United Nations Military Peacekeeping-Intelligence Handbook

2nd Edition

2025

DEPARTMENT OF PEACE OPERATIONS

Produced by:

Office of Military Affairs,
Department of Peace Operations
UN Secretariat
One UN Plaza, New York, NY 10017
Tel. 917-367-2487

Approved by:

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

May 2025

Contact: PDT/OMA/DPO

Review date:2 June 2029

Reference number: 2025.10

Printed at the UN, New York

Foreword

The second edition of the Military Peacekeeping-Intelligence (MPKI) Handbook provides instructions, and guidance to personnel deployed in MPKI roles, at all levels in a UN peacekeeping operation.

The first edition comprised 12 chapters outlining the foundational components of MPKI and how they are applied to support commander's decision-making process. Conversely, the second edition has been revised to 7 chapters to ensure a more concise resource that is aligned with the Peacekeeping-Intelligence (PKI) Policy (2019) and other PKI-related guidelines produced by the Peacekeeping-Intelligence Coordination Team (PICT).

The revised MPKI Handbook incorporates best practices, lessons learned and shared experiences of MPKI staff across UN peacekeeping missions along with valuable insights from field visits conducted by DPO/OMA teams.

The MPKI Handbook is designed to complement the Joint Mission Analysis Centre (JMAC) Handbook as well as the UN MPKI trainings provided by UN certified subject matter experts.

My appreciation goes to the Member States and various stakeholders who have continued to work tirelessly to ensure that UN's distinctive way of practicing MPKI is captured in fit-for-purpose policies, handbooks, guidelines and manuals. We would continue to update these resources to ensure that they remain relevant to the ever-evolving landscape of peacekeeping operations.

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

TABLE OF CONTENTS

GLOSSARY: ABBREVIATIONS vi

CHAPTER ONE: INTRODUCTION 1

1.1 Aim of the Handbook 1

1.2 PKI Policy 2

1.3 MPKI in Context 3

1.4 MPKI Cycle 4

Peacekeeping-Intelligence Overview and Functions 4

CHAPTER TWO: DIRECTION 7

2.1 Direction of MPKI Activity 7

2.2 Direction in a UN Mission Context 7

2.3 How to Establish Direction 7

2.4 Force Information Acquisition Plan (Force IAP) 9

2.5 Production Plan 12

2.6 Request for Information (RFI) Management 12

2.7 Tasking Authority 12

2.8 Management of the Force IAP 12

2.9 Evaluation and Feedback 13

2.10 Annexes 13

CHAPTER THREE: ACQUISITION 14

3.1 What is Information Acquisition? 14

3.2 Basic Acquisition Attributes 14

3.3 Force IAP 17

3.4 Acquisition process 17

3.5 Military Information Acquisition Disciplines 19

3.6 Reports and Returns 22

CHAPTER FOUR: EXAMINATION AND COLLATION 23

4.1 Introduction 23

4.2 Collation 23

4.3 Examination 26

CHAPTER FIVE: ANALYSIS 29

5.1 Concept 29

5.2 Definition 29

5.3 Analysis: Fundamentals, Standards and Skills 30

5.4 Integration 36

5.5 Interpretation 36
5.6 Communicating Uncertainty 37
5.7 End State 38
ANALYSIS OF THE OPERATING ENVIRONMENT 38
5.8 Providing Understanding 38
5.9 Defining the Operating Environment 38
5.10 AOE – The Three Phases 39
5.11 Phase 1a: Analysis of the Physical Terrain 40
5.12 Phase 1b: Analysis of the Human Terrain 44
5.13 Phase 1c: Analysis of the Information Terrain (IT) 48
5.14 Phase 2 - AE 49
5.15 Phase 3 – Situation Integration/Actor-Integrated Scenario Generation 53
5.16 Outputs from AOE 58
5.17 The Peacekeeping-Intelligence Estimate (PIE) 59
5.18 The Short Peacekeeping-Intelligence Estimate (PIE) 61
5.19 Annexes 63
CHAPTER SIX: DISSEMINATION 64
6.1 Dissemination - The Final Phase 64
6.2 Dissemination Formats 64
6.3 Clarity 65
6.4 UN Reporting Formats 65
6.5 Summary 66
6.6 Annexes 66
CHAPTER SEVEN: MANAGEMENT AND USE OF MPKI 67
7.1 UN Peacekeeping-Intelligence Structures, Roles and Responsibilities 67
7.2 UN Peacekeeping-Intelligence Management Mechanisms 68
7.3 UN Tactical Peacekeeping-Intelligence 69
UN MPKI Structures, Roles and Responsibilities 69
7.4 Establishing the MPKI Architecture 69
7.5 Additional MPKI Elements 70
7.6 Support to MPKI - Non-UN Partners 71
7.7 MPKI Practical Principles 71
Support to the UN Military Decision-Making Process (MDMP) 72
7.8 Peacekeeping-Intelligence-Enabled Decision-Making 72
7.9 Peacekeeping-Intelligence Staff Considerations 72

7.10 The UN Military Decision Making Process 73
INFORMATION MANAGEMENT (IM) 76
7.11 Why IM? 76
7.12 IM Definition 76
7.13 IM Responsibilities 76
7.14 IM Basics 76
7.15 Databases 77
7.16 Report Dissemination 77
7.17 Checklists 77
SECURITY OF MPKI 77
7.18 Security Foundation for UN Operations 77
7.19 UN Security Policy 77
7.20 Personnel Security 77
7.21 Physical Security 78
7.22 Information Security 79
7.23 Reports 81
7.24 Security Awareness, Education and Training 81
7.25 Annexes 81

GLOSSARY: ABBREVIATIONS

3CF	3 Column Format
ACH	Analysis of Competing Hypotheses
ACOA	Actor Course of Action
AE	Actor Evaluation
APII	Area of Peacekeeping-Intelligence Interest
APIR	Area of Peacekeeping-Intelligence Responsibility
AM	Acquisition Management
AOE	Analysis of the Operating Environment
ASCOPE	Areas, Structures, Capabilities, Organisations, People, Events
Bn	Battalion
C2	Command and Control
CC	Critical Capabilities
CCIR	Commander's Critical Information Requirement
CIU	Crime Peacekeeping-Intelligence Unit
CMOS	Current Military Operations Service
COG	Centre of Gravity
CONOPS	Concept of Operations
Coy	Company
CPKI	Communications Peacekeeping-Intelligence (Subset of SPKI)
CR	Critical Requirements
CV	Critical Vulnerabilities
DPO	Department of Peace Operations
DTG	Date Time Group
EEI	Essential Elements of Information
EO	Event Overlay
EOD	Explosive Ordnance Disposal
EPKI	Electronic Peacekeeping-Intelligence (Subset of SPKI)
EW	Early Warning
FACES	Feasible, Acceptable, Complete, Exclusive, Suitable
FHQ	Force Headquarters
FOB	Forward Operating Base
FRAGO	Fragmentary Order
G2	Sector-Level Peacekeeping-Intelligence Staff
GIS	Geospatial Information Service
GPKI	Geospatial Peacekeeping-Intelligence
HoM	Head of Mission
HPKI	Human Peacekeeping-Intelligence
I&W	Indicators & Warnings
IAL	Information Acquisition List
IAP	Information Acquisition Plan
IDP	Internally Displaced Person
IED	Improvised Explosive Device
IHI	Items of High Importance
IM	Information Management
INTREP	Peacekeeping-Intelligence Report

INTSUM	Peacekeeping-Intelligence Summary
IPKI	Imagery Peacekeeping-Intelligence (Subset of GPKI)
IO	Information Operations
IR	Information or Peacekeeping-Intelligence Requirement
IRM	Information Requirements Management/Manager
JMAC	Joint Mission Analysis Centre
JOC	Joint Operations Centre
KT	Key Terrain
MDCOA	Most Dangerous Course of Action
MDMP	Military Decision-Making Process
MIAP	Mission Information Acquisition Plan
MICM	Mission Peacekeeping-Intelligence Coordination Mechanism
MISP	Mission Peacekeeping-Intelligence Support Plan
MLCOA	Most Likely Course of Action
MLT	Mission Leadership Team
MPKI	Military Peacekeeping-Intelligence
MPKI HB	Military Peacekeeping-Intelligence Handbook
NAI	Named Area of Interest
NGO	Non-Governmental Organization
OE	Operating Environment
OEE	Operating Environment Evaluation
OMA	Office of Military Affairs
OPKI	Open-Source Peacekeeping-Intelligence
OPORD	Operations Order
ORBAT	Order of Battle
PBIED	Person-borne Improvised Explosive Device
PICINTSUM	Picture Peacekeeping-Intelligence Summary
PKIE	Peacekeeping-Intelligence Estimate
PIR	Priority Peacekeeping-Intelligence Requirement
PKI	Peacekeeping-Intelligence
PKISR	Peacekeeping-Intelligence, Surveillance, and Reconnaissance
PMESII	Political, Military, Economic, Social, Infrastructure, Information
POC	Protection of Civilians
Recce	Reconnaissance
RFI	Request for Information
RM	Requirements Management/Manager
ROMB	Receipt of Mission Brief
S2	Battalion-Level Peacekeeping-Intelligence Staff
SIR	Specific Peacekeeping-Intelligence Requirement
SITMAP	Situation Map
SLT/SMT	Senior Leadership Team/Senior Management Team
SO	Situation Overlay
SOP	Standard Operating Procedure
SPKIE	Short Peacekeeping-Intelligence Estimate
SPKI	Signals Peacekeeping-Intelligence
SRSG	Special Representative of the Secretary General
SWOT	Strength, Weakness, Opportunity, Threat

TAI	Target Area of Interest
TCC	Troop Contributing Country
TPKI	Technical Peacekeeping-Intelligence
TPME	Task, Purpose, Method, End state
TTP	Tactic, Technique, Procedure
U2	Force-Level Peacekeeping-Intelligence Staff
UAS	Unmanned Aircraft System[1]
UN	United Nations
UNHQ	United Nations Headquarters
UNDSS	United Nations Department of Safety and Security
VBIED	Vehicle-Borne Improvised Explosive Device
VG	Vital Ground
WARNO	Warning Order

[1] Whilst DPO/OMA employs gender-neutral terminology wherever possible, aviation terms are drawn directly from the language used by International Civil Aviation Organisation (ICAO) and “Unmanned” is yet to be replaced by “Uncrewed” in ICAO usage.

CHAPTER ONE: INTRODUCTION

1.1 Aim of the Handbook

The aim of this Handbook is to support personnel deployed in Military Peacekeeping-Intelligence (MPKI) roles in UN peacekeeping operations. The Handbook is also intended to guide Troop-Contributing Countries (TCCs) in training MPKI personnel prior to their deployment in UN peace operations to enable them to develop MPKI products and fit seamlessly into the UN MPKI architecture. Since the way the UN conducts Peacekeeping-Intelligence (PKI) may differ from national intelligence methodology, this introduction is designed to explain some of the basic principles, terms and methods for PKI and more specifically for MPKI.

This Handbook focuses on the overarching principles, processes and parameters to manage MPKI within UN peacekeeping missions. Guidance on the specific tools and activities of individual mission components and the functions of mission headquarters in supporting and coordinating mission MPKI systems will be set forth in relevant subordinate operational guidance and mission-specific standard operating procedures. Specifically, the MPKI Handbook describes how to strengthen the MPKI capabilities of field operations by explaining MPKI best practices, including how MPKI is produced while ensuring common methods and standards are adopted in the implementation of MPKI across UN entities and missions. Further, this version of the Handbook incorporates feedback and lessons learnt from field missions as well as MPKI courses conducted for personnel deployed in MPKI positions.

The Department of Peace Operations (DPO) has adopted a policy on PKI, which is the overarching authoritative document for MPKI. A series of guidelines for different PKI disciplines are also being produced.[2] The principles of PKI articulate that it 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." PKI activities are, by nature, non-clandestine, and must always be conducted in full compliance with the UN Charter and the overall legal framework governing UN peacekeeping operations, including the basic principles of peacekeeping. The full list of PKI principles will be explained later in this chapter.

The key to the practice of PKI is understanding its distinction from information. The primary difference between information and PKI is that information is factual reporting about events that have happened, while PKI is an assessment – derived from the analysis of the reporting – and as such PKI employs reasoning, looks at trends and determines the likelihood of future developments. Fundamentally, MPKI is the result of the MPKI cycle, which takes you through direction, acquisition, examination & collation, analysis and then dissemination. The MPKI cycle is displayed in Figure 1 below.

[2] The Policy on PKI and the subsequent guidance documents can be found at: https://unitednations.sharepoint.com/sites/PPDB/SitePages/Peacekeeping-Intelligence.aspx

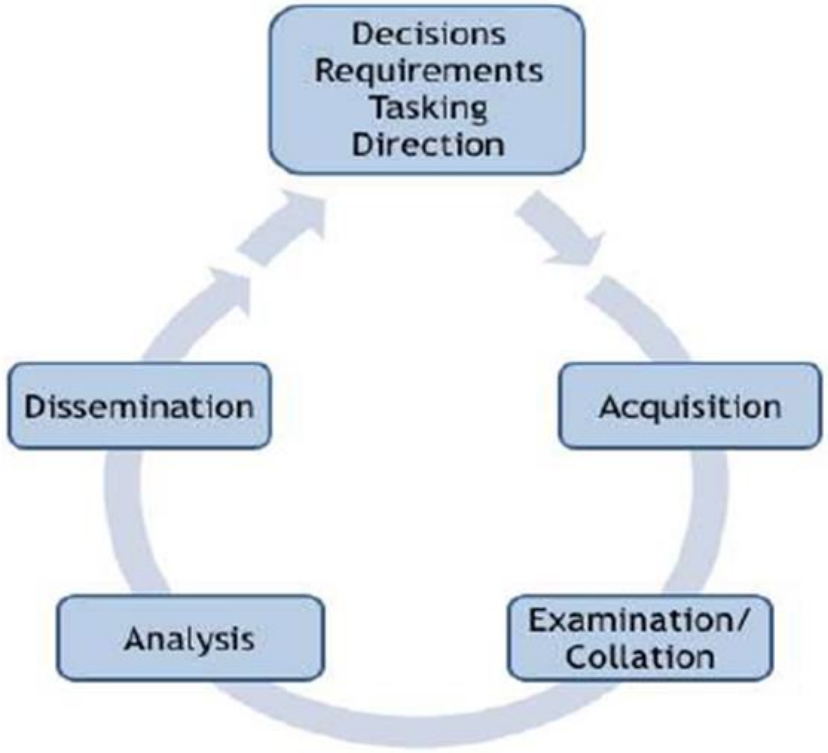


Figure 1: UN (M)PKI Cycle

It is important to note that MPKI entities at different levels have specific names. At the Force HQ level, the nomenclature is U2, at Sector level, it is G2, and at Battalion level, it is S2. This may differ from national norms, but it is the format adopted in UN peacekeeping operations and what will be used throughout this Handbook.

1.2 PKI Policy

As the mandates Operating Environments (OEs) of United Nations peacekeeping missions have evolved, the Security Council, Member States and the Secretariat have come to consider PKI as a critical enabler. The path towards the current requirement for PKI is outlined in subsequent sub-paragraphs.

- After the failure of the peacekeeping operations in Somalia, Rwanda and Bosnia in the 1990s, the Brahimi Report recommended in 2000 that "UN forces should be afforded the field intelligence and other capabilities needed to mount an effective defence against violent challengers".
- In Resolution 1894 of 2009, the Security Council called on the Secretariat to give "priority in decisions about the use of available capacity and resources, including information and intelligence resources, in the implementation of mandates" for the protection of civilians.
- The High-Level Independent Panel on Peace Operations (HIPPO) in its report of June 2015 recommended "more effective Information Management (IM) and significantly enhanced analytical capacities" to deal with environments where there is little or no peace to keep.
- The Security Council highlighted the need for intelligence capacities for MINUSMA considering its complex security environment, notably in Resolution 2295 of 2016.
- The UN General Assembly's Special Committee on Peacekeeping Operations (C-34) has also recognised "the need to improve situational awareness and to enhance the safety and security of peacekeepers, including use of modern technology as a complement to traditional methods, such as human-based information-gathering" (A/70/19, 2016), and that some peacekeeping missions have been deployed in fragile political and security

environments with asymmetrical and complex threats. It encouraged the Secretariat "to develop a more cohesive and integrated United Nations system for situational awareness that stretches from the field to headquarters" (A/71/19, 2017).

- Many points for consideration have been highlighted by the C-34. Firstly, the importance of complementarity with other approaches to safety and security. Secondly, that PKI policies and practices uphold the United Nations Charter and the three principles of consent, impartiality, and non-use of force except in self-defence, for the protection of civilians or defence of the mandate. Thirdly, that respect for the sovereignty of host and neighbouring states be ensured. Finally, that the security and confidentiality of sensitive information be managed carefully and appropriately to ensure it is not accessed by non-authorised personnel.

The objective of PKI is to enhance situational awareness and support decision-making regarding the safety and security of all UN personnel and assets, as well as the protection of civilians. Importantly, PKI is not to be used against or to threaten the Host State or neighbouring States.

MPKI Parameters. All the abovementioned requirements extend to MPKI. UN MPKI is distinct from national military intelligence and must be conducted according to the strict principle that all PKI activity is non-clandestine.

1.3 MPKI in Context

United Nations peacekeeping, a tool developed by the Organisation to support parties to a conflict to maintain peace, has a noble legacy of supporting peace and stability across the globe. Peacekeeping has evolved over the decades in response to the changing nature of conflict. Today's OEs are more complex, dangerous, and high tempo. The spectrum of traditional and non-traditional/asymmetric threats pose a more serious threat to the safety and security of peacekeepers and negatively impact on mandate implementation. This drives a strong requirement for United Nations peacekeeping missions to better understand their OEs, provide assessments to support decision-making, assess the likelihood of specific threats and identify civilian/other vulnerabilities that can be exploited by actors with adverse/hostile intents. These are required to enhance situational awareness and the safety and security of UN personnel, as well as inform activities and operations related to the protection of civilians where these tasks are given in the Security Council mandate.

The changing character of peacekeeping operations – specifically the trend that the blue helmet and the UN flag no longer guarantee protection from hostile forces – has changed the attitude towards the UN using PKI to save lives. It has become increasingly vital to understand and forecast the intentions, capabilities and actions of peace spoilers. As a result, PKI is now an accepted requirement within both the UN leadership and Member States. The UN requires objective judgement on situations and likely future situations based on an independent UN PKI capability. For military peacekeepers within UN peacekeeping operations, this has become known as MPKI.

The fundamental purpose of MPKI in UN peacekeeping operations is to *enhance situational awareness and enable UN decision-making for the protection of UN personnel and the protection of civilians.* Specifically, MPKI is intended to:

- Provide situational awareness and forward-looking peacekeeping-intelligence products to better enable planning and decision-making. Leadership who has access to good PKI is better able to take appropriate actions.
- Provide situational awareness and contribute to early warning on threats to the life of UN personnel, both uniformed and civilian.
- Provide situational awareness and contribute to early warning on threats to life within the local population, in support of the protection of civilians, where this is mandated. Linked to this, is early warning of any planned destruction to critical infrastructure or necessary natural resources.

- Support the substantive civilian lead sections in providing situational awareness of civilian vulnerabilities and opportunities to strengthen their resilience to enable the peacekeeping planning and decision-making to take preventive and anticipatory actions.
- Enhance the mission leadership's understanding of shifts in the strategic, operational and tactical landscape through the early identification of relevant trends and threats. This will facilitate the identification of risks and opportunities for the protection of UN personnel and civilians within the scope of the mandate.

There may also be a role providing support to any UN information and communication operations. This may be through the appropriate provision of information and/or PKI to the responsible commander or organisation. Thus, MPKI may have a supporting role in enabling the UN to communicate the truth, and potentially counter disinformation and misinformation, or factually untrue reporting.

1.4 MPKI Cycle

The MPKI cycle (Figure 1) is the mechanism used to produce MPKI. It is typically represented as a closed cyclical path of activities starting with Direction and moving through Acquisition then Examination & Collation before Analysis and finally Dissemination. It is termed a 'cycle,' as it is an ongoing process both because the production of PKI is a constant process throughout a peacekeeping mission, and because disseminated PKI may feed and drive further Direction and thereby the cycle starts again. The MPKI cycle is the fundamental tool for MPKI practitioners. It outlines how the MPKI practitioner receives direction from their commander, acquires the relevant information, and analyses the information to produce PKI, which is then disseminated to the commander and the command team to ensure they are informed timely and precisely of the situation in the OE. A pictorial representation of this cycle is given in Figure 1. Subsequent chapters will explain each of the steps in detail and provide examples to help those deployed in MPKI roles.

It is important that MPKI staff 'own' the MPKI cycle and understand all its elements. MPKI must normally run as a cycle, as the order and links between each respective stage are vitally important. Direction must lead to coherent and effective Acquisition; Acquisition outputs must be thoroughly Examined and Collated before they are used in Analysis to produce all-source, fused PKI products; those fused products must then be Disseminated efficiently and timely, to the right people, to enable decision-making and initiate further Direction.

1.5 Peacekeeping-Intelligence Overview and Functions

For PKI to be effective, all UN PKI entities must work collaboratively together – PKI should be considered a 'teamwork'. The Force, Sector, and Battalion's PKI organisations should all look to support and learn from each other. Furthermore, other UN PKI, integrated analysis and other entities - such as the Joint Mission Analysis Centre (JMAC), the UN Police (UNPOL), the UN Department of Safety and Security (UNDSS) and the Human Rights & Protection Division (HRPD), should be collaborating closely. One of the tools for such collaboration is the establishment of a Mission Peacekeeping-Intelligence Coordination Mechanism (MICM). The objectives are the same: to produce PKI that enables decision-making in support of mandate implementation relating to the protection of UN personnel, critical infrastructure and civilians, in line with the given mandates.

There may also be other entities in the mission area - such as Non-Governmental Organisations (NGOs) – who have useful information or even intelligence assessments. Working with such non-UN organisations requires additional attention, but where authority to do so is granted and established guidelines are followed, they too may become useful actors in the PKI architecture. Always remember, PKI is not a competition among UN entities, it is a team effort with everyone ultimately working towards the same goals of supporting the accomplishment of the mission mandate and saving lives.

1.5.1 **Direction.** Clear Direction from the commander, at all levels, is the start point for the MPKI Cycle. Direction outlines to the MPKI staff what the commander wants to know and ensures that the PKI staff have a clear focus for their Acquisition and Analysis efforts. It is also important to understand that information acquisition and analytical capabilities are usually limited, and therefore

Direction should ideally include prioritisation (whether or not an Information or Peacekeeping-Intelligence Requirement (IR) is Mission Critical, Mission Essential, or Mission Desirable), so limited capabilities can be focussed on the highest priorities.

1.5.2 **Acquisition.** After ascertaining the requirements and according to priority, the next step is the acquisition of the data or information, which is required to feed the analytical step of the cycle. While many MPKI acquisition resources will be the same across missions (e.g., UN Military patrols and observers), some acquisition capabilities will only be available in certain mission areas. Therefore, MPKI personnel must be aware of all the sources and agencies they are able to task with Acquisition. It should be noted that data and information should be sought from the broadest sources available including all genders.

Effective Acquisition greatly depends on the clarity of requirements to ensure that resources are used in the most effective manner. Experience suggests that some requirements warrant one specific type of Acquisition, whereas others may require several different types of Acquisition. It is important to highlight that military information Acquisition can be broken down into two types, IR and Request for Information (RFI).

- An **IR** is made when the MPKI entity owns the capability required to acquire the information. The acquisition assets are considered organic to the organisation. e.g., a Battalion S2 tasking a Company patrol.
- An **RFI** is made when the MPKI entity does not own the assets required to acquire the needed information and thus must send an external request to another part of the PKI architecture in the form of an RFI. All RFIs must receive a response, even if it is a nil response from those asked.
- It is important to note that more than one acquisition capability can be applied for a requirement. If deemed necessary, it is possible to task multiple Company patrols through IRs **and** request support from a higher formation, perhaps one that owns a specialised acquisition asset such as an Unmanned Aircraft System (UAS), through an RFI.

1.5.3 **Prioritisation**. The prioritisation of IRs is important to make the acquisition effort more efficient and focused. Prioritisation is the ordering of IRs according to whether they are mission critical, essential, or desirable. IRs can also be time-sensitive and often include a 'Not Later Than' (NLT) or 'Last Time Information is of Value' (LTIOV) label. This also helps the MPKI cell to focus its acquisition effort. Most RFIs adhere to the same system and will always have an NLT or LTIOV label. There should also be a review process that assesses the degree of fulfilment of the requirement, so that if fulfilled, it can be removed from the list.

1.5.4 **Examination/Collation.** Data and information acquired by missions shall be recorded and stored in a manner that permit convenient comparison, evaluation, assessment, retrieval, analysis and reporting. Participating mission entities shall make use of standardized tools for the collation of data and information, including common databases, taxonomies and planned indexing and menus. DPO will design and promulgate, in consultation with missions, common and, where necessary, specialized tools, which shall be supported by training. The step is composed of the following stages:

- **Review.** Search the information system/database to identify already existing information/PKI about the IR/RFI.
- **Collation.** The grouping and recording of information in a manner that allows it to be readily accessible and traceable when required; it also enables convenient comparison, evaluation, assessment and retrieval whenever required. However, experience suggests that for better collation, all available information should be logged and then evaluated for relevance, degree of urgency, reliability, and probability. This is a result of good IM practices (covered in Chapter 7).
- **Evaluation.** This requires the review of an item of information to assess its reliability and credibility. This evaluation enables analysts to prevent unreliable information from being given too much credibility thus leading to incorrect judgments.

1.5.5 **Analysis.** The key part of the MPKI cycle where raw, unprocessed data and/or information is converted into all-source, fused PKI. This step is composed of the following stages:

- **Analysis & Integration.** The methodical breaking down of information into its component parts; examination of each to find interrelationships; and application of reasoning to determine the meaning of the parts and the whole. The result should be a forward-looking PKI assessment that will enhance current understanding.
- **Interpretation.** This is the interpretation of the new PKI against existing knowledge and assessments. Essentially, interpreting the new PKI in the context of what is already understood or assessed to refine predictive assessments.

1.5.6 **Dissemination.** The final stage of the MPKI cycle is the process of conveying or distributing PKI to the commander and the command team, which must be done without loss of timeliness. Information and analysis should be shared, where relevant, with other mission components through the MICM; the JMAC and MPKI entities should agree on the flow of information across these entities.[3] The dissemination of PKI products shall be done in compliance with the '**Need to Know/Need to Share'** concepts as stipulated in either the PKI Support Plan and/or relevant policies and SOPs. It should be noted that human rights and humanitarian law violations including trafficking, Conflict-Related Sexual Violence (CRSV) and grave violations against children have mandatory reporting requirements. Any information about these offences that is uncovered during the MPKI cycle must be reported through the appropriate channels.

The cycle does not always have to be followed step by step. For example, while trying to follow the Direction, it is possible that the organisation already has all the data and information it needs to answer the question, so no Acquisition is required. Accordingly, all that is required is Analysis of the data followed by Dissemination. In another unusual or extreme case, once Direction has been received, it is possible that the desired or required PKI already exists, and thus Examination/Collation, Acquisition and Analysis can be omitted while disseminating immediately, which would be the only required phase.

[3] Policy on Joint Mission Analysis Centres 2020

CHAPTER TWO: DIRECTION

2.1 Direction of MPKI Activity

Direction is defined as the determination of IRs, issuance/promulgation of orders, for example to acquisition assets, and maintenance of a continuous check on the productivity of such assets. It consists of two parts: direction from the commander/Head of Mission (HoM) to the PKI staff, and direction from the PKI staff to the acquirers. Direction continues throughout the PKI process, since there is a need to maintain a continuous check on the efficiency and effectiveness of that process. This phase of the cycle is very important and will have an influence on the remainder of the cycle.

2.2 Direction in a UN Mission Context

For a MPKI, Direction will be derived from several sources. A U2 cell in a larger peace-keeping mission can expect, for example, to receive Commander's Critical Information Requirements (CCIRs) and Priority Peacekeeping-Intelligence Requirements (PIRs) from the MICM. The MICM will draw these PIRs from its engagement with the HoM, which will normally be based on his/her strategic priorities. The MICM will then task mission-level entities, such as the police and military components, the JMAC, UNDSS, and the JOC to acquire information on a number of these PIRs, based on their respective acquisition capabilities. It should be noted that the MICM will issue/promulgate when and in what format the PIR response should be provided.

Generally, the PIRs that the U2 cell receives from the MICM will be very broad and general in nature. For example, the HoM might ask ‘what threats exist to UN personnel’. It is the U2’s role thereafter to break this broad question down into a series of more specific questions (Specific Peacekeeping-Intelligence Requirements (SIRs)) that its military sensors can understand and respond to. These mission-level PIRs, and the linked IRs, form the basis for the initial Force Information Acquisition Plan (Force IAP).

After the military component has received its mission-level PIRs from the MICM, it is incumbent upon MPKI cells at every level to augment this initial PIR list with additional PIRs that will reflect the unique operational concerns of commanders at all levels (Force, Sector, and Battalion). For example, the MICM will focus on mission-level PIRs, but the commander of each level of the military component will have additional PIRs which are unique to his/her Area of Peacekeeping-intelligence responsibility (APIR). These additional PIRs, SIRs, and Essential Elements of Information (EEIs) will therefore complement the Force IAP.

It should be noted that if the military commander has not specifically given his/her direction, MPKI staff at all levels can propose a direction for the commander to endorse. However, it is normal practise for the step direction to be a collaborative product of the commander and the MPKI staff. In all cases the commander must approve/endorse the final Force IAP. This is helpful to the MPKI cell, as it demonstrates to all relevant sensors that the Force IAP has the commander’s full support.

2.3 How to Establish Direction

Organizing direction depends on the level and personnel available. At the Force level, designated officers and personnel may fill the separate roles of Chief MPKI, Information Requirements Manager (IRM), Acquisition Manager (AM), and other such appointments. However, at Sector, Battalion, or Company level, where the MPKI cell is likely to be smaller, one person may fill several roles and be responsible for Direction, IRM and Acquisition. Notwithstanding this, there must be at least one individual who holds the responsibility for obtaining and reviewing the commander’s PKI Direction. It is essential that the directing function takes place on each level of command, with the following aims:

- Define the IRs (what does the commander want to know).
- Prioritise those requirements into PIRs (which are most important to the commander’s mission and mandate).

- Break these general PIRs into smaller SIRs and, when necessary, into EEIs, on which sensors can reasonably be expected to report.
- Ensure resources with the appropriate capabilities are tasked with the acquisition of information.

2.3.1 The Process. To deconflict and understand the focus areas for information acquisition, there is a requirement to identify and stipulate the military unit's APIR. The APIR is the geographical domain, normally limited by the UN mandate, where unit commanders are responsible for the acquisition of information and production of peacekeeping-intelligence with their own resources.

There may be a larger area outside of this APIR where the commander needs to understand what is happening now and in the (nearby) future but is not responsible for the PKI production. It is always important that a commander knows what is happening within the APIR of a neighbouring military unit, or in any other area in which events can have an operational impact on their APIR. For example, a commander needs to know if an armed actor uses a particular area to recruit personnel, or to otherwise prepare for violent activity that would undermine the implementation of the mandate, even if this is outside the APIR. Or maybe the commander needs to know the air activities in a particular neighbouring area, because they may serve for the same purpose as the air violations in own APIR. This larger area is called an Area of Peacekeeping-Intelligence Interest (APII). There can be no acquisition activities outside of the APIR. For example, if the APII includes border areas with another country, there is NO acquisition activity on the other side of the border in the other state.

When the understanding on APIR and APII is developed or changed, there must be a PKI dialogue with the commander. This discussion takes place between the local PKI leader and the commander or user of the PKI products. This dialogue is to ensure that the right questions are asked, that IRs are prioritised, thereby ensuring that the subsequent information acquisition and production effort is prioritised and focused.

In a UN context, the local decision-maker (from HoM to Force Commander to Company Commander) should make their IRs known to their local PKI leader. These IRs should relate to their specific mission and should cover all areas relevant to the mandate.

It is part of the MPKI cell's responsibility to make suggestions and assist their local commander in drawing up their IRs. It is vital that PKI leaders have a detailed knowledge of the mission, the mandate, operational tasks, the OE, and of all relevant local actors, including those that are supportive, neutral, and threatening. The type of issues that should be discussed, and questions that should be asked are as follows:

- What do you want to know?
- What do you need to know to ensure effective mandate, mission or operational task implementation relating to the protection of UN personnel and civilians?
- What specific threats to mandate or task implementation relating to the protection of UN personnel and civilians do you require MPKI?
- What geographical areas do you require acquisition coverage?
- What are your information priorities?
- When, where, and in what format (written product or brief, for example) do you need the reporting?

Furthermore, the acquisition tasks or requests shall determine potential protection risks that the acquisition process might expose victims, witnesses and other sources to and how these risks can be mitigated.

Based on the requirements and operational priorities of the commander, the MPKI cell will draw PIRs from what is discussed. After the commander's approval these PIRs will form an important part of the Force IAP.

Overall, the PKI dialogue helps the PKI element identify requirements, prioritise acquisition, direct production, and decide the type of dissemination needed for the various decision support that mission leadership requires. The PKI dialogue makes decision-makers aware of the PKI structure as a resource. It is important that the limitations of information acquisition assets are made known to the commander. This helps to manage expectations.

It is important to note that the Force IAP is a living document and will be added to on an ongoing basis. For example, when a MPKI cell engages in an Analysis of the Operating Environment (AOE), many information gaps will become apparent. This approach is elaborated on further in Chapter 5, but two common framework approaches to identify relevant factors are the acronyms PMESII and ASCOPE. (see Annex C to Chapter 5 for further information).

- **PMESII.** Political, Military, Economic, Social, Information and Infrastructure.
- **ASCOPE.** Areas, Structures, Capabilities, Organisation, People and Event factors.

This technique allows the analyst to cross reference these columns and ask themselves what is known, and what is not. This will help to establish the information gaps that exist. These gaps can be fed into the IAP to enhance knowledge.

2.4 Force Information Acquisition Plan (Force IAP)

The Force IAP is the most important direction tool, expressing as it does all PIRs and SIRs that have been set, and as such it is the catalyst for the MPKI cycle. It is a requirement for each military component to have developed one, and that it is cascaded down to all sub-units. It is a living document that represents the link between Direction and Acquisition and is constantly changing in line with a developing situation, new CCIRs, new plans, and new operational taskings. The Chief U2 has ultimate ownership of the Force IAP but it is the responsibility of an Information Acquisition Manager (IAM) to oversee and manage. It is important to note that Acquisition is not just a PKI function and requires coordination and liaison across the U3/5, which often has tasking authority of the various acquisition sensors.

When ready, it is important that the Force IAP is communicated to all acquisition sensors according to their capabilities, and in such a way that makes sense. For example, a broad PIR relating to a UN mandate might make no sense to a soldier at a checkpoint. If you ask the soldier ‘what are the threats to the protection of civilians,’ they may not be able to give an answer on the basis of what they have observed. However, if you ask, ‘what kind of weapons does Actor X carry’, they will be able to answer. An example scenario with a Force IAP is at Annex A and a suggested RFI format at Annex B.

The Force IAP is the basis of an execution order. It may be written and published in the operation order format in accordance with the mission’s SOP. Staff use the Force IAP to task, direct, and manage acquisition assets (both assigned and attached assets) to acquire against the requirements. The Operations Officer tasks and directs information acquisition activities with support from the peacekeeping-intelligence branch. Acquisition tasks or requests are formulated and passed to units as orders. The staff provides details that clearly define the acquisition requirements. These requirements identify:

- **Who** will acquire the information?
- **What** information needs to be acquired?
- **Where** to acquire it: normally Named Areas of Interest (NAIs)?
- **When** is the information required (NLT/LTIOV)?
- **Why** is the acquisition required?
- **How** is the acquisition unit to disseminate the acquired information?

The plan may be a word document, excel sheet or any other format. On the left-hand side of the Force IAP, the Commander’s PIRs are listed. These must also be broken down into SIRs, which in

turn can be further broken down into EEI and, if necessary, a series of Indicators and Warnings (I&W). A priority is also assigned to each PIR and IR.

An example:

PIR 1: What is the main threat to the civilian population in the AOR?
SIR 1.1: How are the tribes and clans in the AOR composed?
SIR 1.2: Who are the formal and informal leaders in the region?
SIR 1.3: What is the political ambition of the leaders?
SIR 1.4: What is the level of criminality? Who are the criminals? Who are the leaders?
SIR 1.5: What type and number of weapons are present?

One method of breaking down PIRs into IRs is to consider the equation:

THREAT = INTENT x CAPABILITY

Thus, if a PIR relates to a threat, it can be broken down into subordinate IRs relating to the relevant actor's intentions and capabilities. This can be repeated for many threat actors. But this is not an exact science, it is more of a logic exercise where the MPKI personnel break down the overall PIR into subordinate IRs, the answers to which will enable the PIR to be answered. An example of a typical PIR, broken down further into IRs for a threat group:

PIR 2: What security threats exist in the UN Area of Operations?
Intent:
SIR 2.1: What is the objective of Group X?
SIR 2.2: What is the ideology of Group X?
SIR 2.3: What influences Group X?
SIR 2.4: What does Group X say in public statements or messaging?
SIR 2.5: What is the attitude of Group X to the civilian population?
SIR 2.6: What is the attitude of Group X to the Host State security forces?
SIR 2.7: What is the attitude of Group X to the peace process?
SIR 2.8: What is the attitude of Group X to the UN?

