



United Nations

# Reinforcement Training Package

for United Nations

Peacekeeping-  
Intelligence,  
Surveillance and  
Reconnaissance

For United Nations Peace Operations

The Specialized Training Materials (STM) and Reinforcement Training Packages (RTP) for United Nations (UN) peacekeeping operations have been developed by the Integrated Training Service (ITS) of the UN Department of Peace Operations.

This version has been released for use by Member States in their pre-deployment training for UN peacekeeping operations. The suite of STM and RTP products will be regularly updated to be fully responsive to the needs on the ground. Therefore, we strongly suggest checking for updated versions before a training programme is conducted.

The latest RTP versions can be found online at the Peacekeeping Resource Hub: <http://research.un.org/en/peacekeeping-community>. A link to receive your comments and suggestions for improvement can be located in the resource hub at the same location.

This document may be reproduced for educational or non-profit purposes without special permission from the copyright holder, provided acknowledgement of the source is made. This document is not to be sold.

Unless otherwise indicated, all photographs have been sourced from the UN and the public domain.

© UN 2022

Integrated Training Service

Department of Peace Operations

United Nations

New York, NY, 10017, USA

## Preface

### Background

The UN Department of Peace Operations has developed a suite of training packages to prepare peacekeepers for deployment to UN peacekeeping missions. Amongst these packages are the Specialised / Reinforcement Training Materials for specific military duties and military units.

UN Staff Officers (UNSO), specifically Military peacekeeping-intelligence Officers operating in the field of Peacekeeping-intelligence, surveillance and reconnaissance (PKISR), are required to undergo a robust pre-deployment training programme following DPO's Operational Readiness Assurance and Performance Standards.

### Aim

The PKISR RTP aims to support the pre-deployment training efforts of troop-contributing countries by providing UN DPO training standards to ensure a common approach to work at the Force and Sector levels in UN peacekeeping missions.

The RTP provides Member States with the UN pre-deployment requirements, lessons and materials specifically designed for military PKISR staff officers. The training materials supplement the UN Military Staff Officer (UNSO), the Core Pre-Deployment (CPTM) and the UN Military peacekeeping-intelligence Officer (MIO) training courses.

### Contents

The training materials are a comprehensive training package that combines the conceptual, legal and operational frameworks for PKISR. The RTP mainstreams relevant aspects of the DPO Policy on Peacekeeping-Intelligence, the protection of civilians, gender, security and risk management into the peacekeeping-intelligence frameworks and materials. The RTP includes learning activities and a scenario-based staff exercise to strengthen participants' understanding of how to operate in a UN PKISR staff environment. The training package is designed for application in both pre-deployment and in-mission training. The package is broken down into three modules:

- **Module 1:** Conceptual Framework
- **Module 2:** Legal Framework
- **Module 3:** Operational Framework

## Target audience

The priority target audience for this training package is military peacekeeping-intelligence staff officers employed in a PKISR role. However, the RTP also has utility for military decision-makers and other staff officers deploying to UN Peacekeeping missions.

## Annexes:

- **Annex A:** PowerPoint slide lesson presentations.
- **Annex B:** Staff exercise (TTX).
- **Annex C:** Reference materials.



## Acknowledgements

ITS would like to thank the subject matter experts from across the UN organisation, Member States and other regional and international organisations who provided inputs and feedback during the drafting process, and the numerous training personnel from national peacekeeping training institutions and field missions who participated in the development workshop. Appreciation is extended to the following organisations, Member States and their Permanent Missions to the UN for their contribution in the RTP development:

Bangladesh  
Federative Republic of Brazil  
Germany  
Ghana  
Japan  
Jordan  
Kenya  
Republic of Korea  
Tunisia  
Islamic Republic of Pakistan  
Kingdom of Denmark  
Kingdom of Morocco  
Kingdom of the Netherlands  
Kingdom of Norway  
People's Republic of China  
Office of Military Affairs, Assessment Team

### Contact person

For any proposal of update or improvement of this package, or any questions about these training materials, please contact the project leader Mr. Rafael Barbieri ([barbieri@un.org](mailto:barbieri@un.org)) or write to [peacekeeping-training@un.org](mailto:peacekeeping-training@un.org).

Any relevant update will be posted and explained on the Peacekeeping Resource Hub website (<http://research.un.org/en/peacekeeping-community>). Instructors are encouraged to check the site regularly.

## TABLE OF CONTENTS

Instructor guidance

### **Module 1 – Conceptual Framework**

Lesson 1.1 – UN Peacekeeping-Intelligence Overview

Lesson 1.2 – PKISR Fundamentals

Lesson 1.3 – PKISR Structures

Lesson 1.4 – Information and Data Management

Conceptual Framework Wrap Up

### **Module 2 – Legal Framework**

Lesson 2.1 – Legal Framework for Peace Operations: General International Law

Lesson 2.2 – Legal Framework for Peace Operations: Mission Specific

Legal Framework Wrap Up

### **Module 3 – Operational Framework**

Lesson 3.1 – PKISR

Lesson 3.2 – PKISR Process

Lesson 3.3 – PKISR Key Roles

Lesson 3.4 – RFI Management

Lesson 3.5 – Requirements Management and Prioritisation

Lesson 3.6 – Analysis and Dissemination

Lesson 3.7 – PKISR Plans

Lesson 3.8 – PKISR Operations

Lesson 3.8a – Unmanned Aircraft System Unit

Lesson 3.8b – Field HPKI Team

Lesson 3.8c – Long Range Reconnaissance Patrol

Operational Framework Wrap Up

### **References, Annexes**

# Instructor Guidance



## General Considerations for Instructors

This package is a compendium of training content for PKISR staff officers operating in a UN peacekeeping mission. When designing a PKISR course, trainers should adapt these materials to the needs and experience of the audience.

The PKISR RTP will help prepare participants to perform PKISR staff functions in a UN peacekeeping mission at Force or Sector level according to DPO policies and guidelines.

It is recommended that the minimum criteria for personnel attending the PKISR RTP is:

- Completed national or international staff officer training.
- Attended a national or international peacekeeping-intelligence officer course.
- Completed the UN CPTM, UN Staff Officers STM and UN MIO RTP.
- Proficient in the English language.

Instructors should develop and implement an initial written test and final test (post-instruction) to reinforce learning outcomes and evaluate participants' training level/knowledge.

The STMs and RTPs can be downloaded from <http://research.un.org>

## Instructor Profile

This training package is best presented by instructors with a credible background in or knowledge of military peacekeeping-intelligence and specifically National ISR. Instructors should have previous experience working in a UN peacekeeping mission or as an MIO at the tactical/operational level. Finally, instructors should be confident with facilitator-based instruction.

## Staff Exercise Considerations

Contained in the RTP is a final exercise (TTX). This is a scenario-based staff exercise to help consolidate the course learning outcomes and reinforce basic PKISR staff

skills. The exercise has been designed to provide a learning environment that allows participants to consolidate and apply their knowledge during the course.




The success of the exercise will be partly down to the instructor's preparation and engagement throughout the activity. Provided notes will help guide the instructor through the various stages of the exercise to ensure maximum benefit for all participants. It is suggested that the instructor read through the exercise notes before the course starts to be confident in delivering the activity.

## Training Characteristics

Training will vary for different troop-contributing countries, based on priorities and resources. However, some fundamental training characteristics should be respected when delivering the course:

- Training should be interactive where participants are encouraged to contribute to discussions.
- Trainers should bring examples and antidotes from actual UN peacekeeping operations.
- Training should be evaluated.
- Training should emphasise the political nature of a UN mission and address how best to leverage and interact with all components.

## Symbols Legend

	Interactive presentation or small exercises to engage the participants
	Suggested film segment to illustrate the content
	Note to the instructor to highlight particular aspects of the materials or point towards additional materials

## General Preparations

Equipment:

1. Computer / internet access.
2. Projector and screen.
3. Flip charts and whiteboards.

Materials:

1. Copies of reference materials in support of lessons.
2. PowerPoint presentations.
3. Any other material required for conducting learning activities.

# Module 1



## Conceptual Framework

### Module 1 at a Glance

#### Aim

The aim of this Module 1 is to:

- Provide an overview of UN PKI and PKISR.
- Explain the relationship between PKI and PKISR.
- Highlight the importance of information and data management in PKISR.

#### Overview

Module 1 provides students with a conceptual understanding of PKI and PKISR. The framework will help to provide the building blocks from which students can operationalise PKISR concepts in a UN peacekeeping environment (delivered during Module 3 of the course).



**Note to Instructor:** The instructor should be familiar with DPO's Peacekeeping-Intelligence Policy, the UN Military Peacekeeping-Intelligence Handbook and the UN Peacekeeping-Intelligence, Surveillance and Reconnaissance Handbook before delivering the lesson.



**Interactive.** Ask students to highlight their experience in military intelligence and whether they have attended the UN MIO training course. The answers will provide you with an initial indication on student knowledge and whether elements of Module 1 will need to be delivered as revision or formal instruction. Be prepared for both situations.



## Module 1 Military Peacekeeping- Intelligence, Surveillance and Reconnaissance Conceptual Framework

Key message: As UN peace operations' mandates and operating environments have evolved, there is a need for peacekeeping missions to better understand their operating environments and produce peacekeeping-intelligence products for situational awareness, protection of peacekeepers and protection of civilians.

This module aims to inform you of the military peacekeeping-intelligence, surveillance and reconnaissance (PKISR) conceptual framework. Much of this module will be revision since all participants should have completed the UN staff officer and UN military peacekeeping-intelligence officer (MIO) courses before attending this course. However, to set the context, this module will reiterate some of the fundamental issues that will underpin the PKISR course.

## Slide 2

### Module 1 Content

- PKI overview
- PKISR fundamentals
- PKISR structures
- Information and data management

Here are the topics that will be covered in this module.

First, students will be reminded of some of the key themes that underpin peacekeeping-intelligence (PKI). This will include the UN Department of Peace Operations (DPO) PKI policy, which establishes the overall parameters within which UN MIO must operate, including those working in PKISR. It is important to note that these parameters might differ significantly from national policies. We will also discuss PKISR structures in the mission, as well as the importance of information and data management.

Throughout this course, lessons and slides will use the abbreviation MPKI to refer to 'military peacekeeping-intelligence', PKISR to 'peacekeeping-intelligence, surveillance and reconnaissance', and MIO to 'military peacekeeping-intelligence officer'.



# Lesson 1.1



## UN PKI Overview

### The Lesson



#### Starting the Lesson



**Interactive.** Ask the participants if they have had experience as a - peacekeeping-intelligence staff officer in a UN peacekeeping mission. Ask them to tell the group about their experience and any challenges they faced in performing their duties. Encourage students to continue to share their experiences with the group throughout the course. Such engagement will enhance student learning.



**Note to Instructor:** The first few lessons of Module 1 should be seen as confirmatory sessions from the MIO course. You should use this lesson to gauge the students' level of knowledge and, where possible, allow them to articulate their understanding of PKI.

Slide 3



## Lesson 1.1 UN PKI Overview

## Slide 4

### Lesson Contents

- UN PKI
- PKI principles

Here are the subject areas we will be covering in this lesson.



**Note to instructor:** *Remind the students that Peacekeeping-intelligence (PKI) refers to peacekeeping-intelligence in UN peacekeeping operations – PKI involves all components in the mission area: civilian, military and police.*

## Slide 5

### Learning Outcomes

- State why UN PKI is important to UN missions
- Apply the PKI principles

Let us first review the learning outcomes. At the end of the lesson, our aim is for you to be able to state why UN PKI is so important to UN peacekeeping missions and to be able to apply the PKI principles to your thinking and staff work.

Please take a moment to read and understand the requirements. As already said, this should be a revision for all participants.

## Slide 6



**Interactive.** Ask participants why they think UN peacekeeping-intelligence is important to UN peacekeeping missions. The instructor should generate and manage a discussion to gauge the students' knowledge and opinions before sharing the information below.

Why has the UN embraced peacekeeping-intelligence instead of Information? Mandates and operating environments of UN peacekeeping missions have evolved, so too have the capabilities, processes and procedures required to acquire and analyse information.

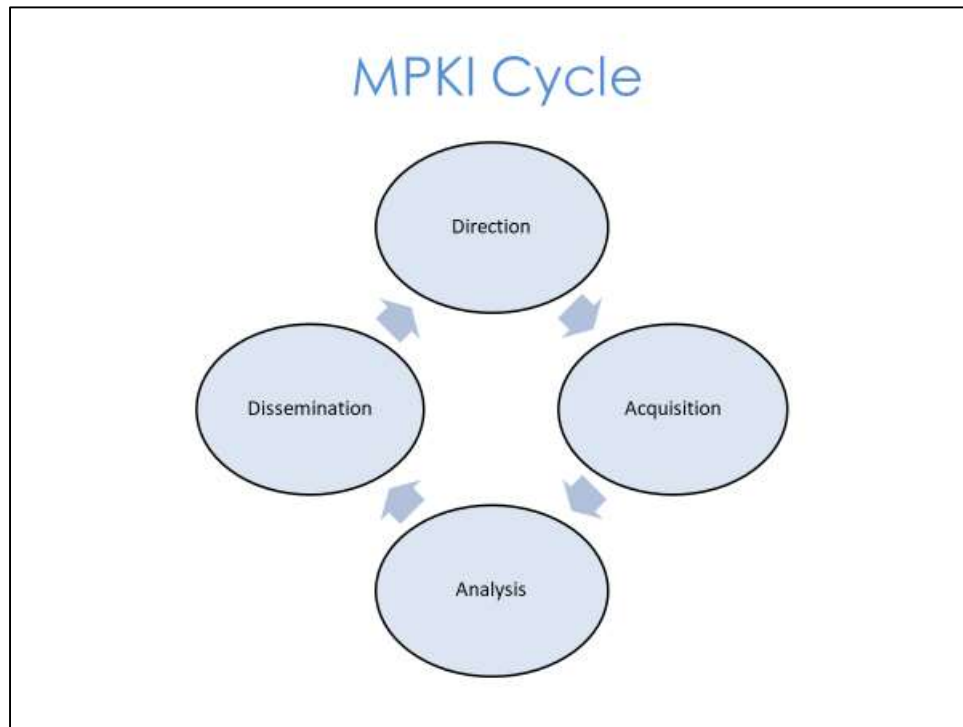
In high-tempo, complex and dangerous environments, asymmetric, hybrid and transnational threats impact the mission's ability to implement the mandate. In these environments, there is a need for peacekeeping missions to understand their operating environments better. This includes maintaining a strategic overview of developments and of threats/spoilers that may impact the ability of peacekeepers to execute their mandate effectively.

