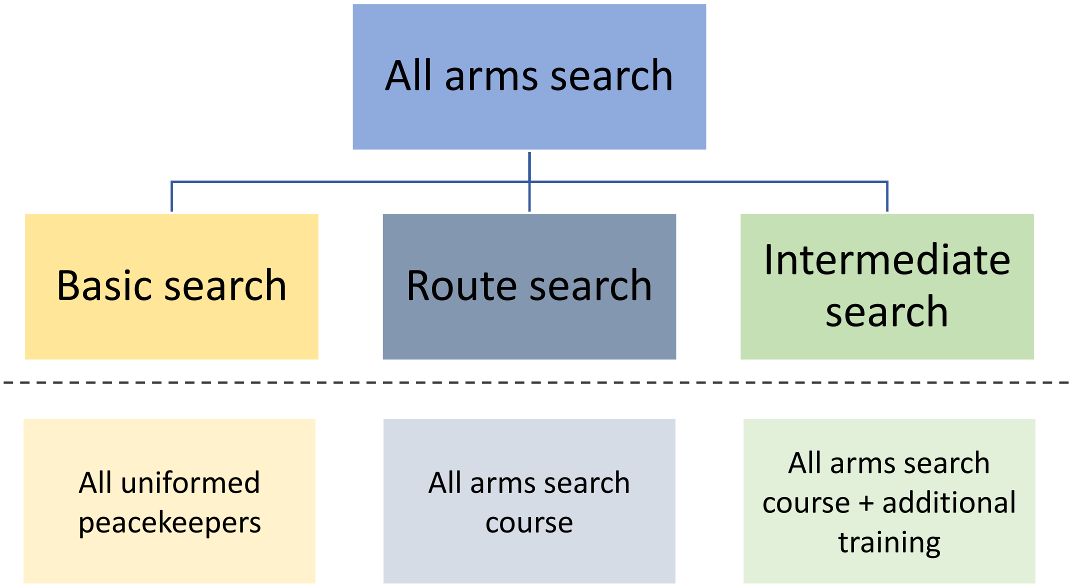


In its broadest terms search can be broken down into all arms search capabilities and specialist search capabilities.

- **All arms search.** Search capabilities employed by non-specialist members of a unit. There are different levels of all arms search capabilities.
- **Specialist search.** Search capabilities employed by advanced search personnel trained, equipped and qualified to do so. Information regarding specialist search is contained in the *United Nations Military Engineer Unit & CET Search and Detect Manual.*

Within all arms search there are three levels of search capability, as shown in figure B.3.

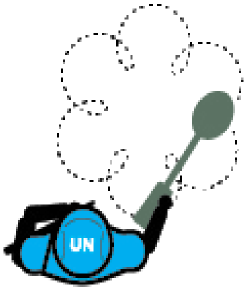
Figure B.3
Search capabilities (2)



Basic search. The lowest level of search capability. It provides all personnel with a fundamental understanding of the prevalent threat and those measures they as individuals can adopt to optimize force protection. Basic search training normally covers search awareness but may also include other procedures. Basic search teams are normally ad hoc. Basic search capabilities may or may not involve the use of search equipment and covers the following capabilities:

- **Search awareness.** Search awareness is the most basic skill level and is utilized for force protection. A search aware person is normally trained to conduct searches of a person or vehicle or conduct a basic threat assessment (subject to a periodic threat update), 5-metre and 25-metre checks and workplace checks.
- **Vehicle search.** The search of a vehicle to detect vehicle-borne IEDs, IED components, weapons, ammunition or any other object that a perpetrator has attempted to conceal. A vehicle search involves an initial check of persons and their vehicles, from which an assessment can be made as to whether any further search is required. Vehicle search within basic search involves initial checks and can involve primary searches.
- **Person search.** Search of a person to detect components, weapons, ammunition or any other exploitable intelligence that a person may attempt to conceal.
- **Property search.** A physical and visual search of areas and property where the concealment of prohibited items is possible. This can include but is not limited to the search of baggage, buildings and urban areas/street furniture without the use of specialist equipment in a low-threat environment.

Basic search is a capability that is required by every peacekeeper and should be part of the basic military training.



Route Search.[6] A unit-level search capability used in the search of assessed portions of a route for the presence of explosive ordnance (EO) and in line with the threat for which the teams have been trained. It may involve the knowledge and skills to be able to assess a vulnerable point or vulnerable area and determine how best it should be searched to isolate areas and locate IEDs so they can be rendered safe by IEDD or other suitably qualified personnel or alternatively confirm the absence of IEDs at a given vulnerable point or vulnerable area. Route search can be a United Nations mission specific or stand-alone capability depending on mission requirements. Route search can be used on roads, tracks, railway lines and along any mounted or dismounted direction of travel. Route search of railway lines can be a route search team task but may require an advanced search team depending on the threat assessment and HEAT factors, as described below.

Military personnel having completed the all arms search team training are capable of conducting a route search.

Intermediate search. Undertake all basic and route search tasks in line with HEAT factors with key additional capabilities of intermediate search being area search and building search. An increased level of training and specialist equipment is required at this level of capability compared to route

[6] Sometimes referred to as patrol search.

search and basic search. Area search involves the systematic search of a target area with the aim of locating items that have been lost, misplaced, discarded or hidden.

Area search can occur in rural environments or open areas in an urban environment. An area search can either locate illegal resources or provide assurance that the area contains no specified targets or resources. A building search refers to the systematic search of a structure or facility to locate threat items therein. Area searches and building searches are typically undertaken as part of planned operations in conjunction with a security element that first secures a cordon around a given target area or location prior to a search element systematically searching for explosive threats, weapons and/or components thereof.

NOTE: Area search or building searches may be an intermediate or advanced search capability. Typically, part of an intelligence-led operation is the distinction between such operations being intermediate or advanced. The search requirement is determined by a detailed assessment.

Intermediate search can be conducted by military personnel having completed the all arms search training and received additional training.

Certain types of searches, such as route, area and building searches, can be either an all arms task or a specialized task. In each case, defined training and possibly equipment support is required for these capabilities to be employed by all arms. The criteria that are used to determine if these search activities are an all arms task or a specialized task are determined by an assessment of the following factors and based on the mission-level threat assessment.

Figure B.4
HEAT

H azardous nature of the operating environment

E quipment requirements are specialized

A ssurance level required is high

T hreat level is high

Figure B.5
Categories of search

The following summarizes the various search tasks as being all arms or specialized. The colour codes used are:

🟩	**Permitted**
🟨	**Possibly all arms or specialized determined by HEAT factors and/or training level**
🟥	**Not permitted**

Search capability	All arms	Specialist
Search awareness	🟩	🟩
Vehicle search	🟩	🟩
Person search	🟩	🟩
Property search	🟩	🟩
Route search	🟨	🟩
Area search	🟨	🟩
Building search	🟨	🟩
Protective building search	🟥	🟩
Aircraft search	🟥	🟩
Vessel search	🟥	🟩
Hazardous environment search	🟥	🟩
Secondary vehicle search	🟥	🟩

B.7. Search personnel and equipment

- **Search adviser** (see section 3.3).
- **All arms search teams**

  Each member of a search team must be suitably trained and equipped for the role and search capability they are to provide during the search activities for that mission. At a minimum, a search team should be composed of the following members:

  ○ **Search team commander.** The search team commander commands the team, coordinates with other agencies and works in close coordination with the search adviser.

  ○ **Search team scribe.** The second in command of the search team. Responsible for providing assistance to the search team commander and for completing the necessary documentation. This includes notes on what the search team is looking for, any items or evidence found and for ensuring all legal documents are in the possession of the team or are completed for judicial evidence in the future.

  ○ **Search pairs.** Searchers shall be deployed in pairs with a minimum of two search pairs for safe, effective and efficient operation. Search pairs work under the direction of the search team commander. They must have received the intent, threat and desired effect in the search adviser's orders.

- **Specialized search teams** (see *United Nations Military Engineer Unit & CET Search and Detect Manual*).

The use of specific search equipment will vary depending on the search capability employed. United Nations units requiring a list of equipment scales for various search capabilities need to refer to the relevant COE manual extract, status of unit requirements and memorandum of understanding, as agreed in the mission planning and preparation phase.

