United Nations
Department of Peace Operations
Ref. 2020.05

Guidelines

Acquisition of Information from Human Sources for Peacekeeping-Intelligence (HPKI)

Approved by:	Jean-Pierre Lacroix, USG DPO
Effective date:	*1 September 2020*
Contact:	*DPO/OUSG/PICT*
Review date:	*1 September 2022*

Provide Feedback Here:

DPO GUIDELINES ON
Acquisition of Information from Human Sources for Peacekeeping-Intelligence (HPKI)

Contents:

ANNEXURES

A. PURPOSE

1. The purpose of these Guidelines is both to provide a legal and operational framework for and to facilitate the safe acquisition of information from human sources for peacekeeping-intelligence (thereafter "HPKI"). These Guidelines are part of the Peacekeeping-Intelligence Framework and should be read in conjunction with the DPO Policy on Peacekeeping-Intelligence[1] (hereafter "the Policy"). Neither these guidelines nor the Policy provide any type of training.

2. These guidelines do not apply to the questioning of detained or captured persons, which is regulated by other SOPs.

B. SCOPE

3. This guidance document shall apply to all serving members of United Nations peacekeeping operations. Compliance with these Guidelines is mandatory[2].

3.1. The Principles of Peacekeeping-Intelligence are to be strictly complied with. They are as follows:

[1] Policy on Peacekeeping-Intelligence, DPO, 2019

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

3.2. **Under rules**: All peacekeeping-intelligence activities will be undertaken in line with the Security Council mandates of peacekeeping operations, in full compliance with the Charter of the United Nations. These activities shall be consistent with the overall legal framework governing United Nations peacekeeping operations, including the basic principles of peacekeeping and all legal and human rights standards and obligations. Peacekeeping-intelligence activities must be conducted with full respect for human rights, including, in particular, the rights to privacy, freedom of expression, peaceful assembly, and association, and with particular care not to expose any sources or potential sources of information to harm.

3.3. **Non-clandestine**: **Clandestine activities, defined as the acquisition of information or intelligence conducted in such a way as to assure secrecy or concealment of the activities, because they are illicit and/or are inconsistent with the legal framework, principles, policies and mandates of United Nations peacekeeping operations, are outside the boundaries of peacekeeping-intelligence and shall not be undertaken by participating mission entities.** Regular training and education, including standardized pre-deployment training for all personnel involved in all aspects of peacekeeping-intelligence, as well as regular audits and oversight of the peacekeeping-intelligence workflow, will reinforce this principle.

3.4. **Areas of application**: The acquisition and management of information or intelligence by United Nations peacekeeping operations will be conducted 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.

3.5. **Respect of State sovereignty**: The sovereignty of states, including Host and neighboring States, must be respected.

3.6. **Independence**: The peacekeeping-intelligence activities of peacekeeping operations will be fully autonomous from and independent in all aspects of any national intelligence system or other operations and will maintain their exclusively international character. Missions may liaise with non-mission entities for the purposes of receiving intelligence and may share specific peacekeeping-intelligence with non-mission entities, including Host States, provided they do so under conditions and within the parameters described in this document and related guidance.

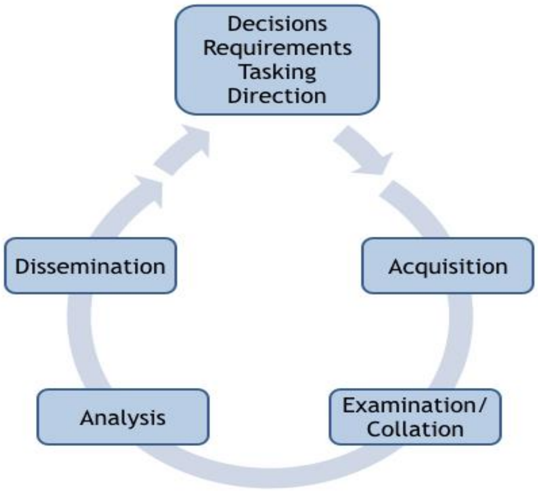
3.7. **Accountability, capability and authority**: Those who are given the authority to make decisions with regard to peacekeeping-intelligence activities must have the appropriate capabilities to execute these functions and remain accountable for the effective execution of these responsibilities within their respective chains of command to the Head of Mission and ultimately to the Secretary-General. Within the mission, the Head of Mission is accountable for the functioning of the peacekeeping-intelligence system. She/He is responsible for ensuring compliance with this Policy and associated guidance by personnel engaged with or using peacekeeping-intelligence products, through effective governance procedures, training and practices.