The Department of Peace Operations (DPO), Office of Military Affairs (OMA) has developed the Military Peacekeeping-intelligence and Peacekeeping-intelligence, Surveillance and Reconnaissance handbooks, which support the military component who work within the Mission PKI system. The way the UN conducts peacekeeping-intelligence may differ from your own national methodology; it is crucial to understand these differences.



**Note to instructor:** *All resources can be found online. If possible, issue each student with electronic copies of the various policy and guidance documents.*

## Slide 7



Key message: The military peacekeeping-intelligence cycle is typically represented as a closed cyclical path of activities that takes you through direction, acquisition, analysis and dissemination.

We will be looking at different elements of the cycle in more detail later in the course. Specifically, activities aligned to the acquisition stage of the cycle.



**Note to instructor:** Ask students if they are familiar with the UN peacekeeping-intelligence cycle, as depicted in the MPKI handbook. You should not spend too much time on this slide.

## The importance of UN Peacekeeping-Intelligence

- Supports situational awareness to enhance decision making.
- Provides early warning of imminent threats to civilians and UN personnel.
- Identifies relevant trends and threats.

Key message: DPO policy states that the fundamental purpose of PKI in UN peacekeeping operations is to aid mission leadership in taking decisions by:

- Ensuring a common operational picture: Establishing and maintaining an up-to-date, accurate peacekeeping-intelligence picture of the mission area helps to support planning and operations.
- Providing early warning of imminent threats: Providing early warning of an imminent threat to life through timely peacekeeping-intelligence allows the mission to act appropriately in accordance with its mandate.
- Identifying risks and opportunities: Peacekeeping-intelligence can provide mission leadership with an enhanced understanding of shifts in the strategic and operational landscape, with respect to the safety and security of UN and associated personnel, the protection of civilians, as well as the political context.



## Slide 9

### UN PKI Principles

#### **PKI Policy**

- Under rules
- Non-clandestine
- Areas of application
- Respect of state sovereignty
- Independence
- Accountability, capability, authority
- Security & confidentiality

#### **MPKI Handbook**

- Command led
- Invest in ISP and MPKI battle-rhythm
- Centralized control-decentralised execution
- Objectivity
- Accessibility and timeliness

[Key message:](#) There are two sets of principles that guide PKI.

The overarching set of principles from the UN PKI Policy is on the left of the slide, and the practical set of principles from the UN Military Peacekeeping-Intelligence (MPKI) Handbook on the right. Both sets of principles also apply to PKISR and will help to guide you in your duties as a military peacekeeping-intelligence officer (MIO).

These principles cover all activities regarding the management and conduct of UN PKI. All subordinate guidance, directives, plans and operations shall comply with these principles.

## Learning activity

- Time – 30 mins
- Sub-group task
- Discuss what you think each principle means
- Be prepared to discuss your answers



**Interaction.** Split the participants into sub-groups. Give the groups 10 minutes to consider 3-4 principles each (each group should consider different principles). Students should be prepared to discuss their results. Student responses should include reasons why they think the principles are important to UN PKI activity.

Hopefully, the students will be able to identify the key points for each principle. Use the following slides to confirm or clarify each principle once the students have presented their thoughts. The time to be spent on the following slides should depend on how the students respond to the learning activity.



**Note to instructor:** Use the remaining time of this lesson to conduct this interactive session. Generate a discussion among students to ensure they all understand the different principles. You should be prepared to assess the level of the knowledge among the students early in the session and, if necessary, teach the remaining slides within the allocated time.

## Under Rules

- Security Council mandates
- Compliance with the UN Charter
- Consistent with the overall legal framework
- Human rights obligations

Key message: All peacekeeping-intelligence activities must follow the intent, goals, tasks, rules and regulations covered in the UN mandate.

Every activity conducted in PKI should comply with the UN legal framework, international humanitarian and human rights law and host nation laws.

## Non-clandestine

- Not conducted in secrecy
- Consistent with the legal framework, principles, policies and mandate of UN peacekeeping operations

Key message: UN PKI is conducted in a non-clandestine manner.

Often, national intelligence is conducted in a clandestine manner, meaning the acquisition of information or intelligence is conducted in such a way as to assure secrecy and concealment of activities. Because such activities are illicit and inconsistent with the legal framework, principles, policies and mandates of UN peacekeeping operations, they are outside the boundaries of PKI and shall not be undertaken by participating mission entities.

## Areas of Application

- Enhance situational awareness
- Ensure safety and security of personnel
- Inform operations and activities related to the POC tasks

Key message: The production of UN peacekeeping-intelligence shall be limited to the following: to enhance situational awareness, to ensure the safety and security of personnel, and to inform operations and activities related to the protection of civilians.

While this may seem restrictive, it establishes quite broad parameters within which MPKI can operate.

## Respect to State Sovereignty

- Respect the sovereignty of the host state
- Respect the sovereignty of neighbouring states

Key message: A UN peacekeeping operation is deployed with the consent of the host government. Therefore, the sovereignty of states, including the host and neighbouring states, must always be respected.

For example, a mission cannot actively track armed groups across national borders without the express permission of that state. A key point regarding PKISR is that it cannot task acquisition assets to operate in other states without the necessary permissions.

## Independence

- Autonomous / independent of national systems or other operations
- Maintain exclusive international character
- Share intelligence with non-mission entities when UN conditions met

Key message: UN PKI activities will be fully autonomous from and independent in all aspects of any national intelligence system or other operations and maintain their exclusively international character.

However, missions may liaise with non-mission entities for the purposes of receiving intelligence and may share specific PKI with non-mission entities, including the host state, provided they do so under conditions and within the parameters laid down by the UN mission. The mission must remain impartial when considering the sharing of PKI.

Generally, it is the Head of Mission's responsibility to determine the entities with which the mission can share peacekeeping-intelligence.

## Accountability, Capability, Authority

- Authority to make decisions
- Proper capabilities to execute functions
- Accountable for effective execution of responsibilities

Key message: It is important to note that authority for the overall PKI cycle resides with the Head of Mission (HoM). However, the HoM will often delegate such authority for UN Military PKI to the Force Commander.

Those who are given the authority to make decisions about PKI activities must have the appropriate capabilities to execute these functions and remain accountable for the effective execution of these responsibilities within their respective chains of command to the Head of Mission and ultimately to the Secretary-General.



## Security and Confidentiality

- Secure information management and communications
- Shared / disseminated on “need to know” and “need to share” concepts
- Disclosed to trusted individuals for official duties

Key message: PKI shall be stored and shared securely while ensuring access for those who require it for decision-making and operational planning.

Peacekeeping-intelligence should be disclosed to mission personnel only if access is required for them to carry out official duties and this is aligned with the need to share principle which is covered later in the training.

Students will hear more on this during the information and data management lesson.

## MPKI Command-led

- Centrally coordinated process
- Leadership is continuous
- Commander sets priorities and directs effort
- Intelligence staffs organize, acquire and disseminate PKI

Key message: PKI is a centrally coordinated process through which information coming from decentralised entities, often deployed over a wide geographic area, is combined with different functions and expertise.

There is thus a requirement for a senior PKI officer to not only be a PKI professional but also ensure that the MPKI structure is being command-led. The requirement for MPKI leadership is continuous.

## Invest in Peacekeeping- Intelligence Support Plan and Battle-rhythm

- Clear responsibilities
- SOPs, timings, reports and returns
- Battle-rhythm sets conditions for success
- Provides a mechanism that makes the MPKI machine work

Key message: A Mission peacekeeping-intelligence Support Plan (MISP) should establish the parameters within which PKI must work, the policy and rules it must adhere to, and allocate clear responsibilities for those working in it.

The ISP will also refer to and, where necessary, create SOPs, and will regulate other things such as reports and returns, timings, and battle rhythm. A strong ISP sets the MPKI structure up for success.

Missions should invest time to ensure that the ISP is clear, up to date, well understood, and disseminated to those that need it. The ISP should be drawn up by the Mission Chief of Staff. Make sure you read it on arrival on the mission.

## Centralized Control, Decentralized Execution

- Peacekeeping-intelligence systems thrive under centralized control and decentralized execution
- Centralized planning and direction essential for unity of effort
- Subordinate elements should be trusted to execute tasks without unnecessary interference

Key message: PKI systems thrive under centralised control but with decentralised execution.

This principle means both the PKI effort is explicitly linked to the commander's peacekeeping-intelligence requirements and that the MPKI organisation is operating as a homogenous system. Decentralised execution means that the subordinate elements of the MPKI structure should be trusted to execute their part in the Information Acquisition Plan (IAP), within the parameters laid out by the peacekeeping-intelligence Support Plan (ISP), without unnecessary interference.

Centralised control also means that unwanted duplication of acquisition effort is avoided.



**Note to Instructor:** We say 'unwanted' duplication of effort because it is often advisable to have more than one acquisition platform responding to the same peacekeeping-intelligence requirement. This helps ensure that you have information from multiple different sources.

## Objectivity

- Unbiased PKI
- Never distorted to fit a preconceived idea or to conform with senior leadership views
- Moral courage is required

Key message: PKI must never be distorted to fit a preconceived idea or to conform to strongly held views of senior leadership.

MPKI must have the moral courage to report what it considers to be the most accurate assessment and avoid analytical biases.

## Accessibility and Timeliness

- Readily available to the user
- Suitable for immediate comprehension
- Reach those who need to know in time
- Appropriate security classification

Key message: PKI is useless unless it reaches those who need to know in time to apply, use or exploit the PKI, in other words, support decision making.

Good PKI that cannot be accessed by the staff that require it, or that reaches a commander after the decision has been made, is worthless.

It is worth noting the challenges associated with sharing information, especially at the tactical level. On occasion, an MPKI officer at the battalion level (S2) may not have regular access to a computer, due to a lack of resources, and as such might find it difficult to pass information to higher HQ. You should make a point to identify these types of challenges once in the mission area and try to identify ways to mitigate them.



**Interactive.** Ask the students if they think there is a tendency for MPKI officers not to share information quickly enough or at all. Discuss the 'need to know' concept and the 'need to share' concept.

## Take Away

- PKI supports UN missions to better understand their environment, anticipate threats to the population and UN personnel, as well identify warning and indicators that impact the execution of the mandate
- PKI principles underpin UN PKI activities

## Summary

In conclusion, PKI helps mission leadership gain a better understanding of the environment in which they are operating. It also helps to anticipate threats to the population and UN personnel, as well as identify any indicators that may have an impact on a mission's ability to implement its mandate.

Keep the PKI principles in mind as you progress through this course – they underpin all PKI and PKISR activities and are key to the success of PKI.



**Note to Instructor:** You should have been able to gauge the knowledge of the students during this lesson and determine whether they attended the UN MIO RTP and are qualified in military peacekeeping-intelligence. Share your findings with other instructors so that they can adapt their presentations accordingly.

# Lesson 1.2



## UN PKISR Fundamentals

### The Lesson



#### Starting the Lesson

As you will recall, the purpose of military peacekeeping-intelligence (MPKI) in UN peacekeeping operations is to provide situational awareness to enhance decision making, provide early warning of threats to UN personnel and the civilian population, and to identify shifts in trends that could impact the mission's ability to implement its mandate. PKISR is an enabler in providing that situational awareness and supporting UN decision-making.



Slide 1



## Lesson 1.2

### UN PKISR Fundamentals

## Slide 2

### Lesson Contents

- PKISR process
- Relationship between PKI and PKISR
- Definitions
- Command and control

Here are the topics that will be covered in this lesson.

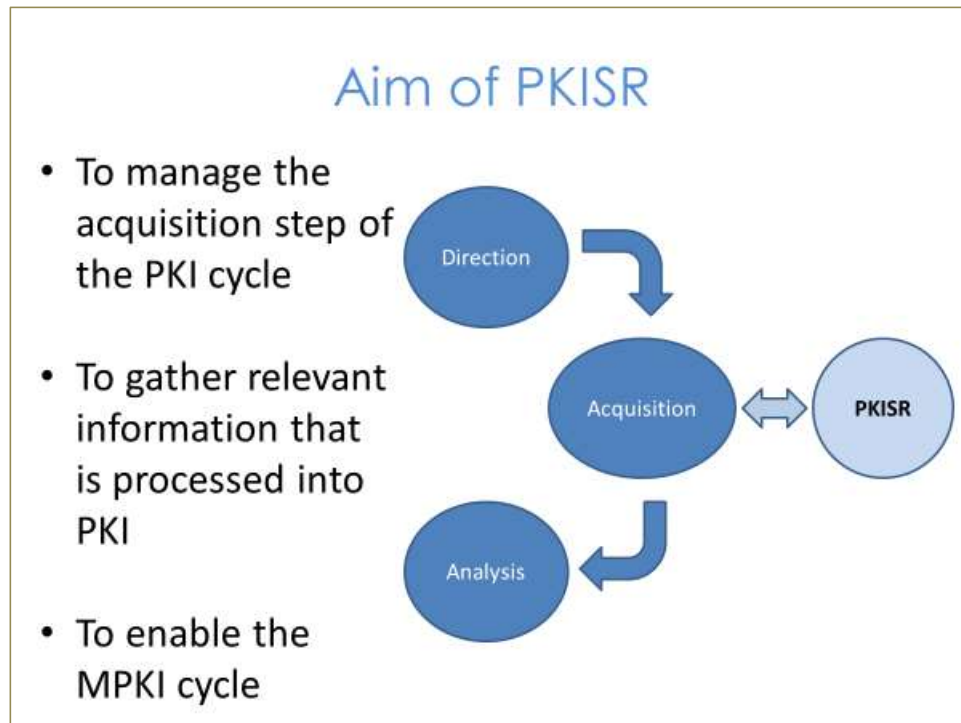
### Slide 3

## Learning Outcomes

- Explain PKISR
- Explain key PKISR definitions
- Explain the command and control of PKISR assets

Let us review the learning outcomes before we start this lesson. Please take a moment to read and understand what you are expected to be able to do at the end of the lesson.