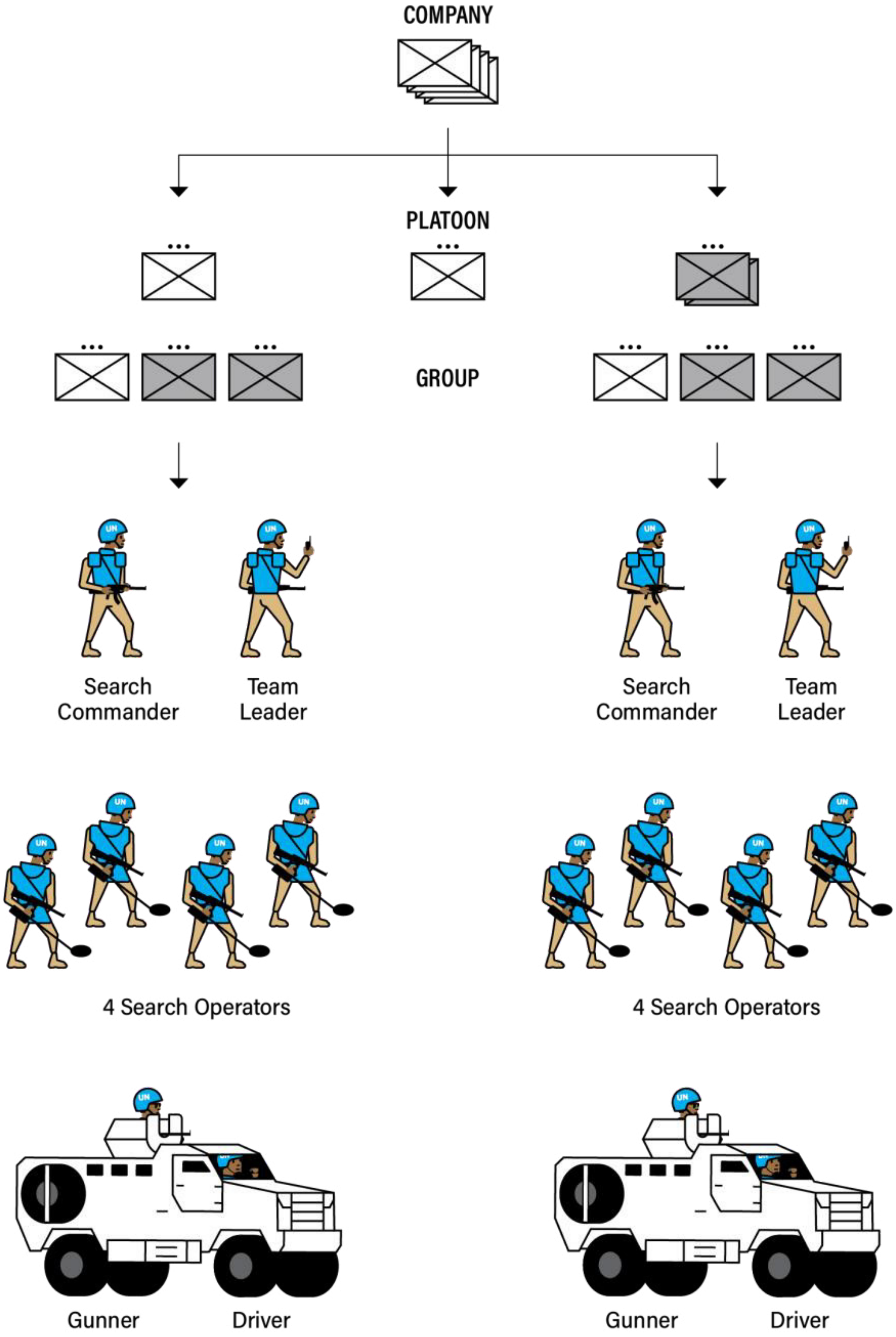
The following table provides major equipment items, which are recommended for an all arms search team:

Category of equipment	Type of equipment	Remarks
All arms search team equipment	Man-portable high-power electronic countermeasure (ECM) (cell/GPS/jammer)	ECM against radio-controlled IED. For units tasked with conducting demounted operations in a radio-controlled IED threat environment. The status of unit requirements should reflect the need for the troop- and police-contributing countries to engage with the mission to programme ECM equipment according to the radio-control threat in theatre.
	Vehicle-mounted ECM (jammer) against remotely activated IEDs	All vehicles operating in an radio-controlled IED threat environment should be equipped with ECM. The status of unit requirements should reflect the need for the troop- and police-contributing countries to engage with the mission to programme ECM equipment according to the radio-controlled threat in theatre.
	Handheld (mine) detector (dual sensor with active metal detection and ground-penetrating radar)	Dual-sensor mine detector for detection of metal and metal-free objects. For the all arms search team in IED threat environments with low-metal-content explosive devices.
	Handheld (mine) detector (active metal detection)	Detectors for larger objects containing metals such as mines and unexploded ordnance, but also IED parts such as pressure plates with a high metal content. For all arms search teams in IED threat environments with high-metal-content explosive devices.

The following table lists items for an all arms search team:

Category of equipment	Type of equipment	Remarks
All arms search team equipment	Handheld bomb/ unexploded ordnance locator (magnetometer to detect ferromagnetic objects)	Detector specifically designed to detect large (buried) objects with a high ferrous content. Mainly used to find unexploded ordnance.
	Handheld cable detector	Metal detector specifically designed to search for (command) wires. For search and detect teams in IED threat environments.
	Machetes	
	Brush saws	
	Under vehicle mirrors	
	Inspection equipment	
	Torches/flashlights	
	Small tool kit	

Figure B.6
All arms search team



B.8. Supporting elements to search teams

The conduct of search operations may require the utilization/tasking of other supporting elements. The following are examples of supporting elements and how they may support search activities:

- **EOD.** Where explosive threats, including explosive ordnance (EO) components or related material are assessed or anticipated to be present, EOD should be incorporated into the search operation. Search teams should have primacy on task until a suspected explosive hazard is discovered. Where possible EOD and search teams should train together, in order to refine understanding of procedures, task handover and minimize risk to life as far as possible.
- **Explosive detection dogs.** When requesting assistance from an explosive detection dog, consideration must be given as to whether the type of dog available will contribute to the search being conducted. Search units should liaise with the military working dog handler to understand the capabilities and limitations of the military working dog assigned to the task prior to conducting operations, as not all dogs may be suited for the type of search being undertaken.
- **Counter radio-controlled electronic warfare.** When available, counter radio-controlled electronic warfare should be utilized in all circumstances to guard against the possibility of a radio-controlled IED threat. Further details on this are provided in the *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual*.
- **Peacekeeping-intelligence, surveillance and reconnaissance.** Where available, intelligence, surveillance and reconnaissance assets are a valuable information source for planning purposes. Aerial imagery and other sources can provide information beneficial to the planning of search operations at all command levels. Further details on this are provided in the *United Nations Peacekeeping Missions Military Peacekeeping-Intelligence Surveillance Reconnaissance (PKISR) Unit Manual*.
- **Geospatial support.** Where geospatial support is available it can provide products beneficial to search operations. Up-to-date maps and aerial photography can be produced in a larger scale with a variety of overlays. Demographics, obstacles, dead ground studies, blueprints, historical and recent IED attacks and all manner of geographical features pertinent to the search area can be highlighted. Search advisers and search team leaders must forge links with those working with geospatial data to ensure that required search products are regularly updated as new data become available.
- **Peacekeeping-intelligence.** The input from U2 at all levels is crucial. The success of a search operation is closely linked to the quality of intelligence provided. The inclusion of intelligence staff at an early stage in the planning process saves time and effort and provides a focused plan from the outset.
- **Law enforcement agencies.** Host nation law enforcement agencies, United Nations police or theatre standard operating procedures may dictate a requirement for the presence of indigenous police forces in support of the search operation. They may also be called upon to provide close liaison on other operations. It is essential that they are accordingly briefed, but not at the expense of operational security.
- **Military police (MPs).** MPs can support search operations using specialized training, equipment and techniques to enable mobility, security, detention and evidentiary chain of custody. MPs may also liaise and take statements from those involved with the search. MPs may provide assistance

in forensic and evidence recovery and/or training and are a key enabler in coordinating with host nation police, if they are to be incorporated in search operations.

- **Interpreters.** Interpreters should always be considered when planning search operations where the native language differs from the language of those conducting the search. In addition to bridging language barriers, they may also gather information from individuals present during the search for reporting purposes. Interpreters may also serve to de-escalate situations by explaining reasons for the conduct of a search. Operational security is paramount when using local interpreters, and information gained must be carefully evaluated.
- **Force protection.** Force protection assets are likely to have a key role in securing the search target/area through domination of the ground and reacting to threats as they arise. Close coordination between the search adviser and the force protection commander during search operations is paramount.
- **Weapons technical intelligence.** Weapons technical intelligence supports exploitation through on-scene forensic collection and analysis processes, as required. Further details are provided in the *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual*.
- **Chemical, biological, radiological and nuclear teams.** Chemical, biological, radiological and nuclear teams support hazardous environment search by providing decontamination, reconnaissance and detection.
- **Transport.** If bulk or multiple finds are expected, transport requirements must be coordinated if additional personnel to load, move and secure the material are deemed necessary. Where circumstances warrant, heavy equipment support may be required.

B.9. Search planning considerations

Search is planned and coordinated in support of the commander’s priorities. Search planning is the process by which the available intelligence is analysed and the appropriate search response identified. Advice from the relevant search adviser should be sought to ensure that appropriate levels of search capabilities are utilized consistent with the perceived threat. Consideration must be given to the collection, custody and movement of recovered items and the subsequent exploitation process.

The level of search capability required is dependent on the known or perceived threat in the theatre of operations and should be tailored to the environmental challenges. Troop-contributing companies should seek to deploy with an appropriate search capability to counter assessed threats, to support the commander’s intent.

The following factors must be considered when planning search operations:

- **Minimize disruption and damage.** The disruption and damage caused by search operations should be proportional to the level of search conducted. Search operations should aim to minimize the disruption to the local population and damage of property. This principle is important to maintaining the goodwill of the local population or at least minimizing the ill will generated. Commanders at all levels have a responsibility to balance the physical and psychological damage caused by search operations with the benefit gained. Compensation of individuals or communities for damage occurring during search operations may be considered by mission/leadership.
- **Rule of law.** Search must be authorized and carried out within the legal framework governing the operation. This framework may include, be drawn from, or refer to, information from

memorandums of understanding, military technical agreements, rules of engagement, standard operating procedures, operating orders, international and host nation law, directives and orders and environmental regulations. National contingents planning search operations must be aware that teams from other troop-contributing countries, including the host nation, may have laws, directives and rules of engagement that are different from their own. Furthermore, the handling of evidence and recovered material must be in accordance with this framework.