3.8. **Security and confidentiality**: Peacekeeping-intelligence shall be stored and shared in a secure manner, while ensuring access for those who require it for decision-making and operational planning. Based on an assessment of risk, missions will put in place procedural, technological and physical security tools in consultation with DPO and DOS Headquarters to ensure secure information management and communications within the peacekeeping-intelligence system. Confidential peacekeeping-intelligence products shall be shared and disseminated on the basis of the “need to know” and “need to share” concepts, which require that peacekeeping-intelligence should be disclosed to mission personnel if and only if access to said information is required for them to carry out their official duties. It also requires a written delegation of authority from the originator or staff member who originally applied the classification level. It implies that peacekeeping-intelligence is only disclosed to trusted individuals to ensure that it is not widely disseminated, in particular where disclosure is likely to result in the endangerment of the safety or security of any individual or group, violate rights or invade privacy. In doing so, missions will seek to establish and maintain a high degree of confidence among all of their interlocutors in their ability to appropriately acquire, protect and manage peacekeeping-intelligence.

C. RATIONALE

4. The Policy "sets out why and how United Nations peacekeeping operations acquire, collate, analyze, disseminate, use, protect and manage peacekeeping-intelligence in support of United Nations peacekeeping operations in the field." The acquisition of information refers to the second step of the peacekeeping-intelligence cycle (Figure 1)

Figure 1. The Peacekeeping-Intelligence Cycle



5. The Policy defines the acquisition step as follows: **"Acquisition refers to the process of obtaining data and information to serve as the basis for analysis. Effective acquisition requires direction and planning to ensure resources are used in such a manner as to most effectively meet the Peacekeeping-Intelligence Requirements (IRs). This includes tasking assets according to IRs, ensuring data and information is reported in a timely manner, tasking assets within their capabilities, and putting in place mechanisms to ensure corroboration and/or verification of information and data as appropriate**."

6. The Policy also states that "The parameters for the effective, responsible, and ethical acquisition of peacekeeping-intelligence shall be described in the mission's Peacekeeping-Intelligence Support Plan. In addition to being compliant with this and other United Nations policies and guidance, the latter will describe acceptable and unacceptable tools, techniques, and procedures of information acquisition by the mission, applicable legal obligations, and considerations that shall be undertaken when acquiring peacekeeping-intelligence, based on the assets available to the mission and in line with operational guidance that is subordinate to this Policy."

7. In UN Peacekeeping, HPKI is the peacekeeping-intelligence derived from information acquired from, and provided by, human sources. It uses human sources as a vector to gather, both actively and passively, information to satisfy IRs.

8. The acquisition of information from human sources can be generally divided into four categories, based on the acquisition methods used. It is considered HPKI only if the acquisition of information is **directed**.

8.1. Undirected, **casual:** Casual, undirected acquisition refers to the gathering of information from human sources, but not in response to specific peacekeeping-intelligence requirements. Examples would include information gained from casual interactions with the local population by infantry units on patrol, or daily reporting of information on the general situation by Community Liaison Assistants based on interactions with members of the local population. This can also be referred to as passive acquisition. **This is not HPKI, and is performed by any UN personnel on a daily basis while they are engaging with any interlocutor.**

8.2. Directed, but **un-incentivized**: This category refers to the same type of acquisition methods as above but conducted as part of the peacekeeping-intelligence cycle. In other words, information is collected in response to IRs developed at the mission level. This acquisition method requires a more active role in order to direct the source to acquire the needed information. **This is the core method of HPKI.**