Capability:
SIR 2.9: What weapons and other assets does Group X have?
SIR 2.10: What other capabilities does Group X have?
SIR 2.11: Where does Group X source its weapons?
SIR 2.12: How many personnel does Group X have?
SIR 2.13: What are its income sources?
SIR 2.14: What is its command structure?
SIR 2.15: How does Group X communicate?
SIR 2.16: Where does it operate?
SIR 2.17: What links to other groups/actors (state and non-state) does it have?
SIR 2.18: Where does it get its supplies?
SIR 2.19: Does Group X have the support of the local population?
SIR 2.20: What are the Tactics, Techniques and Procedures of Group X?

If necessary, these IRs can also be further broken down into more specific questions. These can be termed Essential Elements of Information (EEIs) or Indicators and Warning (I&W). In the chart above, the intent and capability of Group X was considered. In the example below, one IR is enhanced by adding additional sub-questions for response. This is a short list, but it can be exhaustive as necessary.

PIR 2: What security threats exist in the UN Area of Operations?

SIR 2.20: What are the Tactics, Techniques and Procedures of Group X?
EEI 2.20.1 How does the group prepare to conduct attacks?
EEI 2.30.2 What patterns of activity does Group X engage in prior to an attack?

A series of I&W can also be placed in the Force IAP.

- **Indicators & Warnings.** An indicator is an observable behaviour or event that point towards a particular outcome, or that confirm or deny a relevant actor's course of action. Generally, the MPKI cell should always ensure that indicators are linked to a NAI, where such behaviours and events can be observed. NAIs are geographical areas or points where the required information is expected to be observed or acquired. For example, watching a particular bridge using Peacekeeping-Intelligence, Surveillance and Reconnaissance (PKISR) assets could confirm or deny if an armed actor intended to use it to cross with their forces and monitoring hate speech for increased instances and specificity could confirm elevated risk to specific groups of civilians based on their identity. The continuous monitoring of indicators can help to prevent operational or tactical surprise.
- Indicators are observable at all levels, from the strategic to the tactical. Considered at the national strategic level, indicators could include a shift to a war-time economy, a change in use of national infrastructure, or the co-option of strategic airlift capabilities. At the operational level, an indicator could include local population movements, the stockpiling of fuel or ammunition by a certain group, or escalations of domestic violence and CRSV, or increases in human rights violations and abuses, including not only increased incidents but also increases in the scale of impact (number of victims) and gravity of human rights violations and abuses.

There are several types of indicators:

- **Alert/Warning Indicator.** Alert/Warning Indicators are those which reflect the intention of a threat group to initiate hostilities; they relate to preparations for aggression.
- **Tactical/Combat Indicator.** Tactical/Combat Indicators are those which reveal the type of operations the enemy is about to undertake. For example, indicators of a forthcoming large-scale attack might include the pre-positioning of fuel, ammunition and other combat supplies, and intensified reconnaissance.
- **Identification Indicator.** Identification Indicators and signature equipment are those which enable the nature of a formation, unit or installation to be determined on the basis of known characteristics regarding organisation, equipment or tactics. For example, a particular piece of equipment may be issued only to a particular type of unit.
- **Gender Early Warning Indicator.** Early warning indicators specific to gender can also inform requirements for information acquisition (a list of potential indicators is included at Annex D). The MPKI cell should also decide where Gender Early Warning indicators can be monitored by linking these indicators to geographic locations[4].
- **Civilians Population Vulnerabilities Indicator**: Early warning indicators of civilian vulnerabilities can inform, for example changes in patterns and trends in human rights violations and abuses, or observable behaviour of local population or event that affects the local population, or that confirms or denies the local population risk, action or movement. Where there is a risk of genocide, war crimes, ethnic cleansing, crimes against humanity, or other serious crimes, specific indicators may be found in the UN Framework for Analysis of Atrocity Crimes.[5]

Because these types of indicators are observable, they can be sent to units and assets using RFIs and are generally linked to NAIs where they can be monitored. The prioritization of the acquisition effort is determined by carefully examining the mission, the mandate, and the commander's specific information or IRs. An IR may be prioritised as:

- **Mission Critical.** A PIR that is critical to the success of the mission. The mission cannot proceed or succeed unless the PIR is answered. These are rare.

[4] Child Protection Handbook 2023
[5] United Nations, Framework for Analysis of Atrocity Crimes, 2014.

- **Mission Essential.** A PIR that is deemed essential to assist in mission success. The mission can succeed without it, but success would be easier / more likely if the PIR is answered.
- **Mission Desirable.** A PIR / IR that is important to know but not essential to the success of the mission.

To deconflict sensors and IRs, it is wise to establish **NAIs**. These are geographical areas or points where the required information is expected to be acquired.

2.5 Production Plan

This plan ensures the direction to produce MPKI products per the decision-makers' needs. The responsibility for developing the production plan is either with the director/leader of the PKI organisation or the Chief / Senior Analyst. The plan lists:

- Regular products (daily, weekly, monthly), timings, formats and who has responsibility.
- Ad-hoc products per situation, formats and who has responsibility.
- Release authority for different products (i.e., checking quality, content and relevance before dissemination).
- Preferred dissemination (when, how and to whom).

The production plan is a living, dynamic, situational, flexible and internal peacekeeping-intelligence production tool that normally is based on more static Reporting Directives and/or Standard Operating Procedures (SOPs).

2.6 Request for Information (RFI) Management

An RFI is a tool that may be used when the MPKI structure is unable to acquire the required information with its own resources. The MPKI cell produces and sends an RFI to higher or parallel entities or organisations for which it does not have the authority to task to obtain the relevant information. RFI management is an Acquisition Management (AM) responsibility. A record of issued RFIs must be established and monitored, with the Acquisition Manager tracking the RFI and updating its status on a regular basis in order to determine if the IR has been fulfilled or not in a timely manner. An example RFI format is at Annex B to this Chapter.

2.7 Tasking Authority

Generally, tasking authority resides with the operations section, unless specific acquisition assets are assigned operational control (OPCON) to the MPKI section. The MPKI cell should generate the Force IAP, complete with PIRs, SIRs, Indicators and link these to NAIs, but the Operations section is best positioned to understand the capabilities of its assets and, as such, to generate and deconflict information acquisition tasks. Correct tasking for Information Acquisition should include:

- Mission description (patrol, surveillance, check point, etc).
- The question which may be a PIR or a subordinate IR.
- When reporting is needed.
- How to report, and in what format; and
- Where to report (a point of contact).

2.8 Management of the Force IAP

2.8.1 **Monitoring progress.** Once units and assets have been tasked, their productivity must be monitored constantly to ensure that the necessary information will be forthcoming. Wherever possible, information should be requested from more than one source. This has the advantage that, when confirmed by more than one source, it is more likely to be true, and ensures that should one

source fail, then the other might still acquire the information. There are several principles which govern the productivity of units and assets:

- **Training and Equipment.** The productivity of a Unit will be higher, the better trained and equipped it is.
- **Range and Effectiveness of Surveillance Devices.** The surveillance device being used must have sufficient range for the task it is to undertake. Consideration must be given to siting and the terrain.
- **Speed of Communications.** The speed with which the Unit can report the results of its surveillance will affect its usefulness. The more immediately vital the information, the quicker the reporting method must be.
- **Mobility and Access.** For a Unit or asset to acquire information effectively, it must be sufficiently mobile and the target sufficiently accessible. For example, mountain ranges can not only screen enemy communications traffic but also prevent the mobile collector from getting near enough to acquire the information. Equally, although Tactical Air Reconnaissance might be able to fly over a target and obtain excellent results in a benign air environment, it cannot do so when the Surface-to-Air threat is very high.
- **Resource Availability.** Information-gathering assets are at a premium in the battlespace. Their allocation must be carefully controlled by the responsible commander.
- **Priority.** The priority afforded to an acquisition operation will affect the availability of resources.
- **Weather and Terrain.** Weather and terrain will have many different effects on PKISR systems. For example, thermal imagers, while unaffected by darkness, are affected by rain and fog. Thermal imagers and image intensifiers are degraded by smoke.

2.9 Evaluation and Feedback

Direction ultimately includes feedback to the peacekeeping-intelligence elements involved. This may consist of dialogue with the sub-units commenting on their reporting, timeliness, formats and content. It also involves evaluating the final peacekeeping-intelligence products in a more prolonged context. This will include the PKI product user, and the decision-makers, in a further PKI dialogue. This is done to evaluate the products in the longer term to examine the accuracy of assessments or lack thereof, so as to identify needs for correction.

The value of this is to identify shortfalls in acquisition capacities/assets and resources, as well as evaluate the quality of the analysis and assessments. It could, if needed, lead to adjusting the PKI architecture, which may include changes to acquisition capacities as well as identifying training needs.

2.10 Annexes

A. Example of a Force IAP

B. Example RFI Format

C. Gender Early Warning Indicators

CHAPTER THREE: ACQUISITION

3.1 What is Information Acquisition?

Information Acquisition follows on from Direction, and the two are very closely linked. Direction determines IRs, while Acquisition refines IRs into Acquisition Requirements (ARs), turns these into tasks, and feeds the resulting information back into the cycle. Most UN missions have many Acquisition assets, such as: individual soldiers, specialist peacekeeping-intelligence personnel, and airborne assets, such as crewed aircraft and/or UAS. It is also worth noting that Acquisition can also be conducted through means such as searching the internet (which would fall under the category of Open-Source Peacekeeping-Intelligence (OPKI) or by searching through existing databases and repositories for (including generating RFIs if required) information that is already known (enabled by robust Information Management structures in a mission). Regardless, it is important that the information is acquired and passed/forwarded to the analytical elements of MPKI in the right format and at the right time.

The Acquisition process has its own language and terms, which, if misunderstood, or not known, will lead to poor PKI support to the commander. Outlined below is a list of definitions:

3.1.1 Peacekeeping-Intelligence, Surveillance and Reconnaissance (PKISR). The term PKISR is generally used in two ways. The first way is to describe the various entities used to acquire PKI, such as airborne sensors, Human Peacekeeping-Intelligence (HPKI) teams, or OPKI feeds; these are often referred to as "PKISR assets". The second way in which the term is used is to describe the process by which the acquisition step of the cycle is managed.

- **Acquisition.** The utilisation /use of sources of information by Acquisition units and assets, and the delivery of this information to the appropriate Unit for use in the production of PKI.
- **Acquisition Management (AM).** The process of converting IRs into Acquisition requirements, establishing, tasking, or coordinating with appropriate acquisition units or assets, monitoring results, and re-tasking as required.
- **Information Management (IM).** The process designed to ensure that operational PKI reaches those who need it, efficiently and in a timely manner, while units and assets are used to optimum effect.

3.1.2 Area of Peacekeeping-Intelligence Responsibility and Area of Peacekeeping-Intelligence Interest (APII). A commander will be given an area of responsibility by the higher command or by a UNSC Resolution and it is required that the peacekeeping-intelligence effort be devoted mainly to that area. However, PKI about/concerning adjacent areas will also be required if armed actors/threat can jeopardize a commander's mission or if a commander can influence the progress of operations. This concept is contained in the following terms:

- **APIR.** The APIR is an area allocated to a commander, at any level, in which they are **responsible** for PKI production. This area is limited to the range of their organic acquisition assets.
- **APII.** The APII is an area in which a commander requires PKI on those factors, actors and developments that could affect the **outcome** of their current or future operations. Therefore, per definition, is it a larger area than the APIR because it will also include the areas in which the commander has not an AOO responsibility.

3.2 Basic Acquisition Attributes

3.2.1 **Every personnel is a sensor.** The most readily available and best military acquisition capability UN missions have is their personnel, and leveraging their abilities can be of great benefit to the success of UN military information acquisition. UN personnel may acquire information through patrolling, through the manning of observation posts, by conducting base security patrols, and during most routine operational activities. Furthermore, information may be acquired if they positively interact with the local population. Therefore, it is very important that the Force IAP is communicated

to all personnel in a manner that is understandable to all. For example, broad, strategic PIRs should be broken down into questions that everyone will understand, as shown in the chapter on direction.

3.2.2 **Technical Acquisition Assets.** In addition to UN personnel, there may be specialist acquisition assets deployed to the UN mission. While these assets enhance information acquisition capability, it is important to remember that the information personnel acquire remains of vital importance. Technical acquisition assets are normally employed in a system of systems approach that seeks to ensure the acquisition asset is supported by the necessary architecture and is integrated into the other acquisition assets that are in use. In the case of a UAS, for example, this would require the air vehicle to be deployed with the associated pilots/operators, specialist analysts, communications and logistics networks, etc. This principle also applies across Acquisition capabilities, where it is considered optimal to employ a variety of technical acquisition assets to ensure that the most detailed answer is found to each IR (for example, tasking multiple different sensor types against the same IR).

Acquisition assets are becoming more sophisticated and capable. A step change in a mission's acquisition capabilities can occur as new systems are brought into service. This requires a flexible approach to acquisition management that ensures assets are used together to provide an integrated effect rather than being seen as a series of stovepipes. This can be aided by seeking a robust mix of assets at each level of command ensuring interplay between them, while seeking to avoid an over-reliance on any one type of asset. Within the Force, reconnaissance by ground personnel is now considered to be a core capability at each level of command. This, combined with other systems such as UAS, OPKI and HPKI, provide the ingredients for this robust mix of assets.

3.2.3 **Sources of Information.** There are three types of sources from which information can be obtained:

- **Controlled.** Units or assets which can be tasked by a PKISR officer to provide answers to their questions.
- **Uncontrolled.** Units, assets, sources or agencies which provide information, but over which a PKISR officer has no control. In cases such as these, the MPKI cell can request but cannot task.
- **Casual.** Sources or agencies which may or may not be known to exist and which provide useful information unexpectedly. These were not tasked or requested to provide specific information; however, their reports are useful anyway.

In formulating an acquisition strategy, acquisition staff will normally rely on controlled units and assets to obtain their PIRs within the specified time limit. Information from uncontrolled sources will normally be received in the form of peacekeeping-intelligence summaries from higher formations, or reports from specialist agencies, which is of value in preparing assessments and other Peacekeeping-Intelligence Estimates (PIE). Information from casual sources is often unreliable, and in the absence of collateral information or confirmation from a reliable source, it is difficult to establish its authenticity. However, by applying evaluation techniques outlined in Chapter 5, uncertainty can be reduced to a more acceptable level.

3.2.4 **Controlled Sources.** The controlled units and assets available to the MPKI and/or PKISR cells in UN missions may include:

- Observation posts.
- Foot patrols.
- Reconnaissance patrols.
- Aircraft.
- HPKI assets.
- Open-Source peacekeeping-intelligence.
- Technical Peacekeeping-Intelligence.

- Imagery and Geospatial Peacekeeping-Intelligence (IPKI/GPKI).

Processed PKI products and information can also be obtained from the following additional sources, although they may or may not be tasked directly, but through higher formation headquarters. It is essential that the MPKI cell at its own level creates and maintains a PKI and information-sharing relationship with these entities:

- The MICM.
- Other UN entities which either acquire information or produce PKI such as the JMAC, JOC, UNPOL, and UNDSS.
- Flanking formations or units.
- Higher formations; the company S2 with the battalion S2, the G2 with the U2, the U2 with the MICM. It is important that information and PKI is shared both horizontally and vertically, and that the effort at all levels is both to 'push', down to subordinate units, and to 'pull', from subordinate units to higher HQ.
- Patrols from specialist units such as the Special Forces (SF), PKISR units, Civil Affairs, UNPOL and UNMOs who may be operating in the area.
- HPKI Teams. The availability of HPKI will depend on the UN mission's mandate and capability. All HPKI work must be conducted in accordance with the Peacekeeping-Intelligence Policy, and with mission SOPs.
- Other UN entities such as Political and Civil Affairs personnel, and other smaller units such as the Disarmament**,** Demobilization, and Reintegration (DDR) unit.

3.2.5 **Uncontrolled Sources.** MPKI/PKISR/IRM officers at all levels must recognize potential uncontrolled sources, which could include units, assets, sources, or agencies that provide information, but over which MPKI/PKISR entities have no formal command or control. In dealing with such sources, the MPKI cell can request but cannot task. Information provided by uncontrolled sources must be treated with caution as it may be intended to deceive or influence.

In general, uncontrolled sources can provide written material of all sorts and radio or television broadcasts, relating to forces and areas of operations, actual or potential. They could provide useful information thus should be considered a worthy examination. Examples of uncontrolled information sources are:

- Newspapers and periodicals - containing details of personalities and current events, or political and economic developments.
- Maps, charts, town plans, guidebooks, directories and tide tables - containing detailed topographical information, Open-Source Geospatial Datasets available online, including Electro-Optic (EO)/Remote Sensing and Events Data e.g., Landsat/Sentinel-2, Sentinel-1 SAR Data, NASA Fire Data, ACLED Events Data etc.
- Annual reports of commercial concerns, state-owned and private commercial agencies, international enterprises, etc. - containing indications of industrial and economic capabilities, growth and development potential.
- Scientific and technical journals and papers - containing detailed studies of activities in their respective fields.
- Reference books - containing a variety of details, from lists of naval vessels and aircraft types to the professional, technical and academic qualifications and positions held by individuals.
- Monitored radio broadcasts - containing information on current events, future intentions, morale and administration, in general.

It is desirable that an OPKI section exists at U2 and G2 level. If there are sufficient personnel, S2 and Company S2 sections should also endeavour to establish such a section. If this is not possible,

both the S2 and Company S2 sections should request a daily OPKI summary from their higher HQ. Ideally, the OPKI should focus on the region, the country, and then on individual sectors.

3.2.6 **Casual Sources.** Casual sources include:

- The local civilian population in an area of operations.
- Refugees and Internally Displaced Persons (IDPs).

3.2.7 **Source Register**. Often, units reporting to the MPKI cell have acquired information from the same location or from the same source. This problem of different reports with the same information, and ultimately from the same source, is called 'circular reporting'. Therefore, it is important that the MPKI cell at each level maintains a source register. A source register makes circular reporting less likely.

3.3 Force IAP

All acquisition assets and other acquisition resources are included in a single plan to maximise the different capabilities. The plan synchronizes and coordinates acquisition activities in the overall scheme of manoeuvre. A good Force IAP fits into and supports the overall operations plan or order. It positions and tasks acquisition assets to acquire the right information or be able to react and change priorities in response to a changing situation.

Acquisition Management and coordination must be conducted at every staff level. The Force IAP is a tasking matrix that links information acquisition with sensor assets. It lists the IRs with the organizations or databases that might hold the information or with the sensor assets that might be used to gather the information. The Force IAP is not a static document frozen in time, but a continuous process. It will react and respond to changes in the operational situation and the information gathered by the assets tasked.

3.4 Acquisition Process

To maximize the effect of acquisition assets and deconflict the acquisition in a designated area, the Acquisition Manager must have a good understanding and knowledge of the mission PKI architecture and organization. Acquisition is based on the commander's direction and the PIRs/IRs received (See Figure 2).

3.4.1 **Step One** is a review of available information in order to reply to PIRs/IRs with information already stored on file by the mission. This is often referred to as basic or current information or PKI. It should be noted that there will be few occasions that IRs can be entirely satisfied with information already on file. When there is insufficient data available to answer the IR, new acquisition is required. Those IRs that cannot be satisfied are then collated and, if they are not already reflected in the Force IAP, will be incorporated.

3.4.2 **Step Two** is using the AOE prepared by the Analysis Team, which provides a general indication of the location to which assets need to be deployed, to acquire the necessary information. These areas are often referred to as NAIs. The Acquisition process also includes the identification of the assets that can most effectively meet the various IRs, by matching the appropriate sensor/platform combination to the task. The acquisition assets are tasked through an operations or tasking order (OPORD or TASKORD) via the mission U/G2 branches or S2 section.

3.4.3 **Step Three**. Once identified, broad PIRs/IRs will normally not be passed directly to units and assets. Rather, as outlined in the Chapter on Direction, each will be broken down into smaller SIRs and EEIs. The sum of these IRs should answer the broad PIR or IR. It will be these SIRs, EEIs, and/or indicators that the units and assets should look for. All acquisition assets and resources must be placed into a single plan to capitalize on the different capabilities. This plan is known as the Force-level IAP. The plan synchronizes and coordinates acquisition activities. A good Force IAP fits into and supports the overall operations plan or order. It positions and tasks Acquisition assets to acquire the right information or shift priorities as the situation develops. Effective information acquisition focuses on answering the commander's requirements through Acquisition tasks translated into orders.

3.4.4 **Producing the Force IAP.** To produce the Force IAP, a spreadsheet, or other graphical tool can be used. The following steps are a guide:

- The U2 Branch or subordinate MPKI cells should take the Force IAP, which lists all PIRs, SIRs, and EEIs on the left-hand side of a spreadsheet and should then detail all controlled (military) sources in columns to the right-hand side. This should be done in close conjunction with the U3 Branch. It is good practice to link SIRs and EEIs to particular geographic areas where this information can be acquired. As stated above, these areas are known as NAIs.
- In close conjunction with the U3 Branch, subordinate units (controlled sources) are tasked to acquire specific information based on their unique capabilities. Depending on the mission assets, structure, role, SOPs, and mandates, these units could be dedicated PKISR units specialising in HPKI, Signals Peacekeeping-Intelligence (SPKI), Imagery Peacekeeping-Intelligence (IPKI), etc., as well as non-dedicated units with the ability to acquire some information of potential value (such as utility helicopters carrying visual observers, ground patrols, etc.).
- The stated Force IAP may task several units to acquire the same information to ensure that high-priority information is acquired, and that information is not based purely on a single source. However, this must be carefully planned to avoid unnecessarily duplication of acquisition efforts.
- Units that are tasked to acquire information should be represented on the Force-level IAP with a simple tick or other symbol. This will allow the information Acquisition Manager to follow-up on Acquisition taskings, as shown in Annex A to Chapter 5.
- If subordinate units are using sources, then all sources must be registered with the higher HQ. This avoids circular reporting. An example of a source register is at Annex F to this Chapter.

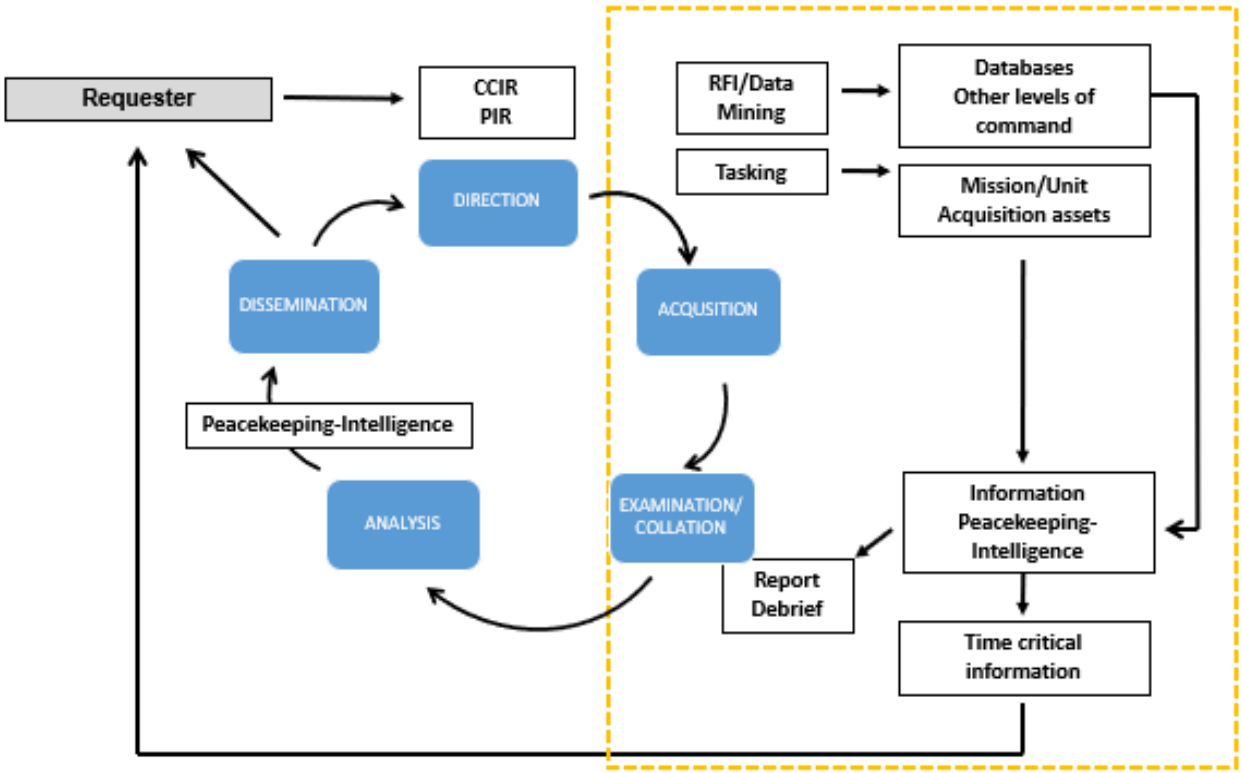


Figure 2: Acquisition Process

3.5 Military Information Acquisition Disciplines

Specialised MPKI capabilities, some of which are listed in subsequent paragraphs, will be deployed to some peacekeeping operations (PKOs); this will depend on the mission and mandate. Often, the more specialized the capability is, the more likely it is that it will be OPCON to the Force Commander, or that it will be provided by a Troop Contributing Country (TCC) with these specific capabilities. To make the information acquisition process and the MPKI cycle as effective as possible, all PKI staff must have good knowledge of the kind of acquisition assets that are present in the mission. It is important to note that all MPKI capabilities will be deployed overtly, in line with the PKI Policy, and will adhere to all relevant legal norms. Specialist MPKI acquisition assets common in today's UN missions are:

3.5.1 **HPKI** concerns information that is elicited or otherwise provided by human sources. Human sources can provide timely, accurate, and specific interesting information, but must be carefully scrutinised to ensure its validity. Contact with human sources needs to be deconflicted, controlled, and coordinated at unit staff level. It is important to ensure that HPKI is acquired by (and from) both men and women, young and old, rich and poor etc. in order to access the widest possible range of views and perspectives[6].

- **Advantages**
  - Information is more readily available than from other acquisition capabilities.
  - HPKI operations are cost effective when compared to technical acquisition assets such as aircraft or satellites.
- **Disadvantages**
  - HPKI operations may take time to develop and to shift the emphasis of sources onto new IRs.
  - Communication with potential sources is essential, but interpreters with the knowledge of local language and dialects might not be accessible when needed. Local interpreters must be vetted; otherwise, there is a risk of bias in interpretation or Operational Security (OPSEC) lapses.
  - HPKI sources need to be validated to ensure the information they provide is credible. This can take a significant amount of planning and requires experience in managing HPKI sources.

3.5.2 **Geospatial Peacekeeping-Intelligence (GPKI)** refers to the use and analysis of imagery and geospatial information in response to PKI requirements. The production of GPKI combines, *inter alia*, mapping, charting, imagery, IPKI and geospatial information. IPKI relates specifically to the use of imagery alone. The source of the imagery (satellite, UAS) is not relevant to the term; it is the analysis and interpretation of the imagery itself that is important. Examples of geospatial data are roads, transportation networks, elevation data, shapes and locations of buildings and installations, vegetation, waterways, etc. Geospatial products can take the form of three-dimensional information (3D) such as areas of interest, dead ground studies or slope analysis[7], all of which are valuable products for planning purposes. When taking into consideration geographically referenced activity, it is possible to produce powerful geo-visualization to display activity and trends. For example, overlaying publicly available information, such as social media posts, on maps, to show over time how a demonstration is building up to assist with policing is a valuable resource. In other words, GPKI acquires, organizes and combines data around its geographical (physical) location on earth[8].

[6] Guideline on Acquisition of Information from Human Sources for Peacekeeping-Intelligence, September 2020

[7] Dead ground is ground that cannot be seen from a certain point due to the shape of the terrain, for example, hills and valleys. A slope analysis is made, for example, to assess whether a sloping hillside is suitable for a helicopter to land on.

[8] Guidelines on Geospatial Peacekeeping-Intelligence, September 2023

- **Advantages**
  - Provides readily understood products that can be quickly absorbed by decision-makers via an all-source analysis product.
  - Depending on the sensor, the asset may be able to mitigate the effects of some environmental conditions. For example, use of Infra-Red sensors to observe activity at night, or use of Small Aperture Radar (SAR) sensors to detect objects/changes in ground surface.
  - Depending on the sensor and platform employed, it may be able to acquire information from considerable distances away, reducing risk to the platform and avoiding alerting the subject.
  - Mitigates risk to human life and detection during acquisition when compared to HPKI.
- **Disadvantages**
  - Requires highly trained, specialist personnel to interpret the images that are acquired.
  - Weather, climate, and physical obscuration (from foliage or buildings, for example) might limit the use of certain sensors.

3.5.3 **Open-Source Peacekeeping-Intelligence (OPKI)** is information obtained from sources accessible to the public, such as radio, television, Internet, press and other unclassified information. OPKI can be used as a platform for the monitoring of actors' use of different media[9]. OPKI sources can be divided into categories:

- **Media:** Print newspapers, magazines, radio, and television from across and between countries.
- **Internet**: Online publications, blogs, discussion groups, citizen media (i.e., cell phone videos, and user created content), YouTube, and other social media websites (i.e., Facebook, Twitter, Instagram, etc.). This source also outpaces a variety of other sources due to its timeliness and ease of access.
- **Publicly Available (Government) Data**: Public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although the acquired information comes from an official source, it is publicly accessible and may be used openly and freely.
- **Professional and Academic Publications**: Information acquired from journals, conferences, symposia, academic papers, dissertations, and theses.
- **Commercial Data**: Commercial imagery, financial and industrial assessments, and databases.
- **Grey Literature**: Technical reports, pre-release prints, patents, working papers, business documents, unpublished works, dissertations, and newsletters.
- **Advantages**
  - The use of OPKI is accessible to all, though for best results personnel should receive a specialised training. It is normally inexpensive, easy to use and can produce results quickly.
  - OPKI is readily shared in its raw form due to its inherently unclassified nature.
- **Disadvantages**
  - Source evaluation and verification can be difficult, meaning OPKI may need to be combined with additional sources of information to provide the necessary confidence for decision-makers.

[9] Guidelines on Open-Source Peacekeeping-Intelligence, March 2023

- Deception through OPKI channels is relatively easy; mis/dis-information are significant risks that must be guarded against by analysts working with OPKI. As such, the use of OPKI sources must be vetted to ensure information provided is authentic.
- Accessibility of open sources is often misunderstood. In many UN PKOs AOOs, the local population has no access to, for example, social media. Many accessible reports on open sources could therefore be assessed as a representation of the population although this is not the case.

3.5.4 **Signals Peacekeeping-Intelligence (SPKI)** is the overarching term for PKI derived from exploitation of signal-emitting systems, be those communication and non-communication focused. Exploitation of communication emitters (such as radios) is specifically referred to as Communications Peacekeeping-Intelligence (CPKI) and exploitation of non-communication emitters (such as radars) is referred to as Electronic Peacekeeping-Intelligence (EPKI).

- **Advantages**
  - Provides a 24hr, all-weather capability.
  - SPKI systems are passive and therefore inherently non-detectable by a hostile actor's Electronic Warfare (EW) capability.
- **Disadvantages**
  - SPKI can only be employed when a hostile actor is emitting signals that can be intercepted.
  - Depending on the range of the system, it might need to be deployed relatively close to the subject, thereby increasing the risk of compromise.
  - Host Nations must give consent for the employment of SPKI systems in their territory and may have significant concerns regarding its use, since SPKI systems may detect all communications, not just those of hostile actors.

3.5.5 **Technical Peacekeeping-Intelligence (TPKI)** is peacekeeping-intelligence derived from the acquisition and analysis of threat and foreign military equipment and associated materiel. A subset of TPKI is Weapons Technical Peacekeeping-Intelligence (WTI), which is a category of PKI derived from the forensic acquisition and exploitation of Improvised Explosive Devices (IEDs) and associated components, improvised weapons and other weapons systems. WTI can be utilized to support prosecution, identification of material sources and to inform force protection measures. For the United Nations, WTI is primarily utilized to inform Force Protection measures. The WTI enterprise is comprised of several levels of exploitation: Level 1: Tactical exploitation of the scene utilizing Explosive Ordnance Disposal (EOD) or Weapons Peacekeeping-Intelligence Teams (WIT) to record the details of an IED Event and preserve, describe and recover physical, technical and forensic material; Level 2: In-Mission exploitation of recovered items to identify switch type and function, frequency, voltage, explosive analysis and biometrics (where legally relevant). *The UN's WTI capabilities will likely conclude at Level 2.*

- **Advantages**
  - Reveals the technological capabilities of occurring factions in a mission area.
  - Informs Force Protection measures by identifying the necessary equipment needed to detect IEDs or the protective measures needed to mitigate their effects.
  - Informs training and adjustments to tactics, techniques and procedures (TTPs) based on the evolution of the IED threat.
- **Disadvantage**
  - Time consuming and demands special analysis equipment.

3.6 Reports and Returns

3.6.1 Reporting formats may vary according to mission SOPs for particular types of Acquisition, but the primary means of reporting are outlined in the Dissemination Chapter of this Handbook. The format for an RFI is included as an Annex B to Chapter 2.

CHAPTER FOUR: EXAMINATION AND COLLATION

4.1 Introduction

Data and information acquired by missions shall be recorded and stored in a manner that permits convenient comparison, evaluation, assessment, retrieval, analysis and reporting. Participating mission entities shall make use of standardized tools for the collation of data and information, including common databases, taxonomies, and planned indexing and menus. DPO will design and promulgate, in consultation with missions, common and, where necessary, specialized tools, which shall be supported by training.

4.2 Collation

Collation consists of procedures for *receiving, recording*, and *grouping* all information acquired. Collation is the foundation of the Analysis stage and well-trained, efficient, conscientious and thoroughly briefed collators are of vital importance to the effectiveness of the PKI cell. The collators ensure that no piece of relevant information is lost. They ensure that every piece of relevant information is registered, sorted and recorded and, most importantly, that every piece of information can be retrieved by the MPKI analysts, on demand. It is also the collators who, if properly briefed and thoroughly familiar with the IRs, will provide the first analysis of information as it is received.

Collation tends to be the work of junior staff as such busy MPKI officers can also easily overlook its supervision; thus, there is a danger that the collation system will not be successful. It is important that it is supervised closely and maintained conscientiously if it is to be effective. Collation involves:

- Assimilation of large volumes of information and PKI.
- Identifying and registering each incoming piece of information and PKI.
- Recording the source of each incoming piece of information without compromising source security. Often a human source will be given a cover/code/nickname.
- Recording the reliability of the source in line with the evaluation methods shown in the next section.
- Categorizing each piece of information or PKI through the accurate and effective use of tags such as: Date information was acquired; Date information was received; information type (social, security, political, economic, military); type of source (OPKI, HPKI, SPKI, etc); name of source (protecting sources' security); reliability of the source and credibility of the information.
- Maintaining an efficient system or 'peacekeeping-intelligence log' for conducting these procedures. This system will ideally be in a database (a MS Excel or Word document, for example) that must be accessible to all analysts, in line with the Peacekeeping-Intelligence Policy and relevant SOPs.

4.2.1 **Establishing and operating a collation system requires:**

- **Information Technology.** All collation systems, especially at Unit level, should be as simple as possible to maintain and operate, using the minimum personnel. Wherever possible, the maximum use should be made of Information Technology (IT), and other means of visual presentation, for example, on maps or overlays. Visual displays, whether digital or on paper are probably far more readily understood and assimilated than pages of detailed summaries and notes. In many modern PKI cells, the collators and analysts, together with their databases, will be linked by an IT network. This is highly desirable; it enables analysts to pull information from the database as it is required and collators to flag information of relevance to a particular analyst as it arrives. Such a system does, however, depend upon both availability of the system and its supporting communications architecture. However, there are limitations in the use of IT. A collation system based on IT is vulnerable to certain difficulties and mitigating factors must be in place to ensure PKI business can be conducted despite the potential loss of IT. IT considerations are:

- Continuous Electrical Supplies.
- Sufficient Communications Availability.
- Effective and Capable Software.
- Suitable Security Clearance.
- Systems Compatibility.
- Memory Usage.
- Skilled operator/human resources.

