DECLASSIFIED

United Nations
Department of Peace Operations
Ref. 2025.04

Guidelines

Technical Peacekeeping-Intelligence (TPKI)

Approved by:	Jean-Pierre Lacroix, USG DPO
Effective date:	1 March 2025
Contact:	DPO/OUSG/PICT
Review date:	March 2032, or as needed

DPO GUIDELINES ON
TECHNICAL PEACEKEEPING-INTELLIGENCE (TPKI)

Contents:

ANNEXURES

A. PURPOSE AND RATIONALE

1. The purpose of these Guidelines is both to provide a framework for and to facilitate the safe and effective acquisition of technical information for peacekeeping-intelligence (hereafter "TPKI"). These Guidelines are part of the Peacekeeping-Intelligence Framework and should be read in conjunction with the DPO Policy on Peacekeeping-Intelligence (PKI)[1] (hereafter "the Policy").

2. The Policy sets out why and how United Nations peacekeeping operations acquire, collate, analyze, disseminate, use, protect, and manage PKI in support of United Nations peacekeeping operations in the field (Figure 1).

[1] Policy on Peacekeeping-Intelligence, DPO, Ref. 2019.08.

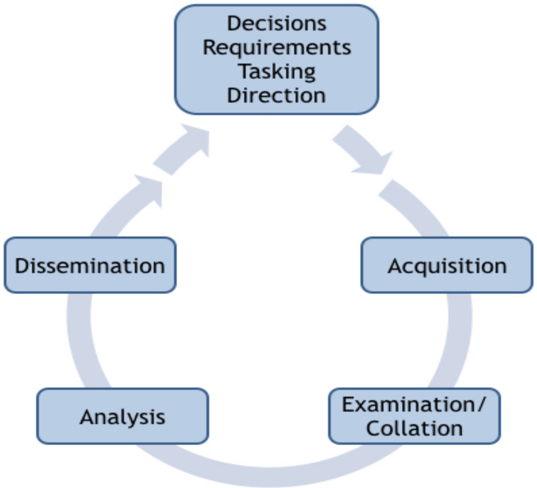


Figure 1. The Peacekeeping-Intelligence Cycle

3. In UN Peacekeeping, TPKI refers to PKI derived from the acquisition, exploitation, and analysis of military equipment and any material posing a potential threat, including conventional and asymmetric threat weapons systems and associated components.

4. TPKI activities within most peacekeeping operations are heavily concerned with the exploitation of Improvised Explosive Devices (IEDs).[2] Examples of other areas of application are: Explosive Remnants of War (ERW), Small Arms and Light Weapons (SALW), and equipment confiscated from hostile, unaligned or unknown actors[3]; for example, micro/mini Unmanned Aircraft Systems (UAS) or digital/hardcopy documents. TPKI may enable trend identification, as well as assist in force protection and the protection of civilians. Specific technical information may potentially serve as evidence for the purpose of prosecution[4] and/or the investigation of international crimes.

5. Based on the above parameters, the present Guidelines have been developed to provide guidance to peacekeeping operations on the parameters concerning TPKI.

B. SCOPE

6. This guidance document shall apply to all United Nations peacekeeping personnel assigned to support the direction, acquisition, examination and collation, analysis, and dissemination of information from technical sources for PKI. Compliance with these

[2] Also referred to as Explosive Ordnances (EOs).

[3] In these Guidelines, an actor is considered as follows: 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 force against UN staff and/or peacekeepers.

[4] Police forensic doctrine recommends ensuring the provenance of evidence and a recorded or registered chain of custody. For more information, see the UNODC Crime Scene and Physical Evidence Awareness Manual: https://www.unodc.org/documents/scientific/Crime_scene_awareness__Ebook.pdf. The final word about evidence value in court or for prosecution is for the local/competent (prosecution/judicial) authorities. Standards and handling should be included in the criminal procedure codes or similar legislation of each country.

Guidelines is strongly recommended.[5]

7. The Principles of PKI are to be strictly complied with. The seven principles are explained in the Policy. They refer to: the rules under which PKI activities are undertaken; the non-clandestine nature of PKI activities; the areas of application; the respect for State sovereignty; the independence of PKI; the accountability, capability and authority for PKI in missions; and the security and confidentiality of PKI.

8. The main audiences for these TPKI Guidelines are threefold. Firstly, these Guidelines are for those acquiring technical information and will provide a basic overview of tasks related to TPKI. Secondly, these Guidelines will inform the producers of PKI products (analysts) with guidance on the benefits of integrating TPKI in their all-source analysis. Lastly, they are intended to educate consumers of PKI products (decision-makers and planners) on the fact that TPKI is useful, but does not provide the complete answer to all scenarios.

9. TPKI exploitation activities include the acquisition, collation, and analysis of technical, tactical, and forensic information, which often requires expert acquisition knowledge, and technical and scientific exploitation and analysis.

10. The UN does not utilize TPKI, or any associated process, to support the kinetic targeting of individuals or groups, unless this is explicitly mentioned and tasked in the Mission mandate, and carried out with a view to mitigating civilian harm.

C. PROCEDURES

11. General Rules and Characteristics

11.1. The exploitation of technical sources for PKI should be carried out strictly to enhance situational awareness and the safety and security of UN personnel, and to inform operations and activities related to the protection of civilians tasks of the Security Council mandates. TPKI is a subset of PKI.

11.2. All TPKI operations should be conducted in accordance with the UN Charter, basic peacekeeping principles, international human rights law, international humanitarian law, relevant decisions of the Organization’s intergovernmental organs, and other applicable legal frameworks.

11.3. It is important that exploitation activities are conducted persistently and iteratively in order to provide accurate PKI, develop effective countermeasures or mitigation measures, and to contribute to accountability for crimes against peacekeepers.[6]

11.4. The appropriate centralized storage of PKI data is essential to effective operations. PKI data should be correctly named, referenced, and tagged with metadata to allow

[5] This guidance only applies to data, information and products gathered and managed as part of the PKI cycle. Standard information management, and reporting and sharing practices that are not related to PKI will continue to be conducted in line with existing applicable guidance.