8.3. Directed and **incentivized**, but not clandestine: The incentive approach implies trading something that the source wants for information. **This method of acquisition is strictly forbidden under the Peacekeeping-Intelligence Policy (see paragraph 3.3.) and may have serious implications for UN personnel (military, police and civilian), sources and for the United Nations as a whole. This method of acquisition is included here with the sole purpose of indicating what should not be done.**

8.4. Directed, **incentivized and/or clandestine**: ‘‘Clandestine” refers to the acquisition of information in a way designed to conceal the nature of the operation. Activities are undertaken with the intent to assure secrecy and concealment. Sources are approached by an agent, who would use disingenuous methods to build rapport with sources, including presenting oneself under a false identity or misrepresenting the truth about one’s employer **This method of acquisition is strictly forbidden under the Peacekeeping-Intelligence Policy (see paragraph 3.3.) and may have serious implications for UN personnel (military, police and civilian), sources and for the United Nations as a whole. This method of acquisition is included here with the sole purpose of indicating what should not be done.**

9. Mission entities, other than the core members of the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM)[3] as described in Annex B of the Policy, **shall not resort to HPKI** (paragraph 8.2.) to acquire information, unless exceptionally authorized by the MICM. **The undirected, casual method (para 8.1) is a common way to acquire information from human sources for mission components other than the MICM core members.**

10. As far as the core entities of the MICM are concerned, it is not mandatory for them to resort to HPKI. Should it be decided that they would, these guidelines must be followed.

[3] JMAC, UNDSS, JOC (supporting), Force, Police Component.

11. Based on the above parameters the present guidelines have been developed to provide guidance to peacekeeping operations on how to perform HPKI therein.

D. Guidelines

12. General rules

12.1. **HPKI activities shall only be considered after careful determination that the acquisition of the necessary information from other sources has proven impossible or inconclusive.**

12.2. All HPKI operations will 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.

12.3. All HPKI operations will 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.

12.4. In line with the DPO Policy on Peacekeeping-Intelligence, all HPKI operations must be conducted in a **non-clandestine manner** (see para. 3.3.).

12.5. HPKI personnel should neither conceal the fact that they work for the UN, nor, under any circumstances, operate under fake identities.

12.6. All HPKI operations will be conducted strictly in support of the Mission Information Acquisition Plan (MIAP) and in accordance with the Mission Peacekeeping-Intelligence Support Plan (MISP).

12.7. All HPKI operations, while being conducted, must always prioritize the safety and security of mission personnel (including HPKI personnel) and sources.

12.8. Children must not be used as HPKI sources.

12.9. **HPKI sources cannot be Host State employees or affiliated personnel**, unless the relationship has been approved in advance by both the Head of Mission and the Host State.

12.10. HPKI sources cannot be individuals subject to active domestic or international arrest warrants, unless the approvals of the Head of Mission and the Host State have been secured in advance, after consultation with the Senior Legal Adviser.

12.11. The engagement of sources with known human rights violation records shall be first approved by the Head of Mission, in consultation with Headquarters (DPO and OHCHR).

12.12. HPKI sources cannot be tasked to acquire information. They can be asked to acquire information.

12.13. HPKI sources should never be asked or encouraged to break any applicable laws.

12.14. **No amount of money will be paid, nor gifts offered, to HPKI sources, or their relatives, in remuneration for information.**

12.15. Whenever possible, HPKI operations should be carried out by trained human source handlers, and possessing the specific skill sets determined by UN Headquarters. Wherever possible, the establishment of HPKI cells within Mission Components[4] is highly encouraged.

12.16. All HPKI operations - military, police and civilian - will be coordinated by a single HPKI coordinator at the mission level, to avoid, for example, the duplication of efforts, or undesired multiple contacts with the same source from different human source handlers.

12.17. HPKI personnel will occasionally require support (force protection, interpreters), for their operations. Decisions on such support should be based on mission priorities and available resources.

12.18. HPKI personnel are limited by, inter alia: language capabilities; limited resources; force protection requirements; and the time it takes to develop human sources. Acquisition activities should therefore be clearly prioritized and be coordinated, or deconflicted if necessary.