- **Design.** The design of a collation system must have the aim of facilitating the recording of information, the retrieval of individual or related reports and the storage of PKI for dissemination or reference, as well as highlighting related items to aid further analysis. Creating and adhering to a set lexicon of approved activity and event terms in a mission will help ensure consistency in reporting and prevent loss of coherence when staff change over. The indexing and categorization of subject matter must be related to the projected area and scope of operations, and must be based on:
  - The stated or anticipated commander's PIRs.
  - The broader peacekeeping-intelligence needs of the operations staff.
  - The anticipated volume of information, and frequency of reports, at peak periods.
- **Operation.** In operation, the system must ensure that:
  - All relevant reports are recorded and catalogued/provided with a reference to enable swift and easy retrieval.
  - The relationship between separately recorded but related reports is immediately apparent.
  - Analysis can be based on all relevant facts.
  - Significant information is highlighted and not obscured by a mass of trivial facts.
  - Gaps in basic or current peacekeeping-intelligence are highlighted to assist in acquisition planning.
  - Information and PKI are recorded in a manner which minimizes the need for regrouping, rephrasing, or other manipulation prior to dissemination.
- **Standardization.** Time and effort can be saved, particularly at the lower levels of command, if collation systems are standardized throughout a theatre of operations. The use of standardized terminology and definitions will assist in the clarity, brevity and speed of recording and disseminating peacekeeping-intelligence. This is not easy to achieve, particularly in combined operations. It must be addressed by the senior peacekeeping-intelligence officers of cooperating headquarters as early in the operation as possible. In a UN MPKI context, the cooperating headquarters might be another UN Sector Headquarters, or other UN Forces.

4.2.2 Factors to consider when creating a Collation System:

- **Cross-referencing.** All information and peacekeeping-intelligence should be cross-referenced to related materials held in the PKI database to support the identification of related peacekeeping-intelligence and to support the development of trend analysis. IPKI and GPKI should also be considered as methods of cross-referencing information, for example through change detection.
- **Urgency and speed of reaction.** The collation system must include the appropriate human and IT resources to process urgent information and PKI requests rapidly and effectively.

- **Restrictions on the volume of records.** The collation system's capacity to process a volume of information is dictated by:
  - The number of personnel available to operate the system.
  - The nature and tempo of operations.
  - The size of the workspace.
  - The size and scope of the PKI task.
  - The threat actors' activity level in the area.
- **Pragmatism.** It is not possible to process every piece of information and PKI received. The attempt to do so will almost inevitably lead to the processing system becoming overloaded and, in the worst case, halting. A compromise between what is desirable and what is possible is required. Compromise can only be achieved by adopting a pragmatic approach to collation, constantly reviewing collation activity, re-shaping databases, and filtering relevant input. Information, not immediately relevant, is retained for future review.
- **Prioritization.** Collation must consider PIR and IR to ensure that relevant information is prioritized and processed with the appropriate degree of urgency. Furthermore, when actionable, very important intelligence would arise, it should be used instantly to inform the commander. For example, when intelligence from a usually reliable source would indicate an imminent attack. The still important collation step should be considered after disseminating this important, timely message.
- **Data system backup and recovery.** Most data used by PKI organizations is to be held on automated systems. Reliable access to this data is critical to the functioning of the PKI organization. All data systems malfunction at one time or another. Malfunction causes are internal or external and can disrupt or destroy the data stored and websites.
- **Recording aids** serve the useful purpose of providing a tool for data organization. Used alone or to produce solid analysis in the overall PKI production effort, these aids include and are not limited to:
  - Annotated maps (Incident maps, situation maps).
  - Working files (threat analysis, file, reference material, coordinate register).
  - Order of Battle (ORBAT) of all threat groups.
  - Timelines, diagrams and matrices.
  - Microsoft Excel or Word document, with hyperlinks to data files.

4.2.3 **Sample Collation Format.** Often a single work sheet in Excel format will suffice for smaller cells, as outlined below:

Date of Event*	Date of acquisition^	Source	Source grading	Subject	Location Acquired	Security Classification	Link to PIR	Link to Document^^

Table 1: Collation Format

*When the event occurred
^When the information was acquired
^^Hyperlink to original document or file path so that it can be located on the system

The sheet will be developed on a weekly/monthly basis depending on the amount of information the cell must record. If there is a large volume of incoming data, then U2 or G2 cells should consider using other collation formats : **Entity worksheets** (JMAC data and reports, UNCT data and reports, UNDSS data and reports, Civil Affairs data and reports, UNPOL data and reports etc.), **thematic worksheets** (this could be used to record military information, non-state actor information, threat

group information, economic or cultural information etc.), or **specialized worksheets** (this could be used to record incoming HPKI, SPKI or IPKI data).

4.2.4 **Translation.** Capability must be provided to translate the peacekeeping-intelligence into the standard UN languages where required.

4.3 Examination

Examination and evaluation refer to the process of vetting the credibility of the information and reliability of the source.[10] Information acquired must be tested before being accepted for the next steps in the MPKI Cycle. This process is called examination and aims to determine the real value of the acquired information.[11] To do so, the information needs to be evaluated. Evaluation as a process within the Examination stage of the MPKI cycle is where every item of information is examined regarding the reliability of its source and the credibility of its content.

4.3.1 **Process.** In evaluating information, the knowledge and judgment of the PKI analyst plays a major role. The evaluation of acquired information is processed through the following steps:

- Verification of the information accuracy, timeliness and relevancy.
- Comparison/confrontation with other sources, available information and previously acquired knowledge about the subject matter.
- Rating the source's reliability and the information's credibility.

4.3.2 **Verification.** The initial assessment of the acquired information is a critical and objective analysis of the following aspects:

- **Validity of the information** depending on its origin and the circumstances, time and place of acquisition.
- **Credibility of the information** based on the nature and accuracy of its content, as well as on the rating attributed by the Acquisition authority.
- **Relevance of the information** in enabling better situational awareness about the threat and area of interest.

4.3.3 **Comparison.** Every item of information must be compared with other acquired information considering previously developed knowledge of the environment and the threat. This operation consists of:

- **Cross-checking the information** derived from multiple sources. The information may have greater credibility if the sources are distinct and independent. Circular reporting should be avoided at all times!
- **Checking its coherence** with previously processed data.
- **Assessing its conformity** with previously acquired knowledge about the operational environment, including the potential threats and risks.

Confirmation of information by other sources and agencies is always desirable, but it is not always possible to obtain. As more information is received, the situation of the threat, its capabilities, and probable courses of action become increasingly clear. As the body of PKI expands, information that is not compatible with the current threat situation and that is not consistent with the recent pattern of its activity, becomes questionable. Likewise, the in-depth knowledge of the operational environment and the possible actions/reactions of different actors enable the MPKI analyst to make judgments as to the veracity of the information.

In determining the validity of a fact or whether a reported activity is at all plausible, it must be realized that certain events are possible even though they have never occurred previously and thus have

[10] JMAC Field Handbook 2018
[11] UNDSS Security Analysis Handbook 2023

been deemed by past analysis as unlikely to happen, i.e., threat actors can be innovative and act "out of the box". People tend to be biased so this is very important.

4.3.4 **Rating.** Rating information is the result of the evaluation through which every acquired item has been processed. It consists of combining the reliability of the source with the credibility of the information to reflect the level of confidence in the material. The rating to be used by MPKI analysts is indicated by a standard, universally used system. Every item of information must be rated during the analysis phase in the form of an alphanumeric code whereby the '**Letter'** indicates the reliability of the source (Table 5), and the '**Figure'** indicates the credibility of information (Table 6).

Source Reliability		
Rating	**Evaluation**	**Observation**
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	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot Be Judged	No basis exists for evaluating the reliability of the source

Table 2: Rating of the source reliability

Credibility of Information		
Rating	**Evaluation**	**Observation**
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	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Cannot Be Judged	No basis exists for evaluating the validity of the information

Table 3: Rating of the credibility of information

For example, some new data should be assessed as follows: *information* coming from a B-graded source (minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time) that has 'not been confirmed but is logical and consistent with other information on the subject, must be graded as: B2, in line with the chart above.

When grading sources, it is important to remember that the headquarters closest to the source is ordinarily the best judge of its reliability. This judgment is based on experience of other information from the same source or, in the case of information produced by a sensor, on the accuracy or limitations of the system.

A higher HQ normally accepts the reliability evaluation performed by a reporting headquarters. For example, if a MPKI section at S2 level grades a source as 'B' then the MPKI Branch at G2 level, to which it reports, will generally accept this grading, recognizing that the S2 MPKI section has greater experience with that particular source. It does, however, consider the reliability of the reporting

headquarters itself. If, for example, the S2 section has incorrectly graded sources in the past, then the G2 Branch may decide to question the grading. Moreover, sometimes a higher HQ will have access to an overall source register and, as a result, the higher HQ may have a different evaluation or interpretation of the source than that of the unit or sensor that originally acquired the information. For example, if several different Acquisition assets are using the same source (this is often not apparent to the individual acquisition assets), higher HQ will have access to all reports that this source provides. It is therefore possible that it will assign the source a different level of reliability. Further, it is vitally important that all sources used by Acquisition assets are registered with higher HQ. Generally, it is the responsibility of the U2 Branch to maintain the 'theatre source register'.

During evaluation, the reliability and credibility of information are considered independently to ensure each does not influence the other because even the most reliable sources can produce wrong information. Equally, the provision of confirmed information does not necessarily indicate a reliable source. A source's expertise, motivation and access will affect both its reliability and credibility. These coefficients are subject to change if other sources confirm or deny the item of information.

CHAPTER FIVE: ANALYSIS

5.1 Concept

This Chapter is dedicated to the study of analysis in the UN peacekeeping environment and is designed to assist the MPKI staff at the Force, Sector and Battalion levels. It may also be used to train deploying TCC PKI staff on how the UN conducts the Analysis step of the MPKI cycle. During the pre-deployment and training phase, PKI analysis will already occur either in the UN HQ New York or in the mission AOR if a UN PKO is already deployed. As a result, Analysts are likely to deploy with a good analytical starting point regarding the OE and actors.

5.2 Definition

As per the current UN Peacekeeping-Intelligence Policy, Analysis refers to the methodical breaking down of information into its component parts; examination of each to find interrelationships; and application of reasoning to determine the meaning of the parts and the whole. PKI analysis is a whole-of-mission process that makes full use of all resources available to the mission according to the comparative advantages, including expertise in the local situation, languages and cultures; military and police PKI Analysis capabilities; and security threat information analysis techniques.

During Analysis, the acquired information is being turned by the Analysts into a finished product that ideally gives meaning to the individual pieces of information and is therefore more than the sum of its parts. Indeed, MPKI Analysts apply processes of reasoning, integration and interpretation using both qualitative and quantitative methodologies. Ultimately, MPKI analysts are required to provide predictive analysis and scenarios on the evolving tactical and operational situation.

The objective of predictive analysis is not just to establish capabilities of the threat and other actors but to determine their intentions and probable courses of action/scenarios. Analytical processes exist to offer the Analyst a set of tools to help the human mind deal with vast quantities of data. The data available to the PKI Analyst includes both basic and current PKI, and unprocessed or raw incoming data. The human mind is better equipped to deal with large quantities of data by visualizing them. It is important to note that visualization techniques do not replace Analysis. Rather they are tools to reduce ambiguity and help to make sense of vast quantities of data.

Analysis should strive to be predictive. It should consider an event/incident, trend or threat, and establish why such a thing is occurring, what is likely to come next, and what the implications are for the UN mission. Strong Analysis gives advance warning of events or courses of action that could threaten effective mandate implementation relating to the protection of UN personnel and civilians. The objective of predictive Analysis is to, inter alia: determine the capabilities and intent of threat actors in order to establish likely courses of action; and to identify other issues or trends that could pose a threat to missions or mandate implementation relating to the protection of UN personnel and civilians.

The scenarios should, at the operational level, consider all relevant factors. The process should have a long-term focus but include a defined end-date. As explained earlier in the Handbook, two common frameworks to ensure all factors are considered are:

- **PMESII**
  - Political
  - Military
  - Economic
  - Social
  - Infrastructure
  - Information

- **ASCOPE**
  - **Areas**. Physical locations and terrain that affect all relevant actors e.g., boundaries or police districts.
  - **Structures**. Significant infrastructure e.g., bridges, religious sites, hospitals and schools.
  - **Capabilities**. Key functions include administration, food/water supply, health / welfare provision.
  - **Organizations**. Political, social, religious, tribal etc. These must be understood and their likely influence assessed.
  - **People**. The local population including tribes, groupings, political parties, threat actors and any other relevant human actors. Within each, leadership, intentions, relationships, pattern of life, needs and any other sub-factors can be considered.
  - **Events**. Harvest season, market timings, public holidays and religious festivals for example.

When PMESII and ASCOPE are combined (possibly into a table, as shown in Annex C to this Chapter), it will provide the PKI staff with a strong set of factors for analytical consideration. Once the table is filled in, the PKI staff will have a good understanding of the OE and associated gaps, which will assist them with Acquisition planning.

5.3 Analysis: Fundamentals, Standards and Skills

5.3.1 **Fundamentals of Peacekeeping-Intelligence Analysis.** Analysis is the structured examination of all relevant information to develop knowledge, which helps to give meaning to events within an operational environment. Analysis performed by MPKI personnel should be predictive in nature and should support the Commander's decision-making process. It is the step in which items of information are taken and repeatedly subjected to the questions; 'what does this mean?' and 'so what?' until all the relevance and significance of the information is extracted. These fundamentals are then reconstructed, during the Integration step, into PKI with a new significance. To be effective, PKI personnel must have a detailed awareness of their commander's requirements and a thorough understanding of applicable process.

An Analyst must accept a certain degree of ambiguity. Training, knowledge, and experience are all critical parts of dealing with this uncertainty because PKI personnel never have all the information necessary to make an assessment. If this was the case, then the finished product would be fact rather than an assessment. Analysts deal with such ambiguity by using the language of likelihood to express the level of certainty associated with a PKI product.

Operational planning and execution impose time constraints on the MPKI cell. This may require assessments to be provided without all the information the MPKI cell would like to have. No analytical product is perfect, and it is once more highlighted that it reaches the commander in a timely fashion than not at all.

All analytical products should be auditable and preferably also replicable. The Analyst ensures that his/her product is auditable by being able to list the information and any deductions used in the formulation of an assessment. The Analyst ensures that his/her product is replicable by ensuring that if another Analyst had access to the same information, that they would as closely as possibly come to the same conclusion. The information that the Analyst deals with can be both qualitative and quantitative in nature.

- **Qualitative information** are mainly non-numerical data that are descriptive in nature, such as text, images, videos, and audio recordings, etc. It cannot easily be measured, but, most often, it is qualitative information that is used to support predictive analysis, whether out of necessity, or due to limited availability of alternative data. Qualitative information is generally concerned with individual, or group, behaviour and any judgement placed on the significance of that activity.

- **Quantitative information** can be defined as information that can be quantified and measured in numerical values. It is generally information of a scientific and technical nature that can be measured and is, therefore, more likely to be used to form the basis of assessments of capability. Interpretation of quantitative information can also form the basis of assessments about environmental or geographic conditions affecting operations.

All analytical products should be based on multiple sources of data. MPKI personnel should avoid basing their PKI product on a **single source** of information, whatever the reliability of the source. In the context of peacekeeping, **multiple-source peacekeeping-intelligence** is the result of the fusion of different types of information, from a variety of sources, to produce an all-source predictive PKI assessment to inform the commander's decision-making. Although multiple-source PKI normally takes more time to produce, it is more comprehensive, more reliable, and less susceptible to deception than single-source analysis.

Analysts should strive to be objective and be aware of any conscious and unconscious bias that informs their PKI product. To avoid these pitfalls, analysts should take care to list and challenge any assumptions made, and to avoid allowing past experiences play too great a role in the analytical process.

5.3.2 **Peacekeeping-Intelligence Analysis Standards.** The conclusions reached during peacekeeping-intelligence analysis should meet the following qualitative and quantitative criteria:

- **Objective.** PKI products must be based on well-sourced information and must be free from analytical bias, either conscious or unconscious.
- **Timely.** PKI product is not helpful if it reaches the commander late.
- **Accurate.** PKI personnel should apply expertise and logic to make the most accurate judgments and assessments possible given available information. Analysts should always make their commander aware of any information gaps. The MPKI cell should strive to bridge these gaps by adding them to the Force IAP, or by sending RFIs to relevant units.
- **Relevant.** The MPKI cell must provide PKI assessments that are useful to the commander's mission or that will enhance mandate implementation relating to the protection of UN personnel and civilians.
- PKI products must be based on all available sources of information. Whenever possible, an analytical judgement should not be based on single-source information. Please see below an elaboration of single- and multiple-source PKI.
- MPKI cells must use all appropriate analytical tools, such as those outlined in this chapter.
- Properly describe quality and reliability of underlying sources.
- Properly caveat and express uncertainties or confidence in analytical judgments.
- Properly distinguish between underlying factual PKI and the assumptions and judgments used to form a conclusion.
- Consider and explain possible alternative hypotheses for incoming information or data sets.
- Facilitate clear understanding on the information and reasoning underlying analytic judgments.
- Consistent with previous production on the topic or, if the key analytic message has changed, highlight the change and explain its rationale and implications.
- MPKI cells must incorporate a gender perspective. This means that all PKI products should preferably have included information acquired from all genders. Ideally, this information would be gender-segregated during the acquisition and collation processes. This should ensure that during the analysis of the human terrain, the MPKI cell can ascertain perspectives from both men and women, which can lead to a more complete understanding of the operational environment.

5.3.3 **The Process.** Analysis is not intuitive. Rather, it should be a structured process based on the application of auditable approaches. Some of these approaches are listed below.

- **The Visualization of Data.** The human mind does not handle large quantities of data very well. It is therefore helpful to a MPKI cell for data to be visually represented or sorted before being analysed. Often, such visual representation will help the analyst uncover trends and patterns that would otherwise have been hidden. Below are some tools that can assist the MPKI cell in this regard:
  - **Information ordering:** Information ordering means that the Analyst arranges data in a meaningful order. This can be done by sorting data by type, or by depicting events on a timeline. Data can also be arranged in a chronology. See Figure 3 below for a sample timeline.

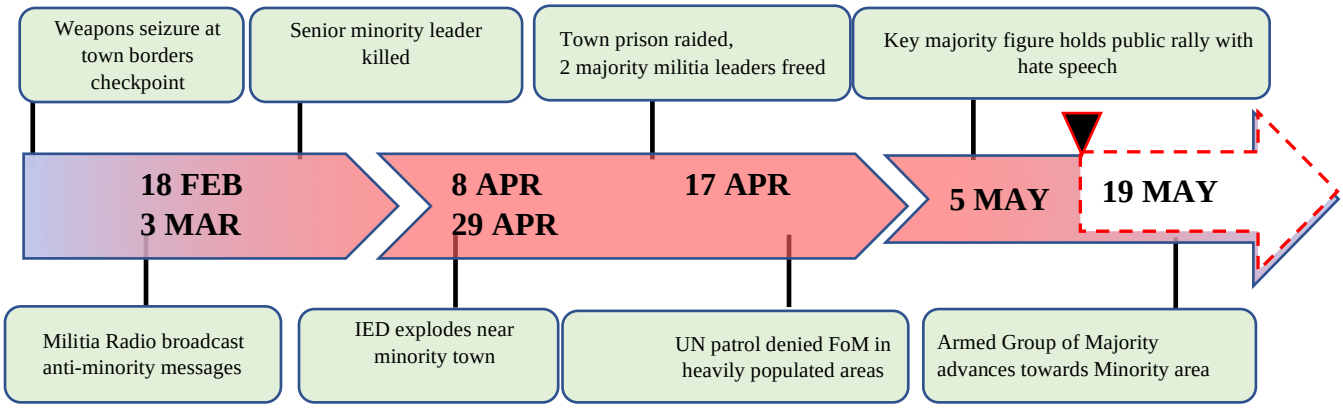


Figure 3: Timeline example

  - **Pattern recognition:** Analysts can sort data temporally, geographically, or by event type. Often this will reveal meaningful patterns. Data can also be visually represented on a series of map overlays. Please see Annex E for additional techniques for placing such information on map overlays. It is worth noting that it is important that the analyst is careful not to 'create' patterns that do not exist, or by correlating sets of unrelated data.
  - **Reasoning:** The ability to reason is what permits humans to process information, and to assign meaning to observed actions and events. There are four types of reasoning that guide analysts in transforming information into PKI: inductive reasoning, analogical reasoning, deductive reasoning, and abductive reasoning. Definitions for such approaches are outlined in Annex C.

5,3.4 Some of the techniques to be used by the MPKI Analyst may involve:

- **Mind mapping:** Drawing visual representations of concepts and the links between them to show connection between ideas (words or images) using lines to explain the relationship between them. Mind maps can help clarify the MPKI analyst's thinking on a topic or help him/her communicate it. Creating a mind map may also help express more clearly a complex issue or problem and thus provide a useful framework around which to write a PKI assessment. Mind mapping can also help to identify weaknesses in an analyst's argumentation, leaps in logic that cannot be explained, or assumptions the analyst may intuitively have made that have not been clearly articulated.
- **Link diagrams:** A link diagram is a tool used to facilitate greater understanding of the relationships/connections between entities (individuals, organizations, and activities. Graphically, link diagrams are created from information contained in a unit's historical files and from information that is currently being reported. Analysts should use a link diagram whenever individuals, groups, group activities, or process networks are being reviewed for insight. The need for link diagrams increases with the increase in data and network complexity. The process and conventions to be followed when creating a link diagram are outlined subsequently in this Chapter.

- **Pattern analysis:** A pattern analysis plot sheet depicts patterns in time and activity. It aids the MPKI analyst in identifying when the threat tends to conduct specific types of activities. The pattern analysis plot sheet is a circular matrix and a calendar. The matrix is divided into sections based on time; generally divided by hour and subdivided into concentric rings that identify days. When using this method, the symbol must be marked on both the time-wheel matrix and the calendar; the footnote is then described separately below the calendar or in a location near the pattern analysis plot sheet. The methodology is the same as chronologies and timelines, with the following specific techniques employed for the pattern analysis plot wheel:
  - Different symbols are used for each type of incident. All symbols are tracked in a legend.
  - All incidents are marked on the time-wheel matrix and the calendar.
  - Noteworthy events may be annotated with footnotes.

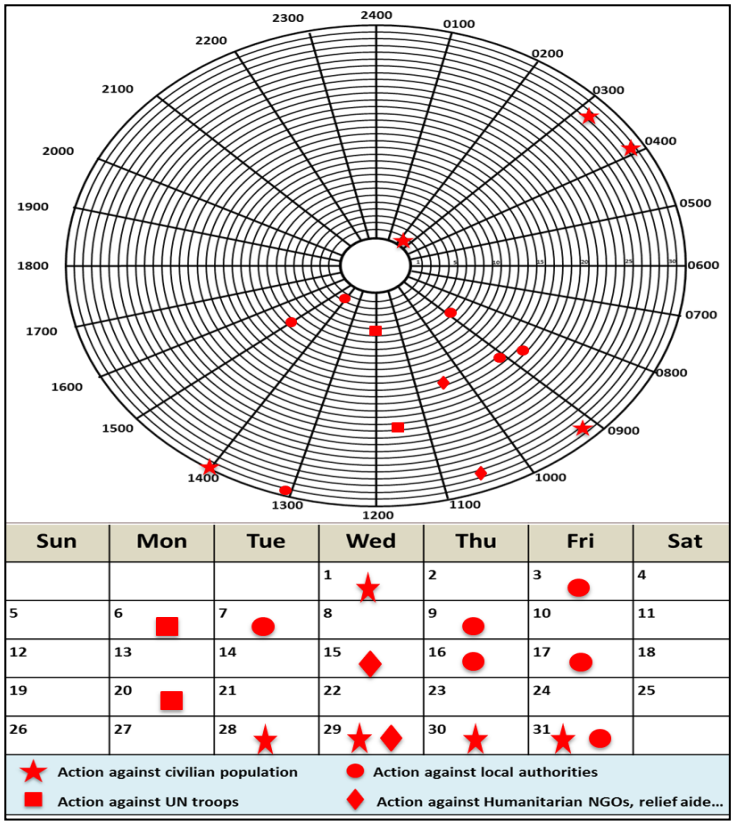


Figure 4: Pattern Analysis Example

Structured brainstorming sessions: Brainstorming is used to stimulate new thinking, and it can be applied whenever a project is started to help generate a range of hypotheses about a key PKI question. To be productive, brainstorming should be a very structured process, with a chair to direct proceedings. The process involves a divergent thinking phase to generate and collect new ideas and insights, followed by a convergent phase in which ideas are grouped and organized around key concepts. Ideally, a brainstorming session would have as many people with different backgrounds present as possible to have different opinions and – hopefully – new thoughts raised during the session.

- **Analysis of Competing Hypotheses (ACH):** This is the process where hypotheses, generated during the brainstorming session, are tested against available and relevant data. All credible hypotheses should be brought forward to the initial ACH, but those with the least evidence to support them should be excluded. This is necessary to leave the Analyst with

approximately four to five working hypotheses. These hypotheses can be represented by assigning a column to each along the X axis of a spreadsheet, with all available supporting evidence listed along the Y axis. If a piece of evidence supports a particular hypothesis, a 'C' can be used to denote that the information or PKI (summarized as 'Evidence') supports that hypothesis. Similarly, an 'I' can be used to denote 'Evidence' that is inconsistent with a particular hypothesis. Evidence that neither supports nor is inconsistent with a hypothesis is Non-Applicable or 'NA'. The hypothesis with the most marks for 'C' becomes the hypothesis that is most credible based on the current information available. It is important to note that ACH is useful for very important PKI questions, and the list of evidence can run to a significant count.

The ACH document is a living document, and as more information becomes available, the 'most credible' hypothesis may change. It is also important to note that working hypotheses can be used for the Force IAP. The analyst can use each working hypothesis to generate a set of I&W that can form additional RFIs. The analyst should ask 'what would I expect to see happening if this hypothesis is true?'.

Evidence	**Hypothesis 1**	**Hypothesis 2**	**Hypothesis 3**	**Hypothesis 4**
Item A	C	I	C	I
Source Report B	C	I	C	I
Report E	C	C	C	I
Assumption A	I	C	C	I
INTREP C	NA	I	I	I
Count	3 C	2 C	4 C	0 C

Table 4: Competing Hypothesis Example

In this example, on the basis of currently available information, Hypothesis 3 is the most credible, and Hypothesis 4 is the most inconsistent with available data. Normally, the first 3 hypotheses would be brought forward for further consideration. However, Hypothesis 4 should not be forgotten.

- **Indicators and Warnings.** An indicator is an observable behaviour or event that point towards an outcome/occurrence or, in this context, a hypothesis or possible explanation for the data the analyst is considering**.** Indicators are observable at all levels from the strategic to the tactical. Considered at the national strategic level, indicators could include a shift to a war-time economy, a change in use of national infrastructure or the co-option of strategic airlift capabilities. At the operational level, an indicator could include local population movements; the stockpiling of fuel or ammunition by a certain group; and the presence or absence of women and children (boys and girls)[12] and the elderly in a location such as a village or marketplace.

  Indicators are generated using the analyst's experience (what is known about a threat group's tactics, techniques and procedures (TTPs) and intentions, capabilities and activities), an unavoidable action that is linked to a particular event such as the test firing of weapons, or the movement of large numbers of vehicles from one location to another (crossing a river), or on the basis of what has happened in the past (trend analysis). As outlined in Chapter 2, gender-specific indicators can also give early warning of emerging tension, Gender-Based Violence and/or CRSV.

[12] For early warning indicators of the six grave violations against children, see DPO-DPPA Handbook for Child Protection Staff in UN Peace Operation, annex 9.

When an indicator is generated, it is only useful for early warning purposes if it is monitored. Therefore, it is good practice to include these indicators in the Force IAP, to link them to an NAI, and to task Acquisition assets to report on them. This will ensure that the PKO is not surprised, and that the MPKI can offer the commander early warning about a particular event (please see direction for an example of an indicator that is linked to an NAI). The MPKI can also monitor changes that may lead to one hypothesis becoming more credible than another.

- **AOE.** Other MPKI analytical tools are outlined subsequently and include, inter alia, physical, human, and information terrain analysis, and the effects of weather on this terrain. The process through which the MPKI Analyst assesses and records information under these headings, using the three-column format of factor, deduction, and task methodology, greatly enhances their understanding of the OE and is critical to supporting the commander's decision-making process. It is important that the MPKI cell visualizes all data on the OE on a series of map overlays. Once more, the visualization of this data will enable the MPKI cell to develop insight into how the environment will impact the UN PKO, and other relevant actors.
- **Conventional Approaches.** Conventional approaches to assessing a threat actor involve acquiring information on ORBAT, and on the disposition, composition, strength, doctrine, tactics, techniques and procedures, arms, logistics, training and combat effectiveness. This information is used to integrate the threat with the OE and is often visually represented on a threat Integration overlay. While this approach is still useful in some PKOs, MPKI cells should focus on System Integration techniques as outlined subsequently in this Chapter.
- **Actor Evaluation (AE).** Other techniques that will enhance understanding of the human terrain particularly of those actors that are likely to have a meaningful impact on the OE are outlined in Chapter 9, and include: Strengths, Weaknesses, Opportunities, and Threats Analysis; Centre of Gravity (COG) Analysis; Positions, Interests, and Needs Analysis; and Actor Evaluation (AE) tools, including threat profiling, and the construction of relational matrices. It is critically important that the MPKI cell examines and assesses all relevant actors in the OE, not just threat groups. This will greatly enhance understanding and will mean that the MPKI can continuously and meaningfully insert into the commander's decision-making process.

5.3.5 **Pitfalls in Peacekeeping-Intelligence Analysis.** The accuracy of a peacekeeping-intelligence product can be undermined by several pitfalls. Those worth mentioning are the following: basing an assessment on flawed or untested assumptions; failing to fuse information from all sources; basing an assessment on a single source; group think; failing to recognize analytical bias; failing to recognize source bias; becoming attached to one particular conclusion, and failing to consider new, contradictory information that could disprove it; and searching for perfection in terms of available data, leading to a slow, unwieldy analytical process. Bias is one of the most common analytical pitfalls and is outlined in greater detail in subsequent paragraphs.

- **Personal Bias.** Personal bias can involve racism, sexism or feelings of superiority, (or inferiority), relating to education, position, type of work, and so on. It may also include an Analyst's preference for a particular source, for example. All Analysts suffer, to a lesser or greater degree, from personal bias: it becomes a problem only if it goes unrecognized.
- **Institutional Bias.** Institutional bias generally relates to a corporate perception of an individual or group. Institutional bias can be difficult for an Analyst to overcome, it is difficult to counter with objective or constructive criticism and it can 'blinker' an Analyst in consideration of events. It also inhibits imaginative thought, an essential aspect of Analysis.
- **Cultural Bias.** Cultural bias will usually relate to those who regard their own culture as superior (or inferior) to another. It may also be concerned with a misunderstanding or lack of comprehension of why another culture conducts itself in the manner it does. As a result, Analysis in some fields can be hampered simply by a lack of relevant knowledge or experience. To overcome cultural bias, the Analyst should try to develop an understanding or empathy with the cultural group being assessed. This can be achieved by enhancing the

MPKI cell's understanding of the human terrain. Furthermore, the MPKI cell could also be more effective if it would include as many Analysts from different cultural backgrounds as possible.

5.3.6 **Tools to Avoid Pitfalls.** Many of the pitfalls outlined above can be addressed by the following:

- **Key assumption checks.** Here the Analyst or Analytical Section should list all their assumptions on a single document and discuss them to ascertain if they are credible. If any of the assumptions in a PKI product are not credible, the product must be revised to reflect this. It is also important to note that if an assumption changes over time, any PKI product based on that assumption must be changed to reflect this. It is also important to remember that any assumptions made in a PKI product must be made known to the recipient of that product; this should make it clear that the assessment is likely to change if the underlying assumptions do.
- **Team A versus Team B.** Almost any peacekeeping-intelligence assessment, or assumption can be challenged by pitting two teams of analysts or two analysts against each other. One team's job may be to argue against an analytical judgement and the second team's job will be to argue for it. This helps identify any issues with the PKI product.
- **Devil's Advocate.** This individual's role is to challenge assessments in a PKI product. Forcing an analyst to defend conclusions or assessments can reveal weaknesses in an analyst's logic.
- **Red and Green Teams.** This is where one team of Analysts (Red) acts and thinks like a threat actor and another team of Analysts (Green) could represent the civilian population (including vulnerable groups with need for special protection)[13], actively challenging your judgements. This can also identify flawed assumptions, and any evidence that the MPKI cell may have overlooked. It also gives a human dimension to the (threat) actor and can ensure that the MPKI must work against a 'thinking' entity that can alter its approach over time.
- Using analytical approaches such as the **ACH**, as earlier outlined.

5.4 Integration

Integration is the process of identifying a pattern by selecting and combining pieces of analysed information, preferably from different sources, to construct a PKI picture. Evaluated information becomes PKI only after it has been integrated/fused with other information available on the threat or the environment. During the integration/fusion process, basic PKI becomes central as it provides the requisite local context to facilitate the assessment of incoming information. Integration involves the combining of selected data to establish meaning. Essentially, the Analyst integrates incoming data to discern what is happening, why it is happening, and what is likely to happen next. It is important that the single-source views are fused effectively and with due weight being afforded appropriately. This is the task of fusion management.

5.5 Interpretation

Information which has been collated, evaluated, analysed and integrated, must finally be interpreted in order to complete the process of conversion into PKI. It involves the following:

- **Sense-making**, which consists of giving a clear meaning to a piece of information in a manner that makes it more concrete and customizes the various aspects of the threat from actors against the UN, civilian population or others.
- **Visualization,** which allows the Analyst to represent the opposing force and determine the repercussions of such new information on what is already known.

[13] Green Team recommendation is based on the "do not harm" principle, as defined in the PoC Policy (para. 32):

- **Extrapolation.** Extreme attention is needed to draw from the slightest indices of change in the threat actor's behaviour/posture, the criteria allowing the confirmation or information of the hypotheses put forward.

Interpretation is the placing of the results of the Analysis and Integration into the context of a prediction. Information has been received, it has been converted into military PKI; now what is the significance of that PKI to the commander, their IRs, their plans and mission? In particular, how can it help to predict what is going to happen? The MPKI cell must remember that a good MPKI product must not simply tell the commander what is happening, but why it is happening, and what is likely to happen next, where it is likely to happen, and how it is likely to manifest.

The key word in Interpretation is 'likely'. This is an expression of probability, and it is vital that such language is used in a consistent manner in all products that go to decision-makers. This concept is explored further in subsequent paragraphs.

5.6 Communicating Uncertainty

Analysts should keep in mind that logical, reasoned analytical conclusions are not necessarily facts. When presenting conclusions, PKI personnel should state the degree of confidence they have in their conclusions and any significant issues with the analysis. This confidence level is based normally on the capability of the Acquisition asset, evaluative criteria, the confidence in the acquired data, and expertise and experience of the Analyst. The accurate communication of uncertainty is one of the most important elements of good PKI assessment. When considering a course of action, commanders must set its likely benefits against its likely costs: if they do not have a clear idea of the probability of various outcomes, the wrong decision might be made.

When expressing probability and uncertainty, MPKI analysts should consider the two key challenges linked with this exercise:

5.6.1 **Misinterpretation.** Due to different experiences and backgrounds, interpretation of the word "probable" may vary from 25% to 90% per different understandings of the likelihood of an event to occur. This wide interpretation exposes readers of PKI assessments to serious risks of misunderstanding.

5.6.2 **Misrepresentation.** In the absence of a common definition, readers of PKI assessments may go on to re-draft or re-represent the assessment (for example, to summarise it for senior echelons or indeed the public) and thereby lose or misrepresent the sense of the original assessment. In response to such challenges, the MPKI analyst uses the 'Uncertainty Yardstick' expressing probability and uncertainty.

Qualitative Statement	Associated Probability Range
Remote or highly unlikely	Less than 10%
Improbable or Unlikely	15 -20%
Possible or Realistic Possibility	25·50%
Probable or Likely	55-70%
Highly Probable or Highly Likely	75-85%
Almost Certain	More than 90%

Table 5: The Uncertainty Yardstick

5.6.3 It is also important that the client of the PKI product is made aware of the following:

- **Assumptions.** Any assumptions must be made clear at the outset of any written PKI product or PKI brief. The recipient must be made aware that the assessment is likely to change if these assumptions prove false.
- **Source Credibility and Reliability.** It is very important that a recipient is aware of the credibility of the data comprising the PKI product. An assessment based on C to E grade

sources or C4-E4 grade information will be weaker than one based on A to B grade sources and A1-B1 information. Again, this must be made clear to the recipient. Indeed, if there is a piece of information that is critical to the PKI assessment, or is of diagnostic value, the recipient should always be made aware of the source's credibility and reliability. For example, 'Source reports (B3) indicate that threat group A intends to prevent UN convoys reaching Town B'.

5.7 End State

At the end of the analytical process, there should be a predictive PKI assessment relating to one of the commander's PIRs. This assessment should have an associated qualifying statement that highlights the assessed probability that the assessed event will happen. If asked, the MPKI staff should be able to tell the commander what original information and analysis the assessment was made from, what credibility and reliability ratings were given to the original material, and the analytical techniques that were used to reach the assessment. Again, each Analytical product must be auditable and preferably replicable, it must be as much as possible free from bias, and any assumptions therein must be challenged.

ANALYSIS OF THE OPERATING ENVIRONMENT

5.8 Providing Understanding

The AOE is the primary method used to develop the understanding of the OE. It is used to support the UN Mission Decision-Making Process (see Chapter 7). The AOE is a comprehensive approach, placing the human factor at its centre, and analysing how they interact with their environment. Critically, it provides an assessment on how these factors influence the protection of UN personnel and civilians.