[6] A4P+, Priority 4: Accountability to peacekeepers.

an analyst to discover that data in the future.[7] For TPKI specifically, correlation to the event, location, and/or context is essential. Mission leadership should consider identifying a lead entity to manage an appropriate TPKI database to ensure a coherent approach and easy access for all relevant entities.

11.5. In line with the PKI Policy, the Head of Mission (HoM) or a delegated authority can share PKI, including TPKI, with non-UN actors. The exchange of PKI, including TPKI, with non-UN security forces, including Host State security forces, shall occur in compliance with the Human Rights Due Diligence Policy on UN support to non-UN security forces (HRDDP) and the Guidelines on Sharing PKI.[8] **TPKI products will often be classified.[9]** The safety and security of UN personnel, the Mission, sources and civilians is paramount, and these considerations shall inform any decision-making regarding such information-sharing. Sharing TPKI with the Host State can be paramount for investigations of those who have targeted UN personnel.

D. ROLES AND RESPONSIBILITIES

12. Direction

12.1. The HoM, via the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM), and the heads of the components[10] via their respective PKI entities,[11] shall ascertain the Information Requirements and ensure that taskings are in line with their component's capabilities and limitations.

12.2. All TPKI activities should be conducted in support of the Mission Information Acquisition Plan (MIAP) and component IAPs. They shall also be conducted within the scope of the Mission Peacekeeping-Intelligence Support Plan (MISP).

12.3. TPKI activities may often be reactive. The exploitation of IED components or other material can only be done when those are found, for example, during an operation or a patrol.

13. Acquisition

13.1. The acquisition of technical information from blast sites, IED components, or military or threat equipment, is a specialized process, and should only be conducted by experts.[12] These tasks, when explosives are present or suspected, are typically conducted by Explosive Ordnance Disposal (EOD) teams. Other teams that

[7] Refer to Mission SOPs on PKI data / information management. In many Missions, Unite Aware SAGE is being used as a database, as well as other local solutions, including MS Excel and i2.

[8] Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities, DPO, Ref. 2022.05.

[9] For reference, on the sharing of classified information: https://unitednations.sharepoint.com/sites/OICT/SitePages/Information-Sensitivity-Toolkit.aspx.

[10] JMAC, Military Component, and Police Component.

[11] Joint Mission Analyses Center (JMAC), Force U2, Police Component Crime Intelligence Unit (CIU), UN Department of Safety and Security (UNDSS), and the Joint Operations Centre (JOC) (supporting).

[12] See the Improvised Explosive Device Threat Mitigation Handbook, and United Nations Peacekeeping Missions Military Explosive Ordnance Disposal Unit Manual, where technical exploitation is explained in more detail.

specialize in site or scene exploitation can acquire technical information when explosive dangers are not present.

13.2. Post-Blast Investigation (PBI): A PBI takes place when an EOD team exploits the scene/site of an explosion caused by explosive ordnance. During a PBI, the initial level of exploitation is conducted in order to identify, collect, preserve, transport, and examine evidence. The EOD team leader is responsible for a PBI, and will conduct site exploitation. Tasks associated with this are scene diagrams, photographs, evidence collection, tactical characterization, and technical characterization.

13.2.1. EOD teams are responsible for rendering safe any remaining explosive hazards, the initial exploitation of all explosive events, and starting the process for TPKI.

13.2.2. When evidence is transported or received, it should be assessed and verified safe by qualified EOD personnel before further exploitation occurs.

13.3. In the presence of suspected Explosive Ordnance, EOD teams should investigate the scene for possible explosive hazards before the acquisition of technical, tactical or forensic information can begin. Every peacekeeper should be prepared to document/photograph at least basic technical information, such as headstamps of ammunition rounds or serial numbers of discarded weapons.

13.4. Digital forensic exploitation can be carried out on captured equipment (UAS, computers, and other electronic items that are not explicitly related to explosive ordnance) by personnel other than EOD teams. Trained professionals in site exploitation and evidence collection should identify, collect, preserve, transport, and examine non-explosive evidence such as UAS, computers, cell phones, documents, and other components.

13.5. The relative cost-benefit balance of TPKI capabilities should be carefully considered by Mission leadership. Given the nature of TPKI, there is the potential for associated activities to consume considerable personnel and financial resources while yielding a relatively low volume of niche information. However, if the context of the Mission environment requires such investment, this would certainly be justified. Mission leadership should therefore seek to make an informed decision based on technical expert advice and the latest threats that may be encountered in their Mission area, as to the appropriate level of investment. Where possible, a modular approach should be considered based on a relatively basic TPKI capability, but with the ability, if required, to upscale in capacity and complexity based on changes in the threats faced by the Mission.

14. Collation and Examination

14.1. Since TPKI can be conducted in relation to a range of technical sources – for example EO-related or digital data carriers – it is important to note that the terminology regarding the levels of examination may differ between these categories. The definitions of examination levels for TPKI-related to EO/IED sources are not directly equivalent to the levels used when discussing the examination of captured UAS, documents, computer components, or other non-EO/IED sources.

14.2. Processing material acquired at the scene of an IED strike/find in laboratories is often not sufficient as such to be used in all-source PKI analysis. This material usually needs to be researched in a specialized facility in order for a useful report to be produced for PKI.

14.3. There are different levels of examination for TPKI related to EO/IED components (Level 1/2/3). Level 1 means that the examination is conducted on scene; Level 2, in an in-country, in-mission laboratory; and Level 3, in a laboratory outside of the country. UN peacekeeping missions with EO/IED threats should have Level 1 and Level 2 in place.[13]

14.3.1. Level 1 Exploitation refers to tactical acquisition and exploitation. Tactical units may have dedicated teams to perform an initial forensic analysis to develop actionable information, while providing expertise and material 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.