12.19. **Information acquired through HPKI operations is not inherently more valuable than other sources of information.**

12.20. HPKI operations are never carried out by an individual operating alone. The basis for HPKI operations is that a minimum of two personnel is required for HPKI operations conducted in a permissive environment. Whenever possible, a mixed-gender team is ideal.

12.21. If, after a thorough assessment, it is determined that gender considerations may be intentionally taken into account in order to acquire information from a human source, it should always be done in full transparency and with the full consent of the staff members involved, and their safety should be ensured at all times.[5]

12.22. By nature, HPKI operations are sensitive and require a high-degree of operational security. Accordingly, information acquired through HPKI operations should be shared without referring to or providing any details that might lead to the identification of its source or the methods used in its acquisition. The safety of sources must be a paramount concern in HPKI operations and should take precedence over other considerations.

[4] JMAC, UNDSS, JOC (supporting), Force, Police Component.

[5] For example, a human source the Mission would like to acquire information from is known to respond more favorably to being engaged by a woman. While it is acceptable to assign a woman staff member to acquire information from that human source, she should be informed as to the particular propensity of the human source, and provide her consent (or not) to the assignment only once she has been informed. Her safety should be ensured at all times. The same would be applicable, obviously, to a man staff member.

12.23. In line with the Policy, the Head of Mission (HoM) or a delegated authority is permitted to share information, including that acquired through HPKI operations, with non-UN actors (ref to Guidelines on the Exchange of Intelligence/Peacekeeping-Intelligence with Non-Mission and Non-UN Entities). In so doing, some information acquired in HPKI operations may implicate a source, if that information can be linked to a geographic area, or to an event. In such cases, the HoM or delegated authority should consult the Chief of the HPKI cell that acquired the information or DPO for guidance. The safety and security of human sources is paramount, and these considerations must first and foremost inform relevant decision-making.

13. Direction

13.1. The head of the Mission Component[6] must ascertain IRs, and will ensure that tasking is in line with his/her entity's capabilities and limitations;

13.2. All HPKI activities will be conducted in support of the Mission and component IAPs;

13.3. HPKI activities must be structured to ensure that source coverage exists in all required thematic and geographic areas; where gaps in thematic and geographic coverage exist, the component HPKI cell will work to close those gaps with the targeted development of the human source network in its Area of Peacekeeping-Intelligence Responsibility;

14. Acquisition/HPKI operation

14.1. Prior to any HPKI activity, the HPKI cell must ensure the following:

14.1.1. The threat in the area is fully understood;

14.1.2. A full operational risk assessment is carried out;

14.1.3. The operation is deconflicted with other UN elements of the peacekeeping operation in the area;

14.1.4. Adequate protection or safety/security measures are in place, including, if required, a Quick Reaction Force (QRF);

14.1.5. The conversation is planned in line with best practice (see sample conversation plan in Annex D);

14.1.6. A risk assessment is conducted to determine i) whether the source might face threats or be subjected to reprisals, including as a result of their gender, ii) what are the security and/or vulnerability factors that might expose the source to risk of harm, especially as it pertains to their gender,[7][8] iii) what preventive or protective measures (if any) can be taken to minimize the risk of harm, iv) what self-protection measures (if any) can the source adopt, and v) what is the capacity and/or commitment of the Host State authorities to respond to protection concerns for the source, and mitigating measures are identified by the mission;

14.1.7. The information acquisition is in line with the applicable (mission or component) IAP; and

14.1.8. All possible contingencies are prepared and rehearsed.

14.2. During an HPKI operation, HPKI personnel must ensure that:

[6] JMAC, UNDSS, JOC (supporting), Force, Police Component.

[7] All sources, including but not limited to women sources, have possible vulnerabilities as a result of their gender.

[8] Risks should be assessed not only for the UN in approaching a source, but also for the source in being approached by the UN. Only once risks to both sides have been analyzed and weighed against its benefits, a determination should be made as to whether and/or how the UN should engage with the potential source.