The AOE facilitates the UN's requirement to understand and engage with the different population groups, some of which will belong to different ethnic, tribal or religious groups and, as such, may have different attitudes to or perceptions of the UN. All this is conducted to better handle today's complex, more dangerous and high-tempo conflicts, and facilitate a more in-depth understanding of the OE that will enhance Force Protection and mission planning. It is important to note the AOE is a continuous process and MPKI staff are to be mindful that the PKI 'eye' should never 'blink' or avert its focus from the OE.

5.9 Defining the Operating Environment

The OE is the geographical area (including the physical elements, the information environment and actors) that has been given to a commander in order for them to conduct a given mission within the context of a UN mandate. MPKI staff are to identify and understand what they are responsible for and what aspects of the OE they need to focus on. This will be directed to them upon the definition of the APIR and APII.

- **APIR**. This is the area given to a Commander for which they have the responsibility for the production and provision of peacekeeping-intelligence/understanding.
- **APII**. This is an area beyond the control of a Commander, and is outside of their APIR, but one that has relevance to the conduct of the Commander's mission and therefore must be considered and evaluated.

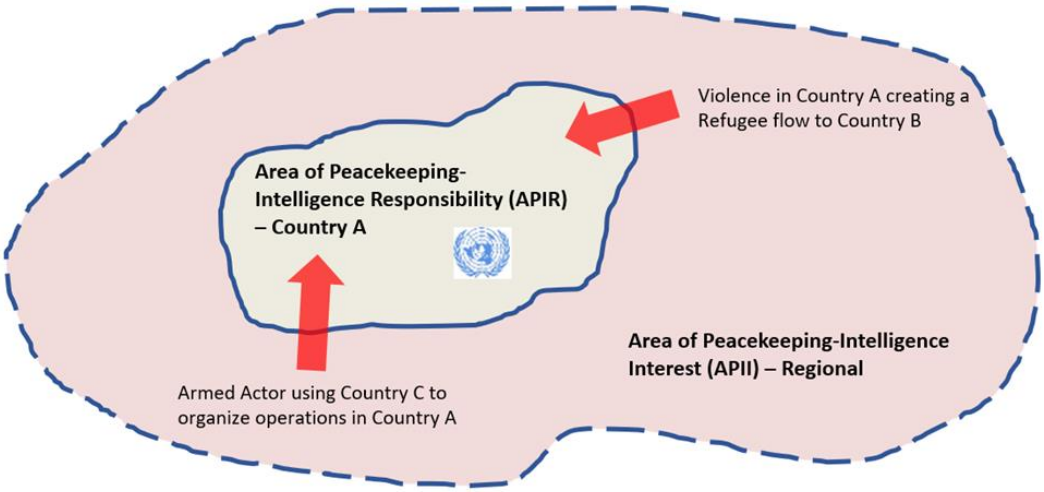


Figure 5. Visualization of the APIR and APII

5.10 AOE – The Three Phases

Conduct of AOE. The following paragraphs will outline how to conduct the AOE, highlighting the required minimum outputs, often referred to as the 'golden products' (due to their importance in support of PKI understanding and informing decision-makers).

5.10.1 **Phase 1 - Operating Environment Evaluation (OEE).** This phase involves three separate but inter-linked steps. These steps are:

- Phase 1a: Analysis of the Physical Terrain (PT).
- Phase 1b: Analysis of the Human Terrain (HT).
- Phase 1c: Analysis of the Information Terrain (IT).

These steps focus on the defined APIR and wider APIIs – MPKI staff will conduct separate mission-specific AOEs at each level (Sector, Battalion and Company) or whenever a mandated task is given.

5.10.2 **Phase 2 – Actor Evaluation (AE).** Key actors are identified in Phase 1. AE is a detailed analysis of these actors, both men and women. This involves understanding the actors' intent, their capabilities, strengths and weaknesses, and what critical factors they require to conduct their activities.

5.10.3 **Phase 3 – Situation Integration/Actor Integrated Scenario Generation.** Once MPKI staff have developed a detailed understanding of both the OE (Phase 1) and the actors within it (Phase 2), they can make an informed, predictive assessment of how the actors will likely affect the Commander's mission/force elements as well as other actors within the OE (such as other tribal groups or population factions). Based on this Situation Integration/Actor Integrated Scenario Generation, a Commander can plan their missions and tasks, with a greater ability to understand the effect of their actions.

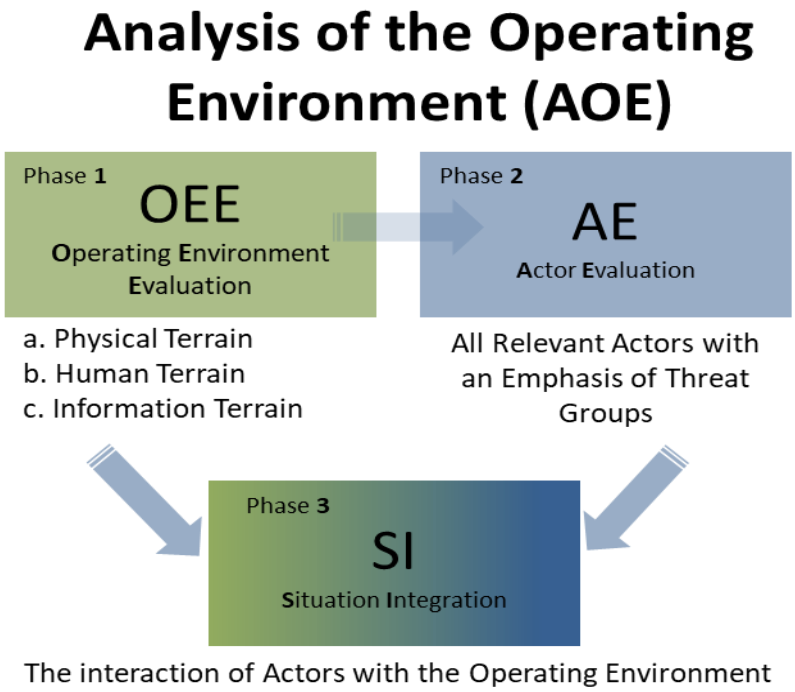


Figure 6: The 3 Phases of AOE

5.11 Phase 1a: Analysis of the Physical Terrain

5.11.1 **Mapping.** Accurate and up-to-date mapping is an essential requirement for physical terrain analysis. There will be certain circumstances where this is not immediately available and MPKI staff, in conjunction with the other staff branches (such as GEO and Ops), are to ensure that accurate mapping of the operating area is sourced. Maps should be at a scale of 1:50,000 or 1:100,000 when assessing the whole operating area but can be as small as an aerial photograph of a compound when conducting AOE for a bespoke/tailored operation.

5.11.2 **Overlays.** MPKI staff should never draw directly onto maps. Instead, separate overlays using a thin, clear sheet of plastic should be employed. Overlays are to be restricted to a specific or related theme to reduce clutter and confusion. Overlays assist in briefing and further analysis and thus require constant updating as the situation evolves. To that end, overlays must be labelled with the following information:

- DTG of when the overlay was applied / last updated.
- Title of what the overlay is depicting.
- A legend with an explanation of the symbols, number and/or colours used on the overlay.
- North pointer in order for the overlay to be correctly orientated on the map.
- The map edition and series in order for it to be overlaid on to the correct mapping.
- At least two northing and easting cross markings – this is to ensure that the overlay is placed on the map in the correct place.

5.11.3 **Methods for Terrain Analysis (TA).** It is to be noted that Terrain Analysis is not solely a PKI staff responsibility. Engineering staff are also well-placed to assist in analysing the terrain, e.g., the assessment of weather effects on terrain, likely routes, and critical infrastructure. It is therefore imperative to make a concerted agreement of who is doing what and at what time the preparations by the different branches should be finalised. The best method of TA is based on reconnaissance of the ground, supplemented by further analysis by the Headquarters staff. MPKI staff can use a number of headings in order to focus their attention to certain elements of the ground, which must be looked at from both UN Forces' and (threat) actors' viewpoints. As a minimum, MPKI staff should

look to provide a detailed analysis of the factors described in subsequent paragraphs, and create the necessary overlays:

- **Routes.** All routes throughout the OE, including roads, tracks and likely transit routes used by UN forces and other actors, are to be identified. This is based on capabilities such as vehicle type (i.e., movement on foot will be graded differently than movement using tracked vehicles). This overlay is known as the Mobility Corridor Overlay:

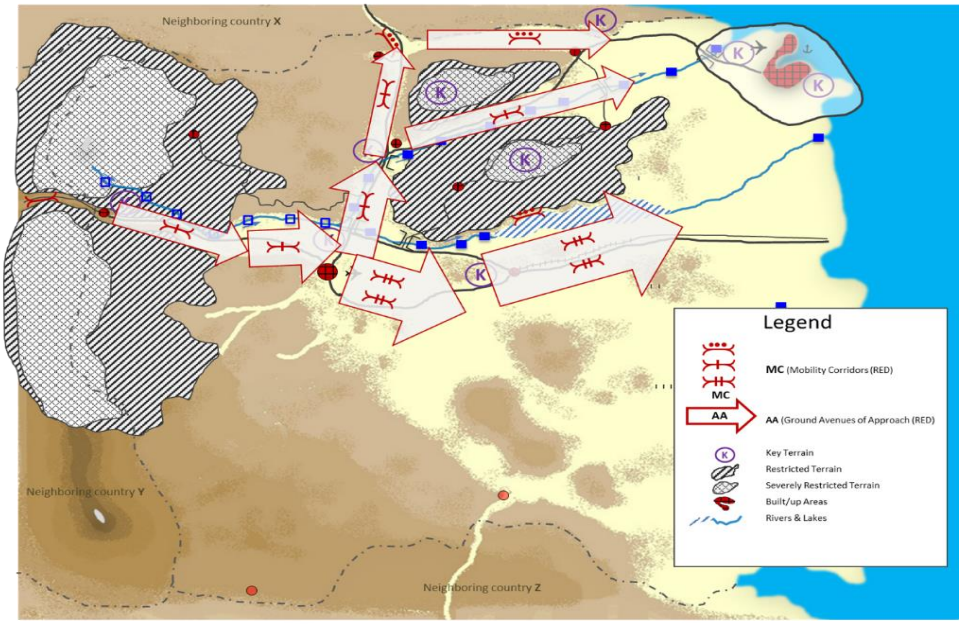


Figure 7: Mobility Corridor Overlay – Conventional

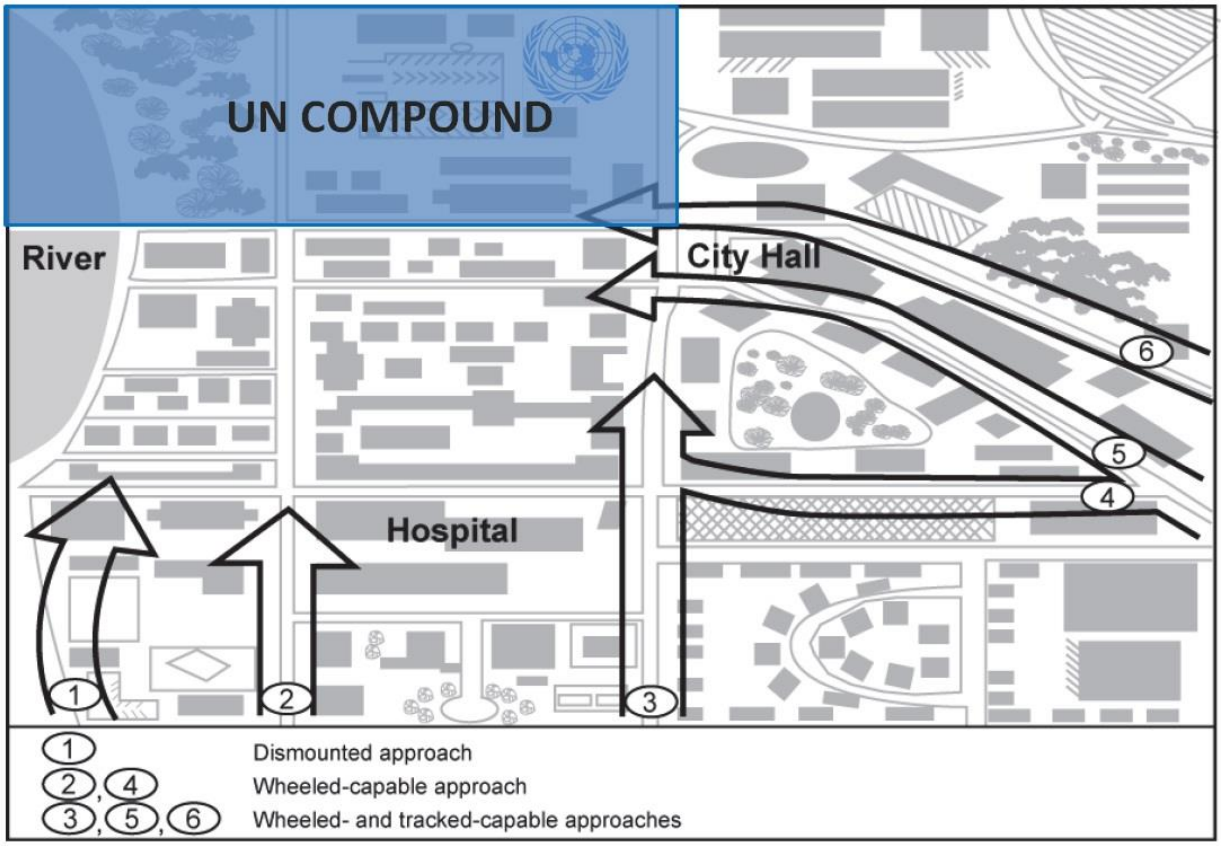


Figure 8: Mobility Corridor Overlay – Urban Terrain

- **Obstacles.** An obstacle is any natural or artificial obstruction designed or employed to disrupt, fix, turn, or block the movement of an (opposing) group. Some examples of obstacles to ground mobility are buildings, mountains, steep slopes, dense forests, rivers, lakes, and built-up areas. When analysing routes and obstacles together, the terrain can be assessed as:
  - **Unrestricted:** Terrain over which movements of UN forces or actor groups (like opposing armed groups or refugees) is not affected by the ground, vegetation, natural and artificial obstacles.
  - **Restricted:** Terrain over which movements of UN Forces or actor groups is only possible at reduced speed, is canalized, or will be possible only with the assistance of additional non-organic assets like improvised bridges, e.g., steep ground, swamps/riverbeds etc.
  - **Severely Restricted:** Terrain over which movements of UN Forces or actor groups being assessed as impractical e.g., rivers that cannot be crossed/forded, known minefields.
- **Areas of Cover.** This overlay identifies areas where UN Forces and (threat) actors can use the ground to remain concealed or ensure protection from observation. This is particularly useful when identifying likely approach routes, observation posts/reconnaissance positions, or likely firing positions.
- **Infrastructure.** It is necessary to identify and understand the important infrastructure within the OE. Consideration is to be given to:
  - Sanitation (including sewerage).
  - Water supply (including water purification or desalinization plants).
  - Power supply.
  - Places of religious importance.
  - Places of academic study.
  - Refugee camps or key NGO facilitation areas.
  - Health and medical facilities.
  - Security infrastructure (prisons).
- **Key Terrain (KT)** is any locality, or area, which gives an advantage to either UN-opposing or UN forces. In natural terrain dominated by restrictive terrain features, high ground can be KT because it dominates an area with good observation and fields of fire. In an open or arid environment, a re-entrant/draw or wadi can be KT because it offers good cover and concealment. In urban environments, infrastructure (such as bridges, medical facilities, choke points, intersections, industrial complexes) can be considered KT.
- **Vital Ground (VG).** This is ground that is of such importance that it must be kept/controlled for mission success.
- **Weather/Seasonal Overlay.** Dependent on the time of year (wet/dry season), weather/seasonal conditions will impact routes, river courses, areas of cover (such as vegetation growth) and will require the re-assessment of all those headings stated above. Separate overlays should be produced to take into account these seasonal changes, and should be stored in order to provide a record of known seasonal conditions e.g., flooding, rises in river levels, loss/growth of vegetation etc.

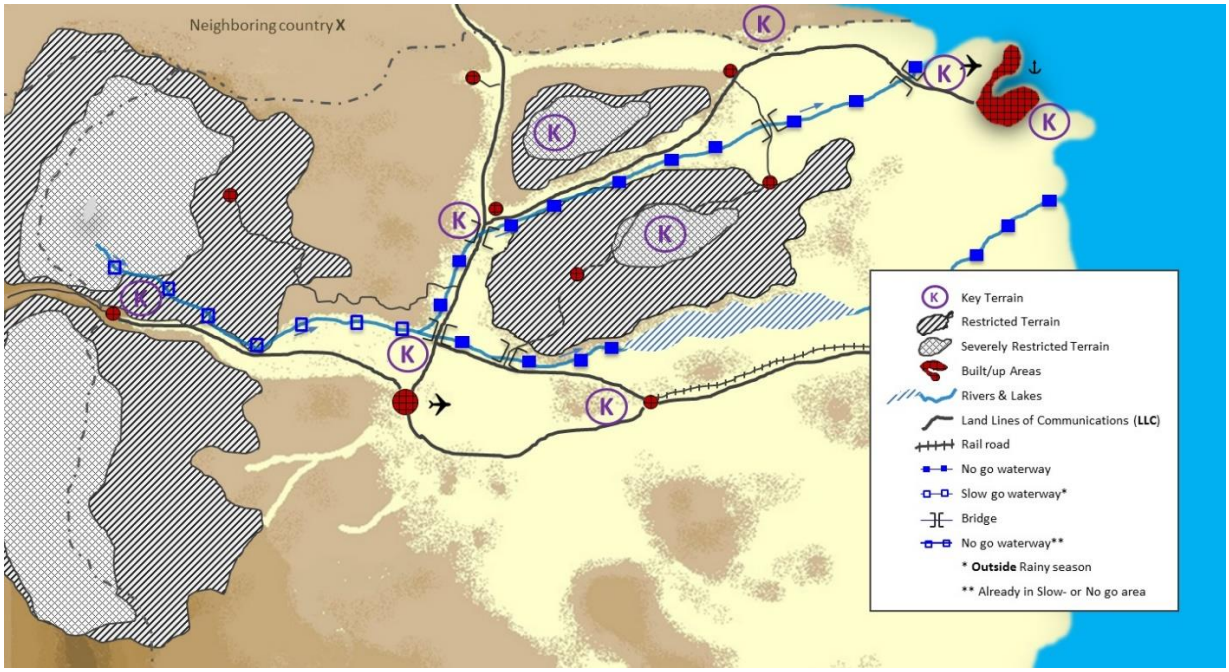


Figure 9: Example Terrain Overlay

Date:	Sat **17** Aug 2019	Sun **18** Aug 2019	Mon **19** Aug 2019	Tue **20** Aug 2019	Wed **21** Aug 2019
Weather type					
Max Temp °C / °F	**44**°C / **111**°F	**40**°C / **104**°F	**36**°C / **97**°F	**31**°C / **88**°F	**32**°C / **90**°F
Min Temp °C / °F	**27**°C / **81**°F	**24**°C / **75**°F	**20**°C / **68**°F	**17**°C / **63**°F	**17**°C / **63**°F
Clouds	Clear	Scattered	Overcast	Overcast - Rain	Overcast - Rain
Precipitation	0 – 15 mm	0 – 15 mm	0 – 15 mm	225 – 290 mm	250 – 300 mm
Humidity	25 %	25 %	60 %	75 %	75 %
Wind direction	**SW**	**SW**	**SE**	**E**	**E**
Sunrise and **set**	06.07 / 18.58 hour LT	06.08 / 18.59 hour LT	06.09 / 19.00 hour LT	06.10 / 19.01 hour LT	06.11 / 19.02 hour LT
Moonrise and **set**	20.26 / 07.47 hour LT	21.04 / 08.33 hour LT	21.37 / 09.19 hour LT	22.17 / 10.04 hour LT	22.57 / 10.51 hour LT
Illumination % night	Illumination 88.5 %	Illumination 81.6 %	Illumination 73.4 %	Illumination 64.1 %	Illumination 53.9 %

Weather effects matrix

Date:	Sat **17** Aug 2019	Sun **18** Aug 2019	Mon **19** Aug 2019	Tue **20** Aug 2019	Wed **21** Aug 2019
UN Personnel	Heat illness			Heavy rain	Heavy Rain
UN Material	Temperature			Heavy rain	Heavy Rain
Rotary wing & MV	Temperature			Visibility	Visibility
Fixed wing - transport				Visibility and wind	Visibility
UAV				Visibility & wind	Visibility & rain
Movements (roads)				Flooding Risk	Flooding Risk
Movements (off-road)					Condition & Flooding
Communications	Distance Reduction			Distance Reduction	Distance Reduction
Specific effects on UN Operating Environment	DPRE /Water Shortage	NSTR	NSTR	IDPs / Flooding	IDPs / Flooding risk
Legend:	NSTR	Favorable	Marginal	Unfavorable	

Figure 10: Example Weather Analysis

5.12 Phase 1b: Analysis of the Human Terrain

Actors cannot be separated from the physical environment, and it is vitally important to understand the population amongst which UN forces will be operating. This includes incorporating a gender perspective in planning to provide a more holistic and informed interpretation of the OE. This will assist commanders and staff in building local knowledge on men, women, boys, and girls to avoid gaps in information, making wrong assumptions and assist in putting the right resources towards the mission. Inclusive analysis provides a more comprehensive understanding of the threat environment, as well as the unique protection requirements of all members of the local population. Data required includes, but is not limited to:

- Specific population groups (ethnic, tribal, belief systems and religious lines), habitat, along with their size, their attitude toward the UN, their links with other groups, and their key leaders.
- Armed groups and military organizations, locations, along with their capability, structure, and intent, their attitude to the UN, their links with other groups, and their key leaders.
- Intent is important to analyse and is needed later to go towards Phase 2 (AE) of the AOE. For example, an armed group can be compliant or non-compliant towards the UN resolution that legitimized the UN mission in the OE. This is important for the actor and threat evaluation later in the AOE process.
- Terrorist groups, habitat, influencing areas, intent, their links with other groups, and their key leaders.
- Host State Security Forces and institutions.
- Organized crime groups; working areas, objectives, their links with other groups, and their key leaders.
- Other relevant actors such as NGOs.
- Refugees and (internally) displaced persons.
- Political organizations and key leaders.
- Economic structures, practices and key figures.
- Social structures, organizations and key leaders.

5.12.1 **Human Terrain Analysis.** This is the process of developing understanding through the analysis of human actors and factors. This process can be time-consuming and laborious; therefore, it is advised that MPKI concentrate their activity in the use of the following five Human Terrain Analysis Tools and their associated outputs/products. A gender perspective should be included in all analysis. Performing a Gender Analysis, the specific instructions for which are included later in this chapter, will provide the data that can be mainstreamed through the other Human Terrain Analysis tools:

- ASCOPE – PMESII matrix.
- Human Terrain Mapping.
- Link Analysis.
- Gender Analysis.
- Items on High Importance List.

5.12.2 An **ASCOPE – PMESII matrix** is a useful guide to the kinds of actors and factors that should be included in the analysis of the human terrain. The intersections will support MPKI staff in filling in the deductions and can highlight weaknesses and/or strengths. Another important output of the use of these tools is that they stimulate direction through identifying pertinent peacekeeping-intelligence gaps and associated IRs and feed the PKI Dialogue between MPKI staff and the Commander. An example Matrix is at Annex A to this Chapter.

5.12.3 **Human Terrain Mapping (HTM).** HTM is a means of portraying key actors within the OE and assists with common understanding. In order to understand the actors' demographics, it is important that they are related to the ground using overlays. The list is not exhaustive, but MPKI staff should produce overlays illustrating the following:

- Tribal group laydown, including locations of key leaders.
- Ethnicity laydown.
- Religious beliefs laydown, including locations of religious sites and key leaders.
- Political affiliation, including locations of known polling sites (if applicable) and key leaders.
- Population densities (where known, in order to identify where most of the population lives).
  - Involves: Areas of social depravation (divide between low and high income).
  - Age and gender distribution of areas.
- Gender-specific information such as power relations and access to resources, including health, education, and employment.
- IDPs and Refugee Camp locations.
- Civilians' vulnerabilities information, including location and status of critical civilian infrastructures, services, installations, resources, as well as the civilians' access to food, water, shelter, education, work etc.
- Host State (military and police) and threat actor force laydowns.

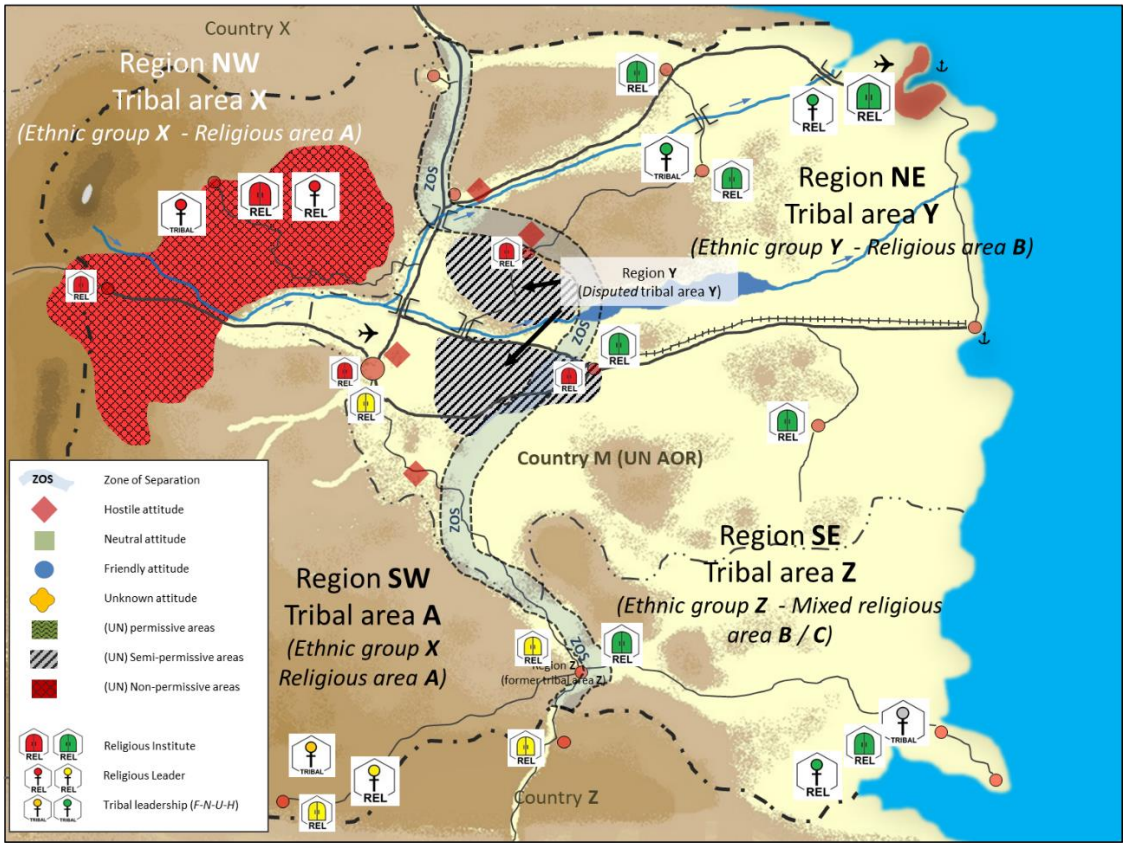


Figure 11: Human Terrain Analysis – Tribal and Religious Overlay

5.12.4 **Link Analysis.** This provides an understanding of how the various actors are linked to each other and describes the nature of the linkages between them. In understanding how the linkages occur and how they are facilitated, it provides MPKI staff the opportunity to analyse them and provide the Commander with options on how to affect them.

5.12.5 **Conducting Link Analysis.** In order to conduct link analysis, the following steps are to be conducted:

- Collate all the pertinent information related to the actor/group.
- Identify all the factors of interest (e.g., individuals, places, objects, events, beliefs and timings etc).
- Identify the associations between these factors. The product will be easier to construct if you group all relevant factors together.
- Assess the nature of the interactions and relationships between the factors e.g., confirmed associations, assumed associations, owned/controlled by the actor, assumed to be owned/controlled by the actor.
- Construct a relational database (**see below at Figure 12**). This will offer a visual depiction of all known relationships before you insert them into the link diagram. It is important to note that nodes are represented with circles, known connections with an unbroken line, suspected connections with a broken line, and organizations by using a rectangle (**see Fig 12**). These are the basic symbols, but this can be further broken down depending on the information that is available to you (see Fig 14 below).

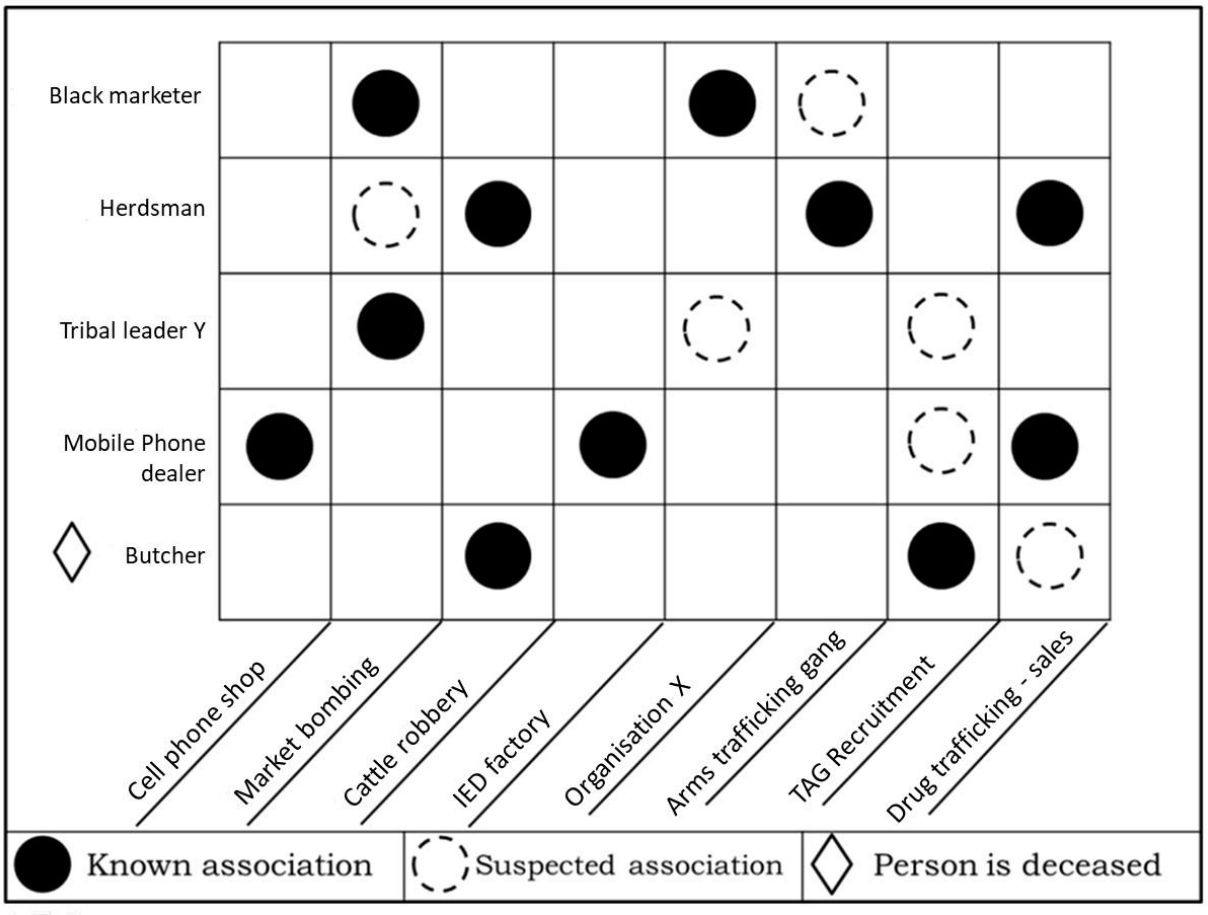


Figure 12: Relational Matrix

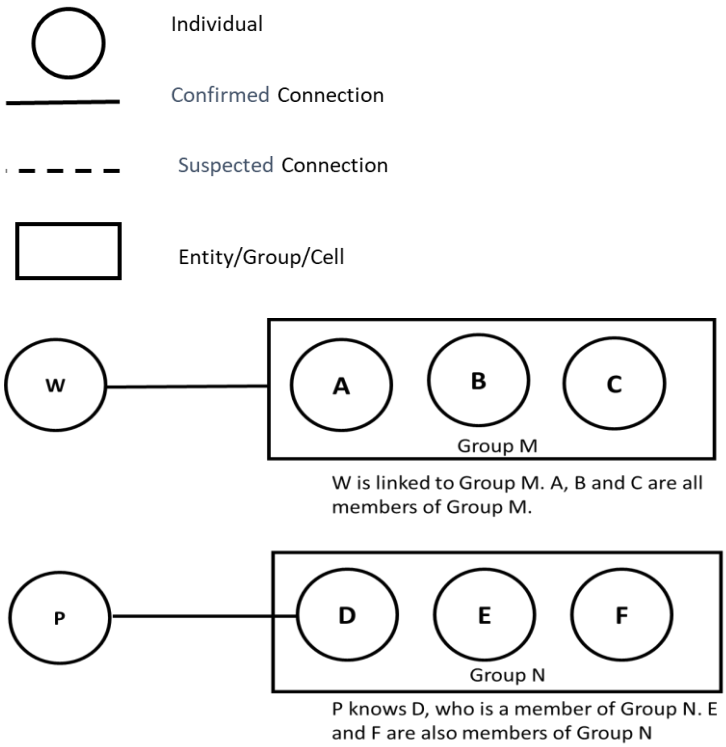
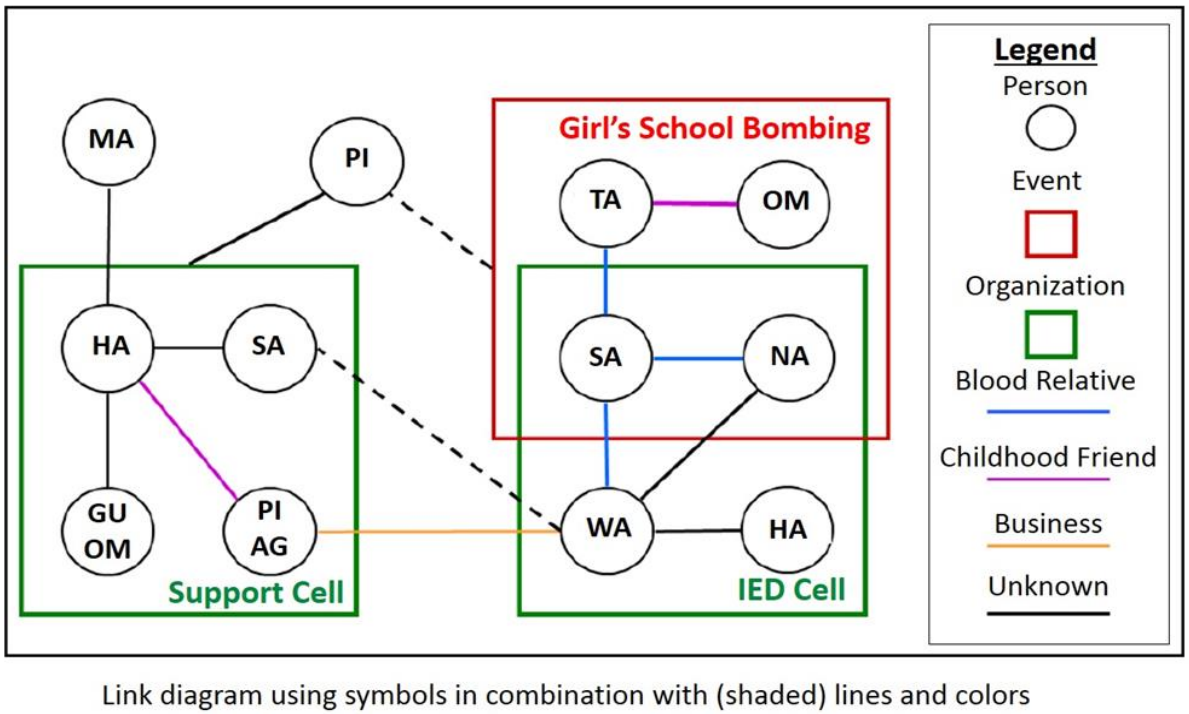


Figure 13: Link Symbols



Link diagram using symbols in combination with (shaded) lines and colors

Figure 14: Link Chart

5.12.6 **Gender Analysis (GA).** GA is a critical examination of how differences in gender roles, activities, needs, opportunities and rights/entitlements affect men, women, girls and boys in certain situation or contexts. GA examines the relationships between women and men and their access to and control of resources and the constraints they face relative to each other. A GA should be integrated into the AOE to ensure that gender-based injustices and inequalities are not exacerbated by interventions, and that where possible, greater equality and justice in gender relations are promoted.

5.12.7 GA can be applied externally to an operational environment as well as internally into the military organization. For example, military operations planning activities should consider the different security concerns of men, women, boys and girls and how they are differently affected by operations and missions, but also how gender roles can affect operations and missions. Furthermore, they should take into account power relations in the community to ensure people have equal access to assistance where the military is engaged in supporting humanitarian assistance. Other examples would include understanding of how customary conflict-resolution mechanisms affect people differently, and how their social status may change as a result of war.