14.3.2. 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 tactical-level capability. Material from an incident location or location of interest is acquired, preserved, and shipped to forensic facilities (centers/laboratories) with advanced equipment and technology for exploitation by trained and qualified forensic examiners/technicians. Their analysis is documented in a forensic report that is shared with analysts working with TPKI. A forensic analysis may result in identifying, sourcing, and tracking materials used to create IEDs, and contribute to force protection and to the protection of the civilian population.

14.3.3. Level 3 Exploitation refers to out-of-country exploitation and analysis. International laboratories and centers have leading scientific and technical experts who, collectively, encompass all the forensic fields to provide the most comprehensive analyses of acquired materials. Some national-level expertise may be provided in support to in-mission centers and laboratories.

14.4. Correct collation – the systematic receiving, grouping, recording, and filing of all acquired information – is a necessity in all PKI disciplines and is of critical importance to technical information related to all forms of TPKI.

14.5. Examples of technical data that TPKI refers to include:

14.5.1. IED sites: The details of the different IED components at the site as well as their placement, and any markers in the area. Identifying individual components of an IED may make it possible to link an event to a specific actor or trace the origin of the component. Detailing the placement of the different components and markers at the scene will inform on the tactics that are used by the perpetrators.

14.5.2. Weapons caches: The type of weapons, the type of ammunition, the gear (uniforms, belts, holsters, communication equipment etc.), their quantities, and the state they are in, can inform the way the actor operates. Technical details may enable analysts to find out where the objects came from.

[13] Improvised Explosive Device (IED) Threat Mitigation Handbook and United Nations Peacekeeping Missions Military Explosive Ordnance Disposal (EOD) Unit Manual (DPO/OMA, pending signature)

14.5.3. Retrieved hostile UAS: Digital flight data (flightpath, point of origin, previous flights, return-to location) may inform on who is operating the UAS. Serial numbers of the hardware can inform on the origin of the object, while modifications made to the UAS can say more about the way an actor uses it.

14.6. In order to underpin the digital forensic capabilities on which TPKI relies, the UN Global Service Centre (UNGSC) has developed a training syllabus for relevant Mission personnel (such as for UNDSS, Field Technology Section (FTS), Information and Communications Technology Security (ICT Security), UN Police (UNPOL), U2, etc.). This training focuses primarily on micro/mini UAS, but also touches on the examination of phones, tablets, computers, etc. The training covers three levels of capability:

14.6.1. Data extraction from digital devices (determined to be free from explosives) by first responders.

14.6.2. Level 1 forensics capability, conducted at the Mission level.

14.6.3. Level 2 forensics capability, conducted at UNGSC.[14]

15. **Analysis**

15.1. The analysis of material and components found on the ground is conducted by specialist teams and dedicated facilities or laboratories. The results of these (technical) analyses are shared with PKI analysts for integration into PKI products, including the U2 and JMAC.

15.2. Where necessary and possible, TPKI will be shared with sections within the Mission (with UNPOL, for example) and Host State counterparts, for investigation and/or prosecution purposes.[15]

15.3. Forensics-derived information, from initial forensic exploitation on or near the incident site, or from laboratories after in-depth examination and analysis, informs PKI analysis. It is used to identify trends and patterns, as well as to develop associations among persons, places, things, and specific activities or incidents. It enables operating forces to identify threats and adds depth and scope to the PKI picture to answer information requirements.

15.4. All-source PKI analysts can use TPKI to build a detailed picture of the threat in the operating area. For example, information on the composition of an IED, the way it is constructed, and the manner in which it is placed on a particular route, can all inform a PKI entity on the development of trends concerning IEDs. At the same time, this may also highlight connections between different IED incidents if similar construction or placement tactics are used. In addition, if obtained, biometric data may help to identify individuals connected to IED incidents.

[14] TDU/TDDPS/SGITT: The Service for Geospatial, Information and Telecommunications Technology at the UN Global Service Center (UNGSC) in Valencia, Spain

[15] Ref. Para. 11.5.

15.5. Examples of products that incorporate TPKI will vary between Mission contexts, and will be influenced by, among other factors, the level of technical expertise available, senior leadership direction, and the specific needs of the recipients of the reporting. Representative products may include: (1) Technical evaluations of incident sites related to IEDs or indirect fire, to update Mission personnel on the capabilities and tactics of hostile actors; (2) General situation updates that summarize trends identified by TPKI acquired at weapons caches to ensure Mission leadership can maintain situational awareness; and (3) Route threat assessments to allow Mission leadership and ground forces to take mitigation measures when planning and conducting ground movements.

15.6. Although TPKI is often gathered in a reactive manner, the analyzed technical data will help gain insight into actors' capabilities and intent. In that way, TPKI reports can be traced back to Priority Information Requirements from the MIAP, to build a better understanding of the threats facing the Mission.

16. **Dissemination**

16.1. PKI products that include technical information may help inform units in the Mission to better understand the hostile actors in the operating area. It may inform them on the actor's capabilities and modus operandi. Likewise, PKI products including trends based on technical data may support the situational awareness of planners and decision-makers in the Mission. Therefore, while single-source reports of technical PKI by themselves may not need to be shared widely, when this data is put in a wider context (analyzed), it may be of great value for all levels in the Mission.

16.2. PKI products referencing the level and type of EO/IED threats in the operating area are not only useful for use in the Mission itself, but also to track related developments to support the equipping and training of UN forces and personnel prior to deployment.[16]

16.3. In addition, since there is a large international element to EO/IED threats (international armed group or terrorist networks, IED component trafficking, instruction of IED construction and emplacement tactics), sharing relevant PKI products with other UN Missions and UN Headquarters will help to foster a better common understanding of the EO/IED threat, and will support a UN-wide holistic approach to such threats by sharing information with other UN entities, such as agencies, funds and programs.[17]

16.4. Information that points to an imminent threat to UN personnel or to the civilian population must be immediately disseminated to the PKI components via the quickest means. The PKI components should then **immediately** alert all other members of the MICM, including the Mission Chief of Staff, so that actions can be taken to prevent

[16] See also the DPO C-IED Strategy (2023)

[17] Strategy on Counter Improvised Explosive Device (C-IED) for Peacekeeping Operations (2024). For procedures regarding sharing PKI with non-(peacekeeping) mission UN entities, please refer to para.8.2. in the DPO Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities (ref. 2022.05).

or mitigate the threat. Missions should establish a robust information system to ensure maximum timeliness of safety-related warnings.