14.2.1. The conversation elicits, as much as possible, the required information;
14.2.2. UN policies are adhered to;
14.2.3. The safety of UN personnel and sources is maintained throughout; and
14.2.4. The source is treated with dignity and respect at all times, in compliance with internationally recognized human rights standards and international human rights law.

14.3. After an HPKI operation, the HPKI cell must:
14.3.1. Report the details of the conversation to its Mission Component[9] in the form of a Contact Report (see outline in Annex C);
14.3.2. Report mission critical/urgent information to its Mission Component[10] via the quickest available means – this may mean by phone; and
14.3.3. Ensure that all information acquired is presented in the form of raw information, and if necessary, accompanied by a qualifying comment and source grading;
14.3.4. Ensure that measures are in place to safeguard the ongoing safety of the source and his or her protection against any retaliation, including by keeping his or her identity as a UN source confidential.

14.4. HPKI personnel are trained and thus expected to consider the source's physical security before, during and after meetings, and to advise the source of the steps that may be necessary to secure such security.

15. Collation

15.1. Information acquired during HPKI operations shall be collated on a stand-alone HPKI component collation system (mostly registers), which will be fully separate from the peacekeeping-intelligence regular collation system;

15.2. Information acquired through HPKI operations will be recorded on a collation system with the following details: date of information; acquisition date of information; source alias; source credibility; information reliability; subject of information; link to the original source document; link to source contact form (see Annex B for an example);

15.3. All sources will immediately be assigned an alias, which is to be used in all correspondence relating to that source, when it is necessary to specifically refer to the source. In all other cases, source information can be transmitted with just a reliability and credibility label (ex. a local source (B) reports that "XXXX" (3)).

15.4. Files containing aggregated information on the sources (particularly name and alias) need to be stored on an encrypted hard drive disk, which will be stored in a secure location with restricted access when not in use and will only be connected to computer that are not linked to a network.

15.5. All human sources will be graded for reliability and information for credibility, using the tables below. Every item of information must be rated in the form of an alphanumeric code whereby the 'Letter' indicates the reliability of the source (Table 1) and the 'Figure' indicates the credibility of information (Table 2).

[9] JMAC, UNDSS, JOC (supporting), Force, Police Component.
[10] JMAC, UNDSS, JOC (supporting), Force, Police Component.

Table 1. Rating of source reliability

Source Reliability		
Rating	Evaluation	**Observations**
A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
D	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
E	Cannot Be Judged	No basis exists for evaluating the reliability of the source

Table 2. Rating of information credibility

Credibility of Information		
Rating	**Evaluation**	**Observations**
1	Confirmed	Confirmed by other independent sources; logical in itself; Consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
4	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
5	Cannot Be Judged	No basis exists for evaluating the validity of the information

15.6. A good guideline for systematic source evaluation is to assess:

15.6.1. The source's **access** (what can he/she reliably report on);

15.6.2. The source's **motivation** (why is the source talking to the HPKI team, does the source display conscious or unconscious bias);

15.6.3. The source's **potential** (can this source be asked to acquire specific information), and;

15.6.4. The source's **capability** (is the source literate, what skill sets does the source have, does the source have situational awareness, does the source have analytical skills).

15.7. In order to maintain operational security, police, military and civilian components will maintain separate up-to-date source registers; all registers will be made available to the HPKI coordinator.

15.8. The registration of sources will be done using a standard UN source registration form (see Annex A), which will contain the personal details of the source. The importance of source registration cannot be overstated, as it enhances the credibility of information acquired by mitigating the risk of undesired circular reporting.

15.9. The HPKI coordinator will be responsible for deconflicting HPKI operations, and for coordinating HPKI information sharing. If necessary, the Chair of the MICM may request that the different HPKI components share source information, if a risk of undesired circular reporting on an important element of information is identified.

16. Analysis

16.1. Although a HPKI cell may engage in analysis, they will not have access to all information available to their respective peacekeeping-intelligence component[11]. It is therefore vital that the raw information acquired by HPKI personnel are systematically shared with the relevant peacekeeping-intelligence component for integration and interpretation;

16.2. When raw information is shared by a HPKI cell with its peacekeeping-intelligence component, it must be transmitted in a manner that ensures the integrity of the information while protecting the identity of the human source. In practice, this would mean giving the information together with an evaluation of the source (see Table 1 above).