## Slide 4



Key message: PKISR is designed to answer peacekeeping-intelligence questions through the tasking of mission PKISR assets. Note that tasking PKISR is not the sole domain of the military element of the Mission – anyone in a mission can ask a PKI-related question. We will go into more detail on this issue later in the course.

This diagram shows 3 of the 4 steps of the MPKI cycle and where PKISR supports it. Note that the cycle is not complete – the 'dissemination' step of the cycle has not been included for the purpose of this slide.

The aim of PKISR is to manage the acquisition of information. This is a complex process that involves the consolidation and prioritisation of information requirements and matches them alongside mission PKISR assets, all in support of current operations. What makes it complex is the ability of the U2 to interpret requirements and acquire the necessary data for it to be processed into peacekeeping-intelligence, all in a timely manner that supports decision making. PKISR enables the MPKI cycle.

## Slide 5

### PKISR Key Terminology

- Peacekeeping-Intelligence requirement (IR)
- Commander's Critical Information Requirements (CCIR)
- Priority Peacekeeping Intelligence Requirement (PIR)
- Specific Peacekeeping Intelligence Requirement (SIR)
- Essential Elements of Information (EEI)
- Request for Information (RFI)
- Indicators and Warnings (I&W)
- Force Information Acquisition Plan (IAP)
- Force Information Acquisition List (IAL)

Key message. There are certain PKISR terms that must be understood by all U2 staff to ensure the PKISR process runs smoothly.

We will go through each term, explaining what it means and how it relates to the other terms and the PKISR process, including the Information Acquisition Plan (IAP), the Mission Information Acquisition Plan (MIAP) and the Force Information Acquisition Plan (FIAP). It is important that the Force leadership and HQ staff are aware of this terminology.



**Note to Instructor:** Explain to students that the definitions of the terminology listed on this slide might be different to their own national doctrine and other UN publications. This course will use the terms as set out in UN PKI Policy and the MPKI Handbook.

## Peacekeeping-Intelligence Requirement (IR)

- IRs are determined during the planning process
- IRs aim to answer the gaps in knowledge important to decision-making process
- All IRs should be prioritized to allow the most effective tasking of acquisition units

Key message: peacekeeping-intelligence requirements are determined during the planning process by reviewing what is already known against what needs to be known to fulfil the mission. When there is a gap in knowledge, a question is posed to form the basis for a peacekeeping-intelligence requirement. Answering questions will assist the commander's decision-making process.



**Note to Instructor:** It is worth noting that the PKISR Handbook defines an IR as 'the basis for tasking of an acquisition unit'. For the purpose of this course, peacekeeping-intelligence requirement (IR) is defined as shown on the slide, and information requirement (IR) is as described in the PKISR handbook.

## Commander's Critical Information Requirement (CCIR)

- Information that is required to allow Force leadership to make timely and effective decisions
- U2 may need to define CCIRs on behalf of the leadership

Key message: Commander's Critical Information Requirement (CCIRs) are the overarching requirements set by the Force leadership. They can be anything the Force leadership determines as critical to the success of the mission or represents a threat to the implementation of the mandate. CCIRs are required to be established from the outset of a UN mission, although they will be reviewed and amended throughout the life of a mission. They can also include information requirements on own forces/friendly forces.

Generally, the CCIRs that the U2 cell receives from the Force Commander will be very broad and general in nature. For example, the Force Commander might ask what threats exist from a certain armed group. It is the U2's role, in this case, to break this broad question down into a series of smaller questions that can eventually be tasked for acquisition, more of which are in the following slides.

On occasion, the U2 will need to define the CCIRs on behalf of the leadership and gain their endorsement of them before progressing.

## Slide 8

### Priority Peacekeeping-Intelligence Requirement (PIR)

- PIRs form the basis of acquisition priorities
- PIRs should be drawn primarily from CCIRs
- U2 will need to define PIRs on behalf of the leadership
- PIRs should be regularly reviewed to ensure that they are still relevant

Key message. There are often insufficient PKISR assets in the mission to acquire all PKI requirements. Therefore, it is essential that the acquisition of information reflects the Force Commander's priorities to ensure the effective coordination of PKISR assets.

Priority peacekeeping-intelligence requirements (PIRs) should be drawn primarily from the CCIRs but can also be derived from the direction given by the Mission and Force leadership. PIRs form the basis of acquisition, and therefore, staff should spend time to ensure they are well written and truly represent the needs of the leadership. The PIRs will form the basis for the tasking of ISR assets.

It is important to note that the commander is unlikely to offer a set of PIRs written in a way that feeds the PKISR process. Instead, they will likely outline their concerns and operational priorities, and it is the responsibility of the Chief U2 to draft PIRs from what is discussed. These PIRs are likely to form an important part of the Information Acquisition Plan (IAP).



**Note to Instructor:** Explain to students that you will cover the IAP later in the lesson.



## Slide 9

### Specific Peacekeeping-Intelligence Requirement (SIR)

- PIRs are broken down into several SIRs to facilitate acquisition efforts
- SIRs are best structured thematically to support the acquisition process

Key message: PIRs can be broken down further into specific peacekeeping-intelligence requirements (SIRs) which are specific questions aimed in a focused manner to be included in an Information Acquisition Plan (IAP).

For example, a broad PIR relating to the protection of civilians might not make sense to a reconnaissance patrol, for example, 'what are the threats to civilians?'. However, asking more specific questions are easier for the acquisition unit to answer, such as:

- What are the threats to civilians in town X?
- Which armed groups are active in the area of town X?
- Where are civilians most vulnerable in town X?
- Why are armed groups attacking town X, etc.?

It makes sense to group the SIRs thematically. This saves duplication of effort and provides the U2 staff with a coherent response to their acquisition questions which in turn allows them to answer PIRs effectively.

## Essential Elements of Information (EEI)

- EEI are individual questions that will be assigned against the acquisition assets.
- The EEIs relate to the SIR, which in turn relate to the PIR.
- There are no set rules on how many EEIs relate to an SIR.

Key message: The EEI is the final step in breaking down PIRs into individual questions that can be assigned against a specific acquisition asset.

EEIs provide the details needed to inform the development of the Information Acquisition Plan (IAP). EEIs, once answered, should provide enough information to allow analysts to give a complete and satisfying answer to each requirement. The EEIs relate to the SIR, which in turn relate to the PIR. There are no set rules on how many EEIs relate to an SIR – this will be the role of the U2 staff to determine, based on its capacity to manage the FIAP.

## Request for Information (RFI)

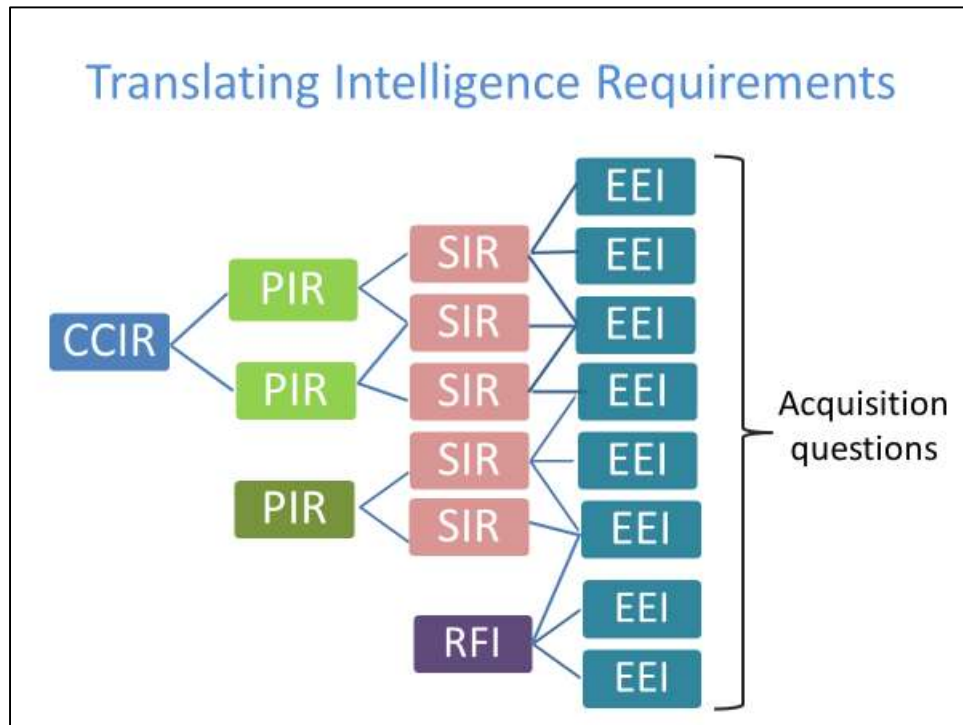
- RFI is a request for information by any individual or entity in the Mission that needs to be answered by PKISR capabilities
- All RFIs must receive a response, even if the request cannot be answered
- RFIs can be prioritised against the EEIs to allow for the effective tasking of PKISR

Key message: PKISR assets are not the sole domain of the military, and as such any component in the mission must be able to request information that helps them implement the mandate, for example, monitoring IDP camps, the movement of internally displaced people, election violence, etc.

The RFI process allows for any individual or entity in the mission or Force to ask a question that needs to be answered by the PKISR capabilities. The Force requires a well-established process that allows all mission civilian and uniformed components to submit an RFI in accordance with the MIAP, which can be prioritised against the EEIs to allow for the effective tasking of PKISR assets. In answering RFI's planners must balance the needs of the MIAP and FIAP in meeting requirements.

Maintaining a relationship with other mission entities helps to facilitate this process.

## Slide 12



This diagram demonstrates how, on the left, the U2 receives direction in the form of CCIRs or PIRs. These requests for information are then analysed and broken down into more detail until eventually specific questions are identified that can be assigned to different acquisition assets based on those assets' capabilities and suitability for the task.

Students will be able to practice this in detail during Module 3 of the course.

## Indicators and Warnings (I&W)

- An indicator is an observable behaviour or event that points towards a particular outcome
- Generally, indicators should be linked to a named area of interest (NAI), where such behaviours and events can be observed

Key message: An indicator is an observable behaviour or event that signals a particular outcome or that confirms or denies a relevant actor's course of action.

Such indicators and warnings are usually based on historical data acquired during the life of a mission. For example, the assembly of armed personnel in a specific area or the pre-emptive movement of civilians away from their village might indicate an imminent attack. Such indicators and warnings can be time-sensitive and, therefore, must be acted on immediately to inform decision-makers.

It is impossible for PKISR assets to monitor all events in the mission area. For this reason, indicators are aligned to specific geographical locations, referred to as named areas of interest (NAI). In other words, they are areas where the mission thinks certain indicators will possibly highlight or identify an imminent event.

## Information Acquisition Plan

- A tool that captures the 'direction' from the mission's leadership
- The IAP is a living document
- There is more than one IAP in the mission
- Basis for execution orders, via an 'information acquisition list'

Key message. The Information Acquisition Plan (IAP) is a tool that captures all the peacekeeping-intelligence requirements (questions) from the Mission leadership, including the Force Commander, and from other sources that need to be answered using PKISR assets.

The IAP is a living document. It must be reviewed regularly to ensure questions have been answered and those new requirements are added to the plan. The plan is the basis for collating requirements, prioritizing them and tasking PKISR, ensuring the right sensor is deployed to answer a specific question.

Several IAPs will exist within the mission, such as a Mission / Force / Sector and Battalion IAP depending on the different assets and questions being asked at each level.

The IAP is the basis for an executive order. The staff use the IAP to task, direct and manage acquisition assets to acquire information against the requirements. The daily tasking of ISR assets will be found in the Force's Information Acquisition List, which we will go on to next.



**Note to Instructor:** Some students will be accustomed to referring to an IAP as an Information Collection Plan (ICP). The instructor can explain they are one and the same, but the UN uses the word 'acquisition' rather than 'collection' due to political sensitivities connected to the latter.

## Information Acquisition List

- A daily list of information to be acquired on a given day.
- Each requirement is tasked against a specific PKISR unit / assets
- Each requirement is prioritized to ensure the most information is acquired first
- A combination of the prioritized EEIs, RFIs and I&W.

Key message. The Information Acquisition List (IAL) is a tool that captures the daily tasking of PKISR assets to acquire against specific information requirements. Tasking is aligned to the prioritisation noted in the IAP to ensure the most important information is acquired first.

The IAL is a daily tasking order that brings together the priority EEIs, RFIs and I&Ws that need to be acquired on that day.

## Command and Control

- A clear C2 structure is essential for the effective management of PKISR.
- Ideally, execute a centralised command and decentralised execution structure.
- C2 of PKISR assets may differ between missions.

Key message. It is important to have a clear understanding of the command and control of PKISR assets within your mission. Arrangements between missions may be slightly different based on mission SOPs. Ensure you understand the PKISR C2 structures once you are in the mission.

A clear C2 structure is essential for the effective management of PKISR to ensure the timely acquisition and dissemination of PKI. The most effective way to manage PKISR assets is to adopt a centralised command and decentralised execution structure. In practice, this means that at the mission level the Director/Chief of Mission Support (D/CMS) is responsible and accountable for the effective utilisation and tasking of UN commercial or military PKISR assets, however, the process of assigning effective tasking to those assets may be conducted at a lower level and managed by Chief PKISR on behalf of the MICM. There might be occasions where the control is delegated to another entity within the Force, e.g., a sector HQ for a specific operation or be retained with D/CMS. Similarly, sectors may have organic assets that are managed locally in line with sector prioritisation.