16.5. Likewise, information that relates to suspected criminal activity must also be disseminated to the PKI components via the quickest means. The PKI components should then alert the Mission's Police Crime Investigation Unit (CIU) or equivalent.[18]

16.6. The following dissemination principles shall be adhered to:

16.6.1. **Timeliness**. Acquired information must be delivered in a timely manner, so that planners and decision makers can act proactively rather than react.

16.6.2. **Relevance**. This is determined by the needs of the recipients, as defined in the applicable (Mission or component) Information Acquisition Plan.

16.6.3. **Brevity**. Reports must be kept as brief as possible, but at the same time include everything that the recipient needs to know.

16.6.4. **Interpretation**. Wherever possible, all facts must be correctly evaluated, and their significance interpreted before dissemination.

E. TERMS AND DEFINITIONS

17. **EO** stands for Explosive Ordnance, and refers to all munitions containing explosives, nuclear fission, or fusion materials, as well as biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket, and small arms ammunition; all mines, torpedoes, and depth charges; pyrotechnics; clusters and dispensers; cartridge and propellant actuated devices; electro-explosive devices; clandestine[19] and IEDs; and all similar or related items or components that are explosive in nature.[20] [21]

18. **EOD** stands for Explosive Ordnance Disposal, and includes the procedures of detection, location, access, identification[22], evaluation, hazard mitigation, render safe[23], recording and recovery, and final disposal of EO or any hazardous material associated with an EOD incident.

[18] With current non-executive mandates, UNPOL cannot always act on the information, but can share serious crimes (as defined by local laws) with local counterparts.

[19] Clandestine devices are EO items that are specifically designed for concealed emplacement or appear like an innocuous item that functions when a person carries out an apparently harmless act. They utilize anti-handling devices or other conventional firing mechanisms in conjunction with a conventional initiator and main charge. The term military boobytrap has been used in reference to clandestine devices in the past.

[20] Other definitions include demolition charges.

[21] See: IMAS 04.10, 2nd Ed, 1 Jan 03, Amd 7, Aug 14, Glossary of Mine Action.

[22] Some EOD definitions have identification and evaluation procedures under the combined heading of diagnosis.

[23] Those courses or modes of action taken by EOD personnel on items of EO that cause such items to be placed in a state of tolerable risk unlikely to cause harm, injury, or damage, through the application of special EOD methods and tools to provide for the interruption of functions or separation of essential components thus preventing an unacceptable initiation.

19. **IED** is an Improvised Explosive Device, which refers to a device placed or fabricated in an improvised manner, incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals, and is designed to destroy, incapacitate, harass, or distract the adversary/ies. It may incorporate military stores but is normally devised from nonmilitary components.

20. **MIAP** is the Mission Information Acquisition Plan. It translates the strategic direction provided by Senior Mission Leadership and requirements communicated by operational planners into information requirements, and provides a roadmap for the fulfillment thereof. Further, the MIAP serves as the primary basis for the development of acquisition plans by the Mission PKI entities. See para. 12.7. of the Peacekeeping-Intelligence Policy for further details.

21. **MICM** is the Mission Peacekeeping-Intelligence Coordination Mechanism. The MICM directs and oversees the PKI cycle within the Mission, and comprises, at minimum, the PKI entities therein. The overall objective of the Mechanism is to serve as the central control and to direct the Mission's PKI cycle. See paras. 12.2.-12.6. of the Peacekeeping-Intelligence Policy for further details.

22. **MISP** is the Mission Peacekeeping-Intelligence Support Plan. It outlines the boundaries within which the PKI cycle will be executed, and identifies key considerations to be observed when providing direction to the PKI cycle or executing tasks within it. See para. 12.8. of the Peacekeeping-Intelligence Policy for further details.

23. **IRs** are Information Requirements. IRs derive from gaps between what is known and what is not about a particular issue. Usually phrased as questions, IRs form the basis of an MIAP. See para. 12.9. of the Peacekeeping-Intelligence Policy for further details.

24. **TPKI** is Technical Peacekeeping-Intelligence. TPKI refers to PKI derived from the acquisition, exploitation and analysis of military equipment and any material posing a potential threat, including conventional and asymmetric threat weapons systems and associated components.

F. REFERENCES

General Assembly and Security Council References

- Report of the Special Committee on Peacekeeping Operations, 2020 Substantive Section (A/74/19)

Normative or Superior References

- DPO Policy on Peacekeeping-Intelligence (2019.08)
- DPO-DOS Policy on Joint Mission Analysis Centres (JMAC) (2020.06)
- DPO Policy on the Protection of Civilians in United Nations Peacekeeping (2023.05)
- DPKO-DFS-DPA Policy on Child Protection in United Nations Peace Operations (2017.11)
- Human Rights Due Diligence Policy on United Nations Support to Non-United Nations Security Forces (A/67/775–S/2013/110) (2011)

- Secretary-General's Bulletin on Record-keeping and the Management of United Nations Archives (ST/SGB/2007/5) (2007)
- Secretary-General's Bulletin on Information Sensitivity, Classification and Handling (ST/SGB/2007/6) (2007)
- Counter-Improvised Explosive Devices (C-IED) Strategy for Peacekeeping Operations (2024)