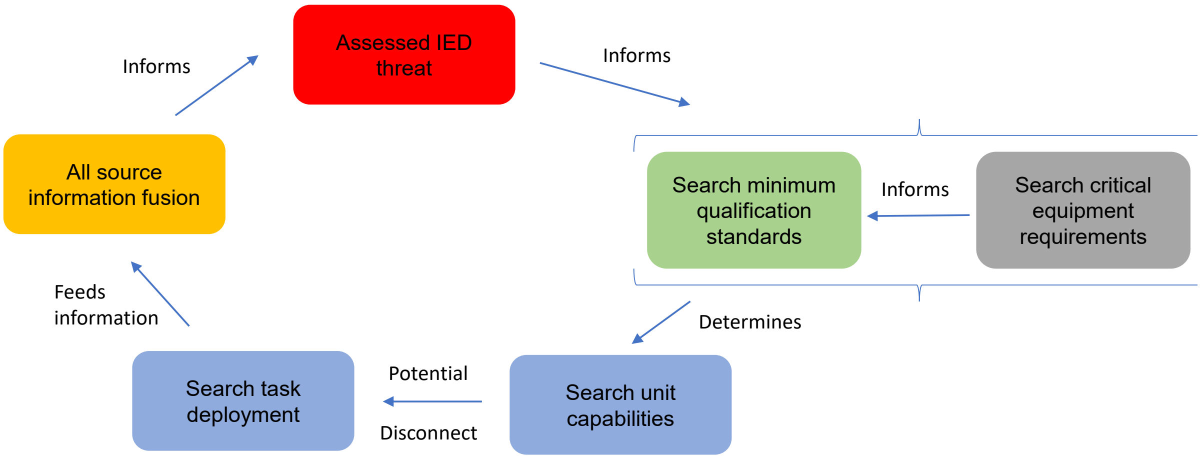
- **Time.** Search operations may be time sensitive and should be planned and conducted in a timely manner relevant to operational imperatives and force protection requirements. Safety and speed must be carefully balanced during planning and execution phases. Operational execution should be timed for optimum effect.
- **Equipment.** Tools and equipment must be appropriate for the level of task being undertaken. As capability deficiencies are identified through changes in the threat and emerging trends, equipment and training must be adapted.
- **TTPs.** Search TTPs must evolve to meet the threat and emerging technologies.
- **Security.** Consideration must always be given to:
    - **Operational security.** The requirement to retain any operational advantage over a perpetrator demands the implementation of the "need to know" principle. Operational security is key so that the possibility of surprise can be preserved.
    - **Tactical security.** Search operations must be conducted with force protection measures appropriate to the perceived threat environment. Force protection measures, including cordons and reaction forces, should be prepared to prevent the escape of target(s).
    - **Information management.**
    - **Documentation.** Search reports may form part of necessary evidentiary or intelligence processes and should be completed during every search operation. These reports may also serve to refute or support any compensation claim or grievance that is submitted. Reports should be adapted to meet local, national or international laws and, where required, be translated into the local language. The authority to conduct a search should be documented on all search reports.
    - **Analysis and feedback.** All available evidence, information and recovered material should be analysed in a timely manner and preserved for future reference where possible. All information collected should be fed into the intelligence chain, to assist in the development of current and future threat analysis, targeting cycles and TTPs.

B.10. Search capability factors in support of IEDD

In relation to IED threat mitigation, search is conducted to locate and isolate emplaced IEDs, to find IEDs prior to emplacement or to find components of IEDs prior to assembly. If this is not possible, it is necessary to find the device prior to initiation. These efforts to mitigate the threat require search activities.

An understanding of the IED threat is essential to identifying the required search capabilities for EOD efforts. Once the assessed IED threat for a mission has been identified, the required search minimum standards and critical equipment requirements can be determined. This is illustrated in figure B.7.

Figure B.7
Search capability factors

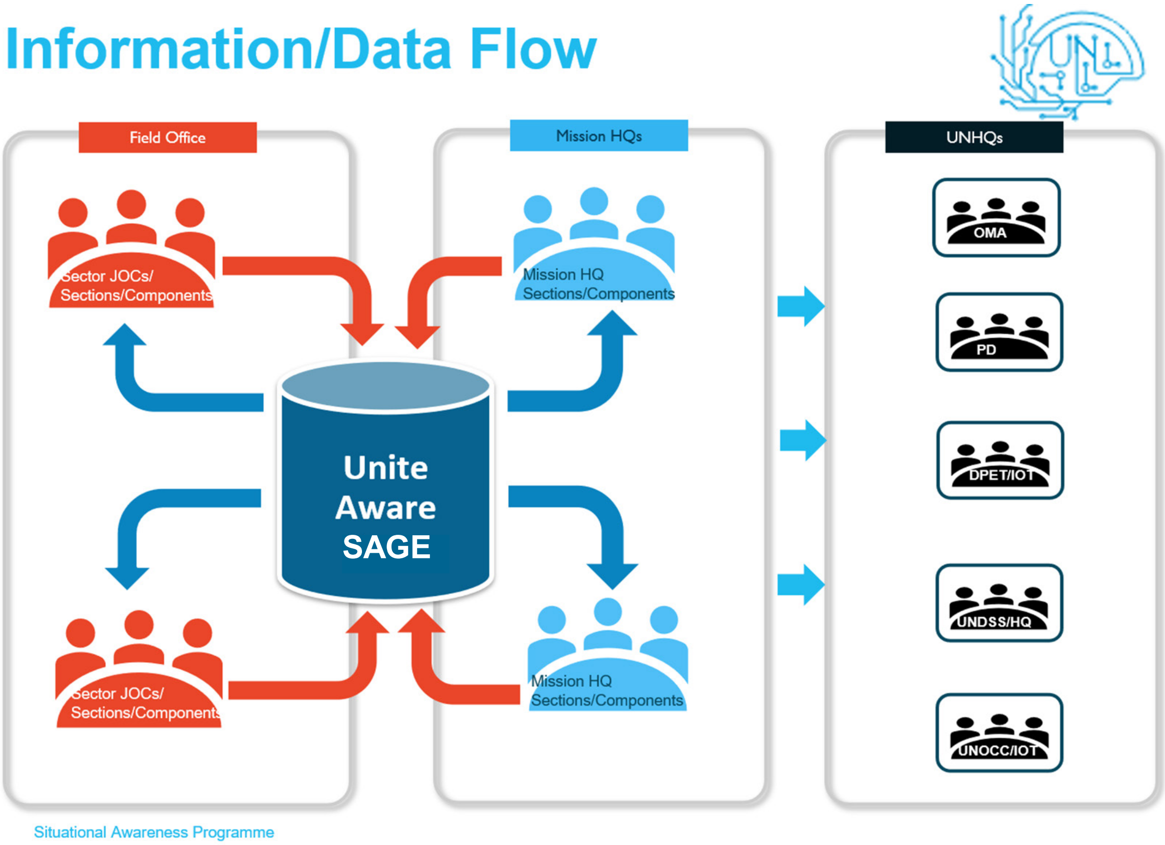


A technical understanding of the type and complexity of the IED threat is necessary to identifying the search equipment required. As an example, the length of command wire in use will influence the type of buried wire detector that is required, and similarly the metallic signature of IED components in use will determine the effectiveness of metal detectors or other buried detectors that a team should deploy with. Some or all of an IED's components may be non-metallic.