5.12.8 GA should be approached using the following steps as a guide:

- Gain initial situational awareness on gender dimensions in an area of interest.
- Conduct an initial analysis regarding early warnings, conflicts and risks and threat interests.
- Review and update any existing contexts/situational analysis.
- Identify and examine gender-related early warning mechanisms that relate to conflict.
- Examine the conflict analyses with a gender perspective.
- Integrate the initial GA in planning, referring to context/situational awareness.
- Identify long-term requirements and initial assessments regarding gender perspectives internally and externally.
- Examine and advise on IRs to support further planning.

5.12.9 Once information is gathered on gender-specific early warning indicators, the next step is to monitor for trends over time from the baseline. Next, based on the trends, one can deduct what this can mean for men, women, boys and girls in the OE.

5.12.10 **Items of High Importance List (IHI List).** This is a compiled list of identified items (including individuals, equipment and infrastructure) assessed as being significant to both (threat) actors and UN Forces, which are required for the completion of their respective mission(s). It is also a method of identifying which of these items critically contribute to the likelihood of (threat) actor or UN forces' success, and which should be denied/protected, e.g., water supplies to an IDP camp.

(Threat) Actor	- Key weapon system - Key communication node, e.g., state media, cell phone tower
UN / Own Mission	- IDP camp water supply (protection of civilians)

Table 6: Example of IHI List

5.13 Phase 1c: Analysis of the Information Terrain (IT)

The Information Terrain comprises all factors that govern how the actors communicate with each other including how they share information and how their attitudes and perspectives are influenced. It is important to outline all Information Terrain factors affecting the specific OE. The inventory, evaluation and analyses of the IT is dependent on the outputs of Phases 1a and 1b. These factors can be subdivided to **Individual-to-Individual Communications**, and **Communication Methods to Groups**. These communications could be either direct or indirect:

- **Individual-to-Individual Communication:** Voice (phone – landline or mobile networks, public address systems, meetings). Social media (Facebook, Twitter etc) and internet network coverage/WiFi availability.
- **Communication Methods to Groups:** Radio and the extent of coverage/who has radios; television and network coverage; print media and availability/literacy of the local population; internet network/coverage/WiFi access availability; meetings and forums.

MPKI staff should consider producing the following overlays:

- Telecommunications infrastructure (mobile network, television and radio masts).

- Cell phone blackspots; internet blackspots.
- Locations of group meeting areas.
- Pro-UN media and extent of coverage.
- Anti-UN media and extent of coverage.
- Electromagnetic Spectrum usage and overview.

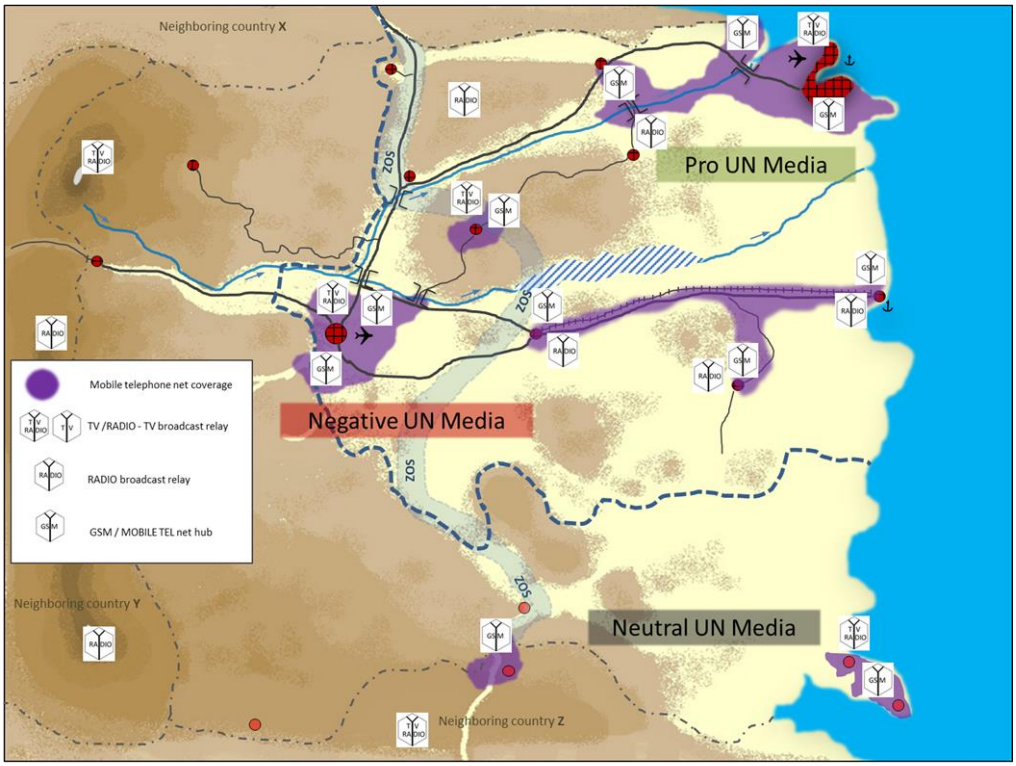


Figure 15: Example Information Terrain Overlay

5.14 Phase 2 – Actor Evaluation (AE)

The Actor Evaluation (AE) has a dual purpose. First, it elaborates on those actors/groups that are likely to have a (significant) impact on UN operations and the OE itself. Secondly, it enables a threat analysis that is critical to Phase 3: Situation Integration (SI).

5.14.1 **The flow from Phase 1.** During Phase 2 of the AOE process, MPKI conducts further analyses on those actors that are identified during the Human Terrain (HT) Analysis. AE will identify how they would conduct activities to achieve their assessed aims/desired end state. In the conduct of AE, MPKI are to produce the following:

- Known actor/group hierarchy charts, including known numbers, leadership and group structure, including gender and age.
- Known (threat) actor equipment capabilities, including vehicles, communications, weapons, links to or influence over state or non-state actors, information activity, logistics and funding/finance.
- Known (threat) actor techniques, tactics. This will likely be based on recent and historical activity.
- Known (threat) actor strengths and weakness (SWOT) analysis and Centre of Gravity (COG) analysis.
- Known (threat) actor attitude to the UN. The MPKI cell should ask whether the perception of this actor could help, harm, or hinder the UN.

- Known (threat) actor ideology. This will help the MPKI cell to evaluate intent.

5.14.2 The PKI cell/analyst records the processed information for each actor/group separately and collated under a file name of the relevant actor/group.

Non-compliant Armed Groups

Group	Category	Ethnicity	AOR	Ideology	Objective	End State	COG	Critical Requirements (CR)	Critical Capabilities (CC) and Vulnerabilities (CV)
Group 1	Terrorist Armed Group (TAG)	X	Sector WEST and NORTH and SOUTHERN regions of country X	Conservative Religion X	Imposition of Theocracy gradually	Religion based X state and law in WESTERN part of the continent	Popular Support and Religious legitimacy	Maintenance of good relations with local leaders and community	CC. Freedom of Movement, Funding, Recruits, Morale support. CV. Requirement to engage in mass casualty attacks. Terrorist approach.
Group 2	TAG	Y	NORTHERN regions of APIR	Nationalistic	Self-rule and/or autonomy	Self-Rule for the Y people	Popular Support	Maintenance of good relations with local leaders and community	CC. Freedom of Movement, Funding, Recruits, Morale support. CV. Requirement to engage in mass casualty attacks. Terrorist approach.
Group 3	TAG	Mix of A and B	SOUTHERN regions	Radical Religion X	Imposition of Theocracy	An independent OE under religious X Law	Popular Support and Religious Legitimacy	Maintenance of good relations with local leaders and community	CC. Freedom of Movement, Funding, Recruits, Morale support. CV. Requirement to engage in mass casualty attacks. Terrorist approach.

Table 7: Example of AE Chart

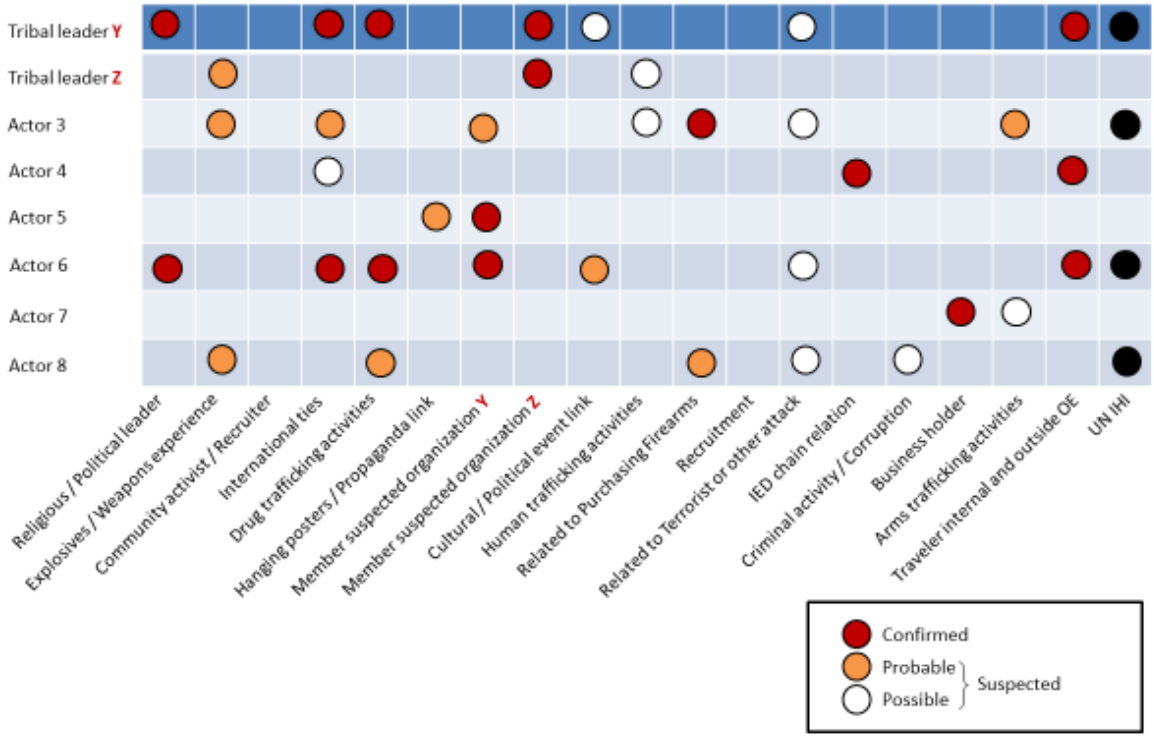


Figure 16: Actor Activity Relation Table

5.14.3 **SWOT Analysis.** Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis is a method of identifying a group's strengths and weaknesses, and the opportunities and threats which arise as a result. As with COG analysis, it is a useful way of breaking down an organization's characteristics so that the PKO can exploit its weaknesses or threats in the case of a threat actor or can support strengths and opportunities in the case of a friendly or neutral actor; all this must be done in line with the mission's mandate, and basic peacekeeping principles.

Strengths (Internal)	**Weaknesses (Internal)**
• Identify the capabilities which give an advantage • Identify the characteristics which give an advantage • Identify how the object might use those capabilities / advantages	• Identify the capabilities which give a disadvantage • Identify the characteristics which give a disadvantage • Identify how they might be exploited
Opportunities (External)	**Threats (External)**
• Identify the external conditions available and helpful to the object • Identify how the opportunities might be enhanced / denied	• Identify the external conditions which could damage the object • Identify how those threats may be enhanced / reduced

Figure 17: SWOT analysis model for Actor Analysis

5.14.4 **COG Analysis.** This method can have applicability wherever a COG can be identified. The key output of COG Analysis is the identification of vulnerabilities, which may then be exploited (adversary) or protected (friendly) or both (civilian). Consider effects, risks, and opportunities for men, women, girls, and boys in relation to each COG:

- Identify CC.
- Identify CR.

- Identify CV.

Centre of Gravity	Critical Capabilities (CC)
Capabilities etc. from which an actor gets its freedoms and ability to operate	What does the COG allow the actor to do?
Critical Vulnerabilities (CV)	**Critical Requirements (CR)**
What are the actor's key weaknesses through which the COG can be critically affected?	What are the essential conditions, resources or freedoms to make it effective as a COG?

Table 8: COG analysis model for Actor Analysis

5.15 Phase 3 – Situation Integration/Actor-Integrated Scenario Generation

Phase 3 of the AOE fuses the results of the OEE and AE from Phases 1 and 2, respectively. It aims to identify how the OE will shape (threat) actor/group capabilities and Tactics, Techniques and Procedures (TTPs), and effectively turn it into practice, identifying potential integrated scenarios and Actor Courses of Action (ACOAs), including Most Likely (ML) and Most Dangerous (MD). These have a predictive purpose to support the planning of missions and operations, and function as Indicator & Warning templates during the execution of the mission and/or operation. The key outputs of the Situation Integration (SI)/Actor-Integrated Scenario Generation are:

- Situation Overlay.
- Event Overlay.
- Actor Course of Action (ACOA) Scenarios (ML and MD) for all pertinent actors within the OE.
- Consolidated ACOA.
- ACOA Statement.

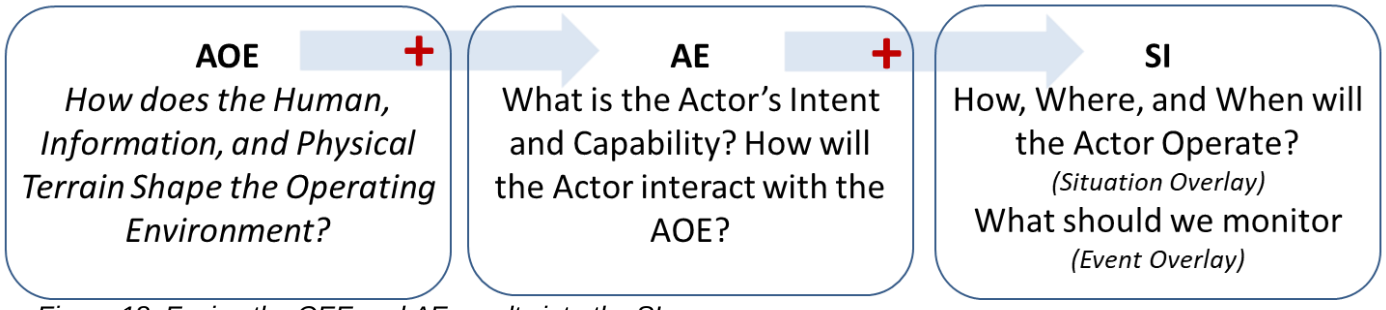


Figure 18: Fusing the OEE and AE results into the SI

The purpose of an integrated scenario as output of the SI is to 'catch' all the actors and factors in the OE in an explaining and predictive 'story'. In a complex UN mission environment, it is not enough to manage individual ACOAs without showing the correlation and mutual effects during a UN operation or in a period (depicted by the Situation Overlay) in the OE.

5.15.1 **The Situation Overlay (SO).** A SO is a sketch of the ACOA that visualizes the narrative of how the actor is going to conduct their course of action. The production of a situation overlay (SO) visualizes the Most Likely (ML)/ Most Dangerous (MD) ACOA using the layers from the PT and conclusions of the AE/Threat Evaluation (TE).

- TTP overlay over the Operating Area.
- SO produced for every adversary.
- Showing the Mobility Corridors of the actor/groups in the terrain.
- Showing the actor's objectives, boundaries and time-phased lines of critical time and space.

At a minimum, each ACOA sketch will include the relevant actor/threat groups:

- Name.
- Avenues of Approach or Mobility Corridors.
- Objectives.
- Boundaries (the actors Operating Area).
- Key and Decisive Terrain.
- Likely location of military capabilities (indirect fire, anti-tank, Forward Observation Officers, etc.).

Each ACOA should provide answers to the FACES criteria. Each ACOA must be Feasible, Acceptable, Complete, Exclusive and Suitable for the actor/group.

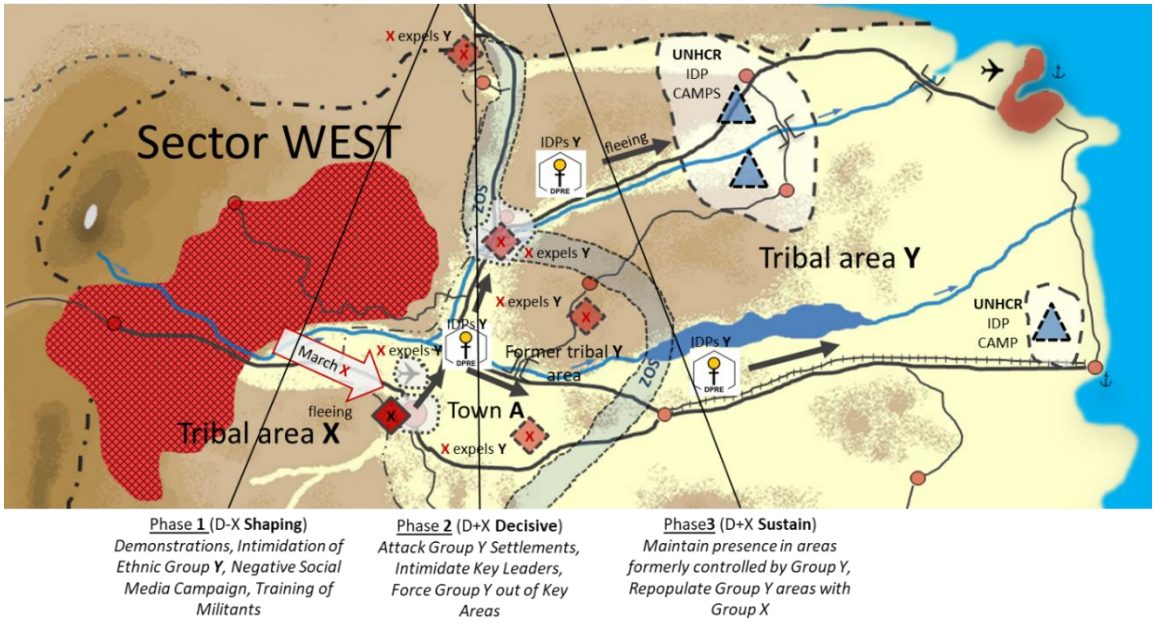


Figure 19: Example Situation Overlay (SO)

5.15.2 **The Event Overlay (EO).** The EO is a graphic representation of the Acquisition areas of interest, based on the threat group's ML/MD ACOA. EO are used to develop Acquisition plans and to view critical events or information positions. It is a graphical representation of where critical events are likely to occur (in time and space) and where some critical targets are likely to be located. An event overlay consists of NAIs – monitored areas (in sequence with time) for indicators, such as the presence of refugees or IED emplacement at known areas. NAIs can be areas, specific points or individual compounds. There is also a growing use of 'conceptual NAIs', for example, an individual's telephone number.

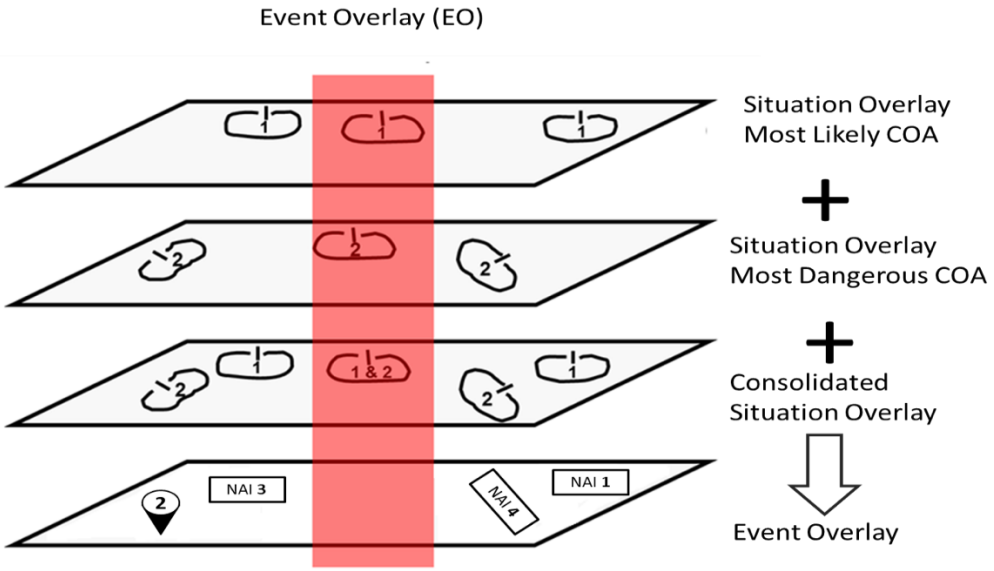


Figure 20: Relation Event Overlay and ML / MDACOAs

The production of an EO visualizes the identified NAIs and potential Target Areas of Interest (TAIs):

- **NAI**: An area where an actor is expected to engage in activity that would confirm or deny a potential ACOA. NAIs must always be covered by an information acquisition asset, which must be tasked appropriately in the Force IAP (for a visual representation of NAIs, please see Figure 21).
- **(P)IRs** in the Force IAP are always connected to NAIs.
- **TAI**: Area or point in the OE where it is assessed as possible to influence the adversary/actor in order to induce them to abandon or alter the ACOA (Figure 22).

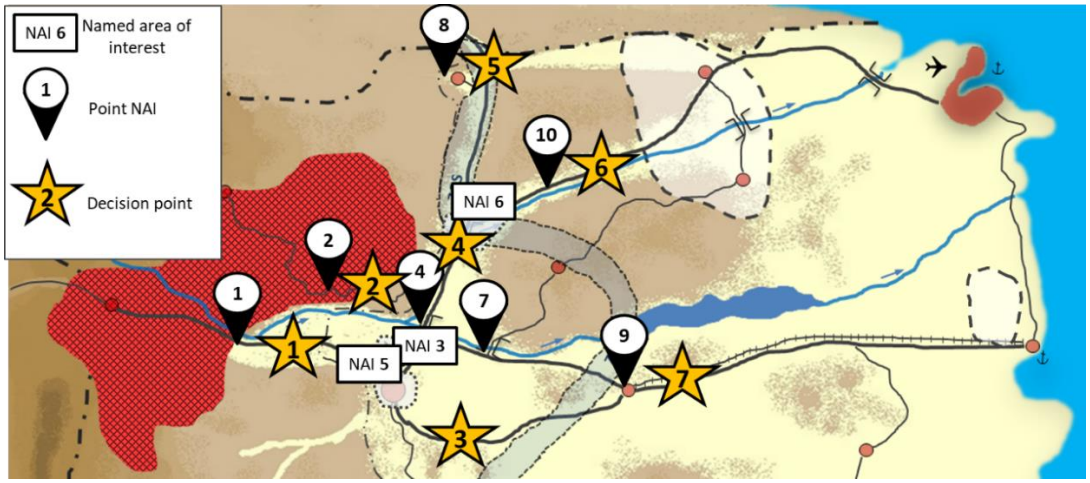


Figure 21: Example Event Overlay (EO)

For each NAI, the MPKI cell should identify detailed IRs. These IRs should serve to confirm which ACOA the threat group or relevant actor is taking. Such IRs are often referred to as I&W. It is therefore essential that ACOAs have a set of indicators linked to it, by which analysts can identify the events that are likely to unfold. UN assets can monitor identified NAIs and, as such, the MPKI must work closely with the operations section at this point.

5.15.3 **The development of ACOAs.** It is important to note that the ACOA is developed from the perspective of the relevant (threat or influencing) actor. It comprises a possible outline of its plan to accomplish its assessed mission or end state, is based on the detailed AE, and describes how the cell assess that the Actor will interact with the physical, human and information terrain. For each

relevant (threat) actor, the MPKI staff must develop a MLACOA, and a MDACOA. The MDACOA I&W are used to observe if the adversary actor/group is staying within the MLACOA. If indicators show the adversary or situation shifting towards the MDACOA, they provide the Commander enough time to adjust and activate contingency plans to counter this development.

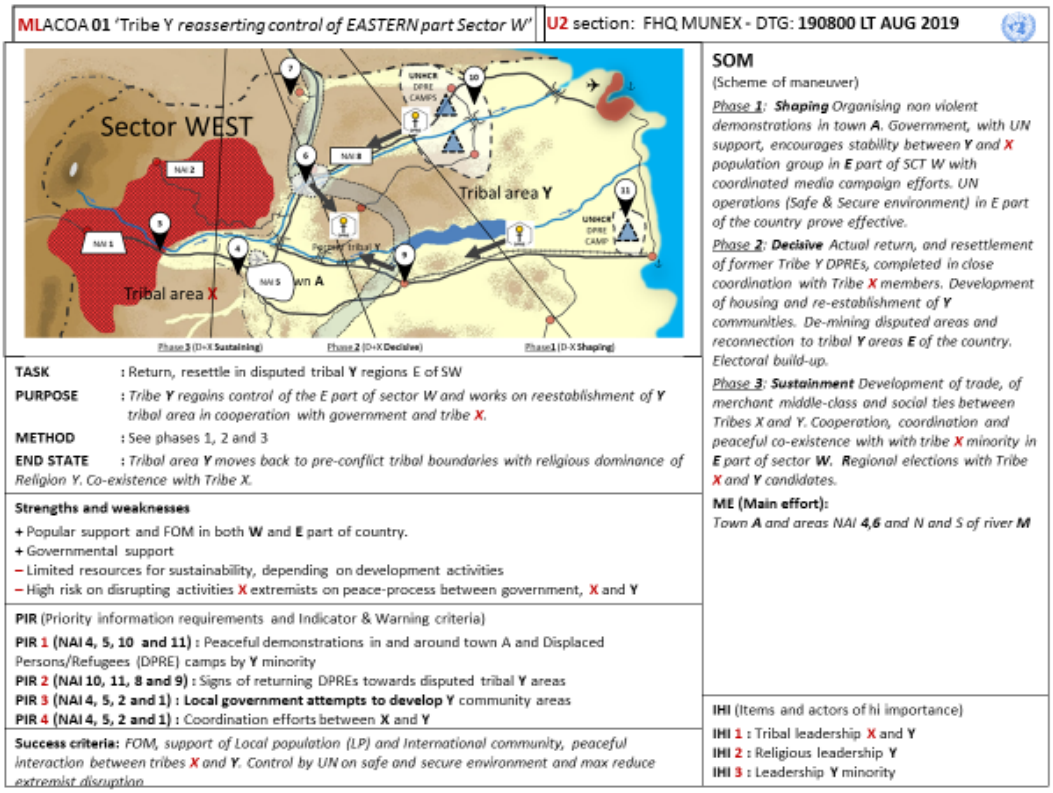


Figure 22: Example MLACOA

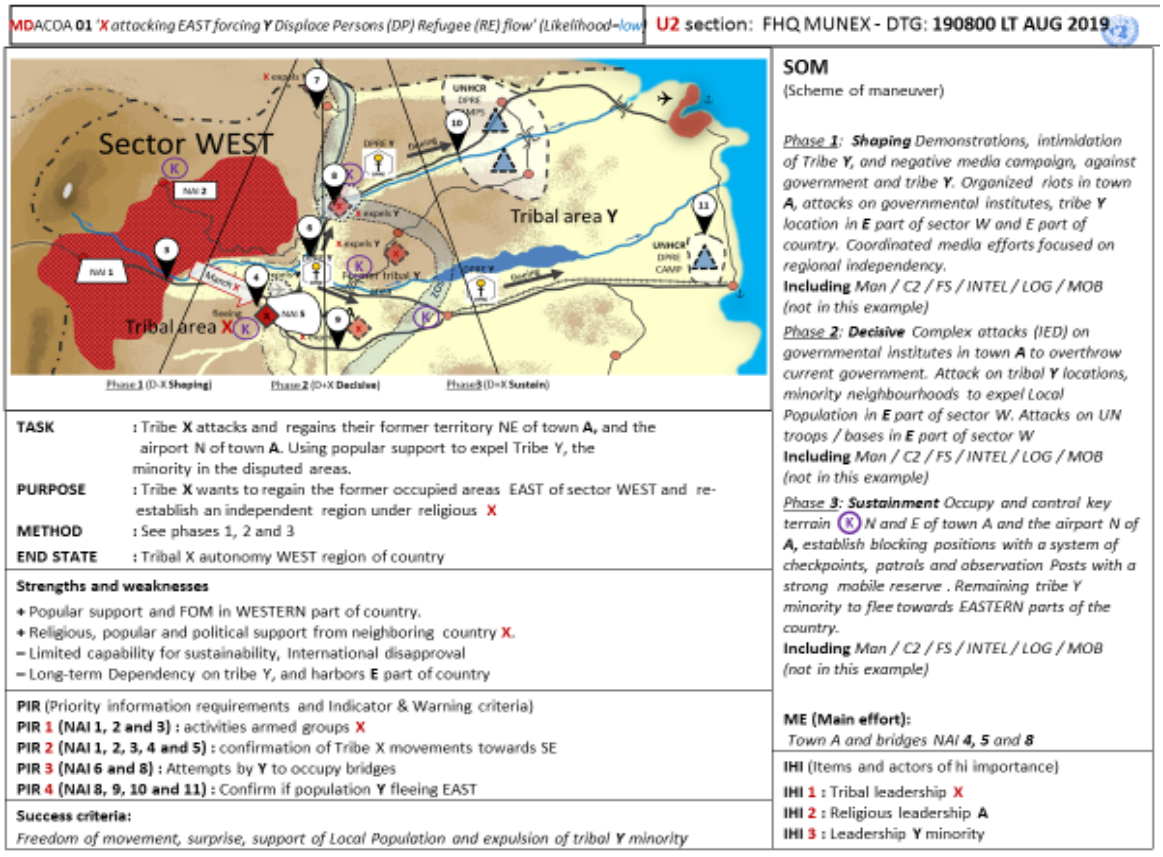


Figure 23: Example MDACOA

5.15.4 **ACOA Statement.** An ACOA statement consists of **WHAT** (form of manoeuvre operation, defend, delay, disrupt, etc) the relevant actor/threat group will seek to do, and the tactical tasks involved with respect to the UN and various forms of terrain. **WHEN** (the actor/threat group is most likely to act), **WHERE** (the critical geographic reference inherent in the mission which can be key/decisive terrain for the threat actor as identified in the Mission Analysis), **HOW** (what capabilities will the relevant actor or threat group employ) and **WHY** (the intentions of the relevant actor or threat group's mission). The ACOA will also include a set of indicators: what actions or behaviour will we (the UN) be able to observe that are indicative for this ACOA (see 9.11 on indicators).

Each relevant actor/threat group in the presented ACOA must pass the **FACES** test: is the ACOA F*easible*, *Acceptable* (risk and losses to the relevant actor or threat group), *Complete*, *Exclusive* (different from other COAs), and *Suitable* (will it accomplish relevant actor or threat group objectives).

5.15.5 **Sample of an ACOA statement:**

*(WHO) Threat group **X** will (WHAT) execute a complex attack on UN FOB Clara, combining asymmetric and conventional approaches. (WHEN) This attack will take place in early daylight, and during the dry season as the group can profit from increased mobility. (WHERE) The group is likely to launch its asymmetric attack at the main gate, while the conventional armed attack will come from the east where approaches to FOB Clara are covered from view and fire. (HOW) The group is likely to deploy a Vehicle-Borne IED (VBIED) and Person-Borne IED (PBIED) as part of its asymmetric attack, and to employ small and heavy machine guns and its indirect fire capabilities as part of its conventional attack. (WHY) Threat Group **X** will launch this attack to deter further UN presence into its area of operations and influence.*

An easy way to describe the ACOAs is to use the Tasks, Purpose, Method and End State (TPME) format in addition to a SO. The overlay should be designed so that the time, space, and force ratios as well as strengths and weaknesses of the alternative can be seen. The actor's different resources such as manoeuvre, command and control, fire support, use of information, and logistics are, if relevant, plotted on the ACOA SO. The example below shows how to use the TPME format describing the ACOA. This will help in building an ACOA SO that address the different factors and resources used in the ACOA.

Threat group X ACOA attack FOB	**Description**
Task	Attack UN FOB Clara
Purpose	Deter further UN encroachment into its area of Threat Group **X** operations and influence
Method	• A combination of VBIED and PBIED directed at the GATE. • Complex attacks from the east towards the FOB using a conventional armed force supported by machineguns and indirect fire.
End state	UN will leave FOB Clara or at a minimum not conduct operations outside of the FOB.
Resources	
Manoeuvre	First: VBIED will drive up to the gate and detonate to open up a gap so that people carrying PBEID can enter the base and detonate their IEDs inside to achieve mass casualty and focus the UN defensive effort towards the gate. Second; Conventional force will approach from the east to take advantage of the cover and concealment as they approached the FOB. When the IEDs detonate will they launch an assault on the east perimeter trying to breach it. This will be supported by machineguns and indirect fire.

Command and control (C2)	The coordination and command for the attacks will likely be done from the small hill east of the FOB that has line-of-sight towards the gate. (Area A on the overlay).
Fire support,	Light and heavy machineguns will most likely be deployed at Area B where most of the FOC can be observed.
Use of information,	Starting about two weeks before the attack, will the actor likely send messages to the villages near the FOB that only Actor A can provide security and stability in the area.
Air defence	Actor A most likely lacks any weapons to engage helicopters or aircraft and will use foliage concealment. If observed or attacked from the air they will use small arms to deter air assets.
Peacekeeping-intelligence	6-8 weeks before the attack, Actor A will start to monitor UN movements outside of the FOB. He will try to get some from the group employed inside the FOB to gain access to the specific layout. One to two weeks before the attack, he will conduct close reconnaissance of the routes for the different parts of the attack.
Logistics	The VBIED and the PBIEDs will likely be delivered to a village close by where a supporter to Actor **A** will receive and store them a few days before the attack. There will be pre-stored ammunition and food in the vicinity of the starting areas for the conventional force.
Mobility/counter mobility	IED or visual mines will be used to prevent the UN force leaving camp and counterattacking.

Table 8: TPME format (draft)

5.15.6 Examples of indicators that the UN force could monitor for to determine whether this ACOA will be adopted could include: reconnaissance of the UN FOB; persons taking photos/videos of the UN base; the testing of UN defensive systems (using kinetic or non-kinetic means); reports of VBIED preparations; unusual build-up of forces to the east of the FOB; and a generally unusual level of activity across the AOR including women and/or children disappearing from the area, the local attitude to the UN changing, and increased anti-UN propaganda. Once developed, these ACOAs are elements of the Peacekeeping IE, and are included in other MPKI products.

5.16 Outputs from AOE

As stated earlier in this Handbook, the conduct of AOE is continuous. Throughout the process, there are a number of outputs that are generated in addition to the constant update of the products and overlays defined in the previous paragraphs. The main outputs from AOE are:

- The identification of I&W that will confirm/deny an Actor's assessed COA.
- The update of the Force IAP, which should link NAIs to IRs and to acquisition assets.
- The Military Decision-Making Process – Phase One brief (detailed in Chapter 10).
- The SPIE.

5.16.1 **The development of I&W.** An indicator is an observable behaviour or event (or absence of): for example, "the absence of local population along the road," can be an indicator of an imminent attack or an IED along the road) that points towards an outcome/occurrence or, in this context, a

hypothesis or possible explanation for the data the analyst is considering. Indicators are observable at all levels from the strategic to the tactical. At the operational level, an indicator could include local population movements or the stockpiling of fuel or ammunition by a certain group.

Indicators are generated using the MPKI analyst's experience regarding what is known about a threat group's TTPs. Examples could include unavoidable actions linked to an event, such as the test firing of weapons, or the movement of large numbers of vehicles from one location to another and may be based on what has happened in the past (trend analysis). There are several types of indicators:

- Alert/Warning Indicator.
- Tactical/Combat Indicator.
- Identification Indicator.
- Temporal Dimension.
- Imminent.
- Medium-Term Indicators.
- Long-Term Indicators.

Because these types of indicators are observable, they are incorporated in the IAP, so that units and assets can use them. The acquired information should assist the analyst in determining the threat group ACOA.

5.16.2 **Update Force IAP.** As the MPKI staff conducts AOE, there will be a constant identification of peacekeeping-intelligence and acquisition gaps. These gaps are to be annotated in the Force IAP and are to initiate the production of RFIs and IRs (as detailed in previous chapters).

5.16.3 **Military Decision Making Process – Phase One Brief.** The Phase One Brief orients the planning staff at the start of the Military Decision-Making Process. It is a logical summary of the analysis following from AOE.

5.17 The Peacekeeping-Intelligence Estimate (PIE)

A PIE is a tool that provides a basis for analysis. It does not assist in the execution of a mission but enables the identification of deductions and key outputs to increase understanding and inform planning staff and decision-makers. The method used is the 3-column format (3CF). This is the most reliable means of ensuring that a PIE adds value by providing useful outputs rather than simply stating facts or making observations.

Factor	Deduction	Output
Input factor or question	Analyses process (So What)	Output for staff
Example		
High temperatures and no rain-season	Drought, Famine and increasing flow of refugee	Focused questions (PIR's – RFI's) Effects on OE, population and UN Potential actions by UN Tasks for UN / UNCT Constraints for UN Risks for population and UN mission

Table 9: Basic 3-Column Format example

AOE and the PIE are complimentary activities, and MPKI staff should conduct both where time allows. The AOE is the mechanism which supports the Military Decision-Making Process (MDMP) but does not provide the same analytical rigour that a full PIE does.