Related Guidelines or Procedures

- Joint Mission Analysis Center Handbook (2018.03)
- Military Peacekeeping-Intelligence Handbook (2019)
- The Protection of Civilians in United Nations Peacekeeping Handbook (2020)
- Peacekeeping-Intelligence Surveillance and Reconnaissance Staff Handbook (2020)
- Guidelines on Acquisition of Information from Human Sources for Peacekeeping-Intelligence (2020.05)
- Guidelines on Open-Source Peacekeeping-Intelligence (2022.03)
- Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities (2022.05)
- Guidelines on Gender and PKI (2022.08)
- Improvised Explosive Device (IED) Threat Mitigation Handbook (2025 update pending signature)
- Guidelines on Improvised Explosive Device Threat Mitigation in Mission Settings (2021.08)
- United Nations Peacekeeping Missions Military Explosive Ordnance Disposal (EOD) Unit Manual (2025 update pending signature)

G. MONITORING AND COMPLIANCE

25. Within Missions, the Head of Mission is accountable for the Mission's compliance with these Guidelines, and shall establish mechanisms or processes to enable the effective monitoring of compliance. All Mission personnel participating in the peacekeeping-intelligence system are accountable through their chains of management/command for compliance with the Peacekeeping-Intelligence Policy and these Guidelines.

H. CONTACT

26. The contact for these guidelines is the Peacekeeping-Intelligence Coordination Team (PICT) in DPO/OUSG.

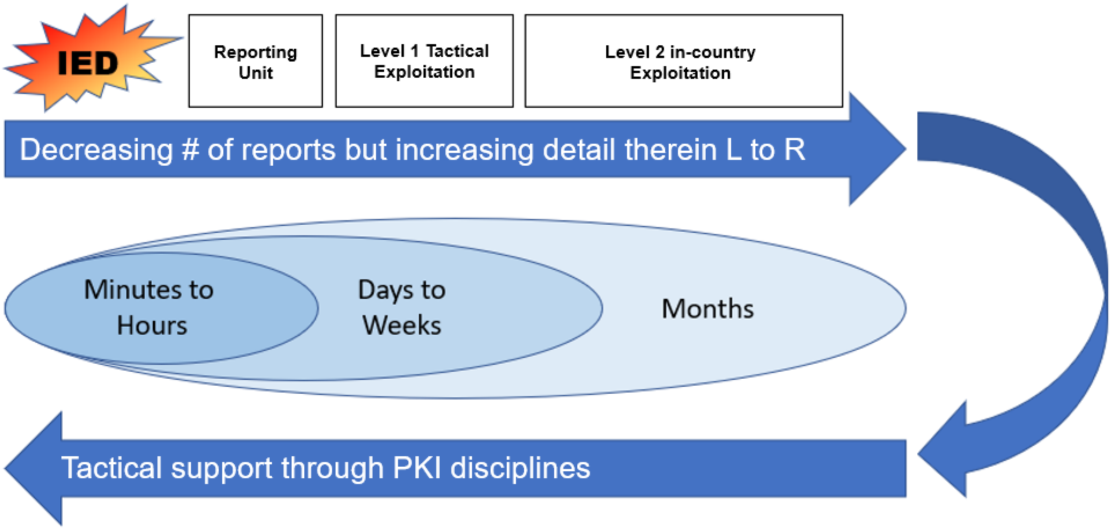
I. HISTORY

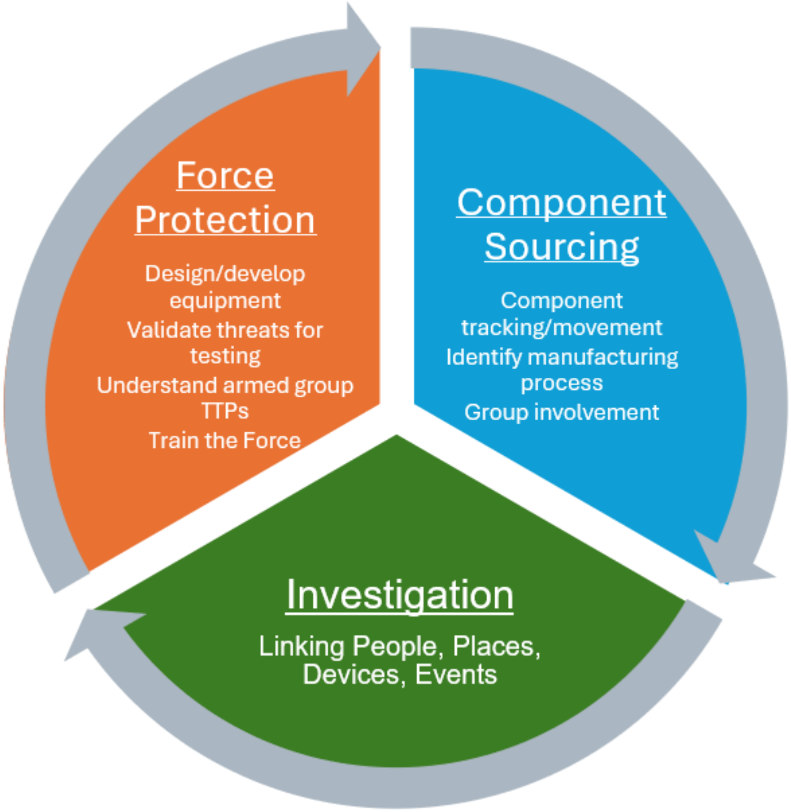
27. This is the first iteration of these Guidelines.