17. Dissemination

17.1. Information acquired by a HPKI cell that warns of an imminent threat to UN personnel or to civilian populations, must be immediately disseminated to its peacekeeping-intelligence component[12] via the quickest and most secure available means. In practice, this means that a mobile phone may be used. The PKI Component will then **immediately** alert all other Members of the MICM, including the Mission Chief of Staff. Regardless of the means used, all HPKI personnel must continue to ensure that source protection is paramount, and be aware of issues related to the security of communication means.

17.2. Routine information acquired will be communicated to the peacekeeping-intelligence component in the form of a Contact Report (Annex C).

17.3. The following dissemination principles shall be adhered to:

17.3.1. **Timeliness** – Acquired information must be delivered in a timely manner so planners and decision makers can act rather than react;

17.3.2. **Relevance** – Is determined by the needs of the recipients as defined in the applicable (mission or component) IAP;

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

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

[11] JMAC, UNDSS, JOC (supporting), Force, Police Component.

[12] JMAC, UNDSS, JOC (supporting), U2, Police Component.

F. TERMS AND DEFINITIONS

18. **Area of Peacekeeping-Intelligence Responsibility** is the geographic area where information can be acquired. It coincides with the UN Area of Operational Responsibility.

19. **HPKI** is the elicitation of information from human sources in a structured, lawful and non-clandestine manner.

20. **Component HPKI cell** refers to a military, police or civilian HPKI cell.

21. **Human source** refers to an individual who is willing to share information with UN HPKI personnel deployed in a UN peacekeeping operation. Potential HPKI sources include hostile, neutral, and friendly individuals. Categories of HPKI sources may include refugees and Internally Displaced Persons (IDPs), the local population, friendly forces, non-state actors, and non-governmental organizations (NGOs).

22. **Human source handlers** are qualified civilian or uniformed UN personnel trained in HPKI techniques, specifically deployed for and tasked with the acquisition of information from human sources.

23. **HPKI operation** refers to the planning and safe execution of an operation in a peacekeeping mission to elicit information from human sources in a safe, legal and non-clandestine manner.

24. **Human source protection** refers to the necessary measures to ensure the human source's physical safety and security before, during, and after a meeting or contact, and maintaining the confidentiality of the human source's personal details and of the fact that the source provided information to the United Nations.

G. REFERENCES

General Assembly and Security Council References

Report of the Special Committee on Peacekeeping Operations, 2018 Substantive Section (A/72/19)

Normative or Superior References

DPO Policy on Peacekeeping-Intelligence, 2019
DPKO-DFS Policy on Joint Mission Analysis Centres (JMAC), 2015 [under review as of July 2019]

Related Guidelines

Joint Mission Analysis Center Handbook 2017
Military Peacekeeping-Intelligence Handbook, 2019
Peacekeeping-Intelligence Surveillance and Reconnaissance (Military) Handbook, 2019
DPO Guidelines on Exchange of Intelligence/Peacekeeping-Intelligence with Non-Mission and Non-UN Entities, 2019

H. 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 Policy and these Guidelines.

I. CONTACT

26. DPO/OUSG/Peacekeeping-Intelligence Coordination Team (PICT)

J. HISTORY

27. This is the first iteration of these Guidelines

APPROVAL SIGNATURE:

DATE OF APPROVAL:

Annex A

STRICTLY CONFIDENTIAL	
Source Registration Form	
Originating Cell	The unit that handles the source
Receiving Cell	The unit that maintains the theatre source register
Human Source Handler	The lead human source handler
Alias	The code name assigned to the human source
Source Name	
Source Date of Birth	
Source Address	
Source Contact Details (Mobile/Cell/Other)	
Source Profession/Work	
Source Next of Kin and Contact Details	
Source Access	Does the source have physical access to the information he/she is sharing?
Source Motivation	Why is the source talking to the HPKI team? Does the source display conscious or unconscious bias?
Source Potential	Can the source be tasked to acquire information?
Source Capability	Does the source have analytical capabilities? Is the source literate? Level of education/languages spoken?
Date of First Contact	When contact was first made with the source.
Circumstance of First Contact	Who, what, when, where, why, and how the first contact was made.
Date of Last Contact	The most recent meeting held with the source.
Source Reliability	Rated from A through F.