## Take Away

- Clear direction from mission leadership ensures PKISR assets are used efficiently
- Clear command and control is necessary to ensure the timely management of PKISR assets
- Establishing a mechanism based on clear terminology helps to manage the PKISR process

## Summary

The mission leadership's direction and guidance play a critical role in making sure PKISR assets are tasked efficiently. The U2, through the MICM, should ensure the leadership remains engaged and provides guidance when needed.

Clear command and control are necessary to ensure the timely management of PKISR assets. However, each mission may adopt a slightly different approach based on the context of the mission, the number of PKISR assets available and the threat. The Head of Mission will determine the approach taken by mission staff.

The PKISR process relies on a commonly understood terminology to make it as efficient as possible. It is possible that different mission entities will use different terminology to describe the same activity / function. MIO staff should not be surprised by this and do their utmost to identify differences and work through them to ensure the PKISR process is managed as effectively as possible, for example, individuals using national rather than UN terminology.

# Lesson 1.3



## PKI / PKISR Structure

### The Lesson



### Starting the Lesson



**Note to instructor:** Use this lesson to revise some of the content from the UN MIO course to ensure every participant understands the structures that form PKI, in which PKISR functions.



## Lesson 1.3

### PKI / PKISR Structure

## Slide 2

### Content

- UN Peacekeeping-Intelligence structures.
- UN PKI and PKISR coordination and management forums.

Here are the subject areas we will be covering in this lesson.

### Slide 3

## Learning Outcomes

- Explain UN PKI structures.
- Describe PKI and PKISR as an integrated process.

Let us start by reviewing the learning outcomes for this lesson. At the end of the lesson, our aim is for you to be able to assimilate these topics. Please take a moment to read and understand the requirements. As said, this should be revision for all students.

## Slide 4

### Learning Activity

- Time – 10 mins
- Mini group task
- List the UN mission PKI / security entities that operate at the operational level and could use or benefit from PKISR.
- Be prepared to discuss your answers



**Note to instructor:** During the UN MIO course, students will have been made aware of the UN entities which are involved in PKI. Use the first part of the lesson to see how much students can remember before showing the next slide. The instructor should be familiar with the next slide and its contents so that they can direct and get the most from the discussion.



**Interactive.** Split the participants into small groups. Give the groups 10 minutes to consider the peacekeeping-intelligence / security entities within a Mission that are involved in PKI. Participants should be prepared to discuss their thoughts in an open forum. Student responses should include reasons why they think the UN entity could use or benefit from PKISR.

Use the next slide to confirm student responses and fill in any knowledge gaps.

## Slide 5

### PKI Operational Structure

- Joint Mission Analysis Centre (JMAC)
- Joint Operations Centre (JOC)
- FHQ MPKI Cell (U2)
- Crime Peacekeeping-Intelligence Unit (CPKIU)
- Chief Security Advisor (CSA)
- Other Entities

Key message: Students should be aware that UN PKI is a mission-wide integrated function. There are various entities that are involved in the acquisition, analysis and dissemination of peacekeeping-intelligence. Collectively the different entities provide the necessary PKI to inform the Mission's senior leadership decision-making, including the Force Commander.



**Note to instructor:** Only refer to the notes to clarify points missed by the students during the previous learning activity or to provide a reminder of the different UN entities involved in PKI and why they would benefit from a PKI product acquired through PKISR.

Joint Mission Analysis Centre (JMAC). 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 Head of Mission (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 Chief JMAC is a civilian, who reports directly to the HoM. All MPKI and other relevant information should be shared with the JMAC and the Mission Peacekeeping-intelligence Coordination Mechanism (MICM), particularly where it relates to the IRs of the MLT and the IAP.

Joint Operations Centre (JOC). It 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. 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 relevant UN Country Team (UNCT)/ Humanitarian Country Team (HCT) entities.

The JOC focuses on current operations and can also support short-term planning. In the context of MPKI, the JOC and the JMAC will align their activities in the MICM (more of which later) 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 ensures that daily situation reports and relevant information are sent to the JOC daily or more frequently, as required. It is important to recognize that the sharing relationship must work both ways ('push' and 'pull'), with the JOC also supplying the military component with relevant information. The principles of sharing such information should be outlined in the Mission Peacekeeping-Intelligence Support Plan (MISP).

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, tactical-level peacekeeping-intelligence makes an important contribution to the mission.

Police Component/Crime Peacekeeping-Intelligence Unit (CPKIU). The CPKIU can provide valuable peacekeeping-intelligence from a police perspective.

UNDSS/Chief Security Advisor (CSA). With a responsibility to provide a coordinated approach to security and enable the conduct of UN activities while ensuring the safety, security, and well-being of UN personnel, premises, and assets, the CSA and other UNDSS personnel have access to security-related information. As such, they have much to offer to the MPKI organisation.

Other Entities. Political Affairs, Civil Affairs, Liaison, Civil-Military Liaison personnel, Disarmament, Demobilisation, and Reintegration (DDR) among others, can be a source of information. Where possible and appropriate, the U2 should develop relationships with them. These entities, on invitation from the Chief JMAC, can be members of the MICM.



## Slide 6

### PKI Operational Management Mechanisms

- Mission Peacekeeping-Intelligence Coordination Mechanism (MICM)
- MICM may also act as the means to discuss PKISR activity.

Key message: UN PKI management mechanisms are established for better cooperation and coordination among the PKI Operational providers throughout a UN mission. Again, emphasize that integration between different PKI entities is essential to inform effective decision making.

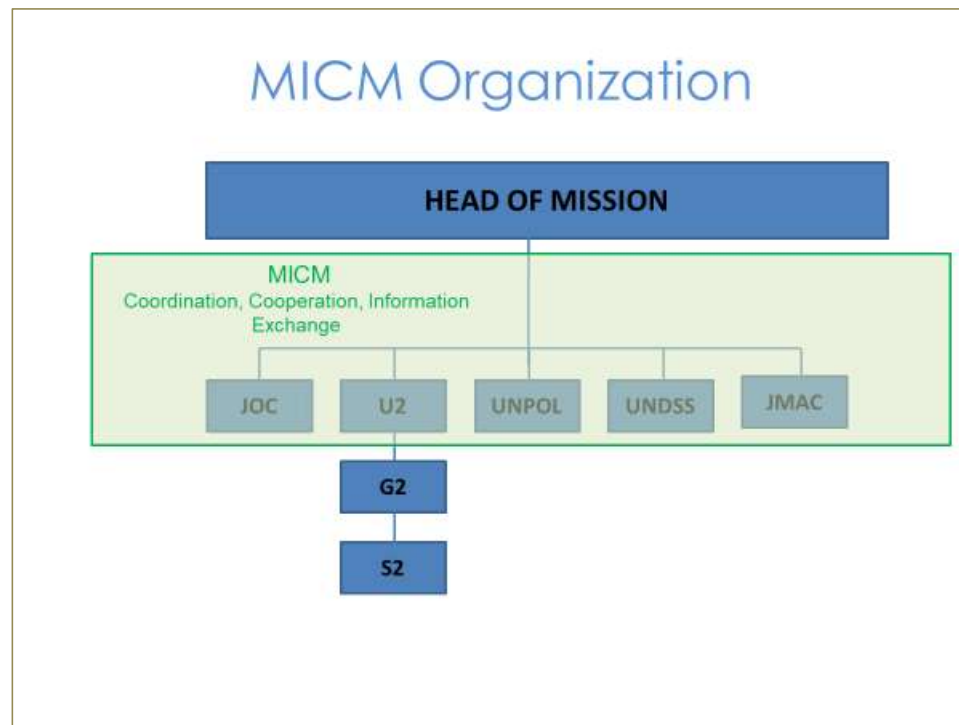
Individually, the different entities of a UN mission (UNDSS, U2, UNPOL, JOC, JMAC) are providers of operational peacekeeping-intelligence; however, when the entities work together, the result is better, more coordinated PKI. This cooperation is achieved through UN PKI management mechanisms at the operational level.

At the centre of the PKI management mechanism is the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM), which is designed to direct and oversee the PKI cycle within the mission.

In some missions, the Mission Chief of Staff fulfils an important leading role in the MICM that directs and oversees the peacekeeping-intelligence cycle within the mission.

The MICM may also be the forum for providing an update on PKISR matters since the interesting entities are the same. The PKISR management board will be covered in a couple of slides time.

## Slide 7



Key message: The diagram demonstrates the integrated nature of PKI and highlights the different entities involved in peacekeeping-intelligence acquisition, analysis, and dissemination.



**Note to instructor:** Prepare students to listen out for PKISR terminology when you talk through the slide to start to get a feel for how PKI requirements are initiated and acquired by the different entities, including the Force.

The establishment of a Mission Peacekeeping-Intelligence Coordination Mechanism (MICM) helps the HoM, or a representative, to direct and oversee the PKI cycle within the mission. Although the HOM is responsible for mission PKI, they will likely delegate the running of the MICM to the Mission Chief of Staff. Note the attendees, those being the other PKI / security entities within the mission area.

The exact nature of the MICM will vary from mission to mission, but the fundamentals are as follows:

- The structure is comprised of mission entities responsible for PKI acquisition, analysis, and dissemination. Other mission entities may be invited to participate, as required.
- The purpose of the MICM is to provide centralised control, direction and coordination of the mission's PKI system

- The functions of the MICM shall preferably be coordinated by the Mission Chief of Staff, in their role as the Chair of the Mechanism, or by the Chief JMAC.

The primary responsibilities of the MICM are outlined in the PKI Policy but include the following:

- Draw strategic guidance from senior mission leadership and translate this guidance into Priority Peacekeeping-Intelligence Requirements (PIRs).
- Manage the Mission Information Acquisition Plan (IMAP) and the acquisition effort, satisfying all senior leadership peacekeeping-intelligence requirements (IRs).
- Develop and maintain the Mission Peacekeeping-Intelligence Support Plan (ISP).

It is important to note that some of the Military PKI IRs will originate from the MICM 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.

## Role of Mission Leadership

- Mission leadership plays a key role in directing PKISR
- Clear direction helps PKISR focus on what is important to the leadership
- Continual leadership ensures PKISR assets are prioritized to acquire critical information requirements

Key message: Mission leadership plays a key role in directing PKISR.

It is important that PKISR resources acquire information that supports the leadership's decision-making process. Because there is a finite number of resources, it is essential that peacekeeping-intelligence requirements are prioritised based on the needs of the leadership. As such, it is important that the leadership provides continual direction and guidance as part of the PKISR process.

The commander must be prepared to provide direction in times when the staff cannot resolve resourcing issues themselves.



**Note to instructor:** *The direction of PKISR is something that requires co-ordination between the mission leadership and the Force Commander.*

## Slide 9

### Mission Peacekeeping ISR Management Board (PKIMB)

- A forum to provide a monthly summary of PKISR activity.
- Allows leadership to maintain an overview of PKISR activity in order to confirm acquisition priorities.
- Can be a dedicated briefing or encapsulated into another meeting (such as MICM).
- Frequency of the meeting will be determined by the tempo of PKISR activity.

Key message. The Mission PKISR Management Board provides a forum that helps Mission leadership maintain an overview of the use of PKISR assets and to determine whether PKI priorities remain valid.

The Mission PKISR Management Board (PKIMB) is a useful forum to provide leadership with regular oversight of PKISR activity, highlighting PKI priorities and confirming the effective usage and management of PKISR assets. The point of the PKIMB is to validate the priorities to support the development of the Information Acquisition List (IAL). The PKIMB can also be the venue to discuss upcoming operations. The status of PKISR capabilities must also be discussed to ensure a common picture of available assets to manage expectations.

The briefing can be a stand-alone meeting or be part of another planned event, such as the Mission Peacekeeping-intelligence Coordination Mechanism (MICM). The benefit of including it in another meeting is that it increases the visibility of the use of PKISR across the mission.

The frequency of the PKIMB will depend on the amount of PKISR acquisition assets and the complexity of the Mission.

The PKIMB should be run by Chief ISR but be chaired by Chief U2, as a minimum. All the major elements of the PKISR team will be required to brief on their specific areas of responsibility. Sector PKISR staff as well as representatives from each of the acquisition capabilities should also be required to attend via VTC. Voluntary attendance should be

encouraged across all elements of a mission, particularly the U6 or Field Technology Services (FTS) given the reliance of PKISR on robust communications networks.

## Tactical PKI Structure

- Supports UN tactical-level commanders
- Responds to PKISR tasking – feeding local PKI up the chain to inform operational & strategic PKI picture
- For MPKI, relates to G2 Sector and S2 Battalion levels
- Likely to be similar representation from police and other mission components

Key message: Tactical peacekeeping-intelligence (TPKI) is required both to support the UN tactical-level commander and respond to PKISR tasking from Force HQ.

For MPKI, TPKI relates to the G2 at the Sector level and S2 at the Battalion level; there is also likely to be similar representation from police and civilian mission components.

In many large UN peacekeeping mission areas, the Sector G2 must also be able to provide a short- and medium-term analysis by conducting its own PKISR 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.

## Establishing MPKI Architecture

- Force HQ PKI Branch (U2)
- Sector HQ PKI Branch (G2)
- Battalion HQ PKI Section (S2)
- Company HQ PKI Support Team (COIST)

Key message: The MPKI architecture is built around a central hierarchical structure of an FHQ MPKI entity (U2), with several subordinate Sector HQ peacekeeping-intelligence entities (G2), which in turn have subordinate battalion-level peacekeeping-intelligence entities (S2). It is also possible to have peacekeeping-intelligence organisations and capacities at the company level. PKISR will follow the same architecture with representation at each level.

Regardless of the exact size and scale, this hierarchical structure has two main functions:

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

This architecture relies on the adoption of common policies and working practices to allow the PKISR process to work and to allow the free flow of information and peacekeeping-intelligence among the Force. All levels of MPKI need to embrace a collaborative approach to the acquisition of information, the processing and dissemination of peacekeeping-intelligence so that they can contribute to and benefit from the PKI process.



The MPKI battle rhythm is supported and directed by the Force Peacekeeping-Intelligence Support Plan (ISP), which the U2 is charged with producing. The U2 should attend all MICM meetings and ensure liaison is taking place across all MPKI entities.