APPROVAL SIGNATURE:
Jean-Pierre Lacroix, USG for Peace Operations

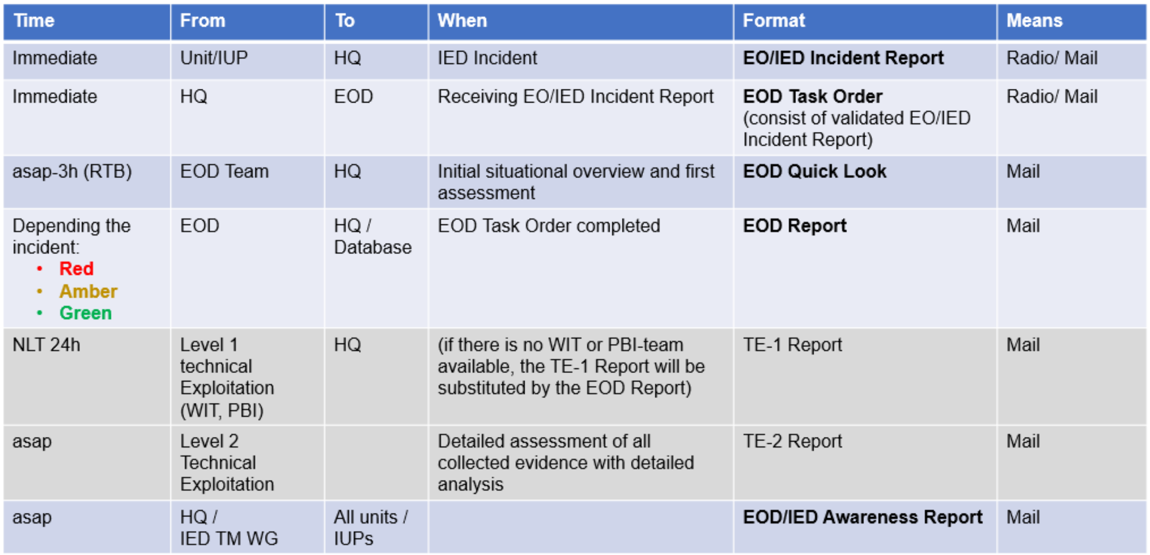
DATE OF APPROVAL: 19 February 2025

ANNEX A: TPKI FLOW AND TPKI SYSTEM DIAGRAM


IED
Reporting Unit
Level 1 Tactical Exploitation
Level 2 in-country Exploitation
Decreasing # of reports but increasing detail therein L to R
Minutes to Hours
Days to Weeks
Months
Tactical support through PKI disciplines


Force Protection
Design/develop equipment
Validate threats for testing
Understand armed group TTPs
Train the Force
Component Sourcing
Component tracking/movement
Identify manufacturing process
Group involvement
Investigation
Linking People, Places, Devices, Events

ANNEX B: TECHNICAL EXPLOITATION (TEMPLATES AND EXAMPLES)



Time	From	To	When	Format	Means
Immediate	Unit/IUP	HQ	IED Incident	**EO/IED Incident Report**	Radio/ Mail
Immediate	HQ	EOD	Receiving EO/IED Incident Report	**EOD Task Order** (consist of validated EO/IED Incident Report)	Radio/ Mail
asap-3h (RTB)	EOD Team	HQ	Initial situational overview and first assessment	**EOD Quick Look**	Mail
Depending the incident: • **Red** • **Amber** • **Green**	EOD	HQ / Database	EOD Task Order completed	**EOD Report**	Mail
NLT 24h	Level 1 technical Exploitation (WIT, PBI)	HQ	(if there is no WIT or PBI-team available, the TE-1 Report will be substituted by the EOD Report)	TE-1 Report	Mail
asap	Level 2 Technical Exploitation		Detailed assessment of all collected evidence with detailed analysis	TE-2 Report	Mail
asap	HQ / IED TM WG	All units / IUPs		**EOD/IED Awareness Report**	Mail

(TEMPLATE) Level 1 Technical Exploitation (TE-1)

Date of report:	*Date-Time-Group (DTG) of when report was created* *DD, hh mm, Time Group, MMM,YY*
Date of release:	*Date-Time-Group (DTG) of when report was release* *DD, hh mm, Time Group, MMM,YY*
File reference:	*This-file-filename.docx*
Attachments:	
Case number:	##### (From TOC)

Assessments are made using the following confidence levels:

<10%	10-40%	40-60%	60-90%	>90%
Highly unlikely	Unlikely	Possible	Likely	Highly likely

LEVEL 1 EXPLOITATION REPORT

Priority Level:	**RED** *See classification of EOD Report*

BLUF:

Brief Executive summary of the report assessing the likelihood of the events, findings, etc.

e.g.:

Due to the findings of weapons and ammunition in the vehicle it is unlikely that the XY was the intended target, instead it is possible that the perpetrator initiated the PBIED when being approached at the reinforced checkpoint.

Findings on the scene indicates that it is possible that the perpetrator had been tasked to conduct an attack on the nearby HNSF Camp that is located in XY.

Device Description:

	Primary description:	
	Secondary / Tertiary Devices description:	

Basic Information:

DTG of event:	*Date-Time-Group (DTG) of event* *DD, hh mm, Time Group, MMM,YY*
Associated reports:	

Location:	**MGRS:**	*MGRS Grid reference (8-digit)*
	Village:	
	District:	
	Region:	
Timeline of events:	XX:XX	*Zulu time (Z) or Local time (L)*
	XX:XX	
	XX:XX	