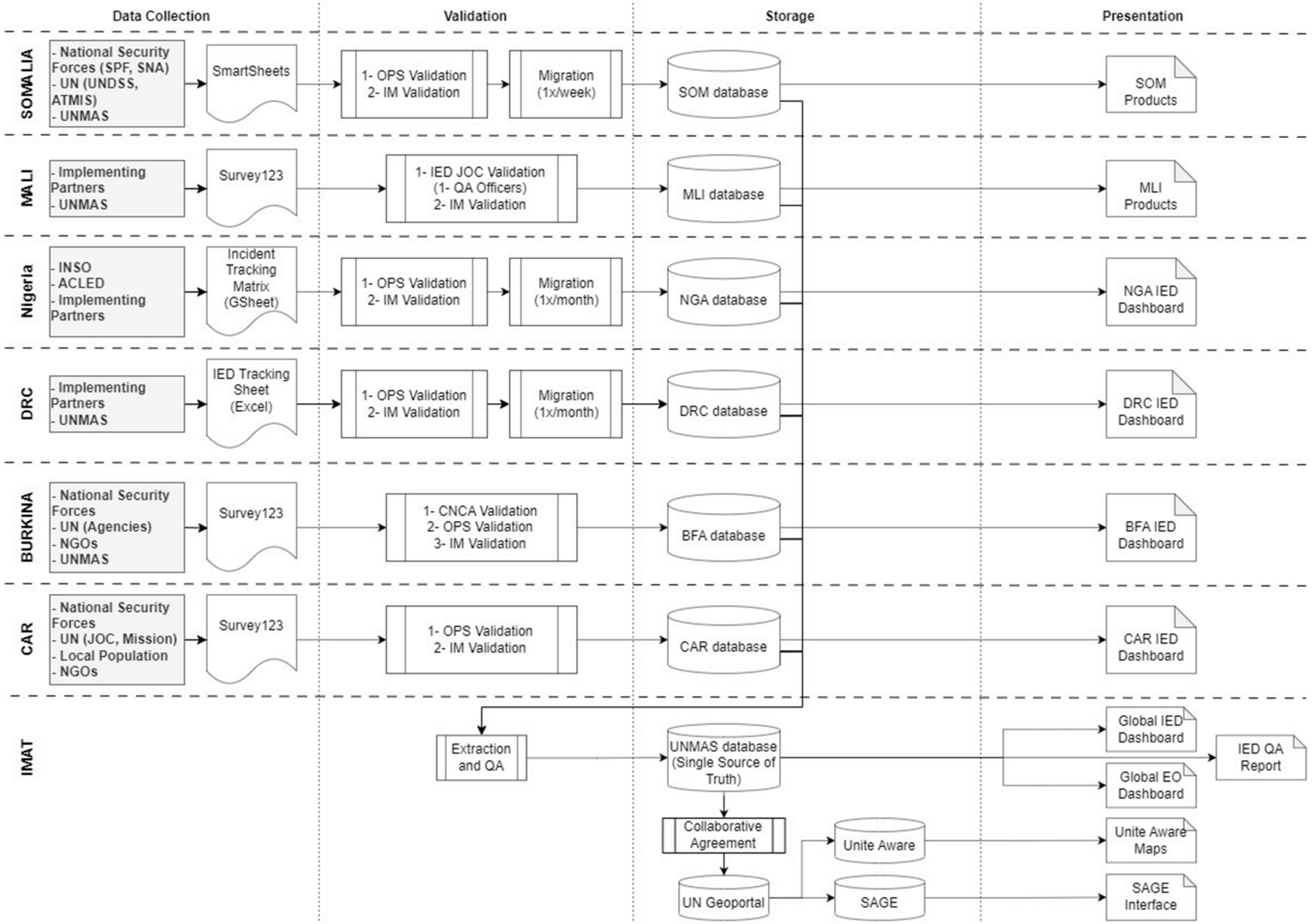
Perpetrators utilizing IEDs will adapt technically and tactically to circumvent search efforts introduced to mitigate IEDs. Such evolution in the IED threat will often require an ongoing evaluation of the search assets required to mitigate such threats (e.g. an evolution in the metallic signature of buried IEDs). The minimum requirements will be determined by the tasks that the search capability is required to be able to undertake. This leads to several search levels which vary according to HEAT factors.

Annex C.