5.17.1 **The conduct of the PIE.** The PIE should be conducted in the event of a new or complex mission (especially when deploying to a new area for the first time). Within the MDMP, the PIE is typically conducted by MPKI staff during Phase 2 (Mission Analysis). The senior PKI Officer owns the process; it can either be conducted in isolation before seeking wider MPKI staff input or done collaboratively with the senior PKI Officer acting as the Chair and collating the thoughts of their MPKI staff.

5.17.2 **PIE Outputs.** The aim of the PIE outputs is to provide the Commander with PKI (and often operational) considerations. These considerations will fall under the following headings:

- Task. An action that needs to be undertaken.
- Planning Guidance. A piece of advice on what to consider during the planning process.
- IR. A requirement for an internal answer.
- RFI. A request to an external audience for an answer.
- Constraint. A factor that will prevent freedom of action during conduct of a mission.
- Freedom. A factor that will provide physical or conceptual room for action during the conduct of a mission.

Factor	**Deduction**	**Output**
Weather	The operation will be conducted during the wet season and river levels are likely to be higher than normal.	**TASK (T)** – Engineer Recce is to conduct reconnaissance of current crossing points to see if they are still usable.
Actor Equipment	The Threat Actor has no night vision capability	**PLANNING GUIDANCE (PG) –** Night operations are likely to provide UN forces an advantage.
Religious Affiliations	On current peacekeeping-intelligence, it is uncertain as to what religious affiliation the village of WINFORNIA has.	**IR:** What is the religious affiliation of WINFORNIA and how will it affect the UN forces there?
Bordering Forces	Host State security forces are operating to the East of our APIR. Their operations are not understood.	**RFI:** What operations are being conducted by HNSF to the East of the APIR?
IDP camps	IDPs remain in the AO and are being used as cover by threat actors	**CONSTRAINT (C):** Operations against threat actors will have movement and increased ROE constraints due to likelihood of collateral damage.
Local Tribal Leaders	The local tribal leaders and senior women are known to be trustworthy and are supportive of UN presence.	**FREEDOM (F):** UN forces can engage with local tribal leaders and senior women during the mission and can seek advice without compromise.

Table 10: Example of PIE Outputs

5.18 The Short Peacekeeping-Intelligence Estimate (SPIE)

The SPIE is a method of disseminating the AOE in written and graphical form. The SPIE uses the same logical process as the AOE and ends with detailed assessments of the ACOAs. It is not as detailed as a full PIE but is more easily disseminated. At times MPKI staff will not have time to conduct a full estimate, therefore the SPIE is a useful format.

THE SPIE

The Current Situation
(Summary paragraph)
Own Mission / Objectives
(Summary paragraph)
Relevant Actor Situation
(Summary paragraph)
Key Assessments / Deductions
(Summary paragraph)

AOE

Factor	**Deduction**	**Output**
Physical Terrain		
Human Terrain		
Information Terrain		
Weather Effects		
Actor Evaluation		

Threat Evaluation

Aim and End State		
Assessed Actor/ Threat Actor Aim	*(Summary paragraph)*	
Assessed Actor/Threat Actor End state	*(Summary paragraph)*	
Factor	**Deduction**	**Output**

Threat Integration

Relevant Actor MLACOA		
MLACOA Schematic	*(Summary paragraph)*	
Factor	**Deduction**	**Output**
Relevant Actor MDACOA		
MDACOA Schematic	*(Summary paragraph)*	
Factor	**Deduction**	**Output**

Table 11: Template for the SPIE

5.18.1 **SPIE Estimate Explained.** The headings may vary depending on the operation and the commander's requirements.

- **The Current Situation.** An indication of events within the area of interest that have led to the estimate. May include a brief description of political events, national relations, diplomatic relations, regional situation and third state and non-state actors.
- **Own Mission/Objectives**. This includes mission and commanders. Friendly dispositions and incidents may be addressed in brief. Can also include other identified stakeholders in the situation who are not direct adversary or friendly forces. May include international NGOs, aid agencies, political factions, etc.
- **Actor/Threat Actor.** Brief picture describing current relevant or threat actor situation. May include his/her aims and intent.
- **Key Assessments/Deductions.** List key points identified from the PIE process.
- **AOE.** Includes key elements of the Physical, Human and Information Terrains. Some factors that may be considered include geographic/hydrographic aspects, socio/political features, demography, stakeholder groups, economic features and infrastructure, economic activity, transport, industry, information and health. Deductions can be made under each area.
- Tools that can be used to assist AOE include Observation, Cover and Concealment, Obstacle, Key Terrain (KT), Avenues of Approach (OCOKA), and ASCOPE - PMESII. Other example factors for consideration if not already covered in the above tools include land/terrain; urban; infrastructure; maritime/littoral; aerospace; international and political issues; demographics and power bases; environmental hazards/health issues; information; weather; and terrain history.
- **Threat Evaluation.** Can include several factors dependent on the situation. Detail on known dispositions, recent activity, composition and C2 are all useful. Detailed exploration of the actors'/threat actors' doctrine, Modus Operandi (MO), or TTP as appropriate. If in the early stages of a conflict, a review of recent attacks with a view to establishing TTP may be conducted. Could include graphical templates of any doctrine/MO/TTP.

Threat Integration. A list of broad COAs available to the actors/threat actors. COA should be consistent (with adversary doctrine and activity), suitable (to achieving the adversaries' aim), exclusive (different from one COA to the next), acceptable (casualty-wise or politically), and feasible (within the realms of probability). COA Analysis should compare various COA against an appropriate set of criteria such as principles of war, principle of offensive or defensive operations, functions in combat, etc. Following COA Analysis, a MLACOA and MDACOA should have been identified and a brief explanation as to why the respective COA have been identified as either ML or MD should be provided. Factors deductions and outputs should then be listed for each of the COAs.

Factors/Deductions/Outputs

Factor (Key factual information you have identified)	**Deduction** (Your analysis of the Factor)	**Output** **(As per table below)**
Example. The clock in the classroom has been losing 5 minutes each day for the past week.	1.1 - It is highly likely that the batteries in the clock have diminished. 1.2 - It is almost certain this has contributed towards lessons not being delivered on time.	1.1.1 - IR – How many batteries does the clock need? 1.1.2 - IR – What type of batteries does the clock require? 1.1.3 - IR – Where can the batteries be purchased?
Example. The size of the insurgent grouping within the AO is approximately 7-8pax.	2.1 - Likely they will have a similar structure to our Sections; a Commander, 2IC and several fighters. 2.2 - Given their size, they will likely be limited to conducting Shoot and scoot attacks. They will almost certainly not be able to carry out F2F ambush type attacks.	2.1.1 – IR – What type of attacks have they carried out previously? 2.1.2 – IR What level of experience do the fighters have? 2.1.3 – IR – How does the Commander communicate with the rest of the section?
Example. The Bn HQ is situated in the town Elwood in the south of the AO.	3.1 – The enemy will use the population as protection – will likely place key assets in highly populated areas such as schools. 3.2 – Elwood is assessed as their VG – Likely the enemy will use the infrastructure and resources available in the town as part of their re-supply efforts.	3.1.1 – PIR – What does the HQ comprise? 3.1.2 – IR – What is the population size of Elwood? 3.2.1 – R – Collateral damage possible 3.2.2 – What resources are available to the enemy in Elwood?

Table 12: Factors / Deductions / Outputs

5.19 Annexes

A. MPKI Analysis Working Files

B. Peacekeeping-Intelligence Analysis Definitions

C. Example ASCOPE – PMESII Matrix

D. Peacekeeping-Intelligence Support to Base Protection – Example

E. Peacekeeping-Intelligence Support to Patrol – Example

CHAPTER SIX: DISSEMINATION

6.1 Dissemination - The Final Phase

The final phase of the MPKI cycle is Dissemination. PKI which is not disseminated has no value. Equally, PKI that is disseminated but which cannot be understood has no value. Dissemination must assure that PKI is delivered at the right time, in the relevant quantity and quality, to the right people.

- **Timely.** Peacekeeping-intelligence must be delivered in a timely manner so planners and decision-makers can act rather than react – thus ensuring that they retain the initiative. Some acquisition assets can send information they acquire to the MPKI cell on a real-time or near real-time basis, vastly increasing their utility.
- **Relevance.** Relevance is determined by the needs of the recipients as defined in the Direction phase of the Peacekeeping-Intelligence Cycle.
- **Brevity.** Reports must be kept as brief as possible, but at the same time include everything that the recipient needs to know. Commanders seldom have time to wade through lengthy documents or listen to verbose oral briefings. Full use of traces, annexes, and facsimile processes should be made to cover additional detail. One possible way to achieve brevity is by ensuring the most important message or key information is mentioned first with an explanation, thereafter, following the Bottom-Line Up Front (BLUF) principle.
- **Interpretation.** Wherever possible, all facts must be correctly evaluated, and their significance interpreted before dissemination. In all PKI reports, a clear distinction must be preserved between established facts and the deductions, assumptions, and assessments made from them.
- **Standardization.** Reports are understood more quickly if they are laid out in a logical sequence under convenient standard headings using the same language of probability. The format should be covered in standing operating procedures.
  - **Recipients.** Distribution is based on a thorough knowledge of the IRs of units, planners and decision-makers. This knowledge is based on the Force IAP and RFIs.
  - **Need-to-Know.** Access to classified PKI should be limited to those who have a need to know to carry out their duties.
  - **Need-to-Share.** PKI can be shared between UN and with non-UN entities in accordance with the published guidance[14] as well as relevant mission policies or mission specific arrangements[15]. Key issues that must be considered include the need to protect sources, as well as the possible need to sanitize certain peacekeeping-intelligence products for this purpose. Sharing peacekeeping-intelligence with non-UN entities must comply with the United Nations Human Rights Due Diligence Policy (HRDDP)

> Peacekeeping-intelligence that is not disseminated to those that have a need to know has no value.

6.2 Dissemination Formats

Dissemination consists of both 'push' and 'pull' concepts. The 'push' concept allows the higher command to push peacekeeping-intelligence to lower levels of command. The 'pull' concept involves direct electronic access to webpages, databases, peacekeeping-intelligence files, or other

[14] *Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission Entities,* UN DPO 2022.05 (1 December 2022). *United Nations Human Rights Due Diligence Policy on UN Support to non-UN security forces (HRDDP)*, October 2011.

[15] In some UN peacekeeping operations, the Force concluded with the Human Rights component to systematically exchange military peacekeeping intelligence and human rights analysis.

repositories (where applicable). PKI should be provided in a format that the recipient readily understands and is readily usable.

- **Verbal.** Verbal briefings are useful for timeliness and for providing an opportunity to emphasize significant issues, as well as providing the briefer with immediate feedback and the potential for further direction. A verbal presentation can be organized and supported by a Picture Peacekeeping-Intelligence Summary (PICINTSUM) (see Annex C). When preparing for verbal briefings, the following should be considered:
  - The language the brief recipients speak.
  - The level of security clearance the group has.
  - The level of knowledge the group has on the subject. This will determine the detail or background information that will be given.
  - The time that you are allocated. It is vital that your message is disseminated in as little time as possible, and that you do not run over your allotted time. Failure to adhere to this may mean that your commander or recipient will not ask you to brief again. Only tell your recipient what they need to know.
  - Work out the questions you are likely to be asked and prepare responses. This will be done based on your knowledge of your commander's requirements.
  - What visual aids you require to brief; and
  - Is your brief compatible with the technology in the briefing room.
- **Written.** Written dissemination encompasses Peacekeeping-Intelligence Reports (INTREP), Peacekeeping-Intelligence Summaries (INTSUM) and Thematic Reports. INTSUM should be disseminated at regular intervals relevant to the situation. Time-sensitive material is disseminated using INTREPs.
- **Graphical.** PKI products such as: PICINTSUMS (see Annex C), aerial photographs, Sketch Maps, physical, human, and information overlays (see Chapter 9), system integration overlays (see Chapter 9), link charts and wiring diagrams all help a commander assimilate new and complicated information and PKI. Whenever possible, PKI staff should always make maximum use of graphical products.

> Peacekeeping-intelligence indicating an assessed imminent threat to life must be conveyed immediately. The source and any classified information may be left out / protected as required, but the threat to life must be passed on by the fastest means.

6.3 Clarity

Both briefings and reports should be characterized by clarity and brevity. PKI should be presented in an unambiguous way – clearly identifying facts from assessments. The originator must ensure that they have focused their thoughts before briefing or writing. The briefings and reports should follow a standard format. The use of visual aids, maps, drawings and diagrams will enhance the verbal briefing and clarify the PKI being discussed. To be brief and precise is the key to the successful dissemination of PKI. A good presentation – verbal or written – is one which contains the most information in the fewest possible time or words.

6.4 UN Reporting Formats

The UN uses standard report formats to guarantee multinational interoperability.

6.4.1 **Peacekeeping-Intelligence Report (INTREP).** An INTREP may be originated at any level of command and is a non-routine report that is sent whenever the information it contains is considered likely to require the urgent attention of the receiving units, commander, or their staff. The INTREP should include any relevant deductions made in the time available. The distribution of an

INTREP will conform to explicit instructions laid down at each level of command. An example format of an INTREP is at Annex A.

8.4.2 **Peacekeeping-Intelligence Summary (INTSUM).** An INTSUM is a periodic summary of PKI on the current situation within a commander's APIR. It is designed to update the current PKI assessments and highlight important developments during the reporting period. Its distribution should include all those whose responsibilities and interests may be affected by the contents. An INTSUM may be written in prose or with graphics (PICINTSUM). INTSUM format examples are at Annex B.

6.4.3 **Thematic Reports.** Thematic reports address relevant aspects of the operational environment, such as a region or town, a political or religious movement or an organization, sometimes covering longer timescales. There is no fixed format for a Thematic Report. It will normally contain at least three main headings: Situation, Comment, and Assessment.

> Dissemination must ensure that peacekeeping-intelligence is delivered at the right time, in the relevant quantity and quality, to the right people.

6.5 Summary

Both unevaluated facts (i.e., information) and the assessments made from them (i.e., peacekeeping-intelligence) will need to be disseminated, but the greatest care must be taken to preserve the distinction between the two. The most accurate and reliable PKI is useless if it arrives too late. PKI assessments must always be stated in a unambiguous form, urgent information must be passed on immediately, and there must be regular summaries of the PKI situation. Briefings, whether spoken or written, must be clear, relevant and concise; the shorter a message or briefing, the easier it is to remember. A record of all dissemination, written or spoken, formal or impromptu, must be entered in the peacekeeping-intelligence log.

6.6 Annexes

A. INTREP

B. INTSUM

C. PICINTSUM

CHAPTER SEVEN: MANAGEMENT AND USE OF MPKI

7.1 UN Peacekeeping-Intelligence Structures, Roles and Responsibilities

The UN MPKI cycle is designed to direct, acquire, examine/collate, analyse, and disseminate PKI at the strategic, operational, and tactical levels. This is necessary to inform decision-making at all levels of the UN structure.

7.1.1 **United Nations Headquarters (UNHQ).** At this level, all UN departments involved in PKO have elements dealing with information and analysis. For example, the Department of Safety and Security (DSS) has a Threat and Risk Assessment Service in charge of providing security threat information through regional- and country-specific levels to support field duty stations, and to ensure the safety and security of all civilian personnel. Within DPO, the Office of Military Affairs (OMA) has the Current Military Operations Service (CMOS) dealing with current information from the military channel in UN peacekeeping missions, as well as an Assessment Team (AT), comprising trained MPKI officers, focused on the production of regional MPKI assessments. In addition, the Single Regional Structures reporting to both DPO and the Department of Political and Peacebuilding Affairs (DPPA) serve as a mechanism to deliver strategic and operational guidance to field missions. The United Nations Operations and Crisis Centre (UNOCC) has a Research and Liaison Unit (RLU) that provides integrated analysis for DPPA-DPO leadership as well as the Executive Office of the Secretary-General. Furthermore, the Peacekeeping-Intelligence Coordination Team (PICT) in the Office of the Under-Secretary-General for Peace Operations oversees coordination of PKI activities by all participating actors at UNHQ and in the field by ensuring compliance with the PKI Policy Framework.

7.1.2 **Operational Military Peacekeeping-Intelligence.** Operational-level MPKI refers to products that inform the UN Force Commander's decision-making process. Information acquired, and PKI produced at this level, when combined with that of other mission entities, will inform the decision-making process of the HoM/Special Representative of the Secretary-General (SRSG), which often has a more strategic focus. The below entities are likely to be participants in the management of operational peacekeeping-intelligence.

7.1.3 **JMAC.** The JMAC is an integrated entity comprising civilian, military, and police personnel, established to support mission-level planning and decision-making through the provision of integrated analysis and predictive assessments. It manages the Peacekeeping-Intelligence Requirements (IRs) of the HoM and the Mission Leadership Team (MLT) through the development of a Mission-level Information Acquisition Plan (MIAP), through collating and analysing all-source information, and by identifying threats and other challenges to the mandate. The JMAC acquires and analyses multi-source information to prepare mid-to long-term integrated analysis and assessments for strategic, operational and contingency planning, decision-making and crisis management. In many missions, the JMAC fulfils an important leading role in the MICM that directs and oversees the peacekeeping-intelligence cycle within the mission. The Chief JMAC is a civilian, who reports directly to the HoM. The Peacekeeping-Intelligence Policy indicates that the Chief JMAC may, in some instances, lead the MICM. All MPKI and other relevant information should be shared with the JMAC and the MICM, particularly where it relates to the Peacekeeping-Intelligence Requirements (IRs) of the MLT and the MIAP.

7.1.4 **Joint Operations Centre (JOC).** The JOC is an integrated entity established to support the decision-making processes of the MLT and UNHQ through the provision of integrated situational awareness in routine and special incident reporting. JOCs also facilitate crisis management decision-making and, in some cases, help to facilitate integrated operations coordination and planning. The JOC acquires and collates all current reporting, receiving reports from all in-theatre UN entities, and has a 24-hour monitoring capability. The JOC strives to establish information exchange and working relationships with appropriate Mission components and with relevant UNCT/Humanitarian Country Team (HCT) entities. JOC reporting to its clients must reflect the composition (multidimensional or more traditional PKO) of the mission. In the context of MPKI, the JOC and the JMAC will align their activities in the MICM to avoid any gaps in the provision of situational awareness and analytical support to mission leadership. The JOC should be co-located in the same operational space as the

Military Operations Centre (MOC), Police Operations Centre (POC) and the Security Operations Centre (SOC), or their equivalents where they exist. The military component should ensure that all daily situation reports, and other relevant information is sent to the JOC on a routine and frequent basis, as required. The joint nature of JOC staffing, with civilians and uniformed personnel working together, should also help to ensure regular exchanges of information between the JOC and all Mission components. The principles of sharing such information should be outlined in the Mission Peacekeeping-Intelligence Support Plan (MISP).

7.1.5 **Force Headquarters (FHQ) MPKI Cell (U2).** While the U2 cell is obviously part of the MPKI structure, it is important to recognize that it is also part of the Mission's operational PKI structure. Military units beneath the FHQ level often have unique access and a valuable perspective on the tactical situation. As a result of MPKI provided through the U2, this tactical-level PKI makes an important contribution to UN operational PKI.

7.1.6 **Police Component / Crime Peacekeeping-Intelligence Unit (CPKIU).** The CPKIU is normally similar to the military component, with Sector- and Battalion-level deployments. The CPKIU can provide valuable peacekeeping-intelligence from a police perspective.

7.1.7 **UNDSS/Chief Security Advisor (CSA).** With a responsibility to provide protection and security advice for UN civilian personnel, the CSA and other UNDSS personnel have access to security-related information. As such, they have much to offer to the MPKI organization.

7.1.8 **Other Entities.** Political Affairs, Civil Affairs, Liaison, Civil-Military Affairs personnel, as well as those working with Disarmament, Demobilisation, and Reintegration (DDR) mandates can be a rich source of information. Where possible and appropriate, the U2 should strive to develop relationships with them. These entities may also, on invitation from the Chief JMAC, be members of the MICM; see below for details.

7.2 UN Peacekeeping-Intelligence Management Mechanisms

7.2.1 **Mission Peacekeeping-Intelligence Coordination Mechanism (MICM).** Individually, the different entities of a UN mission (UNDSS, U2, UNPOL, JOC, JMAC) are providers of operational PKI; however, when the entities work together, the result is better, more coordinated operational peacekeeping-intelligence. This cooperation is supported through MICM. The exact nature of the MICM will vary from mission to mission, but the fundamentals are as follows:

- The Mechanism comprises mission entities responsible for peacekeeping-intelligence acquisition, analysis, and dissemination. This will typically include the JMAC, JOC, UNDSS, and the relevant military and police components (such as the U2). Other mission entities may be invited to participate, as required.
- The purpose of the MICM is to provide centralized control (allowing de-centralized execution), direction and coordination of the mission's peacekeeping-intelligence system.
- The MICM is a meeting chaired by the Mission Chief of Staff, while in some cases, the role of Chair can be fulfilled by the JMAC.

The primary responsibilities of the MICM are outlined in the Peacekeeping-Intelligence Policy, but include the following:

- Draw strategic guidance from senior Mission leadership, and translate this guidance into Priority Peacekeeping-Intelligence Requirements (PIRs) and other IRs;
- Manage the MIAP and the acquisition effort, satisfying all senior leadership IRs;
- Develop and maintain the MISP.

It is important to note that some of the MPKI IRs will originate from the MIAP, and that these IRs will form part of the Force IAP. Representatives of the Force Commander (most likely the Chief U2) must also participate in regular MICM meetings. Five core members of the MICM are JMAC, JOC, UNDSS, Force U2 and UNPOL CIU. Other entities can be core members or ad-hoc members, depending on the mission: e.g., PAD, CAD, POC, HRD, DDR, etc.

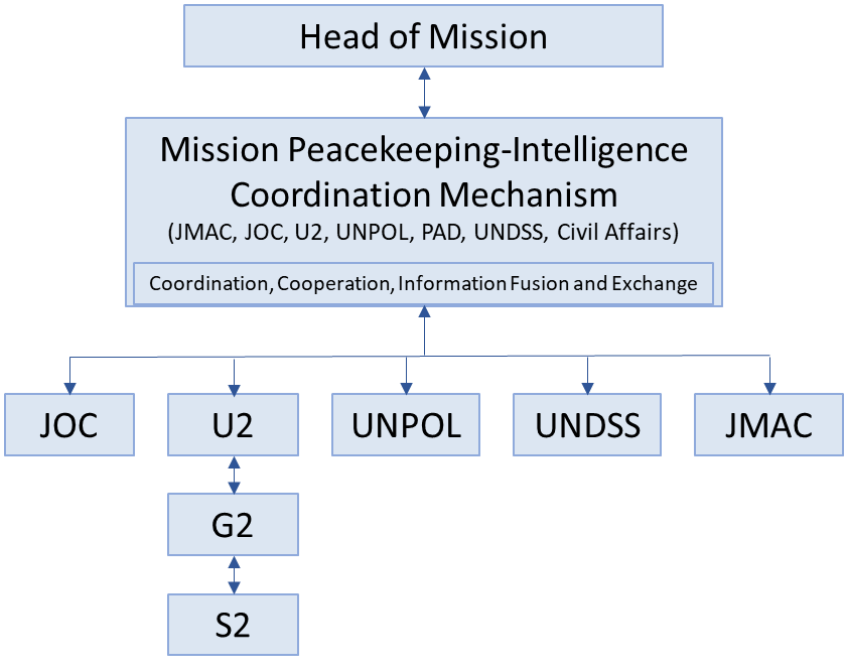


Figure 24: MICM Organization

7.2.2 **Additional networks.** Missions may liaise with non-mission entities, such as other international organizations as well as non-governmental organizations, to share PKI products. As already outlined, the HoM or those to whom he/she has delegated authority are responsible and accountable for the sharing of such products.[16] Consideration should also be given at this level to the extent to which the MICM may wish/need to liaise with the Host State's intelligence structures. The level of engagement of the Host State is likely to vary across missions, depending on the mandate, situation and Host State's stance towards the UN presence.

7.2.3 **Key persons.** There are a number of key persons who are, necessarily, involved in the PKI process. The SRSG, for example, must give guidance on their PKI priorities to the MICM and is the main customer. Always remember, due to their unique position, access and attendance at meetings, key persons can be a significant source of information.

7.3 UN Tactical Peacekeeping-Intelligence

For MPKI, tactical PKI relates to the G2 at Sector level and S2 at Battalion level; there is also likely to be similar representation from police and civilian mission components. Tactical PKI is required both to support the local commander and to feed localized PKI up the chain to inform the operational and strategic PKI picture. Just because it is conducted at the lowest level does not mean that tactical PKI is not important. Tactical PKI or even unprocessed information acquired at the tactical level may have strategic importance. In many large UN peacekeeping mission areas, it is crucial that the G2 is also able to provide a short- and medium-term analysis by acquiring and analysing information from multiple sources and preparing integrated analysis and predictive assessments to support the decision-making, planning, and crisis management of the Sector Commander.

UN MPKI Structures, Roles and Responsibilities

7.4 Establishing the MPKI Architecture

The MPKI architecture is built around a central hierarchical structure of an FHQ MPKI entity (U2), with several subordinate Sector HQ PKI entities (G2), which in turn have subordinate Battalion-level PKI entities(S2). It is also possible to have PKI organizations and capacities at the Company level. The non-specific word 'entity' has been deliberately used as several factors, including size of

[16] Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities 2022.

mission, nature of mission and threat level, will determine the exact construct at each echelon. It may range from a PKI Company to a smaller PKI cell all the way down to a two-person PKI team at Company level. Regardless of the exact size and scale, this hierarchical structure has two main functions:

- To provide PKI support to the UN military component to which it is aligned.
- To form part of the MPKI network in a chain to maximise PKI success.

The outline of functions and tasks at each level are as follows (a more detailed list of roles and responsibilities, together with recommended structures are included at Annexes A and B):

7.4.1 **FHQ U2 Branch.** Within the FHQ, the U2 Branch is responsible for providing MPKI support to the Force Commander and to the other functions in the FHQ such as planning and operations. All PKI support should aim at enhancing situational awareness and the safety and security of UN personnel, as well as informing activities and operations related to protection of civilians. At this level there are likely to be separate functions within the MPKI structure supporting the Direction, Acquisition, Examination/Collation, Analysis and Dissemination requirements of the MPKI cycle. At this level the PKI assessments are generally mid- to long-term and designed to support the Force Commander's planning process, although there may also be a need to respond to crises. Key functions are to provide the PKI assessments to support decision making and Force Protection measures. In addition to the requirement to provide PKI support to the FHQ, the U2 also has the responsibility to lead and direct all MPKI structures in the Mission. This responsibility can involve decisions such as determining how limited analytical or acquisition capabilities are best placed to achieve the commander's priorities, the MPKI battle-rhythm, and the development of MPKI SOPs. The MPKI battle rhythm is supported and directed by the Force Peacekeeping-Intelligence Support Plan (ISP), which the U2 is charged with producing, which will be based on and in line with the Mission Peacekeeping-Intelligence Support Plan (MISP). The U2 should attend all MICM meetings and ensure liaison is taking place across the MPKI entities at the operational level. The use of dedicated PKI liaison officers should be considered.

7.4.2 **Sector HQ (SHQ) G2 Peacekeeping-Intelligence Branch.** The PKI roles of the G2 at SHQ level are similar to those of the U2. The G2 will also have to action the direction received from the U2 in the Force IAP and must adhere to the provisions of the Force ISP. The size of the branch is likely to be smaller than the FHQ, but it is still probable that separate MPKI professionals will be responsible for each stage of the MPKI cycle.

7.4.3 **Battalion HQ (Bn HQ) S2 Peacekeeping-Intelligence Section.** Again, the roles will largely be the same: enhancing situational awareness and the safety and security of UN personnel, as well as informing activities and operations related to protection of civilians. Due to the tactical nature of the Battalion HQ, the assessment timelines are likely to be shorter. At this level, it is likely that given the small number of MPKI personnel, a single person may be responsible for more than one aspect of the MPKI cycle.

7.4.4 **Company HQ (Coy HQ) Company Peacekeeping-Intelligence Support Team (COIST).** It may be that, due to the nature of the mission, a company is deployed to a remote area or on a specific task. In such instances, it is desirable for the Coy HQ to have PKI support. This is likely to be a two-person team trained in MPKI, and they will have to be robust enough to deploy in relatively austere conditions.

7.4.5 An overall generic structure is at Annex A, and MPKI staffing templates are at Annex B.

7.5 Additional MPKI Elements

Depending on the mission, there may be additional peacekeeping-intelligence elements in the MPKI structure:

7.5.1 **Peacekeeping-Intelligence Surveillance and Reconnaissance (PKISR) Unit.** A PKISR unit may be from a single TCC or may merge capabilities from a number of TCCs. The exact nature of the PKISR capabilities will differ from mission to mission, but fundamentally the capabilities are designed to support information acquisition and PKI production. The range of capabilities have been

discussed in more detail earlier in this Handbook (see Chapter 3: Acquisition), but it is worth noting that reconnaissance patrols often have as much utility as UAS and other advanced assets. A complementary mix of acquisition capabilities is generally best.

7.5.2 **Military All-Source Information Cell (MASIC).** A MASIC is an all-source analytical team designed to increase the thinking and analytical elements of an MPKI entity. This may be required because of scarce specialist resources or because MPKI would benefit from having a range of analysts with different specialities working together to holistically look at a PKI problem; aspects and developments in the OE should not only be viewed from a military perspective. This broad approach ensures that all relevant factors, actors, relations and interactions are considered and analysed to achieve full understanding of the OE.

7.6 Support to MPKI - Non-UN Partners

The decision to share any MPKI with non-UN partners rests with the SRSG. The SRSG may wish to delegate this authority as required. Any decision to share information or PKI will be bound by UN information and PKI sharing protocols. It should be recognized that there are often significant benefits to sharing information, such as the receipt of valuable information or intelligence in return.

When making the decision to share, the SRSG or delegated authority should consider how the non-UN partner intends to operationalise the information or PKI received. The SRSG or delegated authority must keep the principle of impartiality to the forefront of the decision-making process in this regard. Reputational risk – on both sides – is also a factor if such sharing becomes public knowledge. The receipt of any intelligence products from non-UN, third-party entities, as well as the sharing of any PKI products with said entities, are governed by the procedures articulated in the Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities.[17]

7.7 MPKI Practical Principles

When working in the MPKI environment, there are many practical principles that increase the chance of success. These include:

7.7.1 **Command-Led.** Military PKI is a centrally coordinated process through which information inputs from decentralized entities, often deployed over a wide geographic area, are combined with different functions and expertise. Accordingly, there is a requirement for a senior MPKI officer to not only be a peacekeeping-intelligence professional but also to ensure that the MPKI structure is being command-led. At the start of an operation this can be achieved through the Force ISP; however, the requirement for MPKI leadership is continuous.

7.7.2 **Centralized Control – Decentralized Execution.** Linked to being command-led, it is an accepted principle that MPKI systems thrive under centralized control but with decentralized execution. Centralised control means both that the MPKI effort is explicitly linked to the commander's requirements and that the MPKI organization is operating as a homogenous system, maximizing capability and minimizing duplication. Decentralized execution simply means that once the centralized control has been exerted, the disparate elements of the MPKI structure should be trusted to execute their elements of the PKI cycle without unnecessary interference.

7.7.3 **Objectivity.** MPKI must never be distorted to fit a preconceived idea or to conform with strongly held views of senior leadership. The MPKI unit must have the moral courage to report what it considers to be the most accurate assessment and avoid analytical biases such as 'group think'. Equally, analysts must not become too emotionally invested in their assessments as this may skew their judgements. Robust debate, key assumption checks, and 'red teaming' are good ways of ensuring that objectivity is maintained.

7.7.4 **Accessibility & Timeliness.** PKI is useless unless it reaches those who need to know by the time they need to know it. There is always a requirement to protect PKI sources and conform to UN information handling protocols; however, there is also a requirement to ensure that assessments

[17] DPO Ref. 2022.05, 1 December 2022.

are ‘written for release’ and therefore are as widely available as deemed possible (‘dare to share’). Good PKI that cannot be accessed by the staff that require it, or that reaches a commander after the decision on their course of action has been made, is worthless. At all times remember that PKI must be accessible and timely.

7.7.5. **Invest in the Force ISP and MPKI Battle-rhythm.** A strong Force ISP with clear responsibilities, SOPs, timings, reports and returns, and battle-rhythm sets the MPKI structure up for success. Invest time to ensure the Force ISP is clear, up-to-date and well understood. The Force ISP and the battle-rhythm provide the cogs that make the MPKI machine work. A Force ISP template is at Annex B.

Support to the UN Military Decision-Making Process (MDMP)

7.8 Peacekeeping-Intelligence-Enabled Decision-Making

Decision-makers at all levels require detailed understanding of the operating area, and a critical analysis of peacekeeping-intelligence assessments to make informed decisions. The purpose of this chapter is to describe how MPKI supports UN military decision-making in providing situational awareness, supporting the planning staff, and in testing the plan to ensure every contingency and threat has been assessed and considered in detail. The UN MDMP is detailed in Figure 26. This process facilitates planning and describes what peacekeeping-intelligence support is required at each step.

7.9 Peacekeeping-Intelligence Staff Considerations

The exact way in which the planning process will be followed will depend on the type of headquarters, the experience of the staff, time available, and the complexity and nature of the mission(s) being planned. The following are key considerations:

- **The MPKI cell is responsible for the peacekeeping-intelligence process.** Peacekeeping-intelligence staff must ensure that they own and control the PKI process, and that common assessments are used throughout the process and at every level of the mission.
- **The Chief of Staff (COS) will stipulate planning timelines.** It is imperative that the PKI staff meet key deadlines.
- **Concurrent activity** is essential to ensure coherent and constructive planning is conducted. This is assisted by clearly defined tasks for the [KI staff and ensuring that all roles and responsibilities are understood within the stipulated planning process.
- **The Human Factor/Human Terrain should be central to AOE.** Simply understanding the threat actors is not enough. PKI staff must understand in detail the human factors within the Area of Operations.
- **Use simple and clear products.** Overuse of text or images without explanation creates confusion. Ensure your PKI products are clear, concise and convey all the pertinent information that is required – they should ‘stand-alone’ and be understood by individuals with limited knowledge of the subject matter displayed.
- **Naming and referencing.** Make sure that all objects, routes, areas etc. are labelled and named correctly. This ensures clear understanding and removes confusion (e.g., spelling of place names and individuals) and assists with effective IM – see Chapter 11.
- **Peacekeeping-intelligence support does not end after the Phase 1 brief.** MPKI staff engagement is essential at all stages of the planning process.
- **Understand what products are required.** MPKI staff should revise and review products which support the MDMP. These include:
  - Key judgements and assessments.

- Human terrain overlays.
- Geographic overlays.
- Actors' course(s) of action – most likely and most dangerous.
- Force IAP and RFIs/IRs.

- **AOE does not stop.** Despite the concerted effort in supporting the MDMP, the MPKI branch should be mindful that there is a consistent requirement to understand the OE through ceaseless analysis outside those tasks that are required to support the wider staff.

7.10 The UN Military Decision Making Process

The UN MDMP is outlined below.