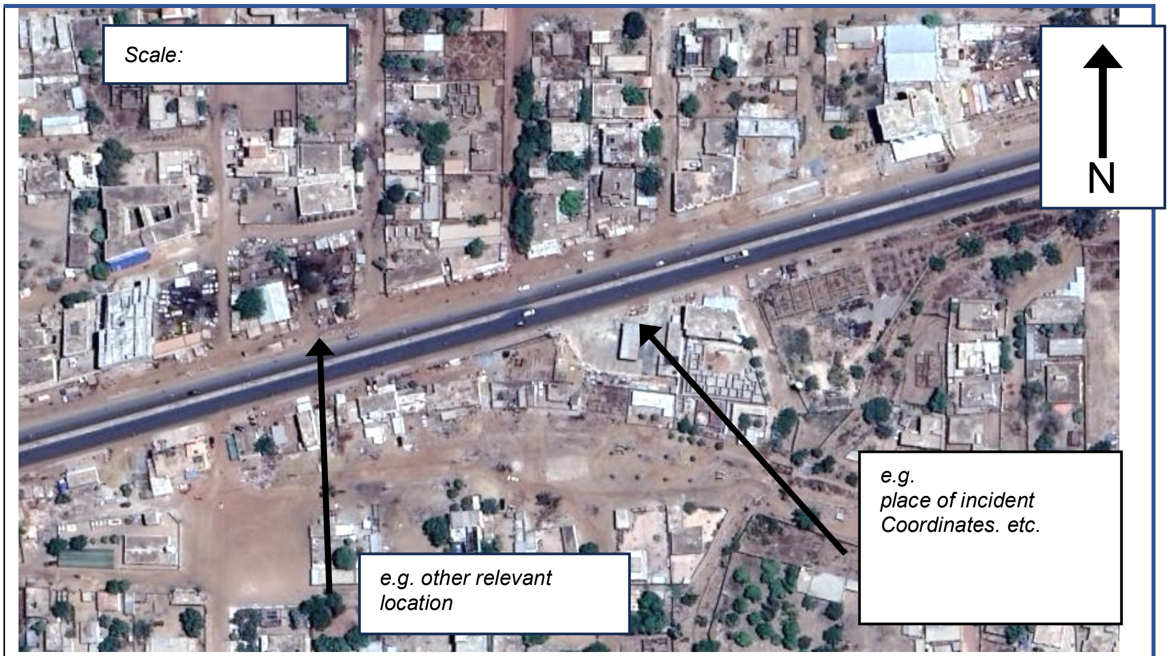
	XX:XX							
Target:								
Detainees:	**YES** ☐ and number:				**NO** ☐			
Casualties:	**UN**		**Perpetrator**		**HNSF** (Host Nation Security Forces)		**Civilians**	
	WIA:	KIA:	WIA:	KIA:	WIA:	KIA:	WIA :	KIA:
Battle Damage Assessment:								

Background to the incident (description)

Supporting Images of the region, location, location of the incident, including satellite images of the incident site with location of the e.g. detonation, position of own forces and host nation, e.g.

Example:

Example:

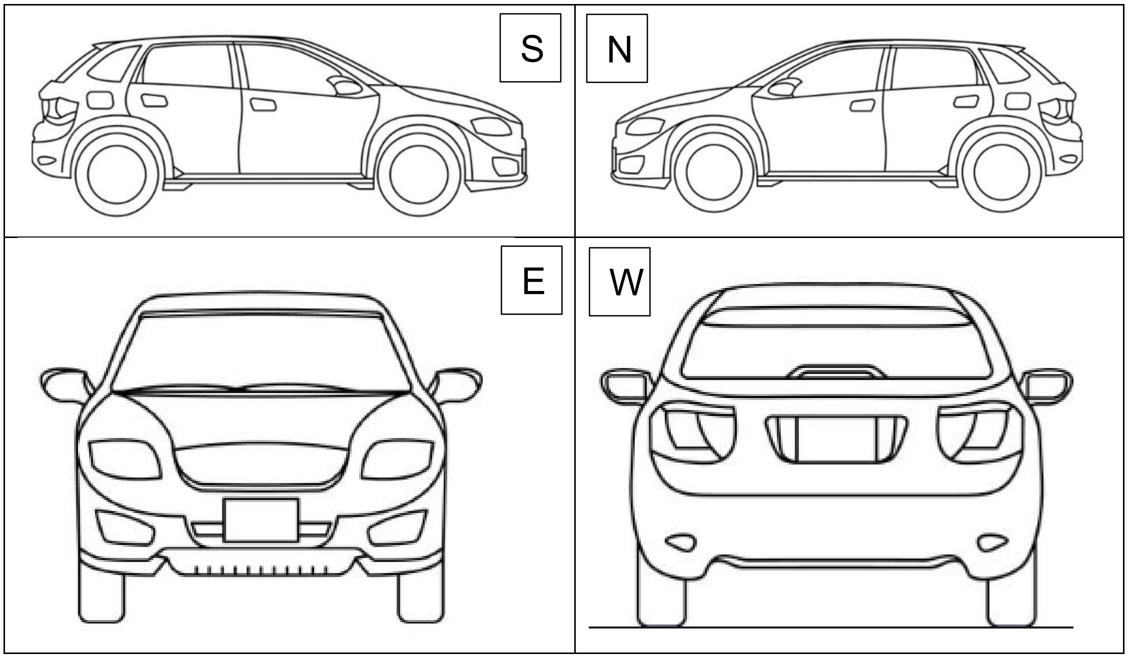


Example:

Scale:
N
e.g. other relevant location

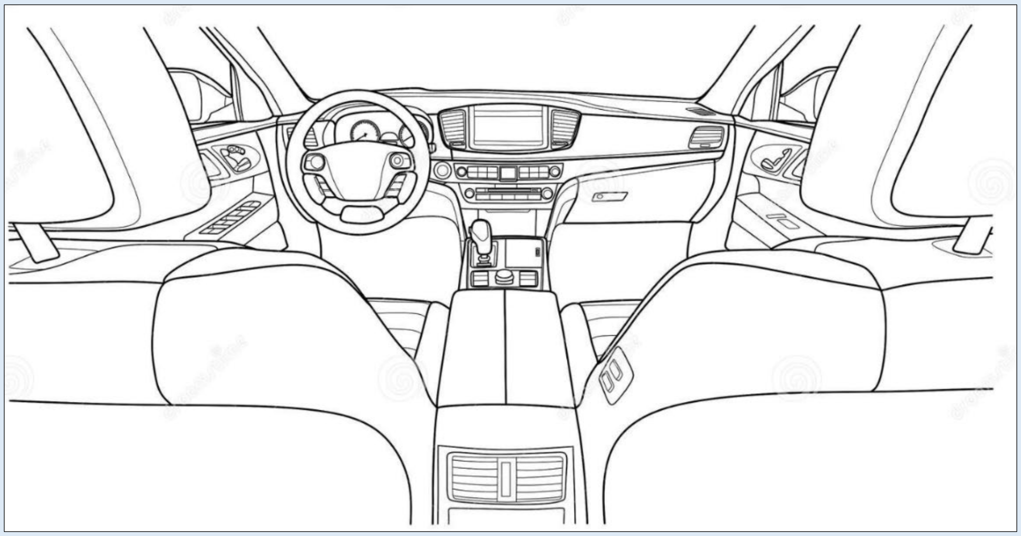
Cardinal pictures of the scene

Example:



Cardinal pictures of the scene (Details)

Example:



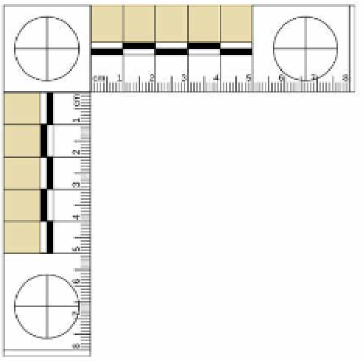
Device Construction and Method of Operation

Evidence recovered:

1.
2.

3.

List of items recovered from scene with short description, followed by a photograph (see below)

Main Charge:	 *Picture of the item with forensic ruler for reference* *Brief description of the item.* *If possible, add weight, length or any other characteristic that is of relevance.*
Power Supply:	
Container:	
Initiator:	
Switch:	
Enhancements:	
Weapons:	*Weapons recovered from scene + ammunition*
Documents:	
Other items of relevance:	*e.g.: mobile phones, clothes recovered from scene,*

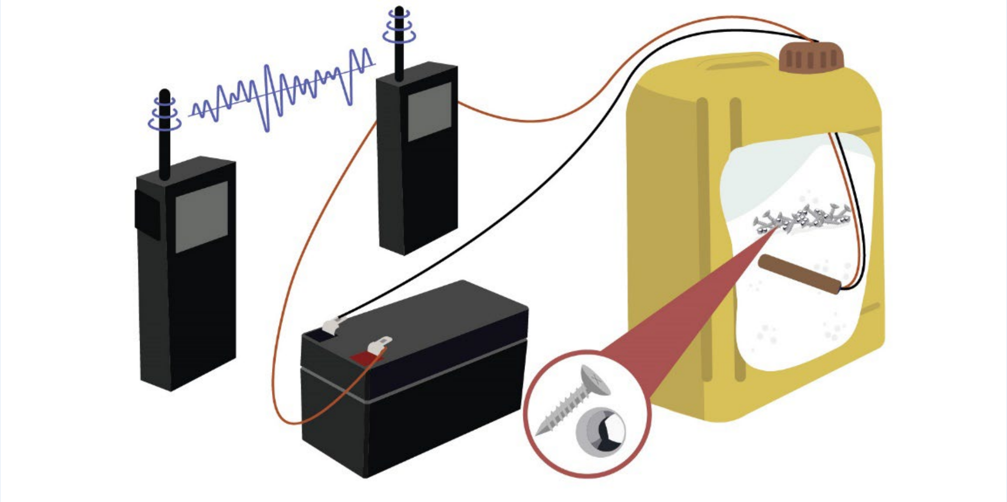
All recovered material sent to Level 2?	**YES ☐**	**NO ☐**	**Not Applicable (NA) ☐**
	Detailed information:		
Requirement for further exploitation (Level 2):	**YES ☐**	**NO ☐**	**Not Applicable (NA) ☐**
	Detailed information:		
Disposition of CEM from Level 1:	*Reason why Level 2 should prioritize the Level 2 Exploitation as GREEN, AMBER or RED.*		

Method of functioning:

e.g.:
The material found on scene indicates the following method of functioning:

Picture of method of functioning:

Example:



If possible, add an picture reconstructing the method of functioning.
Add information which helps the receiver of the report to understand what happened, both tactically or technically.

Delivery Method:			
Emplacement:	*Description of the emplacement methos*		
Geography:	*Description of the geography of the location of the incident*		
Atmospherics:			
History:	**YES** ☐	**NO** ☐	**Not Applicable (NA)** ☐
	Details: *Comparison with identical or similar cases, making*		
Investigators Comments	**Facts:**		
	Comments:		
	Assessment:		
	Recommendations:		
Exploitation Asset:			
Investigators:			

(Template) Level 2 Technical Exploitation (TE-2) Report

Line	Item	Sub item		
Line 1	Intend Lab Commander	A	Priority	
		B	Specification	
Line 2	Weapons Technical Peacekeeping-Intelligence (WTPKI) - Summary Report	A	Free	
Line 3	Exploitation Manager	A	Free	
Line 4	TRIAGE - Summary Report	A	Hazard	
		B	General	
Line 5	Chemical Exploitation (CHEMEX) - Summary Report	A	Explosive	
		B	Precursor	
		C	Initiator	
		D	Igniter	
		E	Blasting Accessories	
		F	Other	
Line 6	Forensic Exploitation (FOREX) - Summary Report	A	Latent Print	
		B	DNA	
		C	Tools	
		D	Firearms	
		E	Other	
Line 7	Electronical Exploitation (ELEX)	A	Switch	
		B	RC-Devices	
		C	Other	
Line 8	Cellphone Exploitation (CELLEX)	A	Free	
Line 9	Documental and Media Exploitation (DOMEX)	A	Documents	
		B	Picture	
		C	Movie	
		D	Electronic Data	
Line 10	Lab Commanders Executive Summary	A	Technical	
		B	Tactical	
		C	TTP	
		D	So What	
Line 11	Annexes	A	Intend Lab Commander	
		B	Weapons Technical PKI (WTPKI)	
		C	Exploitation Manager	
		D	TRIAGE	
		E	Chemical Exploitation (CHEMEX)	
		F	Forensic Exploitation (FOREX)	
		G	Electronical Exploitation (ELEX)	

		H	Documental and Media Exploitation (DOMEX)	
		I	Lab Commanders Executive Summary	
		J	Photo	
		K	Picture	
		L	Movie	
		M	X-Ray	
		N	Other	