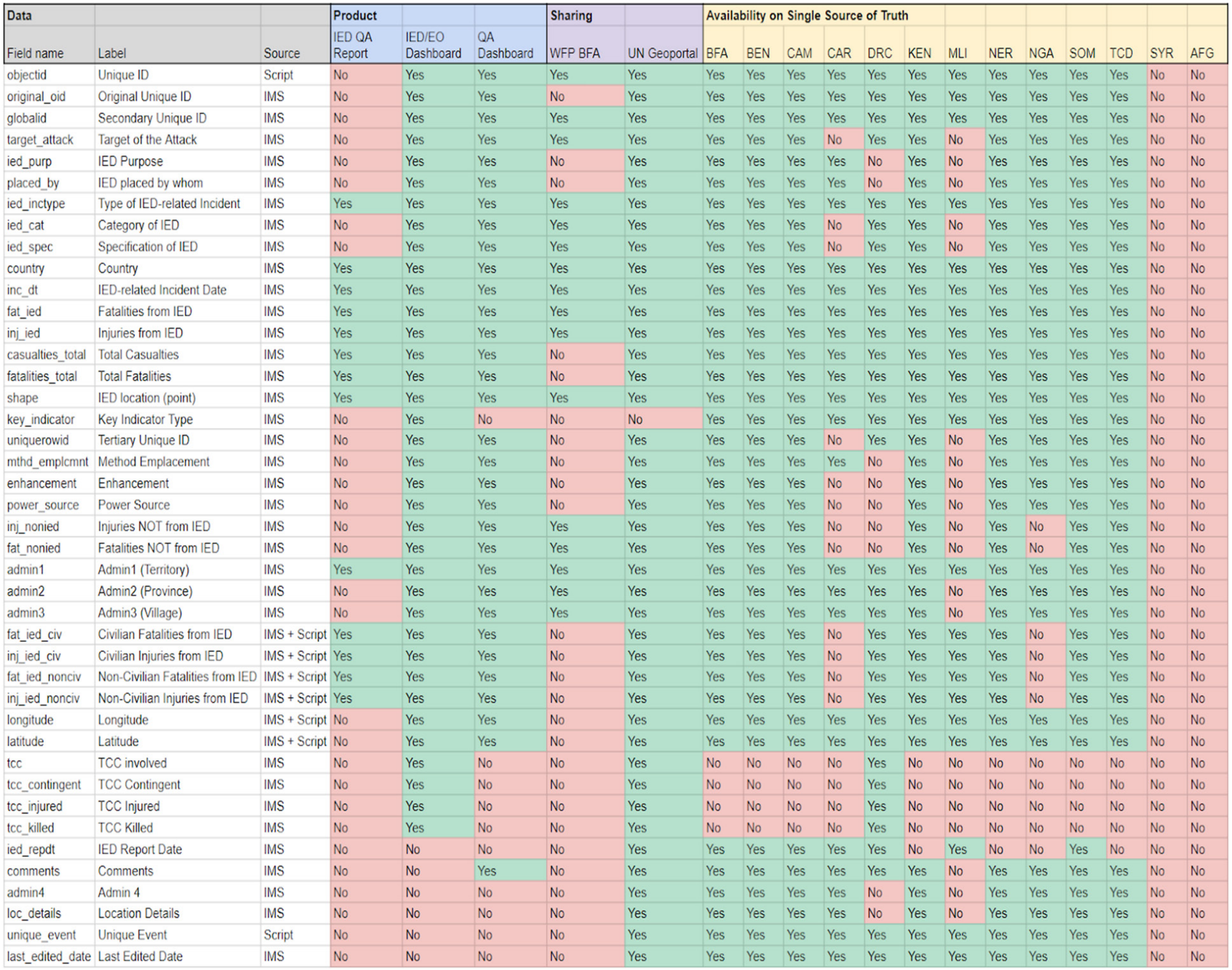
Appendix 1 – Unite Aware/SAGE



Appendix 2 – UNMAS IMS EO and IED reporting diagram

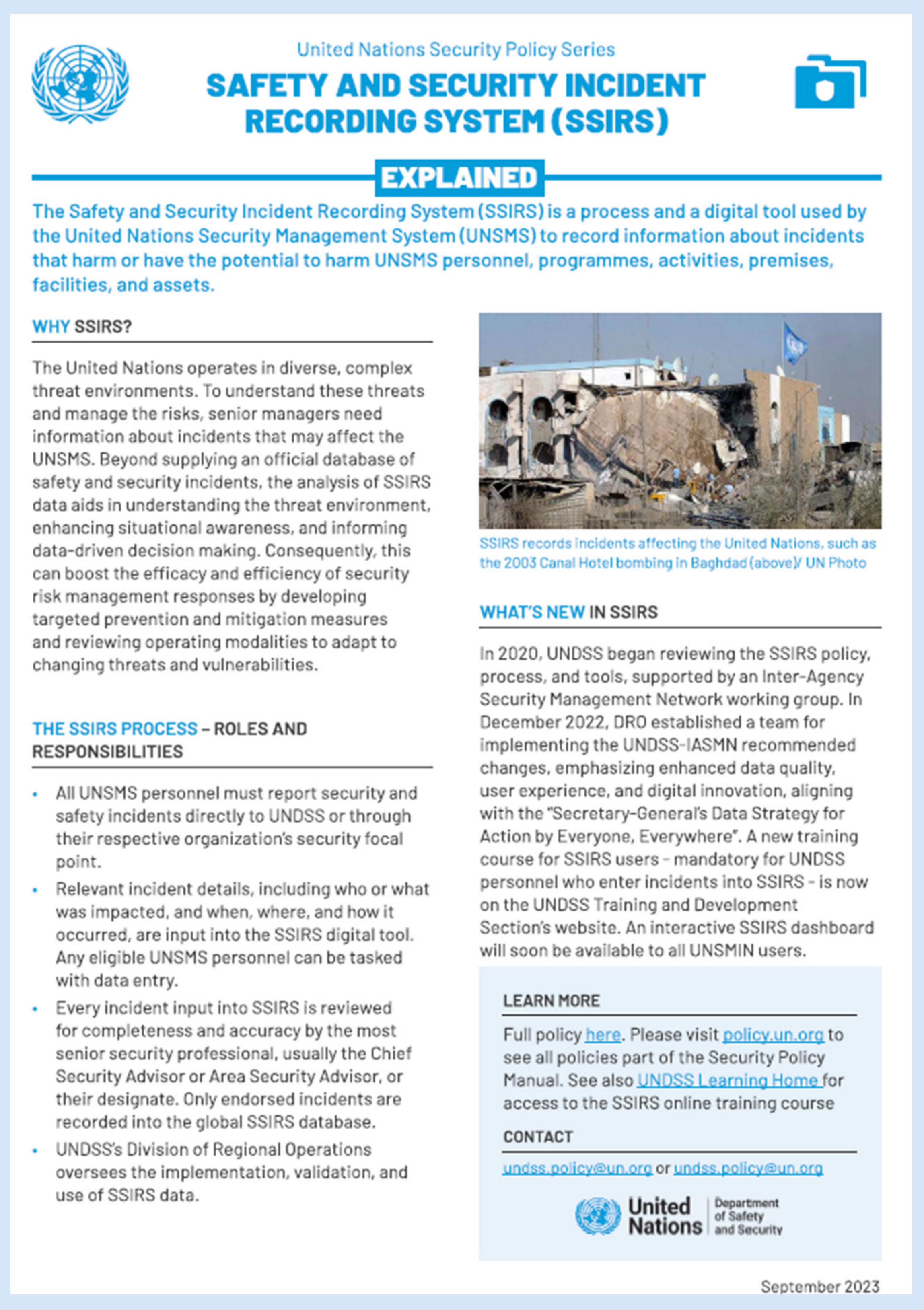


Appendix 3 – UNMAS IMS EO and IED data availability



Data			Product			Sharing		Availability on Single Source of Truth												
Field name	Label	Source	IED QA Report	IED/EO Dashboard	QA Dashboard	WFP BFA	UN Geoportal	BFA	BEN	CAM	CAR	DRC	KEN	MLI	NER	NGA	SOM	TCD	SYR	AFG
objectid	Unique ID	Script	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
original_oid	Original Unique ID	IMS	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
globalid	Secondary Unique ID	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
target_attack	Target of the Attack	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
ied_purp	IED Purpose	IMS	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No
placed_by	IED placed by whom	IMS	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No
ied_inctype	Type of IED-related Incident	IMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
ied_cat	Category of IED	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
ied_spec	Specification of IED	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
country	Country	IMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
inc_dt	IED-related Incident Date	IMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
fat_ied	Fatalities from IED	IMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
inj_ied	Injuries from IED	IMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
casualties_total	Total Casualties	IMS	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
fatalities_total	Total Fatalities	IMS	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
shape	IED location (point)	IMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
key_indicator	Key Indicator Type	IMS	No	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
uniquerowid	Tertiary Unique ID	IMS	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
mthd_emplcmnt	Method Emplacement	IMS	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No
enhancement	Enhancement	IMS	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No
power_source	Power Source	IMS	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No
inj_nonied	Injuries NOT from IED	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	No	Yes	Yes	No	No
fat_nonied	Fatalities NOT from IED	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	No	Yes	Yes	No	No
admin1	Admin1 (Territory)	IMS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
admin2	Admin2 (Province)	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
admin3	Admin3 (Village)	IMS	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
fat_ied_civ	Civilian Fatalities from IED	IMS + Script	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
inj_ied_civ	Civilian Injuries from IED	IMS + Script	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
fat_ied_nonciv	Non-Civilian Fatalities from IED	IMS + Script	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
inj_ied_nonciv	Non-Civilian Injuries from IED	IMS + Script	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
longitude	Longitude	IMS + Script	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
latitude	Latitude	IMS + Script	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
tcc	TCC involved	IMS	No	Yes	No	No	Yes	No	No	No	No	Yes	No	No	No	No	No	No	No	No
tcc_contingent	TCC Contingent	IMS	No	Yes	No	No	Yes	No	No	No	No	Yes	No	No	No	No	No	No	No	No
tcc_injured	TCC Injured	IMS	No	Yes	No	No	Yes	No	No	No	No	Yes	No	No	No	No	No	No	No	No
tcc_killed	TCC Killed	IMS	No	Yes	No	No	Yes	No	No	No	No	Yes	No	No	No	No	No	No	No	No
ied_repdt	IED Report Date	IMS	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No	No
comments	Comments	IMS	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
admin4	Admin 4	IMS	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No
loc_details	Location Details	IMS	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No
unique_event	Unique Event	Script	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
last_edited_date	Last Edited Date	IMS	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Appendix 4 – Department of Safety and Security - Safety and Security Incident Recording System



United Nations Security Policy Series

SAFETY AND SECURITY INCIDENT RECORDING SYSTEM (SSIRS)

EXPLAINED

The Safety and Security Incident Recording System (SSIRS) is a process and a digital tool used by the United Nations Security Management System (UNSMS) to record information about incidents that harm or have the potential to harm UNSMS personnel, programmes, activities, premises, facilities, and assets.

WHY SSIRS?

The United Nations operates in diverse, complex threat environments. To understand these threats and manage the risks, senior managers need information about incidents that may affect the UNSMS. Beyond supplying an official database of safety and security incidents, the analysis of SSIRS data aids in understanding the threat environment, enhancing situational awareness, and informing data-driven decision making. Consequently, this can boost the efficacy and efficiency of security risk management responses by developing targeted prevention and mitigation measures and reviewing operating modalities to adapt to changing threats and vulnerabilities.

THE SSIRS PROCESS – ROLES AND RESPONSIBILITIES

- All UNSMS personnel must report security and safety incidents directly to UNDSS or through their respective organization's security focal point.
- Relevant incident details, including who or what was impacted, and when, where, and how it occurred, are input into the SSIRS digital tool. Any eligible UNSMS personnel can be tasked with data entry.
- Every incident input into SSIRS is reviewed for completeness and accuracy by the most senior security professional, usually the Chief Security Advisor or Area Security Advisor, or their designate. Only endorsed incidents are recorded into the global SSIRS database.
- UNDSS's Division of Regional Operations oversees the implementation, validation, and use of SSIRS data.

SSIRS records incidents affecting the United Nations, such as the 2003 Canal Hotel bombing in Baghdad (above)/ UN Photo

WHAT'S NEW IN SSIRS

In 2020, UNDSS began reviewing the SSIRS policy, process, and tools, supported by an Inter-Agency Security Management Network working group. In December 2022, DRO established a team for implementing the UNDSS-IASMN recommended changes, emphasizing enhanced data quality, user experience, and digital innovation, aligning with the "Secretary-General's Data Strategy for Action by Everyone, Everywhere". A new training course for SSIRS users – mandatory for UNDSS personnel who enter incidents into SSIRS – is now on the UNDSS Training and Development Section's website. An interactive SSIRS dashboard will soon be available to all UNSMIN users.

LEARN MORE

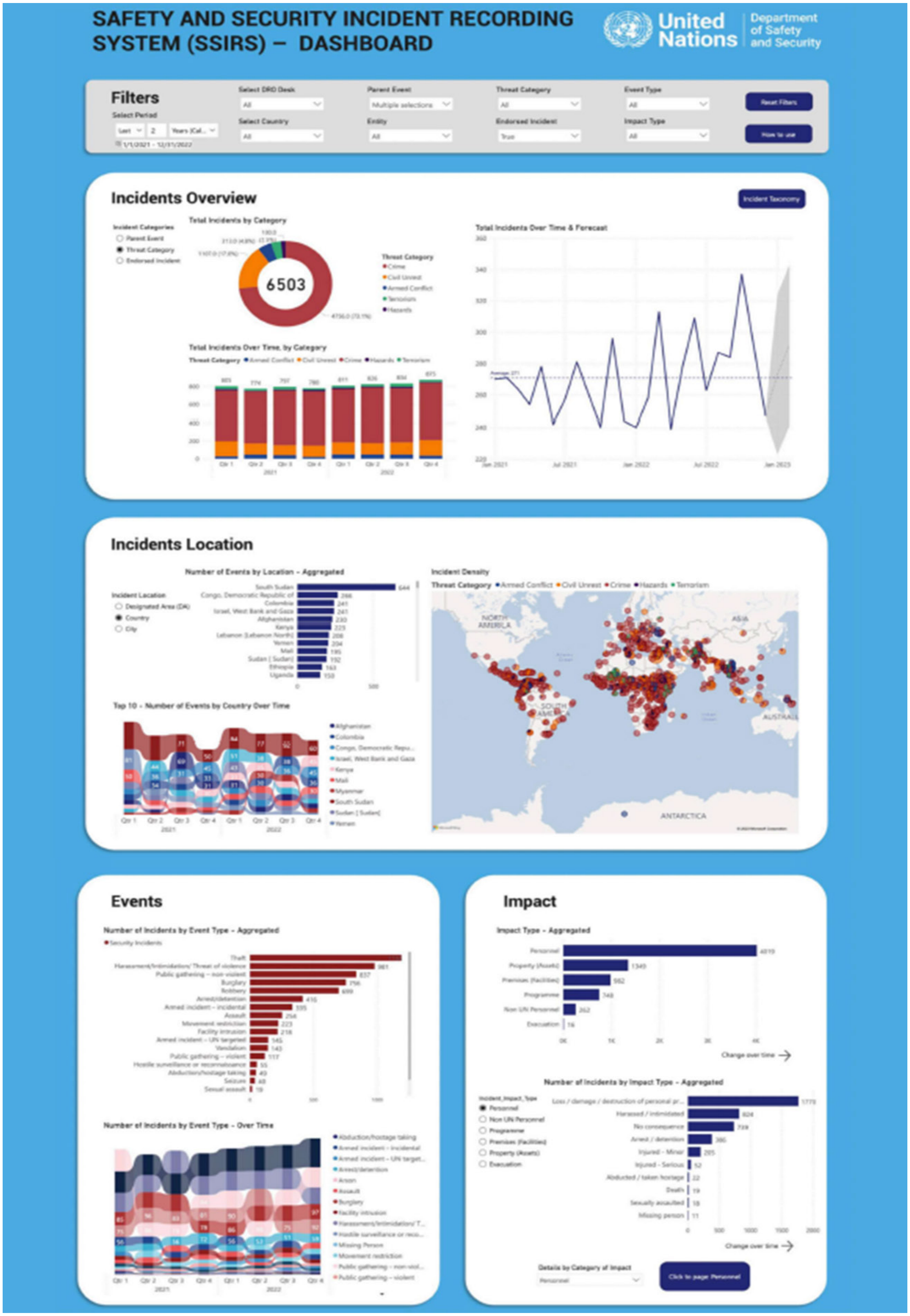
Full policy here. Please visit policy.un.org to see all policies part of the Security Policy Manual. See also UNDSS Learning Home for access to the SSIRS online training course

CONTACT

undss.policy@un.org or undss.policy@un.org

United Nations | Department of Safety and Security

September 2023



SAFETY AND SECURITY INCIDENT RECORDING SYSTEM (SSIRS) – DASHBOARD

United Nations | Department of Safety and Security

Filters

Select Period: Last 2 Years (Cal...