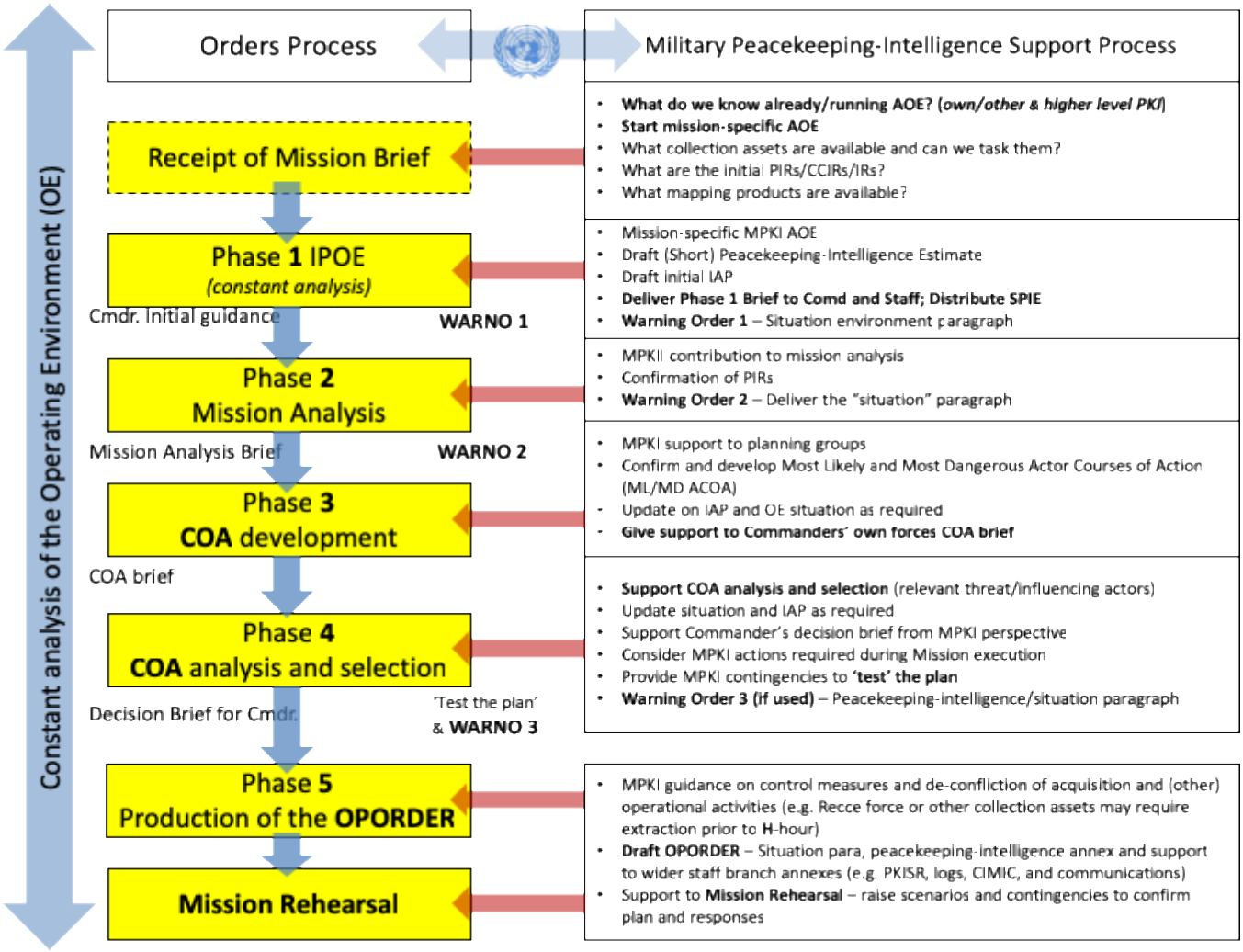


Figure 25: UN Military Decision Making Process

7.10.1 **Receipt of Mission Brief (ROMB).** The ROMB is conducted at the start of the MDMP and should not last more than 30 minutes. It is unlikely that the MPKI branch will have all the information or detailed analysis at hand, but they should brief the following key/critical information:

- The physical OE in general terms.
- The human terrain in general.
- The threat actors in general.
- The acquisition assets that are available.
- The initial PIRs.

- Current MPKI branch focus.
- The mapping that is currently available to planning the staff (with assistance from GIS).

7.10.2 **Phase 1 –AOE.** MPKI staff are not to confuse this effort with the wider AOE. The focus of Phase 1 – AOE is to provide PKI that is **mission-specific.** This will involve the conduct of analysis of a smaller part (e.g., region, town, village, compound etc.) where the mission is to be conducted. This is to be formulated into a brief to the Commander and their Planning Team. This brief sets the understanding of the Commander and Staff and underpins all steps of the MDMP. The format of the **Phase 1 Brief** is at Annex A to this Chapter. It also includes the production of a PIE (see 10.3.5). The AOE ensures the production of key graphical products representing the human, physical and information domains and actors (as detailed in Chapter 9).

7.10.3 **PIE.** The PIE is a tool that provides a structure for the conduct of analysis. It provides key deductions, through the considered examination of all known factors, to increase the understanding of decision-makers using the three-column format (3CF). Whenever there is time, the PIE is conducted in conjunction with AOE, adding more analytical rigour in certain areas. Outputs from both AOE and the PIE are combined and briefed in the Phase 1 Brief.

Factor	**Deduction**	**Output**
Example: Seasonal Weather	The mission will be conducted during the wet season and the roads and rivers may be impassable.	RFI: What are the known historical river levels in previous wet seasons and how did they affect bridging and other crossing sites? Task: S4/G4 to prepare bridging assets for upcoming operation.

Table 13: Example 3CF

7.10.4 **Draft initial Force IAP.** The Force IAP is detailed in Annex B to Chapter 5.

7.10.5 **Commander's Initial Guidance.** At this stage, Commanders will provide their initial direction to the planning staff. The COS will likely initiate the subsequent planning activity including the annotation of the amended planning timeline and planning teams (if more than one has been directed by the Commander).

7.10.6 **Warning Order 1 (WARNO).** The WARNO allows subordinate units to initiate their planning processes based on the current information provided by the Higher Headquarters. WARNO 1 is the first in the MDMP and includes the Commander's initial direction after AOE and what he/she has been ordered to do. **MPKI staff provide the Situation paragraph**. The WARNO Format is at Annex B to this Chapter.

7.10.7 **Phase 2 – Mission Analysis.** This is the domain of Commanders and their key planning staff – which should include MPKI representation. For each mission, the Commander will ask four key questions:

- **What is my Higher Commander's intent?** This question focusses the headquarters on the intent of commanders at the next two levels up and seeks to understand their objectives, outcomes and main effort to ensure that actions taken at one's own level are consistent with that intent.
- **What are the specified and implied tasks?** Commanders and their planning staff will identify the specified and implied tasks. Specified tasks are actions/effects that a Commander has been ordered to do. Implied tasks are those unstated activities which must be carried out in order to complete the specified tasks.

- **What are my freedoms and constraints?** A commander must assume that they have freedom of action unless it is stipulated that they are not to do something. Freedoms and constraints can include considerations due to time, space, legal issues, and resources.
- **Has the situation changed, and in so doing, has it influenced my mission?** Commanders will need to assess whether the situation has changed sufficiently that they must re-visit their estimate.

In conducting Mission Analysis, Commanders and their planning team will identify risks to the plan. These risks must be recorded for the Commander to mitigate or accept at a later stage in the MDMP.

7.10.8 **WARNO 2.** WARNO 2 provides an update to subordinate units and highlights any key changes in their missions, tasks, associated CONOPS and coordinating instructions. This is typically an updated version of WARNO 1. **MPKI staff will provide the situation paragraph and support the wider staff in completing their relevant sections.**

7.10.9 **Commander's Mission Analysis Brief**. The Commander will now state their likely missions and tasks. This will enable the staff to understand the Commander's thinking and then work together on relevant planning teams to develop potential COAs during Phase 3 – COA Development. **During this phase the Commander's PIRs will be developed and refined.**

7.10.10 **Phase 3 – COA Development.** The respective planning teams (if there are more than one) will be working up possible COAs following the Commander's Mission Analysis Brief. MPKI staff will provide PKI support to the planning groups, including the confirmation of Actors' COAs, providing any updates should any PIRs be answered or if the current situation has changed. MPKI staff will also continue to update the Force IAP and AOE as required. This updated PKI picture and 'testing' of the potential COAs will inform planning and shape the Commander's COA Brief.

7.10.11 **Phase 4 – COA Analysis and Selection.** Commanders, supported by their staff, will analyse each of the COAs produced by the planning staff. MPKI staff may be used to providing relevant actor- (including threat actor) assessed actions working through the CoA analysis. The impact of each COA on men, women, boys and girls should be analysed to assist with COA selection. This will assist in enabling the Commander to choose the most effective COA in achieving the mission.

7.10.12 **Commander's Decision Brief.** Upon hearing the COA briefs from the respective planning groups, Commanders will decide on which COA will be chosen. They may combine elements of two or more COAs, in which case the COA development will be re-started but with much of the planning work already done. MPKI staff should consider PKI activities required in support of the chosen COA and provide PKI guidance to mitigate and plan for contingencies. At this stage, the IAP will be updated.

7.10.13 **WARNO 3.** WARNO 3 is the final WARNO to subordinate units and highlights any key changes from WARNO 2. **MPKI staff are to provide the situation paragraph and support the wider staff in completing their relevant sections.**

7.10.14 **Phase 5 – Production of the Operations Order.** In addition to providing the Situation, Ground and Actors paragraphs and PKI annex, the MPKI staff should provide guidance to the Commander and planning staff regarding control measures and de-confliction of acquisition and operational activity such as the extraction of an acquisition asset prior to/on H-Hour. There should also be MPKI liaison with the wider staff functions to support the logistic, PKISR and communication paragraphs.

7.10.15 **Mission Rehearsal.** The role of the MPKI staff during mission rehearsal is to raise realistic/testing scenarios involving the physical, information and human terrain in order to confirm the plan and that the contingencies are viable.

INFORMATION MANAGEMENT (IM)

7.11 Why IM?

IM is a key element for effective PKI delivery. It provides an enduring base of accessible knowledge that enhances PKI processing and mitigates the information anarchy, which occurs in an environment with an increasing number of information sources. Effective IM ensures that knowledge gained is retained both during a tour and when one UN Unit hands over to the next.

7.12 IM Definition

IM relies on the effective organization of information: the acquisition of information from one or more sources, the custodianship and the distribution of that information to those who need it, and its ultimate disposition through archiving or deletion.

7.13 IM Responsibilities

IM is a systematic function that requires patience, consistency, and attention to detail. PKI IM responsibilities include:

- Drafting of IM SOPs for the respective missions.
- Ensure electronic logging, filing, and distribution of all reporting.
- Monitor all relevant IT inboxes and other sources of information.
- Lead on dissemination of reporting.
- Ensure PKI reporting (threat reporting, INTSUMs, INTREPs, PICINTSUMs etc) are received and sent on time and in the correct format from subordinate units, where applicable.
- Ensure that IT, documents and electronic media security protocols are complied with.
- General office administration tasks.

7.14 IM Basics

All PKI practitioners should adhere to the following IM basics:

- **Label peacekeeping-intelligence products correctly.** All MPKI products should have a unique file reference and date. Make sure this is applied to all photography, imagery, video and other media in addition to text documents. This will allow for easier storage, reference and recovery and greatly assists with version control.
- **UN standards.** All MPKI staff must adhere to agreed UN standards and SOPs regarding IM such as file naming conventions and the protection of information. All data is to be gender- and age-disaggregated.
- **Save emails.** Save important emails that have been sent and received rather than deleting them or leaving them in inboxes.
- **Maintain peacekeeping-intelligence distribution lists.** Ensure that all distribution lists for all PKI products are up-to-date and accurate.
- **Standardize names, including file naming.** A standardized list of agreed names and naming conventions for places and people is essential for effective IM and data-basing.
- **Archive and back-up.** Archiving files that are not used frequently on a regular basis is good practice. In addition, the backing-up of files mitigates the effect of lost files.

7.15 Databases

An effective PKI database is an important tool. MPKI staff should start one as soon as an operation commences and coordinate with other stakeholders to ensure that any mission-wide databases and resources such as Unite Aware SAGE and SharePoint sites, if implemented, are utilized. In its simplest form, this can be a collated and cross-referenced log of PKI reports. Peacekeeping-Intelligence Database Management should include:

- Establishing an overall database that allows information to be inputted and retrieved.
- Maintaining the database and checking inputted material for consistency and accuracy.
- Ensuring that information on the database is accessible as possible using security caveats.

7.16 Report Dissemination

One of the most important functions of an Acquisition/IRs Manager is to ensure that all relevant information is disseminated to the relevant client at the right time. This is particularly the case with threat reporting and I&W but applies to all PKI. Handling the dissemination effectively requires experienced oversight and collation of incoming reporting, with the experience to understand who needs to see what elements of information. Mandatory reporting requirements for human rights abuses, humanitarian law breaches and incidents of CRSV, trafficking, and grave violations against children shall be adhered to.

7.17 Checklists

Effective IM involves the repetition of similar actions on a regular basis to provide a disciplined information environment. To ensure that procedures are followed effectively, and all necessary activity is carried out, IMs should prepare a checklist of actions that need to be completed to ensure that nothing is forgotten.

SECURITY OF MPKI

7.18 Security Foundation for UN Operations

Effective security is an essential pre-requisite for success on operations. Protection of UN personnel, information, assets and installations is fundamental. Any security breach of official or protectively marked material or information, whether deliberate or unintentional, undermines operational effectiveness and poses a clear risk to life.

Aim. This supplement provides supporting guidance to commanders, and those filling security appointments, with respect to security on peacekeeping operations.

7.19 UN Security Policy

The UN has several organizations overseeing the provision of security direction, guidance and equipment to UN missions. Whilst the following headings will provide some key considerations, MPKI staff should be aware of and conform with relevant UN security policy and should have a detailed understanding of all security polices and SOPs relevant to their specific Mission. If there is any doubt on such policy, it is necessary to get clarification from the local security officer.

7.20 Personnel Security

Personnel security is a collection of measures that ensure those who have access to vitally important UN assets have a level of reliability and integrity commensurate with those assets. This includes the vetting or security screening of UN employees and the protection of personnel from external threats. This is a UNDSS task, but among the measures available to achieve an effective personnel security system are:

- Thorough enquiries into identity, integrity and nationality before recruitment/employment.
- Security vetting.

- Supervision of personnel.
- A system of reporting security concerns.

Security Vetting. Security vetting is mandatory for all personnel in an area where a security plan is in effect. All security clearances must be directed to the Designated Official for the respective mission. Enhanced security vetting is advised for the following positions:

- Arms/Ammunition Custodians.
- Communications Systems Custodians/Engineers.
- Protective Material Documents Clerks /Information Managers/Information Security Officers.
- Peacekeeping-Intelligence Personnel.

Screening/vetting checks should be mandatory to establish identities and biographical information of locally employed civilians (LECs) and locally recruited workers (LRWs) working/living within UN locations. All individuals selected for civilian employment on UN locations should be subjected to a security screening interview arranged through the local security staff and their details held on a database. It must be noted that screening does not provide the same level of assurance as detailed vetting; however, it does serve as a deterrent.

7.21 Physical Security

Every location must take responsibility for its security. A number of attacks have happened against UN bases that resulted in the loss of life. Strong physical security measures can deter attacks from happening in the first instance and can mitigate effects if they do happen. UN security staff under the UN Security Management System are available to provide advice and carry out security surveys of base locations. However, military commanders also have responsibilities for the physical security of their bases. MPKI staff can assist the Commander in a number of ways including assessments of the likely nature of threats against which the Commander should plan physical measures. The following should be considered by the Commander upon arrival in a new base/Mission location.

- **Perimeter security.** The function of perimeter security is to provide a degree of physical and psychological deterrence to intrusion. The effectiveness of a perimeter can be increased by:
  - Static and mobile surveillance by members of a guard force, e.g., from sentry positions and security patrols.
  - The provision of security lighting.
  - An alarm system.
  - Other surveillance systems such as remote cameras or Closed-Circuit Television (CCTV).
  - Regular integrity checks.
  - Removal of vegetation, refuse and building waste to improve field of vision.
  - Provision of ‘sterile’ cleared zones either side of the perimeter.
- **Control of access.** Establishments should have a control of access system; where possible, they should include a pass system.
- **Searches.** LECs/LRWs should be subject to searches on entry/exit to UN base locations for prohibited items such as weapons, explosives, ammunition and electronic devices.
- **Guarding and Patrolling.** The main duties of a guard force are to deter unauthorized access and to respond to any incursion/security incident. Additionally, they should provide:
  - Supervision of all arrivals to the site.
  - Control and issue of keys and passes.

- Inspect and check perimeter security, communications and perimeter lighting where applicable.
- Internal patrols.
- External patrols to present a high-profile presence to act as deterrent.

- **Security of Arms and Ammunition.** When not in use, arms, ammunition and explosives should be stored in one of the following as advised by UN security staff:
  - Armouries, ammunition and explosive stores that have been approved by UN security staff.
  - Under permanent supervision within a permanently manned location such as a guard post.
  - In the constant care of the individual to whom the weapon and ammunition has been issued.
- **Security of Protectively Marked Equipment/Assets.** All Protectively Marked Equipment/Assets identified during the Security Risk Assessment are to be protected in accordance with the direction given for that specific base location.

7.22 Information Security

7.22.1 The aim of information security is to protect information and material within UN locations. Threat actors will look to acquire information on aspects of UN activity listed below:

- Future UN intentions.
- UN operational plans and activities.
- UN command, control, and communications.
- UN strengths and dispositions.
- UN locations.
- UN equipment and capabilities.

7.22.2 Threat actors will look to exploit the following sources of information:

- **Surveillance and reconnaissance.** Every Unit must recognize that threat actors will seek to gather information through direct observation from the ground and air assets (such as UAS); this may include peacekeeping-intelligence gained from Locally Employed Civilians (LECs), Locally Recruited Workers (LRWs) and Third Country Nationals (TCNs).
- **Radio and line communications** through signals intercepted, including landline and mobile telephones and internet cables.
- **Loose talk** through overheard conversations.
- **Civilians** including interpreters who are in the operating area.

7.22.3 Information sensitivity, classification and handling is outlined in ST/SGB/2007/6 (as referenced below) and the Information Sensitivity Toolkit (2010).

- **Sensitive information** shall include:
  - Documents whose disclosure is likely to endanger the safety or security of any individual.
  - Documents whose disclosure is likely to endanger the security of Member States or prejudice the security of proper conduct of any operation or activity of the UN, including any of its PKO.
- **Classification levels** are used to identify information as ‘unclassified’, ‘confidential or ‘strictly confidential’.

- **Unclassified** shall apply to information or material whose unauthorized disclosure could reasonably be expected not to cause damage to the work of the UN.
- **Confidential** applies to information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of the UN.
- **Strictly confidential** applies to information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work of the UN.

- **Information Handling** requires the application of several processes including:
  - **Accounting and control** of classified information received/produced. This is paramount to effective security. Originators and recipients should maintain a record of the movement of classified information and material within and external to their respective organization. This includes the continued storage or destruction of this classified information or material.
  - **Loss or compromise.** The following actions should be taken within the respective unit location:
    - Thorough search to be made to ensure a simple handling error has not been made.
    - The suspected loss or compromise should be reported to UN security staff immediately.
    - The unit should initiate a security investigation directed by UN security staff.
  - **Downgrading of sensitive information** is to be conducted periodically. Documents may only be downgraded by the person/post/appointment from whom the document originated.
  - **Storage of sensitive documents and material** should meet the standards stated by the UN security staff within the location Security Plan. Advice is to be sought from UN security staff should location-specific security advice be required.
  - **Destruction of sensitive information or material.** All strictly confidential information and material should be shredded or placed in burn bags and stored in a security container or locked room where it cannot be accessed by unauthorized personnel. Destruction is to be recorded in the documents log and is to be certified by two authorized personnel.
  - **Carriage and dispatch of sensitive information.** Strictly confidential information and material may only be carried by authorized personnel as endorsed by UN security personnel. Every effort should be made to pass information electronically over secure means. When required, items should be delivered by hand with the envelope clearly stating the security classification of the information or material contained and signed by an authorized person; in addition, both receiving and sending parties should receive a receipt of delivery.

7.22.4 Need to Know and Need to Share Principles. UN personnel are to be aware of the 'Need to Know' principle and ensure that when discussing sensitive information with another individual, that individual has both the adequate security clearance and requires the information to carry out their duties. These discussions should not take place within the vicinity of those who do not have a 'Need to Know', irrespective of their level of security clearance. This approach is linked to the 'Need to Share' approach, ensuring that information is shared with relevant individuals, formations, and entities. This in turn requires, with the appropriate level of authority, to exercise judgement and make decisions about what to release, to whom and how. This part of the process is called **'Write for Release'**. It requires the owners of the information to:

- Make a conscious decision about what the external entity requires to know.
- Determine what information can be passed on.

- Construct that information in the most appropriate format whilst minimizing the potential for negative impact.

7.23 Reports

Security incidents and investigations must be reported to UN security personnel in accordance with UN Field Security Handbook and UN Security Management System protocols. Staff should make themselves familiar with actions to be taken in the event of a security incident. Reporting templates and submission timelines are stipulated in Chapter 4, Section X to the United Nations Security Management System Security Policy Manual and Annex Q to the United Nations Field Security Handbook.

7.24 Security Awareness, Education and Training

Units or individuals preparing for operations are required to conduct security awareness training. Those filling security positions are to ensure that they have completed the requisite UN security courses and education prior to filling their roles.

7.24.1 **Pre-deployment training** should include as a minimum:

- Description of the threat within the respective OE, including:
  - Local threat environment.
  - Key security vulnerabilities.
  - Security responsibilities and awareness.
- Security of bases and access control.
- Security of arms, ammunition and explosives.
- Security of information.
- Personnel security.

7.24.2 **In-Theatre training** is normally conducted where an individual has not received the requisite pre-deployment training or, where the security situation has evolved, and additional training is required to inform the deployed personnel. This training is to be conducted by UN security staff in accordance with the local Security Plan as directed by the Designated Official.

7.24.3 **Proactive approach.** All personnel are to have the moral courage to confront security issues no matter who is responsible. Transgressors may not know that what they are doing is wrong and informal advice before an incident occurs is much better than a formal investigation afterwards. Security incidents can cause loss of life; even less serious incidents can be damaging to the UN's mission, credibility, and reputation. A proactive approach is required to ensure that security is never neglected during operations.

7.25 Annexes

A. Suggested MPKI Structures (Force, Sector and Battalion Headquarter Structures)

B. Force ISP template

C. Example Phase 1 Brief.

D. Example WARNO Template.

E. MPKI IM – Tactical Aide

F. MPKI Threat Analysis Worksheet

PEACEKEEPING-INTELLIGENCE DIRECTION CASE STUDY - Example of an IAP

PIR	SIR	INDICATORS	ACQUIRING UNIT					NAI	NLT	LTIOV
			A Coy	B Coy	C Coy	Recce	UN Ob			
1. What are the threats to the local population?	1.1 What armed groups operate in the area^ **MC** 1.2 What is the attitude of armed groups to the local population. **ME** 1.3 What is the attitude of the local population to the armed groups. **ME** 1.4. What non-military threats affect the local population. **ME**	Ground sign of Armed Groups close to population in Area X Armed men in areas occupied by subject population. Population displays fear/no fear of Armed Groups in Area X Disease present in Area X Weather impact in Area X Signs of hunger or significant need in Area X	*X*	*X*	*X*	*X*	*RFI*	*NAI 1, 3, 6** *NAI 3, 6, 8* *NAI 1,2, 3*	*10 Sep 2018*	*12 Sep 18*
	PIR: Priority peacekeeping-intelligence requirement SIR: Specific Peacekeeping-intelligence requirement Priority: Mission Critical (MC) NLT: Not later than RFI: Request for Information. Mission Essential (ME) NAI: Named area of interest LTIOV: Last time information of value Mission Desirable (MD)									

Table 1: Example of an IAP

^ A column to the right should be added if the MPKI cell feels that the SIR is too broad and cannot be answered with just one type of question. Please see para 5.4.7 above for further guidance.

*Each NAI should correspond to an area in the APIR and should be visually represented on a Decision Support Overlay

RFI FORMAT

Classification: UN CONFIDENTIAL		**Priority:** Immediate
Serial	**UN MISSION TITLE RFI 001/00**	
1	SUBJECT OF RFI	A general statement of the subject of the RFI
2	Date/Time Group Requested	The Date Time Group (DTG) of the request
3	DTG Required	The latest DTG after which the information will be of little value
4	STATEMENT OF REQUIREMENT	In as much detail as possible, clearly state the nature of the requirement
5	REMARKS	Any amplifying remarks that will assist in clarifying the request
6	SECURITY CLASSIFICATION	Indicate the desired security classification
7	POINT OF CONTACT	Identify (by name and contact number) who is the originator / responsible for handling the RFI
METHOD OF TRANSMISSION: The format in which you want the RFI to be produced.		

Table 2: RFI Format

GENDER EARLY WARNING INDICATORS

All gender early warning indicators should be recorded using age and gender-disaggregated data.

Listed below are some examples of early warning indicators focusing on gender issues.

- Increased incidence of people having to pay for additional security.
- Women notice new actors in their community.
- An influx of money into the community.
- Children are not attending school.
- In a departure from the norm, women and children avoid public areas.
- The placement of a military base/encampment in close proximity to schools, water-points, markets, Internally Displaced People (IDP)/refugee camps and other civilian centres, particularly those frequented by women and girls (Conflict-Related Sexual Gender-based Violence).
- Indicators of women's empowerment:
  - Ratio of men/women in power
  - Average level of women's education
- Indicators of gender norms:
  - Adoption of restrictive laws for women
  - Reward for aggressive behaviour
  - Change in legislation with regards to women's security
- Indicators of gender-based violence
  - Prevalence of female genital mutilation
  - Incidents of domestic violence (at gun point)

The following is an early warning indicator matrix that was developed after being called for by the UN Secretary-General's Policy Committee in December 2010 (Decision No. 2010/30).

The indicators are spread across six pillars, namely military/security; social/humanitarian; political/legal; economic; media-related and health that are not meant to be all inclusive. It is vital to read the indicators in conjunction with the relevant contextual factors provided in the matrix.

Early warning indicators in this matrix are broken into three categories: Potential Risk, Impending Risk, and Ongoing Sexual Violence.

Contextual Factors for Military/Security Indicators	Potential Risk *	Impending Risk **	Ongoing Sexual Violence ***
	Parties/armed groups rely on conscription, abduction or other forms of **forced recruitment**, which increases likelihood of using sexual violence, particularly gang-rape, as a mechanism	Widespread **looting** by armed forces/groups due to lack of supplies or other grievances (Fizi, DRC, 2011).	Observable **signs of rampage**: burned homes, destroyed crops, looted villages, torn clothing, torn mattresses, displaced

	to enhance group bonding and cohesion (RUF in Sierra Leone, 1999). Armed groups reward or otherwise indoctrinate aggressive, hyper-masculine behaviour and/or espouse a **military code or ideology that supports violence** **against women** of opposing communities to alter ethnic identity, humiliate, undermine enemy morale, fragment or eliminate future generations of the target group (e.g., belief that forced impregnation can alter ethnic balance, Former Yugoslavia, 1990s; *Interahamwe Ten Commandments*, Rwanda, 1994; belief that rape bestows powers upon fighters, Mai-Mai elements, E. DRC). Combatants operate under the **influence of alcohol and drugs** (Liberian civil war; E. DRC; E. Chad). Flare-up of remuneration **disputes and other frustrations in army**, when typically vented through drug and alcohol abuse and exactions against civilians (Fizi, E. DRC, 2011). Arms bearers undertake **house raids and searches**, particularly where women are alone in the home (Afghanistan; Iraq; Somalia). Placement of military bases/encampments near	Militias **ambushing vehicles** and attacking women/girl passengers (W. Côte d'Ivoire, 2011). Ex-militias, particularly from groups with a history of sexual violence, recently integrated into armed forces **abscond/desert with their arms** (Fizi, DRC, 2011). Withdrawal/rotation of army, police or peacekeeping presence from an area, leaving a **security vacuum** (Walikale, DRC, 2011). **Infiltration** of refugees, displaced and/or transit camps by arms bearers (DRC; Sierra Leone; E. Chad). Heightened perception of physical insecurity among women and girls following the **reinsertion of ex-combatants into communities** without debrief or follow-up as part of DDR, or due to incomplete disarmament and demobilization (DRC; Liberia). Rest periods/intervals in hostilities during which armed actors **enter population centres**, particularly those devoid of men owing to the circumstances of conflict. Military acts of **revenge/victory**,	women/civilians (Walikale, DRC, 2010) Armed elements engage in violent **reprisals** against civilians in the wake of military operations (after Kimia II, DRC, 2009) **Police reports** of increased sexual violence (noting that increased reporting may signal increased confidence in the authorities/improved safety conditions). Military **defeat and retreat** through an area, increasing likelihood of rape and pillage as a form of „scorched earth" policy (movement of the Interahamwe from Rwanda to E. DRC, 1994) Reports of sexual violence/torture emerging from detention settings/internment/POW camps, often as part of **interrogation or punishment** (Iraq; Libya; Bosnia). Women/girls/boys **recruited and retained** within armed group by coercion (Angola; Uganda; Sierra Leone). Increased reports of a practice of **abducting** women/girls to serve as porters or possible „bush wives" (LRA, Central Africa). Attacks on villages to **replenish supplies**/on farmers en route to fields or

	schools, water-points, markets, IDP/refugee camps and other civilian centres, particularly those frequented by women and girls (E. DRC; South Sudan). **Retaliatory attacks** against the civilian population for perceived support of/collaboration with the „enemy" (Bushani, E. DRC, 2011). Exposure of forces to **pornography, particularly in military spaces** like barracks or vehicles (Serbian tanks, 1990s; Guinea-Conakry, 2009; pornographic depictions of Tutsi women and Belgian forces to set the stage for genocide in Rwanda). Individuals subjected to **security inspection** by members of a different sex at **military checkpoints** (Israel and the Occupied Palestinian Territory)	particularly during the closing stages of a conflict when cities/villages are populated mainly by women and children (Sri Lanka, 2010; Berlin, Germany, end of WWII). Soldiers **not paid, provisioned and/or cantoned** in barracks, increasing the likelihood of preying upon civilians (DRC). **Equipping of forces** to perpetrate sexual violence (supplying condoms/Viagra, as alleged in Libya, 2011; mass supply of condoms to troops in occupied territory during WWII). Women in **detention** held under the immediate supervision of male, rather than female, guards and mixed with male inmates (mass rape, Goma prison, DRC, 2009).	women returning from market, coupled with abduction of civilians to carry the stolen goods (LRA, Orientale Province, DRC, 2011). Women/girls fleeing village/area where armed elements are stationed.

Table 3: Early Warning Indicators

MPKI ANALYSIS WORKING FILES

The MPKI worksheet and the annotated maps serve to isolate problem areas and formulate relationships between items of information acquired. Extensive research material is required, however, to analyse these problem areas.

Extensive working files, such as the threat analysis worksheet, hot files, current propaganda file, personality and organization files, area study files and resource reference files might need to be established and maintained.

Activities Matrix. An activities matrix is used to determine connections/associations between an individual and organizations, events, locations, or activities (excluding other individuals).

Annotated Maps. Depending on the echelon of responsibility, the threat actors' activity in the area, and their degree of knowledge, MPKI analysis requires at least two annotated maps: the **incident map** and the **threat Situation Map**. Each of these recording devices normally is a transparent overlay covering a large-scale topographic map of the area.

Unlike the **peacekeeping-intelligence workbook**, which is maintained for individual use, the incident and threat Situation Maps (SITMAP) provide a ready guide for briefing the Commander, higher UN authorities, or, as required, other interested parties.

If activity in an area is limited, consideration is given to the combination of the two maps. Other annotated maps are valuable aids for recording information, depending on the needs in a headquarters' tactical area of responsibility. These special purpose overlays include, but are not limited to, records of:

- Mining and booby trap incidents.
- Key threat actors' names or codes for local terrain features, such as villages, areas, trails, etc.
- Threat actors' assassination or resource acquisition attempts.
- Other significant activity.

It may be necessary to enlarge, with significant detail, certain areas of interest, either by drawing portions of the map to a larger scale, or by making a mosaic from aerial photos. Past, present, and potential threat actors' activity must be visible with a detailed and thorough understanding of the environment. Comparison of the several annotated maps maintained, often assists the MPKI analyst in estimating the threat actors' intentions and capabilities or to establish trends.

Incident Map. The incident map or overlay provides historical cumulative information on trends and patterns of threat actors' activity. Properly maintained, the entries enable the MPKI analyst to make judgments about the nature and location of threat actors' targets, the relative intensity of their interest in specific areas, their control over or support from the population, and their potential AORs. Judgments concerning threat actors' operations also require knowledge of terrain factors and threat actors' own limitations.

Situation Map. In peacekeeping, the SITMAP or overlay is to be prepared as part of the AOE process and is modified as necessary by information from the incident map. It is difficult to pinpoint the threat actor's installations and dispositions with the same degree of confidence as in a conventional tactical situation. Unconventional threat actors can displace on short notice, making a report outdated before it is confirmed. While the SITMAP presents an uncertain and hypothetical picture, composed less of firm information than of reports of fleeting targets, estimates and abstractions, it graphically substantiates the trends or patterns derived from the incident map. The MPKI analyst can then improve the economy and effectiveness of the reconnaissance and surveillance effort.

Trap Map. In peacekeeping, the Trap Map or overlay is used when the threat actors have a capability for sabotage or terrorist action. Data must be directly annotated on the map on which the situation overlay is placed, or it can be kept separately. This map portrays particularly attractive target locations for the threat actors' sabotage or terrorism, such as UN installations, refugee/IDP camps, road and railroad bridges, and places where the terrain favours ambushes and raids. Such areas are to be identified and analysed as part of the area study. They are plainly marked on this map with attention directed to possible Threat actors' access and escape routes. Photographs which are keyed to the map also supplement this effort.

Population Status Map. This consists simply of an overlay to the SITMAP. Essentially, this map portrays the attitudes of the population to the UN peacekeeping Force and to the threat actors. Different colours are to be used to designate these conditions.

Personalities and Contacts Map. What is known initially about the threat actors' situation primarily is information concerning locations and activities of key leaders, individual enablers, organization, and liaison. The appearances, movements, meetings, and disappearances of these individuals are recorded on a Personalities and Contacts map/overlay. A large-scale map is required (a city street map or town plan if an urban area is involved). Deviations from regular patterns of movement are detected in this manner.

Depending upon the number of individuals under surveillance, the regularity of their habits, and the variety of reports acquired/received on them, it is necessary to maintain a separate overlay for each subject. Old overlays are filed for comparison. Each agent's route is portrayed in a different colour, and regularly travelled routes distinguished from new routes. Observations are dated and incidents noted by symbol. Depending upon the amount of activity, this map is combined with the incident map.

Area Study Files. Area study files contain up-to-date and pertinent data in the geographic, political, sociological, economic, and cultural fields and may consist of a wide PMESII document. In peacekeeping operations, tactical and operational commanders, particularly when operating in the same general operational area over extended periods of time, have a definite requirement for such information.

Coordinate Register. The coordinate register is a valuable analytical tool, and method to store information during peacekeeping operations. It illustrates activity in an area over a period of time. Each page represents a specific geographic area or town that the S/G/U2 determined. The coordinate register has two types of pages. One has written entries to record threat activities with space for the S/G/U2 to add comments.

Civil-Military Operations File. A civil-military operations file includes all material and information concerning civil-military operations, their results, effectiveness and any countermeasures the threat actors take.

Current Information Operations (IO) File. If IO constitutes a major part of the threat actors' effort in the mission's AOR, a current counter-messaging file should contain all pertinent literature, background material, and analyses, to include copies of the threat actors' IO speeches and analyses of local grievances they exploit in their narrative.

Hot File. The hot file is the most important working file. It includes all available material pertaining to an incident or groups of possibly related incidents that are of current interest. This file contains material on persons or places likely to be involved in activities against the mandate of the UN peacekeeping force, together with material on agents or suspects who may be involved. A reported attack on a refugee/IDP camp, for example, could initiate a hot file. The hot file remains active until the report is refuted, the incident occurs, the attention of the armed group/militia is diverted elsewhere, or the conditions which allowed for such an attack have been addressed/mitigated.

Personality and Organization Files. A local file is maintained on each of the threat actors' key leaders. If surveillance is carried out by the local police, basic identifying and biographical information can be sought by MPKI officers to be transferred from police dossiers to a card file dossier. This card file helps train friendly surveillance to recognize key personalities on sight. The organization section of this file includes information on the history and the activities of the threat actors' organizational

charts, other suspected groups, and their leaders, overlapping directorates, memberships and liaison among these organizations.

Link Diagram. A link diagram graphically displays connections between individuals, organizations, and activities. It is created from information contained in the historical files and from information that is currently being reported. Analysts should use a link diagram whenever individuals, groups, group activities, or process networks are being reviewed for insight. The need for link diagrams increases with the increase in data and network complexity.

The MPKI analyst at unit and staff levels should, therefore, have ready/easy access to such data. The topical breakdown of such files concerns events and activities of continuing significance. Thus, for example, if rice/wheat is the basic staple in an economy, the topical breakdown includes files on their production, distribution and marketing, price levels, and black marketeering and pilferage activities. Since this key economic indicator has a continuing influence on local forces/militias that depend on this staple for survival, careful analysis of this data over a period provides patterns based on which the threat actor's actions might be anticipated and their capabilities predicted.

Reference Material. A library is maintained of reference publications, such as manuals on doctrine, tactics, and methods; books on the area and on the threat actors in the AOR; files of newspaper and magazine clippings; and any other useful material. This material is kept at a central library at the Battalion or the Sector/Force staff levels, to serve the MPKI analyst.

Threat Analysis Worksheet. The threat analysis worksheet helps identify information and peacekeeping-intelligence needed to satisfy the PIR and IR. It also provides a guide for analysis of a peacekeeping mission environment (see template).

The second type of coordinate register is visual. Entries are plotted on the overlay square as they appear on the incident map. The coordinate register assists in trend and pattern analysis and is a good way to store data, in an easily retrievable manner, for long periods of time. The written register allows easy evaluation of threat actors' activity by type of action while the visual one allows rapid comparisons of activity between several time periods.

PEACEKEEPING-INTELLIGENCE ANALYSIS DEFINITIONS

Abductive Reasoning

Describes the thought process that accompanies insight or intuition. When the information does not match what is expected, the analyst must determine the reason, thereby generating a new hypothesis that explains why the given evidence does not readily suggest a familiar explanation. Abductive reasoning will lead to the analyst looking at a situation to ask why the dynamic has changed, as well as to develop and test possible explanations.

Analogical Reasoning

A method of processing information that compares the similarities between new concepts and understood concepts; then those similarities are used to gain an understanding of the new concept.

Deductive Reasoning

Applies general rules to specific problems to arrive at conclusions. Analysts begin with a set of rules and use them as a basis for interpreting information. A deductive argument is sound if its premises are true. However, sound deductive reasoning does not mean the conclusions are true. Deduction should not be used in forecasting human behaviour.