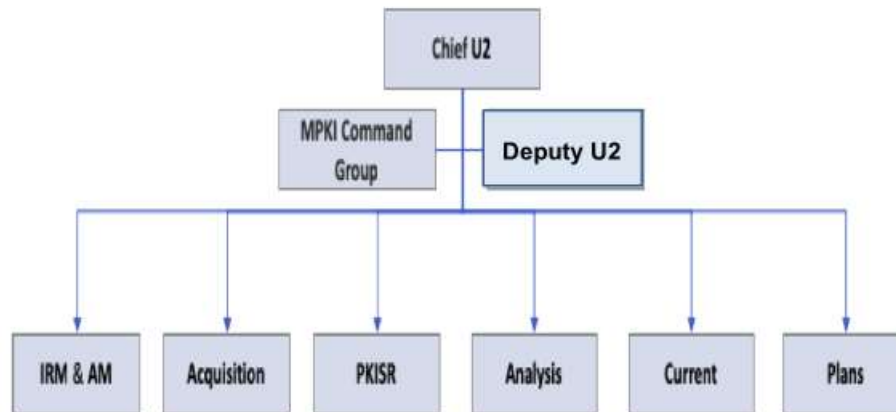


**Interactive.** Ask the students to consider the similarities and differences between the different levels of MPKI, especially regarding PKISR capability and roles. Initiate a discussion on the subject to see how much the students retained from the MIO course. The discussion should focus on issues such as:

- Size: The U2 and S2 are likely to have similar structures, although the U2 is likely to have more staff. Individuals in the S2 will likely have to take on multiple roles regarding PKISR.
- Role/focus: The roles will largely be the same in terms of enhancing situational awareness and the safety and security of UN personnel, as well as informing activities and operations related to the protection of civilians. However, the U2 is likely to be focused more on the operational level and higher tactical levels of mandate implementation, whereas the S2 will be predominantly focused on the tactical level.
- Assessment timeline: The Force HQ is often providing mid to long-term assessments, whereas the S2 is focused nearer to the current operations.

## Slide 12

### U2 Branch Structure



Key message: The structure of the U2 Branch varies from mission to mission, but it is always part of the military component. The structure and staffing of the U2 cell will change to reflect the mission's mandate and agreements in place with the Host State.



**Interactive.** Ask the students to describe the roles/tasks of each element of the U2 branch structure and how they contribute to the PKISR process. The purpose of the exercise is to see whether students understand the coordination required among the U2 entities when conducting PKISR. Use the notes below to supplement student responses or to fill gaps in knowledge.

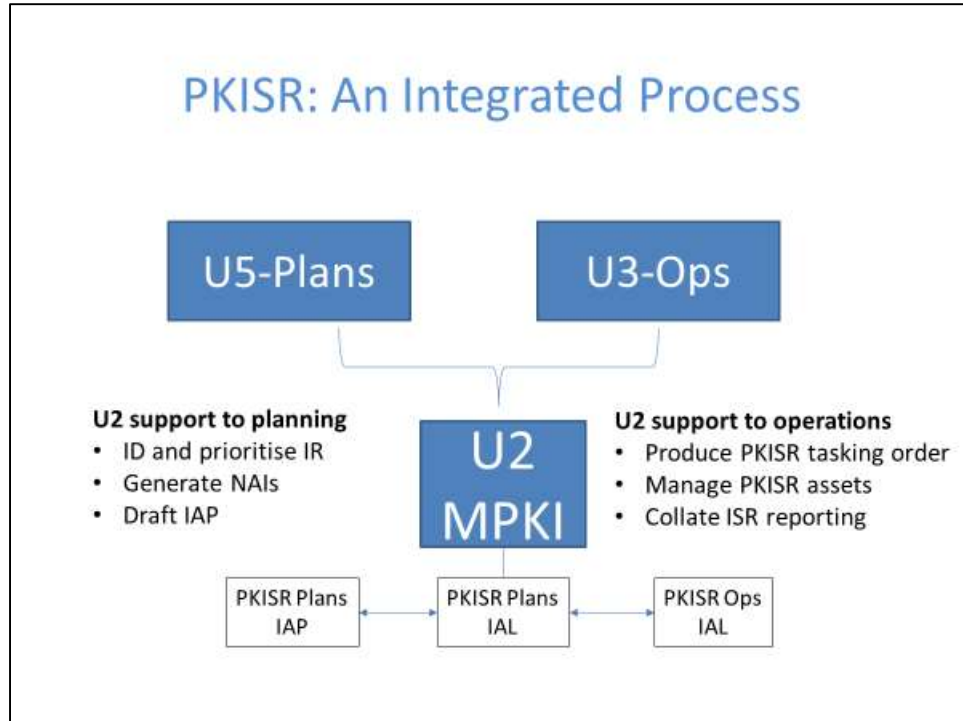
The entire U2 contribute to PKISR, from receiving and refining information requirements to the dissemination of peacekeeping-intelligence. The top tier is the leadership of the branch and provides direction and focus for all MPKI activities. The sections below perform the supporting tasks that manage the MPKI management cycle and within that PKISR. Let us go over each cell/section's responsibilities from left to right.

- **Intelligence Requirements Management and Acquisition Management (IRM&AM)** cell provides oversight and manages requirements received for follow on acquisition of peacekeeping-intelligence from various sources. The acquisition department of a peacekeeping-intelligence organisation may attempt basic initial validation of requirements and possible acquisition sources.

- **Acquisition** is responsible for detailed matching of resources and tasking resources to the information requirements.
- **PKISR** Peacekeeping-intelligence surveillance and reconnaissance section is the section that interfaces between peacekeeping-intelligence disciplines with focus on the military surveillance and reconnaissance assets to assist in employing its sensors and managing the information they gather. This section will likely manage UAS assets as well as Nontraditional airborne ISR assets.
- **Analysis section** gathers information from multiple echelons and sources to produce peacekeeping-intelligence products to meet the commander's requirements and to assist the commander in the UN MDMP.
- **Current section** tracks and disseminates information and PKI upon acquisition, based upon operational necessity and potential impact on current operations. This section supports the common operating picture.
- **Plans section** develops PKI products to support future operations, such as the MPKI estimate and the IAP. The section assists and supports the military planning process of future operations and contingency planning. This section traditionally looks outside of the traditional execution cycle.

Also, other sections/cells can be established if required, and personnel are available. i.e., Open-Source Peacekeeping-Intelligence (OPKI) cell, and production (analysis) cell, depending on the available sensors and units in the mission; the Geospatial Peacekeeping-Intelligence (GPKI) cell, Signals Peacekeeping-Intelligence (SPKI) cell, and Human Peacekeeping-Intelligence (HPKI) cell. There may also be a database/information management cell or function. Note, some of the functions outlined will vary from mission to mission.

## Slide 13



Key message: It is important for students to understand the U2/G2 works with the U5 /G5 and U3 /G3 to support the planning process and implementation of current operations.

This could include U2 support for:

- the identification and prioritisation of PKI requirements,
- the generation of named areas of interest,
- the drafting of the Force Information Acquisition Plan (IAP) as part of future planning,
- managing PKISR assets, and
- developing the IAL as part of current operations.



**Note to Instructor:** Use this slide to highlight the integration needed within the HQ to ensure PKISR is managed effectively and efficiently, and why individuals must understand their role within the process.

## U2/G2 Branch – selected responsibilities

- Manages MPKI Cycle - direction, acquisition, analysis, dissemination
- Information acquisition activities are conducted to support mission / force IRs
- Appropriate acquisition assets are tasked to acquire relevant information
- Incoming information is collated on a central database, and available to relevant personnel

The roles and responsibilities of the U2/G2 Branch are:

- Manages the MPKI Cycle, in line with the PKI Policy and MPKI Handbook, through the direction, acquisition, analysis and dissemination phases. This is to ensure that the Force Commander's decision-making process is fully supported with timely, succinct, and relevant PKI products.
- Ensures that its information acquisition activities are conducted in support of mission and force priorities and other IRs. To this end, the U2 cell will maintain an IAP that fully aligns with HoM and Force HQ IRs. This will be regularly updated.
- Ensures that appropriate acquisition assets are tasked to acquire relevant information.
- Ensures that all incoming information is collated on a central database, and available to the relevant personnel.

## U2/G2 Branch Roles/Responsibilities

- Maintains source registry
- Produces timely, relevant, concise, predictive intelligence
- Identifies trends
- Ensures Peacekeeping-intelligence aspects are included in HQ planning processes.
- Ensures a gender and protection perspective in peacekeeping-intelligence products.
- Timely PKI provided to higher / subordinate HQs

The roles and responsibilities of the U2 Branch are (continued):

- Maintains a source registry.
- 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.
- Ensures that the MPKI Estimate is complete and up to date.
- Supports all operations with a short MPKI estimate.

## Additional MPKI Elements

- Peacekeeping-Intelligence Surveillance and Reconnaissance (PKISR) Unit
- Military All-Source Information Cell (MASIC)

Key message: Depending on the mission, there may be additional PKI elements in the MPKI structure, such as a PKISR unit or Military All-Source Information Cell (MASIC).

A PKISR unit may be from a single TCC or may merge capabilities from several TCCs. The exact nature of the PKISR capabilities will differ from mission to mission, but fundamentally the capabilities are designed specifically to support information acquisition and peacekeeping-intelligence production. An example of this would be the Long-Range Reconnaissance Unit in the UN mission in Mali (MINUSMA).

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 look at a peacekeeping-intelligence problem holistically. It is likely that such a concept is currently only conceptual in nature.

## Take Away

- UN PKI and PKISR requires an integrated approach to ensure success.
- Agreed PKI and PKISR mechanisms should be in place in every UN PKO mission, however, each may differ slightly.

## Summary

Peacekeeping-intelligence is a mission function and as such requires an integrated and collaborative approach. This is often different to your experiences in a national setting; however, it is essential in a UN peacekeeping mission. Integrated mechanisms should be in place in all mission areas to facilitate this collaboration.



# Lesson 1.4



## Information and Data Management

### The Lesson

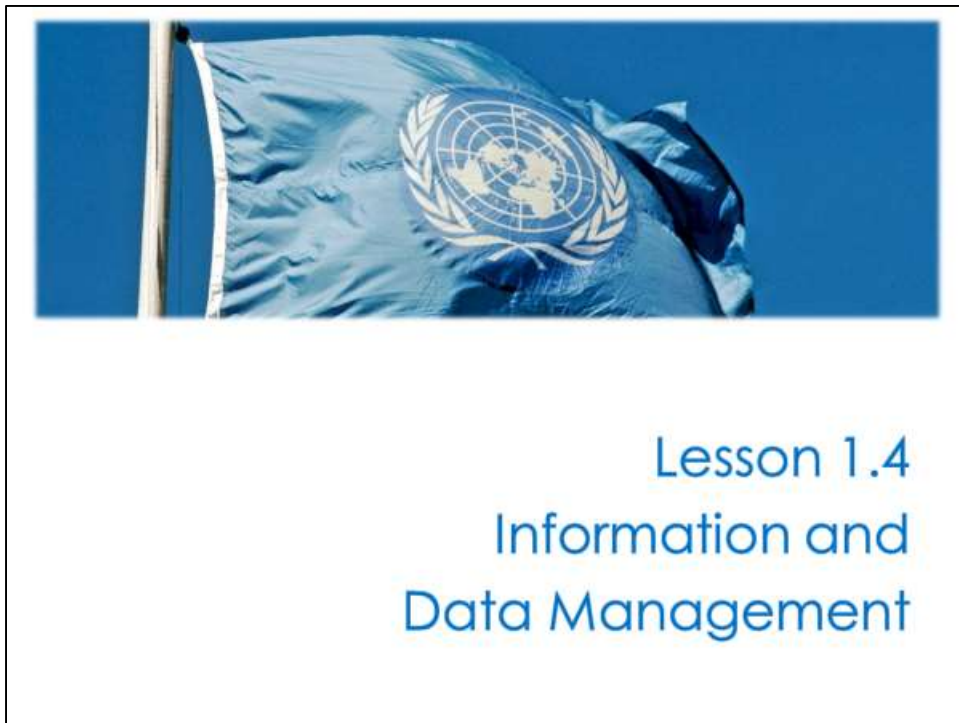


#### Starting the Lesson

The fundamental purpose of information and data management (IM) is to support missions by providing an enduring base of accessible knowledge. IM enhances the PKISR process and mitigates information anarchy – in other words, the uncontrolled use of information.

IM enables you to organize the information in a way that best supports the mission.

## Slide 1



This lesson will provide the basic measures to be considered about IM when PKISR practitioners deal with information and data.

## Slide 2

### Lesson Contents

- Importance of information management (IM) in PKISR
- IM responsibilities

Here are the subject areas we will be covering in this lesson.

### Slide 3

## Learning Outcomes

- Explain why IM is important in PKISR
- Explain IM responsibilities
- Explain the IM basics

Key message: Peacekeeping operations are complex and volatile. In the mission area, the management of information and peacekeeping-intelligence is key to success.

As the situation becomes more complex, more information is generated, which requires an effective management system in place. Information Management (IM) is one of the functions designed to receive, organise and disseminate information. The IM basics are common in any mission. No matter which HQ you find yourselves working, be it Mission, Force or Sector, the management of information in PKISR must follow the same basic guidelines.



**Note to Instructor:** *The instructor should ask whether any students have participated in a UN peacekeeping mission before or are planning to deploy to one in the future. Stress the importance of this lesson for those deploying as PKISR practitioners.*

## Slide 4

### IM in MPKI and PKISR is Common



**Information management**  
The process designed to ensure that operational peacekeeping intelligence reaches those who need it, efficiently and in a timely manner, while units and assets are exploited to optimum effect

Key message: The references for this lesson are the UN Military Peacekeeping-Intelligence Handbook (May 2019) and the Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (September 2020).

Here you can see what information management means in the MPKI context: 'The process designates to ensure that operational PKI reaches those who need it, efficiently and in a timely manner, while units and assets are exploited to optimum effect'. We will explain what this means as we progress through the lesson.