1/1/2021 - 12/31/2022

Select DRO Desk: All

Select Country: All

Parent Event: Multiple selections

Entity: All

Threat Category: All

Endorsed Incident: True

Event Type: All

Impact Type: All

Reset Filters

How to use

Incidents Overview

Incident Taxonomy

Incident Categories

○ Parent Event

● Threat Category

○ Endorsed Incident

Incidents Location

Incident Location

○ Designated Area (DA)

● Country

○ City

Number of Events by Location – Aggregated
South Sudan 644
Congo, Democratic Republic of 266
Colombia 241
Israel, West Bank and Gaza 241
Afghanistan 230
Kenya 223
Lebanon [Lebanon North] 208
Yemen 204
Mali 195
Sudan [Sudan] 192
Ethiopia 163
Uganda 150
0
500
Top 10 – Number of Events by Country Over Time
● Afghanistan
● Colombia
● Congo, Democratic Repu...
● Israel, West Bank and Gaza
● Kenya
● Mali
● Myanmar
● South Sudan
● Sudan [Sudan]
● Yemen
Qtr 1
Qtr 2
Qtr 3
Qtr 4
2021
2022
Incident Density
Threat Category ● Armed Conflict ● Civil Unrest ● Crime ● Hazards ● Terrorism
NORTH AMERICA
SOUTH AMERICA
ASIA
AUSTRALIA
ANTARCTICA

Events

Number of Incidents by Event Type – Aggregated
● Security Incidents
Theft
Harassment/Intimidation/ Threat of violence 981
Public gathering – non-violent 837
Burglary 756
Robbery 699
Arrest/detention 416
Armed incident – incidental 335
Assault 254
Movement restriction 223
Facility intrusion 218
Armed incident – UN targeted 145
Vandalism 143
Public gathering – violent 117
Hostile surveillance or reconnaissance 55
Abduction/hostage taking 49
Seizure 48
Sexual assault 19
0
500
1000
Number of Incidents by Event Type – Over Time
● Abduction/hostage taking
● Armed incident – incidental
● Armed incident – UN target...
● Arrest/detention
● Arson
● Assault
● Burglary
● Facility intrusion
● Harassment/Intimidation/ T...
● Hostile surveillance or reco...
● Missing Person
● Movement restriction
● Public gathering – non-viol...
● Public gathering – violent
Qtr 1
Qtr 2
Qtr 3
Qtr 4
2021
2022

Impact

Incident_Impact_Type

● Personnel

○ Non UN Personnel

○ Programme

○ Premises (Facilities)

○ Property (Assets)

○ Evacuation

Details by Category of Impact: Personnel

Click to page: Personnel

Annex D. Reporting

Accurate and complete event reporting serves a critical function to provide stakeholders with a situational understanding at the tactical level. The information provided in improvised explosive device (IED) and explosive event reports informs all interested parties of current threats, impacting decision-making, resourcing, standards, training and mitigation strategies. Force protection elements should balance specific reporting requirements with the tactical situation, but wherever possible, every effort must be made to allow for the adequate investigation and reporting of explosive events. In addition, tactical commanders must allocate adequate and realistic amounts of time to conduct thorough on-scene exploitation, when safety allows.

This annex provides a common framework and general guidelines for the reporting of explosive events. This annex includes recommended formats that are adaptable to meet specific mission requirements but should not be considered an exhaustive list. In the absence of a weapons intelligence team or post-bast investigation team, an explosive ordnance disposal (EOD) team should be utilized to collect items, record the area where an incident has taken place and provide a tactical and technical assessment of the incident. EOD personnel deployed within an operation should have basic training in evidence collection and documentation.

If no properly trained assets are deployed on the scene, all attempts should be made to at least provide the minimum information requirement of reporting to higher level by answering the six generic questions (who, what, when, where, why and how) with photographs of the incident area and of the point(s) of interest.

D.1. Report types

EO/IED incident report (10-liner)

The purpose of the explosive ordnance (EO)/IED incident report is to provide immediate communication from the reporting unit or individual to a higher echelon, command or other entities regarding the basic nature and characteristics of an incident. The intent is to notify external stakeholders not at the scene, to give a basic common operational picture and allow controlling entities and decision makers on the necessary assets required to manage the situation. This report is formatted so that the information can be transmitted quickly, accurately and over radio communication.

Units and missions must establish rigorous quality control processes to ensure that information provided in the EO/IED incident report is complete, accurate, free of errors and does not omit critical information. The mission should have a standard format across all sectors and templates should be approved and published by the appropriate authority at the highest level required.

EOD task order

See *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual*.

EOD quick look

See *United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual.*

EOD report

The purpose of the EOD report is to provide all stakeholders with a detailed look of the incident that includes IED-related incidents including complex attacks. This report will provide all technical and tactical elements of the situation on the ground, providing the headquarters detailed information within a reasonable time frame. Depending on the gravity of the incident, the priority of reporting timeline is defined through a colour code (see below) and reporting is to be produced accordingly.

Technical exploitation 1 report

See United Nations guidelines on technical peacekeeping (under development).

Technical exploitation 2 report

See United Nations guidelines on technical peacekeeping (under development).

IED incident awareness report (FLASH)

The purpose of the IED incident awareness report is to provide all units in a mission theatre with information on evolving IED threats and give recommendations on how to adapt their own tactics, techniques and procedures (TTPs). This report is drafted by the C-IED cell and disseminated to all units and United Nations agencies in theatre. The report is structured into background, key findings and recommendations and is a maximum of one page in length. An example in provided in appendix 5 below.

Medical evacuation/MEDEVAC (9-liner)

D.2. Timeline for reporting

EOD report

The reporting units should submit the EOD task report **no later than 24 hours** after return to base. In case the team does not immediately return to base or is lacking in information technology facilities, the unit commander, operations section or other designate person should take over the task of completing the report. This person then uses all necessary means to gather the required information through radio or other available communication.

An example for predetermined priority settings and recommended timelines is as follows:

- **Red**: Immediate – submitted immediately after return to base.

  Incidents that include death, serious injury, missing in action affecting the unit or mission.

  Detainee in custody.

  Force countermeasures/TTPs defeated.

  New TTPs, emplacement methods.

- **Amber**: Urgent – submitted no later than 12 hours after return to base.

  Death, serious injury, missing in action.
  Emerging perpetrators TTPs suspected.
  Existing TTPs improved.

- **Green**: Routine – submitted no later than 24 hours/1 day after return to base.

  All explosive incidents that do not imply new TTPs or causing serious damage or injuries.