Inductive Reasoning

An approach in which a drawn conclusion is based upon observed facts. It is a process of discovery in which an analyst establishes a relationship between events under observation or study. Induction normally precedes deduction and is the type of reasoning analysts are required to perform most frequently. It requires objectivity and the elimination of prejudices and preconceptions. The first step of inductive reasoning is reaching a conclusion formulated on facts gathered by direct observation. Inductive reasoning is dependent upon accurate observation and statistics. Tainted data negatively affects inductive reasoning; therefore, this reasoning cannot produce absolute truth, only very high probabilities.

X (Cross) **PMESII** – factors **ASCOPS** aspects	**P** Political	**M** (Military) Security including Police	**E** Economical	**S** Social	**I** Infra-structural	**I** Information incl. Cyber
A Areas	Political areas (District, Prov / Nat boundaries, enclaves, party affiliation areas) INS / (N)CAG / TAG shadow government influencing areas	(Semi)-military areas (Coalition / LN / AOR's, (historic) ambush and IED sites) Organizational areas, (N)CAG areas (UN(CT) bases, AOR's) Tribal areas,	Economic areas (Bazaars, shops, market places, livestock-, industrial-, black market- and mining areas, smuggling and trade routes)	Social areas (Refugee camps, ethnic-, social-, tribal-, clan enclaves, neighborhoods, boundaries of influence, markets, other popular places to gather)	Infra-structural areas (Commercial, industrial, residential, rural, urban, road systems, LLC, power grids, irrigation networks, water tables)	Information areas (broadcast coverage areas, word of mouth, gathering / meeting points and places, visual and audio comms)
S Structures	Political structures, (Provincial, district centres, meeting halls, polling sites, court houses, mobile courts and political related monuments)	Military / security / police buildings (Police HQ and military HQ locations) Other military and security structures	Economical structures (Banks, fuel distribution, industrial plants, warehousing, markets, storage facilities, farms, manufacturing)	Social structures (Clubs, jails, libraries, schools / universities, stadiums, bars and tea-shops, social gathering places, restaurants, coffee-shops)	Infra structures (Energy, medical, public buildings, transportation, waste distribution, construction sites)	Information (infra) structures (comms, WIFI and internet services, cellular (GSM) phone network, Postal and packet service, TV and radio stations, print)
C Capabilities	Political capabilities (Public administration, executive local leadership, INS / (N)CAG / TAG ability to have impact, judiciary capacity)	Military / Security capabilities (Security posture, decisive power, strengths and weaknesses)	Economical capabilities (Energy, imports – exports, external support, food aspects, market prices, raw material, inflation, black markets)	Social capabilities (Medical (traditional or modern), social networks academic, strength or weaknesses of tribal / AG / village traditional structures, judicial	(Construction, clean water, comms. systems, fire fighting, medical, sanitation, main roads, dams, irrigation & sewage, environmental)	Information capabilities (availability, indigenous networks, internet access, intelligence services, prints, propaganda mechanisms, Radio and TV, Social media)
O Organisations & capacities	Political Organizations (Political parties, INS / (N)CAG / TAG group, affiliations, Gov / NGO / UNCT organisations and other power-brokers, Court system)	Military / Security organizations and capacities (What units, personnel, material of police, military, LN, (N)CAG's are present	Economical org. and their capacities (banks, business orgs., labor units, large landholders, cooperatives, NGO)	Clans, comm. Councils and orgs. School councils, Criminal organizations, familial, patriotic / service orgs. Tribes.	Infra-structural orgs. and capacities (construction companies, government and contacters)	Information orgs. and capacities (media groups and news orgs. (N)CAG media orgs. Governments groups, PR and advertising agencies)
P People	Political People (Governors, councils, Tribal leaders, elders, clerics, judges, parliamentarians, prosecutors, UN key leaders)	Military / Security people (Key-leaders from coalition, LN and (N)CAG)	Economic related people (employers/employees, consumption patterns, unemployment rate, key actors, black marketers, criminal key-leaders and members)	Community leaders, councils and members, educators, key figures, language / dialect, vulnerable populations, DPRE's, Families, migration patterns)	Builders, infra-structural contactors, engineers, architects, local development councils	(Decision makers, media personalities, media groups and news orgs. Community leaders, elders, heads of families)
E Events – Days Remembrances	Political events (Elections, Tribal meetings, provincial council meetings, significant speeches)	Military / security events (kinetic events, fighter seasons, historical, loss of leadership, operations)	Drought, harvest, yields, domestic animals livestock, market cycles, illegal growth (drugs), labor migration effects, market days, loss of business.	Celebrations, civil disturbances, national holidays and observance days, weddings, birthdays, funerals, sports events, family gatherings.	Infra-structural related events (Scheduled maintenance LLC, natural man-made disaster effects, well digging, constructions)	Information related to events (Disruption of services, censorship, Publishing dates, inform and influence activities, project openings)

Peacekeeping-Intelligence Support to UN FOB protection

- Review the current situation in the context of likely future UN operational military activities.
- Undertake a detailed terrain analysis, per Chapter 9 guidelines, for ascertaining strength and weaknesses of camp security. MPKI personnel are to focus on the following:
  - Observation from and to the camp – what can we see, where is the dead ground, what can the adversary see?
  - Cover and concealment.
  - Avenues of approach.
  - KT features.
  - Physical security of the camp including fences, walls, guard towers.
  - Security of camp access and exit points such as gates.
  - Weather including visibility, temperature, first & last light and moon phases. It is also necessary to examine how the weather affects terrain to make it more or less passable.
- A detailed analysis of the Information terrain is also required:
  - Where are the communications blackspots, and what impact will that have on UN and threat actor activity?
  - What is the messaging of relevant actors in the AO in relation to the UN?
  - Is the media pro, anti, or neutral towards the UN?
  - Monitor all the above for changes.
  - In the current era, communication is of great importance and is aptly used by threat actor(s) for fulfilling their mission. Accordingly, it is very important for peacekeeping-intelligence personnel to ascertain how threat actors communicate and then work with U2 and the Force Commander to determine what to do with this information.
- Assessment of relevant threat actors/Human Terrain with special focus on the following:
  - Who?
    - Individuals and groups that are likely to threaten the base.
    - Focus on the strength, capabilities and intentions of these actors.
    - Identify how these threat actors have operated in the past.
    - What are their TTPs, and where is the UN vulnerable to them.
    - Identify local leaders and power centres of threat actors which warrant the special attention of the MPKI personnel.
- Ascertain the most vulnerable part of the camp through liaison with other staff members including Operations and Logistics branches.
- How will the threat actor manifest his/her activity? Ascertain the threat actors' courses of action along with their possibility of materialisation.
- Analyse the pattern of attacks in the past to ascertain any patterns that might point to the likely nature and timings of a future attack. Undertake time-based analysis to ascertain the possibility of threat activities in relation with:
  - Timings: point in year / month / harvest / anniversary, etc.

    - Specific time within a day when threat actors are more likely to be active (dawn, dusk, cover of night).

- It is worth noting that threat actors often undertake activities on days of important and pronounced activities i.e., commemoration days, change of troops, national day(s), religious festivals and important events.
- Remember that with passage of time, most threat actors evolve. This means that what was true about their capabilities today, may not be true tomorrow. Continuous AE, as outlined in Chapter 9, is vital. For example, a threat actor may not deploy suicide bombers today but will that still be the case in six months; these questions need to be asked.

Peacekeeping-Intelligence Support to Patrol – Example

- Prior to any patrol leaving a UN base, the following information should be given to its leaders by MPKI staff:
- Recent and significant activity in the area of the patrol.
- New information pertaining to the area of the patrol, including new peacekeeping-intelligence reports.
- Detailed Terrain brief to include the following: obstacles to patrol; ideal avenues of approach to objective area; areas of cover and concealment, and how friendly and threat actors could use them; KT to both UN and threat actors; observation – what are the limits of UN observation, and what does this mean?
    - So what? What are the implications for the UN patrol? Where is it vulnerable, where is it canalised? Where will the patrol be forced to slow down?
- Detailed brief on Human Terrain: Identify locations of supportive and threat actors; Highlight the capability, intent and TTPs of threat actors; Identify locations of key leaders; identify areas likely to be supportive of and hostile to the UN.
    - So what? Tell the patrol what this means. Where, how and when is the patrol most likely to be targeted?
- Detailed brief on Information terrain. Where are the communications blackspots and what does this mean for the patrol and for threat actors?
- Detailed information on the specific threat actor. How is the threat actor likely to react to the patrol?
- Based on what we know about the threat actor, what are its most likely and most dangerous courses of action against the UN patrol?
- Take questions from the patrol leader.
- Outline IRs for the patrol, and key leaders that the patrol should engage with.
- Tell the patrol leaders that on the return of the patrol they must report to MPKI staff to be debriefed.

PEACEKEEPING-INTELLIGENCE REPORT (INTREP)

Purpose

Used to report information. The INTREP should provide information regarding incidents/events that could influence current or pending operations. Despite its name, it is not always a peacekeeping-intelligence product; information only becomes peacekeeping-intelligence after it has been fused with other information during the analysis phase.

Timings

An INTREP is sent without regard to a specific time schedule, whenever the peacekeeping-intelligence it contains is considered likely to require the urgent attention of the receiving commander or their staff.

Content

An INTREP is a report of incidents/events issued as soon as possible after their occurrence. It should include any information that may be relevant to the IRs of any commander to whom it is disseminated. It should include the issuing peacekeeping-intelligence analyst's assessment of the significance of the information.

Classification (Protective Marking)

An INTREP will be classified per content, either UN CONFIDENTIAL or UN STRICTLY CONFIDENTIAL.

Format

The report should include at a minimum a 5WH with possible reactions from own forces, namely:

- Who?
- What?
- Where?
- When?
- Why/How?
- Own CoA or response

Classification: UN CONFIDENTIAL		**Precedence:** IMMEDIATE.
SUBJ:	**INTREP 001/00 241200 C DEC 23**	
1	DETAILS	• Who • What • Where • When • Why/How • Own CoA or response
2	COMMENT	*The peacekeeping-intelligence analyst's deduction of the implications of the incident or event.*
ORIGINATOR: U2-G2-S2/UN Mission XX. **Releasing officer:**		

Table 18: INTREP Example

Two further points:

1. Proof of sending is not proof of receipt. INTREPs are used for important and urgent peacekeeping-intelligence, and thus it is the responsibility of the originator to ensure the recipients are aware of an INTREP they should read.

2. Where there is a credible threat to life that is time sensitive, the mitigating actions to prevent the threat must be passed as soon as possible by whatever means. Thus, it is possible to use a mobile phone to tell a person not to do action X. The details of why, the source, and the analysis should not be communicated over insecure means, but the action to be taken can and should be.

PEACEKEEPING-INTELLIGENCE SUMMARY (INTSUM)

Purpose

Used to periodically update units and HQ on military and related political, security, humanitarian and economic peacekeeping-intelligence assessments that give an indication of change in capabilities, activities, and intentions.

Timings

When appropriate.

Content

It should include any information that may be relevant to the IRs of any commander to whom it is disseminated. It should include an assessment of likely developments and/or threat actors' intentions.

Classification (Protective Marking)

An INTSUM will be classified per content; either as UN CONFIDENTIAL or UN STRICTLY CONFIDENTIAL.

Format

Classification: UN CONFIDENTIAL		**Precedence:** IMMEDIATE.
SUBJ:	**UN INTSUM 001/00 FROM 241200A DEC 23 TO 281200A DEC 23**	
1	HIGHLIGHTS	A synopsis of significant events and possible implications on the Mission and/or civilian population within the APIR within the reporting period.
2	THREAT ACTORS	Describes threat actor activity, capabilities, intentions and/or provides updated information for threat actor ORBAT records.
3	FORCE PROTECTION	A synopsis of events that impact, or may impact, the Mission's force protection. This should include CI-related events.
4	OPPOSITION TO COHA	A synopsis of events that demonstrate opposition to the implementation of the Cessation of Hostilities Agreement, whether intentional or inadvertent.
5	MISCELLANEOUS	A description of events/incidents affecting other factors such as the humanitarian situation, etc.
6	POLITICAL	A description of political events that may affect the mission.
7	UPCOMING EVENTS	Significant upcoming events (e.g., – public holidays, etc.)
8	ASSESSMENT	A synopsis of peacekeeping-intelligence concerns and an overall assessment.
ORIGINATOR: U2-G2-S2/UN Mission XX. **Releasing officer:**		

Table 19: INTSUM Example

PICTURE PEACEKEEPING-INTELLIGENCE SUMMARY (PICINTSUM)

Purpose

Used to verbally report essential elements of information that has already been processed into a PKI product. The PICINTSUM provides timely PKI regarding incidents/events that could influence current or pending operations.

Timings

A verbal presentation of a PICINTSUM is used without regard to a specific time schedule, but whenever the PKI it contains is considered likely to require the urgent attention of the receiving commander or their staff.

Content

A PICINTSUM is a presentation of incidents/events issued as soon as possible after their occurrence. It should include any information that may be relevant to the PIRs or CCIRs of any commander to whom it is presented. Furthermore, it should also include the issuing peacekeeping-intelligence analyst's assessment of the significance of the information.

Classification (Protective Marking)

An PICINTSUM will be classified per content, either UN CONFIDENTIAL or UN STRICTLY CONFIDENTIAL.

Format

The PICINTSUM should include:

- Map.
- Reported peacekeeping-intelligence related to the map.
- A Peacekeeping-Intelligence Assessment.

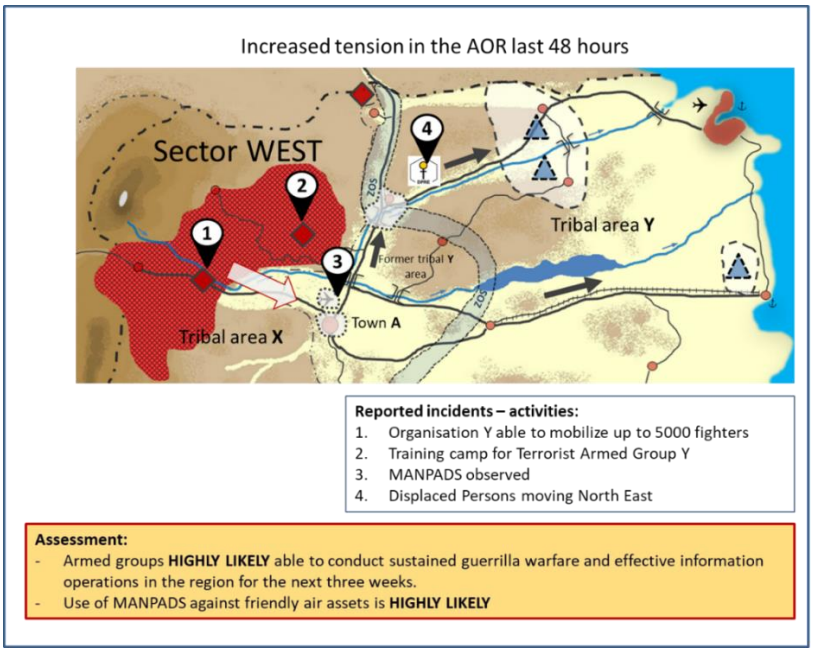


Figure 26: PICINTSUM Example

SUGGESTED MPKI STRUCTURES (FORCE, SECTOR, AND BATTALION HEADQUARTERS STRUCTURES)

U2 Branch Structure and Organization. The structure of the U2 Branch will vary from mission to mission but will always be part of the military component. The structure and staffing of the U2 cell will change according to the mission's mandate, the Status of Forces Agreement (SOFA) in place between the Host State and the UN, the information acquisition parameters as outlined in the Mission ISP, and according to the information acquisition capabilities within the Military Component.

In order to have a solid structure, the U2 cell should have a Chief U2, and the following: a command team (C2), an Information Requirements Management and Acquisition Management (IRM&AM) cell, current peacekeeping-intelligence section, plans section, Open Source Peacekeeping-Intelligence (OPKI) section, and production (analysis) cell. Depending on the available sensors and units in the mission, the U2 Branch may also include a PKISR cell, Geospatial/Imagery Peacekeeping-Intelligence (GPKI/IPKI) cell, Signals Peacekeeping-Intelligence (SPKI) cell, and/or Human Peacekeeping-Intelligence (HPKI) cell. The U2 acts as focal point to coordinate with other components and entities in the mission and may request support from UN headquarters when necessary. It is important to note that all personnel should have the rank and training commensurate with their roles and responsibilities.

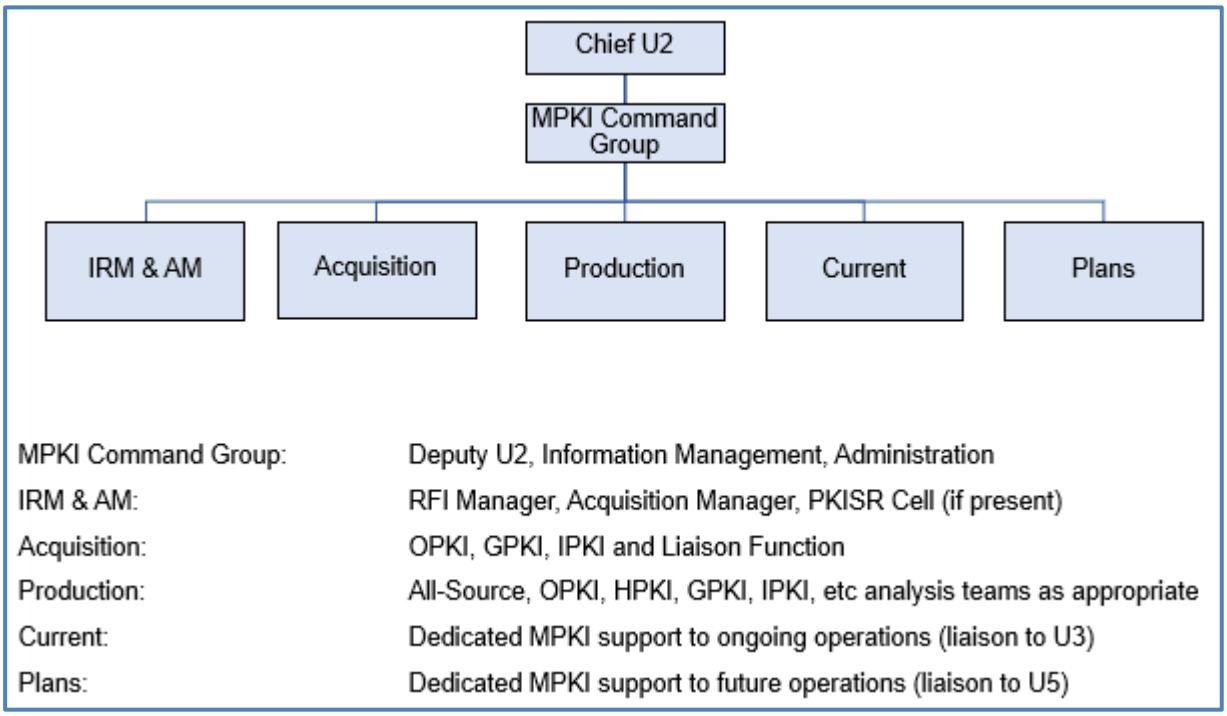


Figure 27: U2 Branch Structure and Organization

Roles and Responsibilities of the U2 Branch:

- Manages the MPKI Cycle, in line with the PKI Policy and MPKI Handbook, through the direction, acquisition, examination/collation, analysis and dissemination phases. This is to ensure that the Force Commander's decision-making process is fully supported with timely, succinct, and relevant PKI products.
- Ensures that its information acquisition activities are conducted in support of mission and force Priority and other IRs. To this end, the U2 cell will maintain a Force IAP that fully aligns with HoM and FHQ IRs. This will be regularly updated.
- Ensures that appropriate acquisition assets are tasked to acquire relevant information.
- Ensure that all incoming information is collated on a central database, and available to the relevant personnel.
- Maintains a source registry.
- Produces timely, relevant, concise, and predictive peacekeeping-intelligence products to support effective mandate implementation relating to the protection of UN personnel and civilians, and to enhance situational awareness, as required.
- Identifies relevant trends.
- Ensure that the Peacekeeping-Intelligence Estimate (PIE) is complete and up to date.
- Supports all operations with a Short Peacekeeping-Intelligence Estimate (SPIE).
- Conducts a full Assessment of the Operating Environment (AOE) and Actor Analysis for the entire Area of Operational Responsibility (AOR), per the guidelines in Chapter 5.
- Ensures that a full AOE and Actor Analysis is carried out by all subordinate units down to Company level, or whenever a new Forward Operating Base (FOB) is established. A detailed AOE must be carried out for all areas of interest for the military component, to include Protection of Civilian sites, all FOBs, and other areas related to mandate implementation, and as directed by the FC.
- Ensures AOE and Actor Analysis, the assessments/reports, all need to be made available to avoid duplication of work and promote situational awareness/ knowledge Management.
- Works with the Military Gender and Protection Advisor, as well as the Prevention of Sexual Exploitation and Abuse (PSEA) Mission Focal Point, to ensure that a gender, protection and PSEA perspective is mainstreamed into all peacekeeping-intelligence products.
- Ensures that all relevant information and PKI is provided to higher and subordinate HQs in a timely fashion.
- Represents the Force Commander at the MICM.

MPKI staff G2 Branch. The G2 peacekeeping-intelligence branch in a Sector deal with all matters concerning MPKI and military security operations at tactical/ operational level within the battalion AOR. Its recommended structure is depicted below.

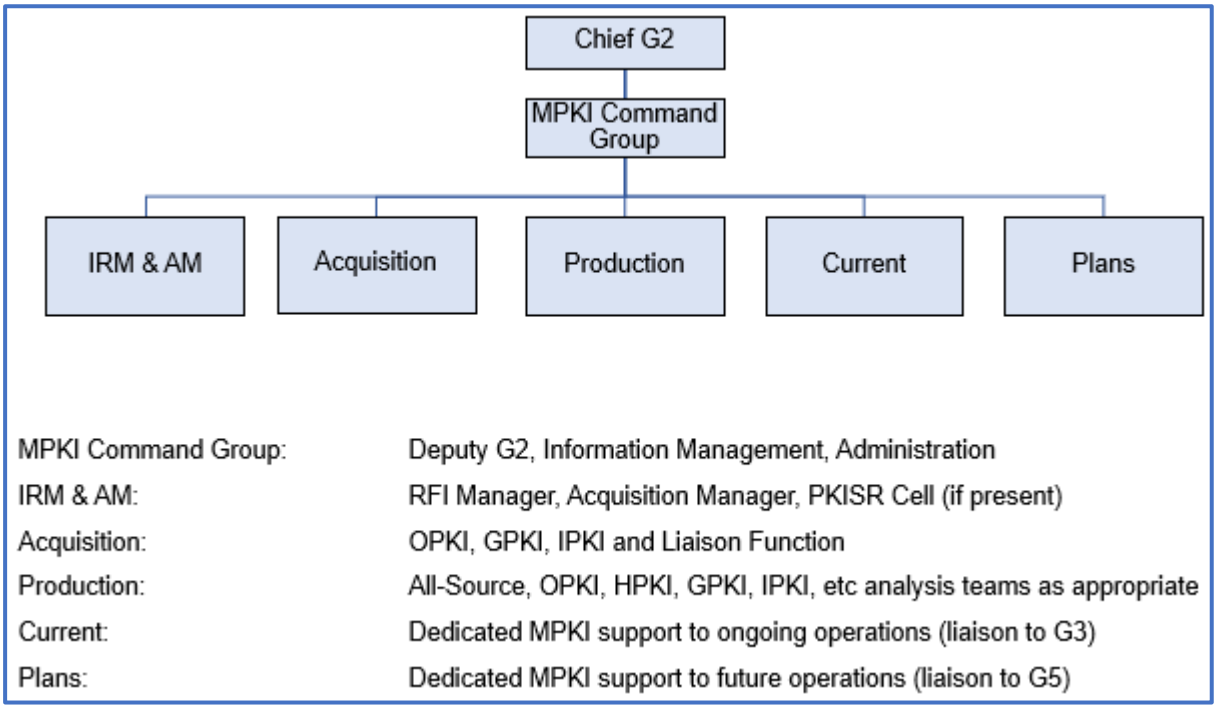


Figure 28: G2 Branch Structure and Organization

Roles and Responsibilities of the G2 Branch:

- Manages the Sector MPKI Cycle, in line with the PKI Policy and MPKI Handbook, through the direction, acquisition, examination/collation, analysis and dissemination phases. This is to ensure that the Sector Commander's decision-making process is fully supported with timely, succinct, and relevant peacekeeping-intelligence products.
- Ensures that its information acquisition activities are conducted in support of Force Priority and other IRs. To this end, the G2 branch will maintain an IAP that fully aligns with FHQ IRs. This will be regularly updated.
- Ensures that appropriate acquisition assets are tasked to acquire relevant information.
- Ensure that all incoming information is collated on a central database, and available to the relevant personnel.
- Maintains its own source register and registers its sources with the U2.
- Produces timely, relevant, concise, and predictive PKI products to support effective mandate implementation relating to the protection of UN personnel and civilians, and to enhance situational awareness, as required.
- Identifies relevant trends.
- Supports all operations with an SPIE.

- Conducts a full AOE and Actor Analysis for the entire AOR, per the guidelines in Chapter 5.
- Ensures that a full AOE, and Actor Analysis is carried out by all subordinate units down to Company level, or whenever a new FOB is established. A detailed AOE must be carried out for all areas of interest for the military component, to include Protection of Civilian sites, all FOBs, and other areas related to mandate implementation, and as directed by the FC.
- Works with the Military Gender and Protection Advisor, as well as the Prevention of Sexual Exploitation and Abuse (PSEA) Mission Focal Point, to ensure that a gender, protection and PSEA perspective is mainstreamed into all peacekeeping-intelligence products.
- Ensures that all relevant information and peacekeeping-intelligence is provided to higher and subordinate HQs in a timely fashion.

MPKI Section S2. The S2 section at battalion level supports the battalion commander and staff with peacekeeping-intelligence products. The S2 also deals with security tasks within the battalion. Outside the battalion staff, the S2 is responsible for directing and coordinating the MPKI needs and information acquisition at company level. Although the S2 has limited MPKI organization, personnel and material for conducting MPKI processes, it is an important and integrated element of the mission's MPKI chain. It must therefore be appropriately staffed.

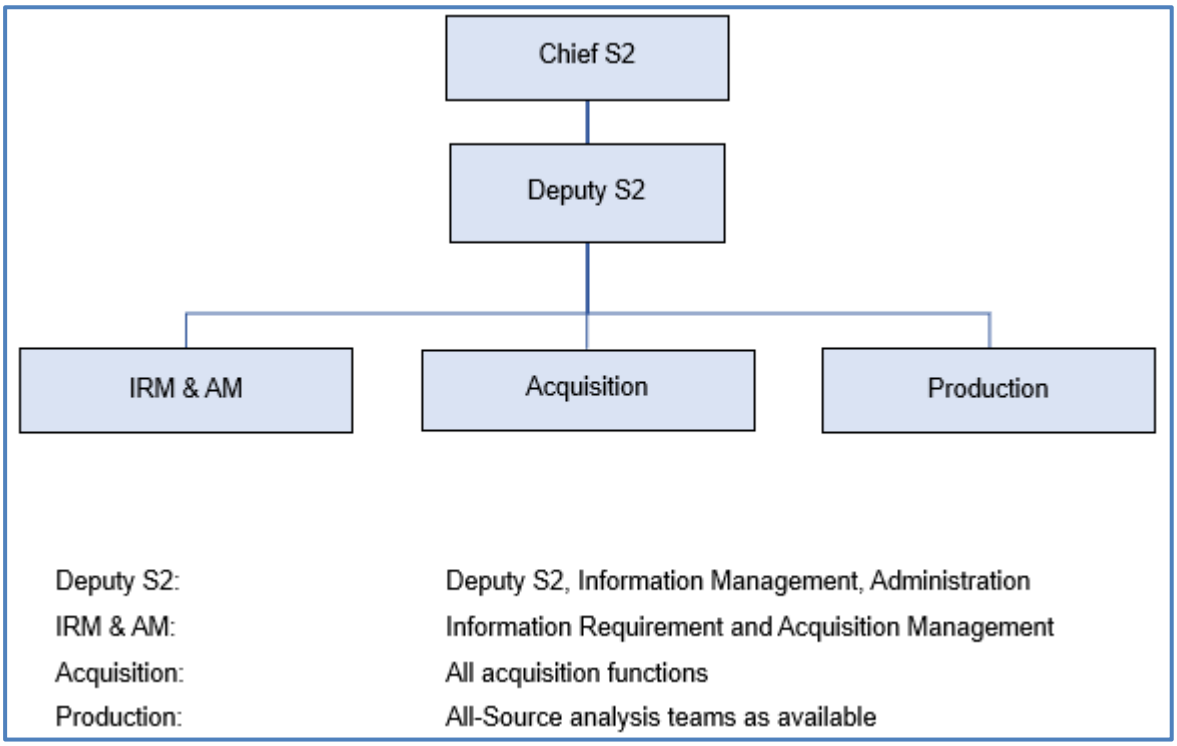


Figure 29: S2 Branch Structure and Organization

Roles and Responsibilities of the MPKI S2 Section:

- Manages the Battalion MPKI Cycle, in line with Peacekeeping-Intelligence Policy and this Handbook, through the direction, acquisition, examination/collation, analysis and dissemination phases. This is to ensure that the Battalion Commander's decision-making process is fully supported with timely, succinct, and relevant peacekeeping-intelligence products.
- Ensures that its information acquisition activities are conducted in support of Sector Priority and other IRs. To this end, the S2 section will maintain an IAP that fully aligns with Sector Headquarters IRs. This will be regularly updated.
- Ensures that appropriate acquisition assets are tasked to acquire relevant information.
- Ensure that all incoming information is collated on a central database, and available to the relevant personnel.
- Maintains its own source registry and registers its sources with the G2.
- Produces timely, relevant, concise, and predictive peacekeeping-intelligence products to support effective mandate implementation relating to the protection of UN personnel and civilians, as required.
- Identifies relevant trends.
- Supports all operations with a SPIE.
- Conducts a full AOE and Actor Analysis for the entire AOR, per the guidelines in Chapter 5.

- Ensures that a full AOE, and Actor Analysis is carried out by all subordinate units down to Company level, or whenever a new FOB is established. A detailed AOE must be carried out for all areas of interest for the military component, to include Protection of Civilian sites, all FOBs, and other areas related to mandate implementation, and as directed by the FC.
- Works with the Military Gender and Protection Advisor, if resources permit at Sector-level, to ensure that a gender, protection and PSEA perspective is mainstreamed into all peacekeeping-intelligence products.
- Ensures that all relevant information and peacekeeping-intelligence is provided to higher and subordinate HQs in a timely fashion.

MPKI SUPPORT PLAN TEMPLATE

Reference:

Date:

UN MISSION TITLE

1. U2 Mission
2. Statement of APIR and APII
3. Situation[18]
   - Physical Terrain (In general and in detail)
   - Human and Information Terrain
   - Threat Evaluation
   - Situation Integration
4. Current MPKI Structures
5. PIRs
6. U2/G2/S2 Roles and Responsibilities
7. U2/G2/S2 Command and Liaison Relationships
8. Allocated Acquisition Assets
9. U2/G2/S2 Battle Rhythm
10. Information Systems and IM
11. Current Security Policy

[18] This is drawn from the Initial AOE outputs (see Chapter 5 of this Handbook for an outline of the AOE process).

Example Phase 1 Brief

Serial	Topic
01	**Scope**. Overview of what the Phase 1 Brief is going to cover and what briefing aids are going to be used.
02	**Peacekeeping-intelligence foundation**. What peacekeeping-intelligence forms the basis of the briefing? Be sure to inform the Commander of any peacekeeping-intelligence gaps that are pertinent to the mission.
03	**Key assumptions and outputs**. Inform the Commander of the key deductions and judgements you have identified while conducting the AOE.
04	**Ground in general**. The physical terrain. Orient the Commander and planning staff to the ground including weather effects.
05	**Ground in detail**. Describe the mission-specific physical terrain in more detail. Depending on the type of mission to be conducted (defensive/offensive), inform the Commander of the specific ground details that will affect his/her mission including any key infrastructure.
06	**Human and Information Terrain**. Factors that are pertinent to the mission are likely to include: • Tribal and ethnic laydown • Displaced persons and refugees • NGOs • Key leaders • Pattern of life • Host State armed forces • Information environment – social media trends (supportive/resistant to UN presence), media reporting, local communication capabilities
07	**Threat Evaluation.** Analysis of all threat actors that are pertinent to the mission, to include: • Threat actor assumptions • Threat actor organizations and hierarchies including key leaders • Threat actor TTPs • Threat actor equipment and capabilities • Strengths and weakness and COG analysis
08	**Situation Integration.** How will the threat actors and human factors affect the mission when considered in relation to the physical environment? To include: • Actors' courses of action. Most likely and most dangerous. • Updated IAP based on known peacekeeping-intelligence gaps

Table 20: Phase 1 Brief

Note: The Phase 1 Brief should not focus too much on the terrain. The main output of the Phase 1 Brief is Threat Evaluation and Situation Integration to inform Commanders and their planning staff throughout the MDMP. In subsequent briefs, only pertinent points in relation to the terrain are to be briefed unless otherwise directed.

Example WARNO Template

WARNO#001		
Preliminary Activity		
Task Organization		
Situation	Ground	
	Human Terrain – civilians	e.g., Government departments, tribal breakdowns etc.
	Human Terrain – Host State or other friendly security forces	Indigenous government-owned armed/security forces
	Human Terrain – Threat Actors	All threat actors including criminal elements
	Human Terrain – Own Forces	Higher Headquarters 2 Levels Up – Intent and Main Effort
		Higher Headquarters 1 Level Up – Mission and Concept of Operations
		Flanking Formations
		Combat Support units
		Air / Aviation assets
		PKISR assets
Mission	Statement of the given mission	
Execution	Concept of Operations	Intent
		Scheme of Manoeuvre
		Main Effort
		Desired End State
	Subordinate Missions	
	Combat Support Missions/Tasks/Priorities	
	Coordinating Instructions	Timings
		Locations
		Control measures
		Fire plan
		Deception and Security
		Movement

		Key information from the annexes
Combat Service Support	Logistics	
	Equipment Support	
	Medical	
	Provost/Policing	
Command and Communications	Command Relationships	
	Communication plan	

Table 21: WARNO Template

MPKI IM – Tactical Aide

- **Taking/Handing Over.** You must understand where information is stored, how to retrieve it, and how to maintain any databases into the future. Also, plan your handover and the need to leave an organized legacy from the day that you arrive in theatre. Do not assume that information is self-evident to your successors.
- **Balance local initiatives vs. conforming to established protocols.** In a relatively new operation, the best database could be prepared at S2 level; if this is the case, take advantage of this and replicate it widely. However, once a database has been agreed on, direct all elements of the mission to use it rather than continuing to rely on local solutions.
- **Use Checklists.** Effective IM involves repeating similar actions on a regular basis to provide a disciplined information environment. To ensure that procedures are followed effectively, and all necessary activity is carried out, IMs should prepare a checklist of actions that need to be completed to ensure that nothing is forgotten.
- **Consolidate Databases and Protective Marking.** It is not uncommon for peacekeeping-intelligence cells to use several different IT systems and have access to many databases at various classifications. However, for enduring operations, try to minimize the number of databases, and consolidate to one or two if possible.
- **Other Peacekeeping-Intelligence Actors.** Ensure that other actors such as GA, Civil and Political Affairs Officers, UNDSS, UNPOL etc. are inputting their data and information into a common database/IM system rather than a separate stovepipe.
- **Hard Copy.** If Communications and Information Systems (CIS) systems are unreliable, make sure that a hard copy archive of key documents is maintained and correctly filed.
- **Distribution lists.** Ensure that peacekeeping-intelligence personnel at all levels are included on all relevant distribution lists and, for your own lists, keep checking that they are up to date.

MPKI THREAT ANALYSIS WORKSHEET

1. UN mandate objectives (immediate, short-term, long-term)
2. Nature of society
    a. Social, economic, political and security conditions
    b. Cause of the conflict/crisis
    c. Issues
    d. Groups (segments of the population) and forces (groups trying to influence the action of the others)
    e. Variables likely to influence the level of violence (coercive potential, institutionalization, facilitation, legitimacy of the regime)
    f. Threat vectors: types of attacks; weapons; frequency of attacks.
3. Nature of the threat:
    a. Leadership
    b. Objectives
    c. Structure/organization
    d. Target groups
    e. External support
    f. Timing
    g. Mass support
    h. Relationship to legitimate political/DDR/SSR processes
    i. Use of violence
    j. Urban or rural base
4. Nature of governance (official/unofficial)

a. Objectives

b. Description of counter-threat measures

c. Evaluation of counter-threat measures
    i. Balanced development, neutralization, and mobilization programs
    ii. Pre-emptive and reinforcing aspects of the threat strategy
    iii. Adherence to operational guidelines
    iv. Evaluation of each counter-threat program in terms of likely impact on each segment of the population

5. UN mission response

a. Possible Courses of Action

b. Evaluation of each course of action

c. Recommendation