## Importance of IM in PKISR

- Key element for effective PKISR delivery
- Provide an enduring base of knowledge
- Mitigate information anarchy



Key message: IM is one of the necessary functions to ensure effective PKISR. It helps to mitigate the need for PKISR to acquire information each time a new question is asked. Indeed, an effective information management system provides a database of legacy information, which could save time and the deployment of limited ISR resources.

IM is one of the necessary functions to ensure effective PKISR delivery. It provides an enduring base of accessible knowledge that supports the PKISR process and helps to mitigate information anarchy. This can be particularly difficult in the mission area, where there is often an increasing number of information sources.



**Note to Instructor:** The instructor should emphasize that the U2/G2 deals with so much information every day. As the situation becomes unstable, the quantity of information increases. Without IM skills and management, PKISR practitioners could miss vital information when trying to answer peacekeeping-intelligence requirements. Less capable IM may negatively impact the commander's decision-making process.

## Slide 6

### IM Responsibilities

- Initiating and maintaining IM SOPs
- Electronic logging, filing and distribution of all reporting
- Timely dissemination of reports

Key message: IM is a systematic function that requires patience, consistency and attention to detail.

This slide highlights the various IM responsibilities. IM is important to ensure an effective outcome. Let us go through each in turn.

First, IM SOPs. Each mission should have its own SOPs, informed by UN policies and guidelines. PKISR will need to ensure it maintains SOPs to reflect mission guidance. SOPs should be updated to ensure compliance.

Second, ensure the management of all reporting. For example, electronic logging, filing and distribution of information and peacekeeping-intelligence. This is a core function of PKISR.

Third, the timely dissemination of reports. Needless to say, the situation changes every day. You need to ensure the right people get the right information for supporting timely decision making.

## Slide 7

### IM Basics

- Label PKISR products correctly
- Follow and maintain UN standards
- Save important emails
- Maintain distribution lists
- Standardize names, including file naming
- Archive and back-up files

[Key message:](#) All PKISR practitioners should adhere to these IM basics.

**Label PKISR products correctly.** All PKISR 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 enable you and your successor to reference information in correspondence, manage version control, and recovery files to support future requirements.

**Follow and maintain UN standards** such as file naming conventions and the protection of information. All data is to be gender and age disaggregated.

**Maintain oversight of all incoming emails.** Ensure you save important emails that have been sent and received rather than deleting them or leaving them in the inbox. This will allow you to access easily the information needed in the future.

**Maintain distribution lists.** Make sure that all distribution lists for all PKISR products are always up-to-date and accurate. You need to make sure the information you send is going to the right people.

**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. You need to be careful not to make a mistake while naming a file – errors could result in



it taking longer to retrieve information in the future, which could affect PKISR requirements.

**Archive and back-up files.** The backing-up of files mitigates the effect of lost files or when systems or hardware fails.

## Slide 8

### Effective PKISR Database

- Establish an overall database
- Maintain the database
- Check stored material
- Database accessible and security caveats



Key message: A PKISR database is an important tool. You must make yourself familiar with the databases used in mission and your role in maintaining them.

A PKISR database is a useful tool to organize information. In its simplest form, this can be a collated and cross-referenced log of PKI reports.

Establish an overall database. It allows information to be stored and retrieved to answer future peacekeeping-intelligence requirements.

Maintain the database and check that information is being stored accurately and in a consistent manner, in accordance with SOPs. It is essential that access to information is monitored and controlled at all times. This ensures individuals do not edit information without permission or make changes by mistake.

Ensuring that information on the database is accessible to the right people by using security caveats. A PKISR team needs to control who has access to the information and what they can do with the information, for example, read-only or edit. Before giving someone access to the database, a PKISR team needs to confirm why it is necessary to do so.

## Slide 9

### Report Dissemination

- Follow "need to know/ need to share" concept
- Understand who needs to see what information
- Disseminate to the right users at the right time
- Mandatory report requirement
  - Human rights abuses, Incidents of CRSV
  - Humanitarian law breaches, trafficking, crimes against children

Key message: The dissemination of PKISR products shall be done in compliance with the "need to know/need to share" concept.

Mandatory reporting is required for certain activities, such as human rights abuse, breaches to humanitarian law, incidents of conflict-related sexual violence (CRSV), trafficking and crimes against children.

Dissemination is the process of distributing formatted PKISR products to users involved in planning and decision-making. You need to determine who needs to see what information before disseminating PKISR products. You should follow the "need to know/need to share" concept. Remember, information is continually changing and as such can be relevant for only a short period of time before it becomes out-of-date. Therefore, you need to distribute products while they are fresh and relevant.

Some information must be communicated directly to the leadership even if there is no time for it to be fully processed. Examples of such information include time-sensitive data such as threats to the civilian population and mission staff. However, this information must be adequately caveated if it has not been processed.



**Note to Instructor:** Remind the students that the best PKISR product ever produced would still be considered a failure if it did not reach its intended audience in a timely fashion.



## Slide 10


### Tactical Aide

- Use checklists
- Be familiarized with IT skills (database, email, video conferencing, etc)
- Control access rights to the database
- Archive data and hard copy information
- Keep distribution lists updated

**CHECKLIST**

<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

To Do  
List: Enjoy  
today ☒



Key message: A PKISR team conducts similar actions repetitively and on a regular basis, known as battle rhythm. Once you understand the battle rhythm in the mission, it is easy to manage. Nothing is complex.

This slide highlights tips for your effective IM. PKISR requires the repetition of similar actions on a recurring basis. That is why the To-Do list (checklist) is a useful guide for the PKISR team. It is also useful when you hand over your task.

Be familiarized with IT skills prior to your deployment. IT and communication techniques are developed day by day. IT is essential to implement a Mission's mandate.

Control access rights to any IM database to manage security. Access to the database of products should only be for those individuals that need to know the information. You need to avoid anyone inadvertently deleting or editing a document that might be needed in the future.

Remember to archive data and hard copy information separately. UN databases can be updated or replaced. Data from older databases must be retained and transferred accordingly. This is particularly important during Mission transitions.

It is essential to keep distribution lists updated always. This is difficult as people move in and out of a mission area and therefore requires continual management. Distribution lists will help you to disseminate information.

## Group Discussion

### Questions

Why is IM important in PKISR?

Discuss what information should be monitored in PKISR?

(5mins for discussion)

Key message: The purpose of monitoring information is to support decision making. Critical information could be changed depending on the situation and peacekeeping-intelligence requirement. You need to be flexible.



**Interactive:** Instructors should split the class into smaller sub-groups and ask each group to consider one of the questions listed on the slide. Groups should be prepared to share their thoughts with the rest of the class.

Give each group 5 minutes to consider the question. This is not a yes/no question. This question will be good for the students' practical thinking.

The followings are possible answers:

Why is IM important to the PKISR? IM provides an enduring base of accessible knowledge that enhances PKI processing. Effective IM ensures that information and peacekeeping-intelligence is retained in the mission area beyond the time of an individual's deployment and as such, is available to follow-on units.

Discuss what information should be monitored by PKISR? The discussion could include some of the following points:

- Deployment of PKISR assets and units.
- Status of PKISR capabilities.
- Threat information.

- *Monthly summary of activity.*
- *Situation in the area of responsibility (AOR).*

## Take Away

- Effective IM supports decision-making
- PKISR has a variety of responsibilities
- Maintain distribution lists
- Follow “Need to know/Need to share” concepts

## Summary

Effective information management enhances PKISR.

PKISR is unlikely to have a dedicated IM team and as such it falls to PKISR personnel to perform this function. It is important that you understand your IM responsibilities to ensure PKISR is handled in the correct way and is accessible to the right people at the right time.



# Module 1



---

## Conceptual Framework

After Module 1, a few concluding points are worth noting:

- Policies and guidelines have been developed to create an understanding of PKI and PKISR operations in UN peacekeeping missions.
- A core set of principles underpin PKI and PKISR activities and are key to the success of peacekeeping-intelligence.
- Clear C2 is necessary to ensure the timely management of PKISR assets.
- Peacekeeping-intelligence is a mission-wide function, which requires an integrated and collaborative approach to be successful.
- Data and information management is critical and falls to everyone to ensure compliance.

# Module 2



## Legal Framework

### Module 2 at a Glance

#### Aim

Module 2 conveys to UN personnel working on peacekeeping-intelligence (PKI) key aspects of the legal framework governing their work.

#### Overview

Lesson 2.1 provides an overview of fields of general international law that relates to PKI work, the UN Charter, international human rights, humanitarian and refugee law. Lesson 2.2 reflects on aspects of the peacekeeping-specific legal framework that are relevant for PKI and PKISR, including Security Council mandates, SOFA/SOMAs and the related issue of privileges and immunities, and binding limits established under the PKI Policy, including the responsibility to protect sources from harm.

# Lesson

## 2.1



### International Legal Framework

#### The Lesson



#### Starting the Lesson

This module begins with an overview of how international law impacts PKI work.

The term 'International Law' commonly refers to a body of law that governs the legal relations between or among States and international organisations. These training materials look at international law as a combination of binding law ("hard law") and standards that are not binding as such ("soft law"). Binding international law refers to rules that are legally binding and that States must therefore apply, such as treaty law (i.e., conventions, agreements and protocols), as well as customary international law. Treaties ultimately become binding through a process of negotiation, adoption and signature, followed by ratification, acceptance, approval or accession. For UN personnel, UN policies also set binding rules.

Slide 1



Module 2  
International Legal Framework

## Slide 2

### Module 2 Content

- Legal Framework for Peace Operations:  
General international law
- Legal Framework for Peace Operations:  
Mission Specific

These are the lessons that will be delivered in Module 2.



Lesson 2.1  
Legal Framework for Peace  
Operations:  
General International Law

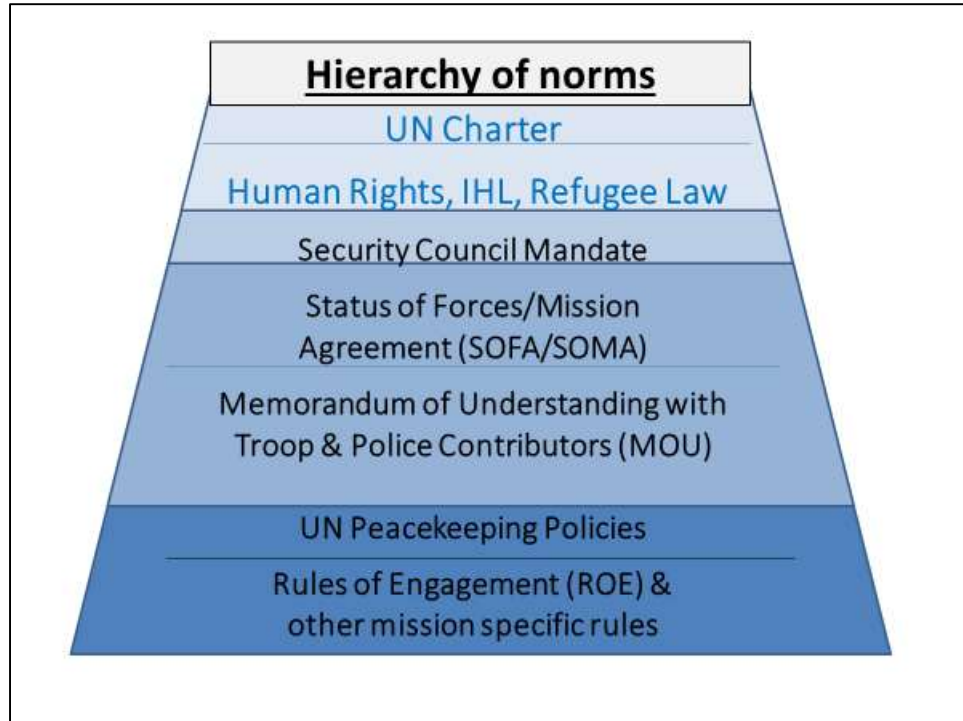
## Slide 4

### Learning Outcomes

- Apply key rules of international law relevant for peacekeeping-intelligence
- Explain what are the host state authorities in line with international humanitarian and human rights law

Here are the learning outcomes for this lesson.

## Slide 5

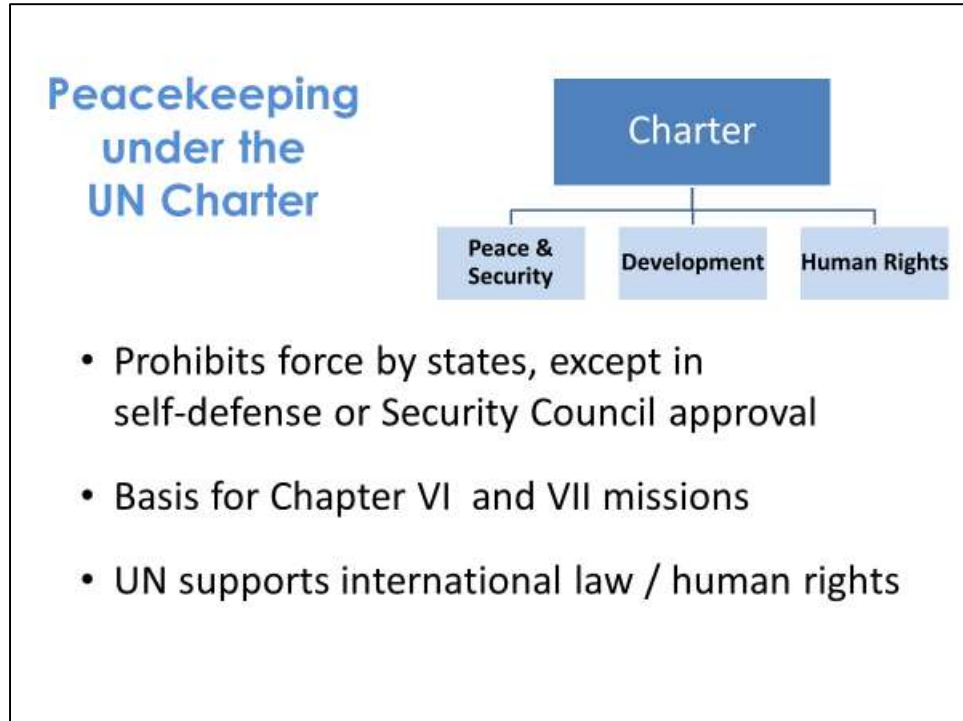


At the top of the hierarchy of norms depicted in this slide are the UN Charter (the “UN’s constitution”) and the fundamental norms of general international law. Even the Security Council must respect these norms (and does so in its practice). For instance, a peacekeeping mission could not be mandated to provide peacekeeping-intelligence to help attack civilians or push back refugees to places where their life is at risk since this would entail breaches of fundamental norms of international human rights, humanitarian and refugee law.