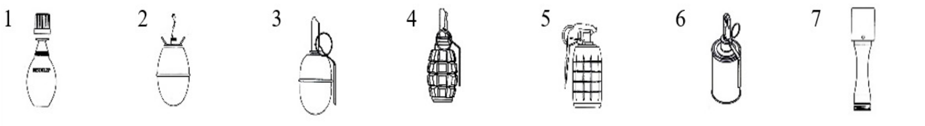
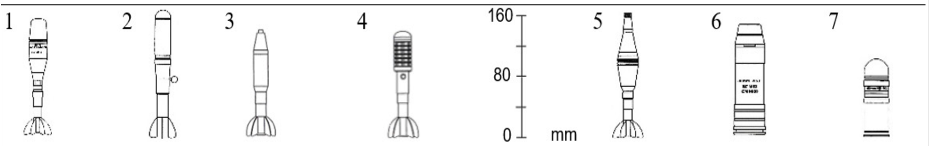
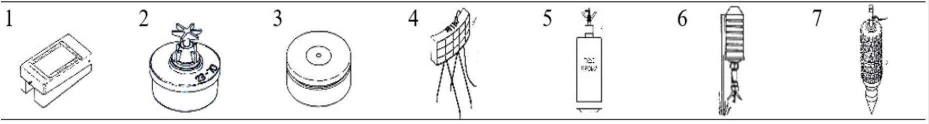
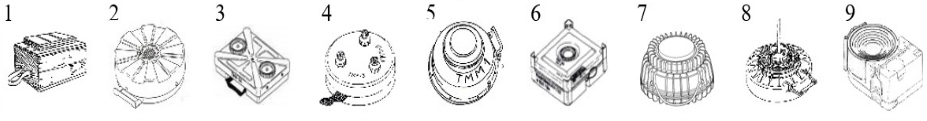
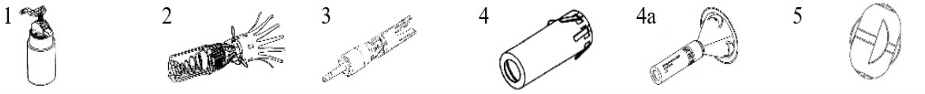
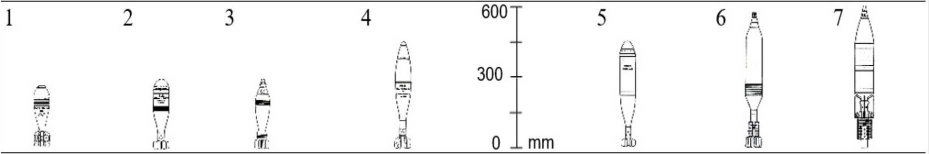
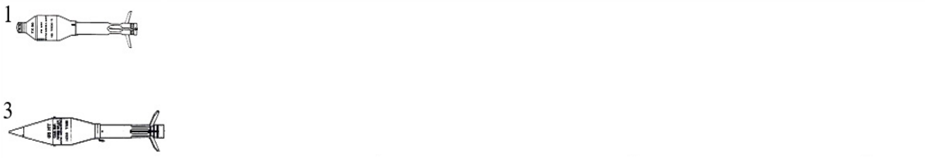
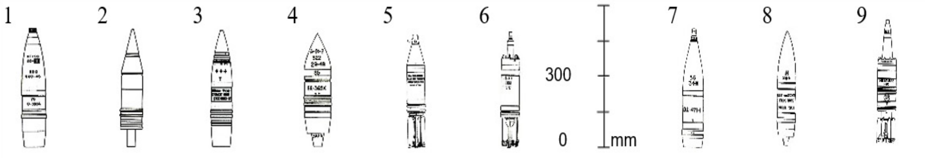
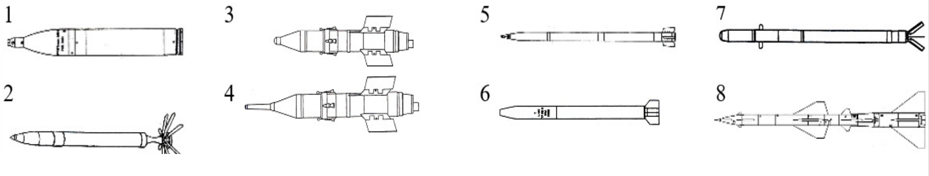
Figure D.1
Reporting scheme

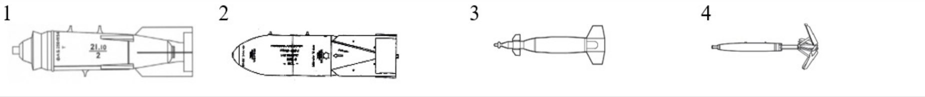
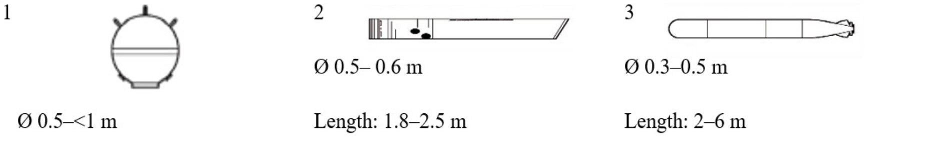
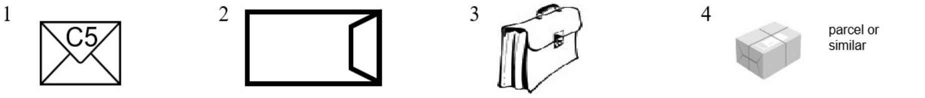
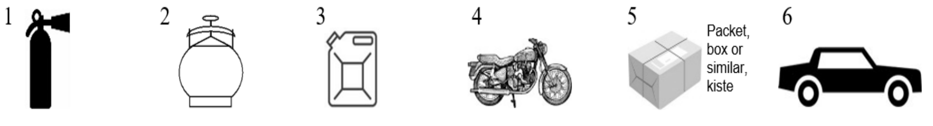
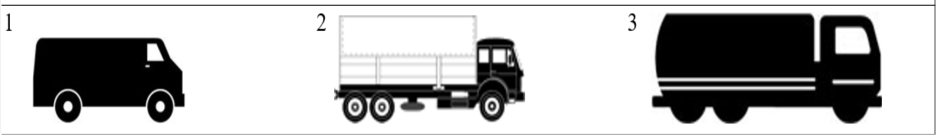
Time	From	To	When	Format	Means
Immediate	Unit/individual uniformed personnel	Headquarters	IED incident	**Explosive ordnance/IED incident report**	Radio/mail
Immediate	Headquarters	EOD	Receiving explosive ordnance/IED incident report (and unit)	**EOD task order** (consist of validated explosive ordnance/IED incident report)	Radio/mail
ASAP-3h (return to base)	EOD team	Headquarters	Initial situational overview and first assessment	**EOD Quick Look**	Mail
Depending on the incident: • **Red** • **Amber** • **Green**	EOD	Headquarters/ database	EOD task order completed	**EOD report**	Mail
No later than 24h	Level 1 technical exploitation (weapons intelligence team, post-blast investigation)	Headquarters	(If there is no weapons intelligence team or post-blast investigation team available, the technical exploitation-1 report will be substituted by the EOD report)	Technical exploitation-1 report	Mail
ASAP	Level 2 technical exploitation		Detailed assessment of all collected evidence with detailed analysis	Technical exploitation-2 report	Mail
ASAP	Headquarters/ IED threat mitigation	All units/individual uniformed		**EOD/IED awareness report**	Mail

Appendix 1 – EO/IED incident report (10-liner)

Line	Item	Sub-item		Example
1	**Date-Time-Group**	A	Date-Time-Group DD, hh mm, Time Group, MMM, YY	*(e.g. 281310BDEC23)*
2	**Reporting unit**	A	Unit/unit identifier	
		B	Name	
		C	Rank	
3	**Location**	A	Link-up location	*MGRS grid reference (8-digit), UTM or WGS84 coordinate*
		B	Additional location information	*(landmarks, reference points, or street addresses)*
		C	Avenue of safe approach	
4	**Communication**	A	Link-up communication method and contact	
5	**Type and description of EO**	A	EO/IED type	*e.g. IED/Explosion/ CACHE or FIND/HOAX/ FALSE/TURN-IN/Other (UXO/ERW/AXO etc.)*
		B	How many items were found	
		C	Position	*e.g. surface, subsurface, elevated, underwater*
		D	Colour	
		E	Markings	*e.g. cyrillic, latin, colours, etc.*
		F	Size estimate	
		G	Nuclear, radiological, biological and chemical, or toxic industrial materials	*Yes/No and description*
		H	Pictures taken	*Yes/No*
6	**Location of EO/IED**	A		*MGRS grid reference (8-digit), UTM or WGS84 coordinate*
7	**Tactical situation**	A	Hostile activity	*Yes/No and description*
		B	Fire hazard	*Yes/No and description*
		C	Unstable infrastructure	*Yes/No and description*
		D	Dangerous terrain	*Yes/No and description*
		E	Other hazards	*Yes/No and description*

Line	Item	Sub-item		Example
8	**Damage**	A	Collateral damager	
		B	What asset/resource is threatened?	
		C	Impact on mission	*- Totally disrupted* *- Major* *- Minor* *- Nil*
9	**Protective measures taken**	A	Markers placed	
		B	Evacuation distance	
		C	Other protective actions taken	
10	**Recommended priority**	A	Immediate	*- Threat to life/critical infrastructure*
			Urgent	*- Threat to mission/ protection of civilians*
			Routine	*- Threat with only minor impact to mission*
			No threat	*- To mission or civilians*

Type	Examples for explosive ordnance (not to scale)	Initial safety distance*
A Hand grenades		100 m
B Grenades/ rifle grenades		100 m
C Anti-personnel mine		100 m
D Anti-tank mine		100 m
E Submunition		100 m
F Mortars		200 m
G Anti-tank weapons		200 m
H Shells		200 m
I Missiles/ rockets		200 m

Type	Examples for explosive ordnance (not to scale)	Initial safety distance*
J Bombs		400 m
K Underwater munitions	 1 Ø 0.5–<1 m 2 Ø 0.5– 0.6 m Length: 1.8–2.5 m 3 Ø 0.3–0.5 m Length: 2–6 m	400 m
L (Small)		200 m
M (Medium)		400 m
N (Big)		800 m

* Initial safety distance = radius of an area, which must be cordoned off in order to ensure a minimum protection level, depending on the type and size of explosive ordnance.

Appendix 2 – EOD report

Line	Item	Sub-item		Example
1	General task information	A	Incident serial number	
2	Reporting unit contact information	A	Unit/unit identifier	
		B	Name	
		C	Rank	
		D	Position/role	
3	Tasking	A	Departure	*Date-Time-Group*
		B	Arrival	
		C	Incident control point location	*MGRS grid reference (8-digit), UTM or WGS84 coordinate*
		D	Force protection location	
		E	CASEVAC location	
4	EO/IED description	A	Location	*MGRS grid reference (8-digit), UTM or WGS84 coordinate*
		B	EO/IED type	*Time/Command/Victim Operated/ Mortar/Other (UXO/ERW/AXO/etc.)*
		C	Quantity	
		D	EO description	*IED/Explosion/CACHE or FIND/HOAX/FALSE/TURN-IN/ Other (UXO/ERW/AXO etc.)*
		E	Additional information	
If more, continue with numbering 4-1, 4-2, etc.				
5	EO/IED detail	A	Main charge	
		B	Switch	
		C	Power source	
		D	Initiator	
		E	Container	
		F	Enhancements	
		G	Anti-handling device	
		H	More information	
If more, continue with numbering 5-1, 5-2, etc.				
6	EOD ammunition	A	EOD ammunition used	
If more, continue with numbering 6-1, 6-2, etc.				