Annex B

<table>
<tr><th colspan="12">STRICTLY CONFIDENTIAL</th></tr>
<tr><th colspan="12">HPKI Mission Cell Source Register</th></tr>
<tr><th>Alias</th><th>Reliability</th><th>Name</th><th>Address</th><th>Contact Details</th><th>Handler</th><th>Handling Cell</th><th>Date of First Contact</th><th>Access</th><th>Motivation</th><th>Potential</th><th>Capability</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Annex C

STRICTLY CONFIDENTIAL	
Contact Report	
Originating Cell	The cell that handles the source
Receiving Cell	The superior HPKI to which the report is being sent
Human Source Handler	The lead human source handler
Alias	The code name assigned to the human source
Reliability	The handling unit's assessment of source reliability
Date, Time, and Location of Meeting	When the meeting took place
Date of Information	When the incidents described in the meeting took place.
Reason for Meeting/Initiator of Meeting	Instructional blurbs to be added?
Information elicited during meeting	
Human Source Handler Comments	
Demeanor of Source	
Human Source Handler Comments	
Analysis	
Date, Time and Location of Next Meeting	

Annex D

CONFIDENTIAL	
Conversation Plan	
Planning and preparation phase	Threat Assessment? QRF required? Weapons state? Communications? Transport? Location of cover team? Has a recce of the meeting venue taken place? Immediate Actions Rehearsal? Deconfliction with other UN forces complete? Support from higher HQ requested? Risk assessment conducted?
Introduction Phase	Start of the meeting – greetings and personal introductions.
Warm-up Phase	Avoid information elicitation unless there are immediate force protection issues. Ask about personal interests and discuss day-to-day events.
Elicitation Phase	Phrase questions correctly – use open questions and try not to lead the source in a particular direction. Focus on details where required (who, what, when, where, and why). Be aware of human source body language.
Warm-down Phase	Transition towards the end of the meeting. Move back to the personal.
Completion	Obtain agreement on another time, date, and location for another meeting.

Annex E

Skill Set of a Human Source Handler (HSH)

1. Although many human source acquisition skills may be taught, the development of a skilled Human Source Handler requires experience in dealing with people in all conditions and under all circumstances. Certain character traits are crucial:

   a. **Alertness:** The HSH must be alert on several levels while conducting human source collection tasks. He/She must concentrate on the information being provided by the source, and be constantly evaluating the information for both value and veracity based on acquisition requirements, current intelligence/peacekeeping-intelligence, and other information obtained from the source. Simultaneously, he/she must be alert not only to what the source says but also to how it is said and the accompanying body language to assess the source's truthfulness, degree of cooperation, and current mood. In addition, the HSH must be constantly alert to his/her environment to ensure his/her personal security and that of the source.

   b. **Patience and Tact:** The HSH must have patience and tact in creating and maintaining rapport between him/herself and the source, thereby enhancing the success of the questioning. Displaying impatience may encourage a difficult source to think that if he/she remains unresponsive for a little longer, the HSH will stop questioning, thus causing the source to lose respect for the HSH, thereby reducing the HSH's effectiveness.

   c. **Credibility**: The HSH must maintain credibility with his/her source. He/She must present him/herself in a believable and consistent manner and follow through on any reasonable promises made as well as never to promise what cannot be delivered.

   d. **Objectivity and Self-control:** The HSH must be totally objective in evaluating the information obtained. The HSH must maintain an objective and dispassionate attitude regardless of the emotional reactions he/she may actually experience or simulate during a debriefing session. Without objectivity, he/she may unconsciously distort the information acquired.

   e. **Adaptability**: An HSH must adapt to the many and varied personalities which he/she will encounter. He/She must also adapt to all types of locations, operational tempos, and operational environments. He/She should try to imagine him/herself in the source's position.