In Module 2.1, we are discussing mainly the top two layers of the hierarchy of norms. The remaining sources of law in this graphic will be discussed in Module 2.2.



## Slide 6



Key message: The Charter of the UN is the founding document of the Organisation and the basis of all the Organisation's work.

The UN was established to “save succeeding generations from the scourge of war” and it, therefore, prohibits force between states, except in self-defence or with Security Council approval.

While the UN Charter does not make explicit reference to peace operations, it is undisputed that the UN Security Council may establish peacekeeping and special political missions. All UN peace operations are deployed based on:

- Chapter VI (deals with pacific or peaceful settlement of disputes), and
- Chapter VII (binding measures to respond to breaches/threats to peace)

Special political missions or observer missions are generally deployed under Chapter VI. Multidimensional peacekeeping missions, which are often deployed after non-international armed conflict, usually have a mandate that invokes Chapter VII. This is done notably to clarify that they may use force to protect civilians, regardless of whether armed groups or state forces threaten civilians.


In addition to ensuring peace and security and promoting development, the UN Charter also commits the UN to promote and encourage respect for human rights. For this reason, all peace mission personnel must respect human rights, including regarding PKI. The 2011 Policy on Human Rights in Peace Operations and Political Missions also requires all missions

to advance human rights through the implementation of their mandate, even if they do not have an explicit human rights mandate or component.

Example: Where a mission is mandated to help reform the security sector, it needs to prioritise that national peacekeeping-intelligence agencies conduct themselves in conformity with international human rights law and are made subject to appropriate civilian democratic oversight mechanisms.

## Slide 7

### International Human Rights Law (IHRL)



- Protects dignity, freedom and equality
- Establishes obligations of states
- Continues to apply during war & national emergencies
- UN must respect & protect human rights (regardless of mandate)

***PKI "must be conducted with full respect for human rights, including in particular the rights to privacy, freedom of expression , peaceful assembly and association"***  
**(UN PKI Policy)**



**Interactive.** Ask participants who are entitled to human rights and whose responsibility it is to protect them. Answers should include that every human being enjoys human rights and that state authorities are primarily responsible for upholding them.

Key message: Human rights are universal. Everyone is entitled to the same fundamental rights.

There are some groups, who may have specific needs or are particularly at risk of discrimination and rights violations. These have been given specific rights protections (e.g., children, women, indigenous people, persons with disabilities).

International Human Rights Law (IHRL) always applies, including during armed conflict and other national emergencies (because that is when human rights are most under threat). Examples of human rights especially relevant to peacekeeping include the right to life, the right not to be tortured, the right not to be discriminated against, rights to food, water, health and education.

First and foremost, states must respect human rights and protect their population from threats by private actors (e.g., by ensuring that private peacekeeping-intelligence agencies do not invade the privacy of other citizens). UN policy also emphasises that UN missions and personnel must respect human rights in their work. Notably, the PKI policy requires that PKI "must be conducted with full respect for human rights, including, in

particular, the rights to privacy, freedom of expression, peaceful assembly and association".

*UN Photo shows the UN Human Rights Council in Geneva, where member states join to advance and protect human rights.*

## Human Rights affected by ISR in peacekeeping

- Right to privacy and family
- Freedom of thought, expression, information, assembly and association
- Fair trial and due process rights in the criminal process
- Protection from arbitrary detention, torture and extrajudicial killing
- Right to an effective remedy for human rights violations

Key message: peacekeeping-intelligence, Surveillance and Reconnaissance (PKISR) plays an important role in protecting peacekeepers and protecting populations from harm, but it also carries inherent risks to human rights. This is especially the case if not adequately regulated or used for ulterior purposes.

While the PKI Policy requires that PKI must be “conducted with full respect for human rights”, detailed UN regulations for all aspects of PKI have not been finalized. Staff Officers must therefore be particularly sensitive to any human rights concern that may arise in the PKI cycle and should also ensure that such concerns are anticipated and addressed in mission-specific rules and procedures. This also extends to interactions with national intelligence and security force partners, some of which may be involved in serious human rights violations.

Concerns that emerge in peacekeeping mission settings are typically linked to the following rights, which are all protected under the Universal Declaration of Human Rights that all member states have endorsed and the International Covenant on Civil and Political Rights (ICCPR), which almost all states are party to:

- **Right to Privacy:** While also analysing open sources, PKISR regularly can gain access to information that others may seek to keep private. International law prohibits arbitrary or unlawful interference and attacks on the right to privacy. Example: A mission peacekeeping-intelligence team is offered the opportunity to buy the medical files of political leaders. In such cases the PKI principles should be referred to and applied.

- **Freedom of Thought, Expression, Religion, Information, Assembly & Association:** Excessive PKISR activities may stifle freedoms of thought, expression, information, assembly and association. This may not be the intended impact. PKISR may be so disproportional in its scope that it triggers this side effect.
- **Fair Trial and Due Process rights in the criminal process:** Human rights contain safeguards that ensure that no one is prosecuted, tried and punished based on a police investigation that does not follow due process or a judicial process that does not respect fair trial guarantees. Care must be taken that PKISR competences are not abused to bypass due process and fair trial guarantees. [Note to instructors: This scenario will be covered in Case Study 1]
- **Protection from Arbitrary Detention, Torture & Extrajudicial Killing:** In some host states to peacekeeping missions, unregulated or abusive ISR activities may be abused to identify individuals that are subsequently subjected to unlawful violence. Whilst this is not PKISR, it is something that PKISR practitioners must be aware of, especially when working alongside host nation personnel.
- **Right to an Effective Remedy for Human Rights Violations:** Any human rights violations must be subject to an effective remedy. Perpetrators of serious human rights violations such as extrajudicial killings, torture or prolonged arbitrary detention must be investigated, prosecuted and adequately punished. Example: intelligence agency personnel receive blanket immunity from prosecution for abusive conduct. Victims of violations must receive effective remedies, including being given the truth about violations and receiving compensation or other appropriate forms of reparation. Example: An intelligence agency wiretapped a group of human rights activists without following due process under the law (right to privacy violation). None of the activists targeted is ever informed about having been an unlawful target of surveillance (effective remedy violation).

## Human rights safeguards in ISR and PKISR

- Publicly defined mandate and powers, limited to national security
- Organisational separation between intelligence and law enforcement services, and clear legal framework for cooperation
- Procedures for acquiring, storing and sharing intelligence
- Limits on untargeted interception of intelligence/mass surveillance
- Approval and warranted processes for invasive ISR measures.
- All ISR must be based on legitimate aim, necessary and proportional
- Intelligence agencies subject to effective internal and external oversight
- Accountable and effective remedies available

Key message: Since ISR and PKISR work is human rights sensitive, peacekeeping-intelligence entities and leadership should be subjected to regulations, processes and limits that ensure their respect for human rights. At the request of the United Nations Human Rights Council, these have been summarized in the United Nations Compilation of good practices that ensure respect for human rights by intelligence agencies.

Staff Officers should familiarize themselves with this document to ensure that their mission's PKISR work complies with the good practices as far as the institutional framework of a UN mission permits (e.g., a mission will not have judges to provide oversight or external remedies). Knowledge of these standards will also help staff officers in assessing to what extent cooperation with intelligence agencies of host states or third states can be pursued from a perspective of international human rights law (see also following discussion of the UN Human Rights Due Diligence Policy).

- The mandates of host nation intelligence services should be narrowly and precisely defined in a publicly available law and limited to national security interests. Mandates should be strictly limited to protecting legitimate national security interests (and not, e.g., to protect a particular leader's position in government). MSOs should be aware of this.

- It is a good practice to limit the tasks of intelligence services to the acquisition, analysis and dissemination of information, rather than also giving them enforcement tasks, especially for domestic intelligence agencies. While intelligence and law enforcement agencies may cooperate on issues such as counterterrorism, there should be clear rules and limits on cooperation to ensure that intelligence powers are not used to bypass due

process limits that apply in law enforcement (e.g., in relation to surveillance). MSOs should be aware of this.

- Clear procedures should outline what surveillance means intelligence agencies may use to acquire intelligence, how long such information may be stored (there should be time limits) and with whom it may be shared. In particular, there need to be limits on mass surveillance that targets entire populations rather than specific target persons. Invasive surveillance measures such as wiretapping should be subject to warrant and other authorization processes. Whilst this mainly applies to host nations, some aspect of this apply to PKISR activities such as information storage.
- All intelligence work should be overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law, the effectiveness and efficiency of their activities; their finances; and their administrative practices. Peacekeeping operations do not have parliamentary or judicial institutions, of course, but DPO rules provide oversight functions to the (civilian) head of mission (HoM). For instance, under DPO rules, the HoM has to authorize the use of a human source that works for the host state or the sharing of peacekeeping-intelligence products with national actors.



### Case Study 1 – Wiretap:

*The host state police wants to wiretap a political dissident but fails to obtain the necessary judicial warrant. Instead, they ask the UN Mission's military intelligence branch (U2) to carry out the electronic monitoring and pass on relevant information (in exchange for information to keep the mission secure).*



**What are relevant legal obligations?**



**Interactive.** *The case studies included in this lesson provide practical examples of legal challenges that arise in PKI work. Depending on the time available and the course size, instructors can ask participants to discuss each case first in groups and then debrief in plenary. For smaller course groups, the case study can also be discussed directly in the plenary. Initially, show only the case study (in italics) and then reveal the relevant legal obligations in the red box only during the debriefing.*

*Ask the students what they believe the relevant legal obligations are. Below are some points that will help you facilitate the discussion:*

- *Opposition enjoys the right to freedom of expression and political rights.*
- *Right to privacy infringements requires legal basis & legitimate objective.*
- *The mission must respect national law as per SOFA/SOMA.*
- *UN must not aid or assist human rights violations.*
- *Risk assessment under UN's Human Rights Due Diligence Policy (HRDDP).*

The case suggests that the host state police is using surveillance for an illegitimate objective, namely, to suppress the freedom of expression and other political rights of dissidents. In addition, wiretapping constitutes an infringement on the right to privacy. It, therefore, needs to have a legal basis in national law. States that respect human rights

and the rule of law will require that law enforcement obtains a judicial warrant for such an invasive measure. However, this is not done in this case.

Law enforcement authorities may not evade privacy safeguards by “outsourcing” their surveillance to intelligence actors, whether to national intelligence agencies or, as in this case, the UN’s military peacekeeping-intelligence resources.

The mission must not accept this request. Firstly, it must respect national law, as per the SOFA/SOMA, and must hence not help the police evade the requirement of a judicial warrant. Secondly, the UN must not become complicit in violations of the human rights to privacy, freedom of expression and other civil and political rights by aiding and assisting the national police based on this illegal request.

To limit the legal risk of aiding and assisting grave violations of international law, the Secretary-General established the Human Rights Due Diligence Policy on UN support to non-UN Security Forces (HRDDP), which will be discussed.

In response to increasing threats against peacekeepers and civilians, many missions are increasing their surveillance resources. This makes it even more important that missions take care that others do not misuse their peacekeeping-intelligence.

## Slide 11

### Human Rights Due Diligence Policy

UN Support to non-UN Security Forces

*UN support to non-UN Forces cannot be provided:*

- Risk of entities committing **grave violations** of Int. humanitarian, human rights or refugee law
- relevant authorities fail to take necessary **corrective or mitigating measures**

**Prevents legal liability for aiding violations, promotes human rights & protects U.N. credibility**



Key message: HRDDP is binding for the entire UN (not just peacekeepers). The Secretary-General established it, and the Security Council has repeatedly endorsed it.

According to the HRDDP, support to non-UN security forces cannot be provided where:

- there are substantial grounds for believing there is a real risk of the receiving entities committing grave violations of international humanitarian, human rights or refugee law; or
- the relevant authorities fail to take the necessary corrective or mitigating measures.

All UN entities that plan to or are already providing support to non-UN security forces must, therefore, assess the risks involved in providing or not providing such support. This assessment needs to consider the risk of the recipient entity committing grave violations of international humanitarian law, human rights law or refugee law. Furthermore, the UN must consider whether any mitigation measures can reduce the risk of violations (e.g., by monitoring the use of peacekeeping-intelligence shared or excluding problematic areas from peacekeeping-intelligence sharing agreement). The guidelines on sharing PKI and receiving Intelligence provide further detail.

It serves to ensure that the UN does not support or collaborate with host state elements that are involved in grave violations of human rights, IHL or refugee law. The policy serves to protect the United Nations and its staff from inadvertently aiding violations committed

by others and related legal liabilities. Distancing the UN from state forces involved in grave violations also protects the UN's reputation and perceived impartiality.

In peacekeeping settings, some national intelligence agencies and other security forces may engage in grave violations such as forcibly disappearing opposition supporters, targeting civilians in military operations or systematically spying on human rights defenders through extensive surveillance. peacekeeping-intelligence shared by the UN can inadvertently further such grave violations. For this reason, the PKI Policy emphasises that "[w]here peacekeeping-intelligence may be shared, either directly or indirectly, with non-United Nations security forces, the Human Rights Due Diligence Policy on United Nations Support to Non-United Nations Security Forces (HRDDP) applies".