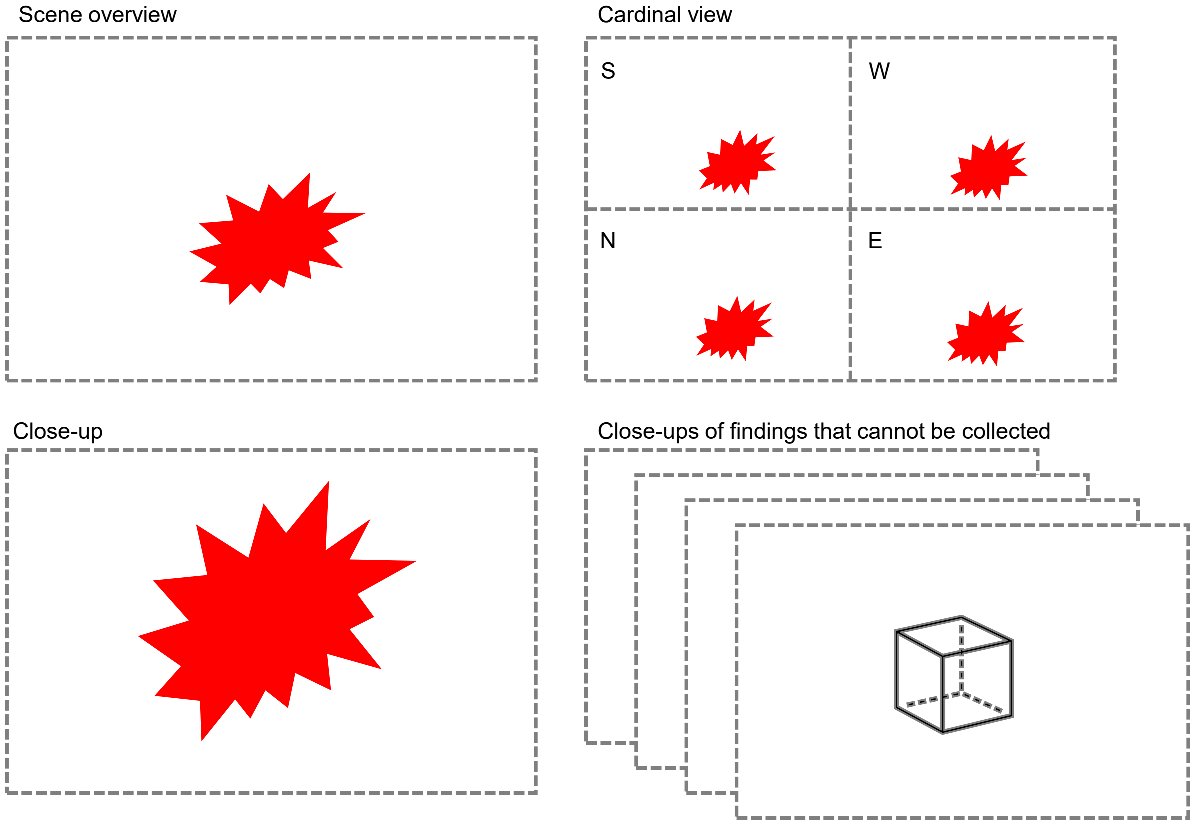
Line	Item	Sub-item		Example
7	Narrative	A		*Provide a detailed account of the tactical and technical characterization of the incident. Examples include:* *- Personnel involved.* *- Who reported the incident?* *- Circumstances and conditions before, during and after the incident.* *- Directions of travel.* *- Terrain.* *- Ground surfaces.* *- Vehicle or foot traffic.* *- Where was the item located?* *- Vulnerable point/vulnerable area.* *- Who is the possible target?* *- Where was the IED emplacement and how was the IED constructed?* *- How the item was emplaced, weather, fragmentation patterns, etc.*
8	Mapping supplement	A	Incident location Main supply routes, line of sight Impact points IED/location Key terrain	*Map overlay (screen capture or picture) of the incident site indicating key information, such as incident location, main supply routes, line of sight, impact points, IED/location, key terrain, etc.*
9	Scene sketch	A	Yes/No	*Scene overview sketch*
		B	Yes/No	*Detailed sketch - show how the components were placed*

Line	Item	Sub-item		Example
10	Pictures	A	Pictures attached that show the overview of the situation and if applicable an overview picture of the recovered items. Incident details: - Detailed picture of the seat of explosion or IED location - Insert photo looking out from seat of blast or out to possible firing point(s) - Ensure you give directions (north, east, south, west) - Ensure you mark and label the IED main charge. Make sure you include direction of travel arrow.	*Incident pictures taken*
		B	Cardinal directions of the scene: Pictures from the contact point, centred at the bottom of the picture, looking out in four directions (north, east, south, west)	*Scene overview*
		C	Pictures showing the location of the incident with details of the travel direction of the target, IED placement on the foreground with components, direction of travel, aiming markers, possible firing point, and escape route(s) of the triggerperson.	*Area overview*

Line	Item	Sub-item	Example
11	Recovered items	A Recovered items	*List the type and quantity of items recovered from the incident (fragmentation, components, wires, tape, etc.)*
		B Recovered samples	*List any samples that were taken from the scene (soil, liquids, residue, etc.)*
		C Evidence pictures taken	*Yes/No* *IED technical characteristics:* *- Include picture of whole device assembled as it was placed.* *- Include a small insert of the device with rulers etc. once removed.* *Ensure picture is labelled with component of the IED*
		D X-ray	*Yes/No*
		E Chain of custody report	*Yes/No*
12	Action list	A	
		B	
		C	
		If required to be continued: D, E, F, etc.	
13	Injuries (as a result of EO/IED actions)	A Number of persons	
		B Severity of injuries	
		C Number of animals	
		If required to be continued: D, E, F, etc.	
14	Damage (as a result of EO/IED actions)	A	
		B	
		C	
		If required to be continued: D, E, F, etc.	
15	Assessment	A Assessment of EOD team	
16	Report completed by	A Unit/unit identifier	
		B Name	
		C Rank	
		D Position/role	
		E Time	*Date-Time-Group*

Appendix 3 – Pictorial guidance

The following diagram shows the minimum of pictures that must be taken at the scene of the event and what should be depicted. The explosion shape in the diagram symbolizes the point of interest.



- Scene overview depicts as much of the area where the event took place as possible, with the point of interest centred in the picture.
- Cardinal view depicts the surrounding area around the event site in the main compass points. The point of interest should be in the foreground in the picture.
- Close-up focuses on the point of interest, showing as much of it as possible in the picture.
- Close-ups of findings taken at the scene are used to describe items that might not be possible to be collected, to facilitate examination in a later phase.

Appendix 4 – EOD/IED incident awareness report

Line	Item	Sub-item		Example/data
1	General task information	A	Incident serial number	
		B	Date-Time-Group DD, HH, MM, Time Group: MM, YY	*e.g. 281310BDEC23*
2	Reporting unit contact information	A	Unit/unit identifier	
		B	Name	
		C	Rank	
		D	Position/role	
3	Receiving units			
4	Subject	A	IED incident type	
		B	Date-Time-Group DD, HH, MM, Time Group: MM, YY	*e.g. 281310BDEC23*
5	Incident background			*Short synopsis on the background. Give a short overview of no more than three incidents that spark this flash report.*
6	Key findings			• *What are the main issues being addressed?* • *How are own units vulnerable to the evolving threat?* • *What is the presumable cause of the vulnerability?*
7	Lessons identified			• *How do units need to adjust to counter the new threat* • *Reinforce TTPs in place that help reduce impact of new threat.* • *Short and to the point bullets*
8	Images			*Insert pictures that underline the issue at hand and support the recommendations made.*
9	Recommendations			

Appendix 5 – MEDEVAC (9-liner)

Line	Item	Sub-item		Example/Data
1	Landing zone location	A		*MGRS grid reference (8-digit), UTM or WGS84 coordinate*
2	Reporting unit contact information	A	Unit/unit identifier	*Call sign*
		B	Name	
		C	Rank	
3	Number of patients/priority	**A**	**Urgent (< 90 minutes)**	
		B	**Priority (< 24 hours)**	
		C	**Routine (< 24 hours)**	
		D	**Deceased**	
4	Special equipment required	A	None	
		B	Hoist/winch	
		C	Extraction equipment	
		D	Respirator	
		E	Other	
5	Number of patient and type	A	Litter/stretcher	
		B	Walking (ambulatory)	
		C	Escort (obligatory for child)	
6	Security at pickup zone	N	No enemy	
		P	Possible enemy	
		E	Enemy in area	
		X	Armed escort required	
		I	IED threat	
7	Pickup zone marking method	A	Cyalume (light stick)	
		B	Fire flares	
		C	Smoke	
		D	None	
		E	Other	
8	Number and status of casualty/patient by status	A	United Nations military/police	
		B	United Nations civilian	
		C	Enemy	
		D	Local civilian	
		E	Prisoner	
		F	Child	
9	Pickup zone terrain/obstacles	A		

24-21580