*The UN Photo shows MONU (now known as MONUSCO) providing transport to national army units in the Democratic Republic of the Congo. When the United Nations found that some national army units who received UN support were violating human rights, the Security Council made further MONUC support conditional on compliance with human rights. The HRDDP was established against the backdrop of MONUC's conditionality policy.*

## Slide 12



- ✓ Applies to **all types of support** to states and regional organizations, including intelligence sharing (exceptions for human rights & mediation work)
- ✓ Supporting entity must initiate risk assessment & **monitor** compliance
- ✓ **Risk mitigation & engagement**, not blunt conditionality
- ✓ Suspension or withdrawal of support is **last resort**

**Application of HRDDP**

Key message: Any support provided by the UN to non-UN security forces must follow the HRDDP.

Relevant support provided by peace operations includes the conduct of joint operations, planning support, sharing of peacekeeping-intelligence, training, capacity building, mentoring, technical cooperation and financial support. As noted, sharing peacekeeping-intelligence amounts to provide technical advice, capacity building or equipment to national peacekeeping-intelligence agencies. Certain areas are exempted from the HRDDP:

- Training and engagement on IHL and human rights [as these activities seek to address the very problems the HRDDP is concerned with].
- Mediation-related support (e.g., transporting officers to peace negotiations) [UN's good-offices role takes preference].
- Medical/casualty evacuation [saving life takes preference].

HRDDP also covers support provided to regional organisations, for instance, support to African Union peace and security operations such as AMISOM.

Applying the HRDDP, notably when sharing peacekeeping-intelligence, requires several steps:

- Before sharing any peacekeeping-intelligence, the entity within the mission that wants to share (e.g., the UN Force) must initiate a risk assessment and determine if there is a

real risk that the recipient is or will be committing grave HR violations. Note that it is not required that there is a causal link between the envisaged support and the violation, i.e., support may be considered too risky even if the support itself does not aid or assist in the violations themselves. Most missions have established standard operating procedures for this risk assessment to be completed that involve input from human rights sections, JMAC and other relevant components.

- Even if the initial risk assessment shows a real risk, this does not categorically exclude peacekeeping-intelligence sharing. The HRDDP is not a blunt conditionality tool but fosters engagement with national authorities intending to find solutions. Instead, the mission must determine whether it can establish mitigatory measures to reduce the risk to an acceptable level (low risk). Example: The mission may exclude certain sensitive areas from peacekeeping-intelligence sharing (e.g., any peacekeeping-intelligence on unarmed civilians). Or it may insist on joint after-action reviews on how shared peacekeeping-intelligence (e.g., on armed groups threatening civilians) was used in subsequent military operations and how IHL targeting requirements were respected. Or it may demand that the host state first upgrades effective civilian democratic oversight mechanisms for the national intelligence sector.
- Before sharing peacekeeping-intelligence, it must also be ensured that the mission can monitor the recipient's subsequent conduct, so that the mission can intervene in advance of the recipient committing grave HR violations, e.g., through advocacy between military counterparts or, where appropriate, the mission leadership. If grave HR violations persist despite such interventions, the mission must temporarily suspend peacekeeping-intelligence sharing or, if no improvement can be expected, terminate peacekeeping-intelligence sharing altogether.

*Photos show the UN training national armies, which must comply with HRDDP.*



## Case Study 2 – Information Request:

*The U2 requests the host state's national military intelligence agency to obtain certain information from armed group fighters detained by the agency. It is well known that the national military intelligence agency systematically uses violence to "break" its detainees and make them speak.*

**What are the relevant legal obligations?**



**Interactive.** Case Study to be discussed by groups or in plenary: Ask the students what the relevant legal obligations are. Below are the points for you to facilitate student discussions.

- IHL and human rights duty to treat detainees humanely
- Torture as a crime against humanity and a war crime
- Prohibition against soliciting the commission of an international crime

Mission components like security (UNDSS), UNPOL or the Force will regularly set up channels of communication to share sensitive information, including peacekeeping-intelligence products, notably to keep the mission safe and protect civilians. Details on the process and relevant safeguards to avoid misuse are set out in the Guidelines on the Exchange of peacekeeping-intelligence/Peacekeeping-Intelligence with Non-UN and Non-Mission UN Entities.

While the HRDDP applies to share information with national peacekeeping-intelligence partners, there are also risks of violations of international law when requesting intelligence from national authorities. In the case at hand, the national intelligence agency is systematically using torture to make detainees speak. This is not only a grave human right and IHL violation but would also amount to a war crime and a crime against humanity.

The mission's request for information extracted from the detainees would inadvertently solicit more such violations and make the mission and PKI personnel legally complicit. The U2 must, therefore, not make the request concerned.

Note, that it does not matter whether host state intelligence officers conduct the investigation or whether the U2 sends its own officers to interrogate. In both cases, the environment of torture forces detainees to speak and UN personnel would become complicit to torture.



## International Humanitarian law (IHL)

- Applies to parties to armed conflict
- Military peacekeepers engaged in hostilities
- Regulates conduct of hostilities
- Restricts means of warfare
- Protects those who do not or no longer engaged in hostilities



Key message: IHL regulates the conduct of hostilities. Example: Requiring parties to minimise as far as possible the harm to civilians not participating in the hostilities. It also outlaws certain means of war to reduce unnecessary suffering by civilians or combatants — for example, the prohibition of the use of any chemical or poisonous weapons in warfare.

Parties must respect International Humanitarian Law (IHL) to armed conflicts, such as States forces fighting each other in an international armed conflict. In a non-international armed conflict involving non-state armed groups, the state military forces, and the non-state armed groups involved must all abide by IHL norms governing such conflicts.

Since impartiality is a central principle of peacekeeping, UN military forces are generally not a party to the conflict. However, IHL may apply temporarily to them for as long as they engage as combatants in armed conflict. Example: a peacekeeping force carries out an offensive operation against an armed group that poses a grave threat to civilians.

Parties must respect IHL themselves and ensure that others respect it as well. Example: following its obligation to ensure respect for IHL, a state has a duty to prosecute and punish non-state armed group members who commit serious violations of IHL amounting to war crimes.

*Illustration* shows the emblem of the International Committee of the Red Cross (ICRC), which initiated the development of humanitarian law in the 19<sup>th</sup> century. The ICRC remains the neutral guardian of IHL in conflict areas worldwide.

## Protected Persons under IHL



- Civilians not directly participating in hostilities
- Medical and religious personnel of armed forces
- Wounded, sick and others *hors combat*
- Prisoners of war & interned armed group fighters
- Peacekeepers (unless engaged in military hostilities)



**Interactive.** Ask participants to point out the civilian in the two pictures. The armed herder on the right may well be a civilian who is only armed to protect himself and his cattle from marauders. In many mission settings, armed civilians are a common sight, and them carrying weapons like assault rifles does not necessarily mean that they are participants in hostilities between militarily organised parties to the conflict.

Key message: Under IHL, any person who is not or is no longer directly participating in hostilities shall be considered a civilian, unless they are a member of armed forces or groups.

In case of doubt, the individual or group of individuals shall be considered civilian and afforded the protection owed to civilians until determined otherwise. Civilians may be in possession of arms, without necessarily being combatants. Under international humanitarian law, civilians who are in possession of arms, for example, for the purpose of self-defence and the protection of their property but who have not been or are not currently engaged in hostilities, are entitled to protection.

Members of armed forces or armed groups that are *hors de combat* ("out of battle") also enjoy protection under international humanitarian law. Notably, those who can no longer fight because they are wounded and sick must not be attacked but collected and medically cared for.

Prisoners of war (POWs) and interned/detained armed group fighters enjoy special protection. They must be treated humanely in all circumstances and not be subjected to any humiliating and degrading treatment. Unlike regular soldiers who become POWs, captured rebel fighters may be prosecuted for their participation in the armed conflict. However, this must be done before “a regularly constituted court, affording all the judicial guarantees which are recognised as indispensable by civilised peoples” (see Common Art. 3 Geneva Conventions.)

Peacekeepers, regardless of whether they are military, police or civilians, are protected under international law. Directing attacks against them may amount to a war crime. An exception applies only for as long as military peacekeepers engage in hostilities.



**Note to Instructor:** *The process and safeguards concerning persons detained by missions are detailed in the UN Standard Operating Procedures on Detention by United Nations Peace Operations<sup>1</sup>, which are binding on all UN personnel. All personnel should familiarise themselves with these important SOPs and the mission-specific procedures to implement them.*

---

<sup>1</sup> 2020.13 Handling of Detention in United Nations Peacekeeping Operations and Special Political Missions (SOP) - [<http://dag.un.org/handle/11176/401086>]

### Case Study 3 – Injured Fighter:

*UN forces capture a badly injured armed group fighter. UN personnel tell him that he will receive medical care once he discloses where his group placed improvised explosive devices (IEDs) that may harm the mission.*



**What are the legal obligations?**



**Interactive.** Case Study to be discussed in group work or in plenary. Ask the students what the legal obligations are. Here are a few points to help in the facilitation of the discussions.

#### *Legal Obligations:*

- *Care for all wounded.*
- *Humane treatment of all detainees.*
- *Prohibition of cruel treatment and torture.*
- *Art. 3 Geneva Conventions & SG Bulletin on IHL.*

IHL also protects combatants who can no longer take part in hostilities, notably because they are incapacitated (hors de combat), injured, have surrendered or are detained.

Wounded persons such as the injured fighter, in this case, must receive, to the fullest extent practicable and with the least possible delay, the medical care and attention required by their condition. No distinction shall be made among the wounded on any grounds other than medical ones, i.e., the UN must provide this detainee with the same level of medical attention that it would give to its own forces.

Medical attention must not be withheld to extract information since this would violate the obligation to treat all detainees humanely that can be found in Common Article 3 of the Geneva Conventions. Given that the fighter's grave suffering is used as leverage to obtain information, withholding medical aid contrary to the UN's obligations would also

constitute a form of cruel treatment and torture, which is prohibited under IHL (and human rights law). It does not matter that the fighter may be able to reveal crucial information about explosives that may harm the mission. The prohibition of torture under international law is absolute and may not be breached even to extract life-saving information. From an operational perspective, it is also highly unlikely that the fighter would provide accurate information under the circumstances because torture most often leads to faulty peacekeeping-intelligence.



**Note to Instructor:** *The United Nations embraces a standard approach to non-coercive interviewing, which is detailed in the UNPOL Manual on Non-Coercive Interviewing. Personnel engaged in any interviews (interrogations) of detainees or others should familiarize themselves with this very effective approach and apply it.*

## International Humanitarian Law: Conduct of Hostilities

- **Distinction** between civilians & combatants
- **Precaution** to minimize risks for civilians
- **Proportionality** to limit incidental harm to civilians



Key message: In their conduct of hostilities, parties to the conflict must abide by basic principles to minimize harm to civilians and civilian objects such as homes, hospitals, places of worship etc.

The protection of civilians in the conduct of hostilities builds on three basic principles:

- **Distinction:** To ensure respect for and protection of the civilian population and civilian objects, parties to the conflict always have to distinguish between the civilians and combatants, and between civilian and military objects. Operations must only be directed against military objects. Indiscriminate attacks that do not distinguish between civilians and combatants are prohibited. Example of violation: shelling an entire village with heavy artillery without trying to distinguish between military targets and civilian homes.
- **Precaution:** In the conduct of military operations, constant care must be taken to spare civilians and civilian objects. All feasible precautions must be taken to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects. Examples of violations:
  - Before launching an assault, no effort is made to verify that the target is a military target.
  - Soldiers take their positions too close to civilians, placing the civilians at risk of getting caught in the crossfire.

- **Proportionality:** Loss of life and damage to property incidental to attacks must not be excessive concerning the concrete and direct military advantage expected to be gained. This means that when considering a target, the damage to civilians and their property cannot be excessive about the military advantage gained. Proportionality is not an issue if the target is purely military, and no civilians are nearby. Example of violation: bombing a private home housing dozens of civilians to kill one ordinary soldier who took shelter there.

*Civilians often bear the brunt of conflict. The UN Photos show civilian homes that were burnt down during armed conflict and an elderly civilian injured.*



## Case Study 4 – Allies:

*The mission's PKI cell shares aerial images of enemy positions in densely populated areas with a regional peace enforcement mission.*

*As was foreseeable, the regional force shells entire neighbourhoods without taking any measures to protect the civilian population.*

**What are the  
legal  
Obligations?**



**Interactive.** Case Study to be discussed in group work or in plenary. Ask the students what the legal obligations are. Below are a few points for your use in facilitating the discussions.

- War crime: Indiscriminate attack
- IHL Duty of Precaution
- Avoid complicity in war crime
- Human Rights Due Diligence Policy

The regional force violates basic principles of IHL by launching what amounts to indiscriminate attacks that fail to distinguish between military targets and the civilian population. Furthermore, no precautions are taken to protect civilians. As these violations would amount to war crimes, PKI personnel must take particular care to ensure that through their peacekeeping-intelligence support, they do not knowingly assist international crimes and therefore incur responsibility themselves.

Once again, the HRDDP, which also applies to support to regional forces, is the appropriate tool to address this legal risk. An initial risk assessment would show a high risk of grave violations and the mission must determine whether mitigation measures can bring the risk down to an acceptable level. For instance, the mission could insist that it will only provide further aerial imagery if the regional force adjusts its rules of engagement in line with IHL and agrees to monitor after-action reviews to make sure the rules of engagement are followed. Training measures can also be envisaged to teach

commanders that the current approach not only violates IHL but is likely to lose the hearts and minds of the local population. The regional force could also introduce a civilian casualty tracking system to monitor the impact of its own operations.

The supporting entity should work closely together with the mission's human rights component and Protection of Civilian (PoC) adviser to monitor the conduct of the regional force. If violations persist despite mitigatory measures, peacekeeping-intelligence can no longer be shared.

## International Criminal Law

- **War crimes**  
Grave breaches -Geneva Conventions / serious IHL violations
- **Crimes against humanity**  
key feature: systematic or widespread inhumane acts
- **Genocide:**  
Intent to destroy national, ethnic, racial, religious groups
- **State duty to prosecute**
- **International tribunals**  
(e.g. International Criminal Court)



Key message: Some violations of human rights and international humanitarian law are considered so grave by the international community of states that they are regarded as international crimes, namely war crimes, crimes against humanity and genocide.

All states have a duty to prosecute and punish such crimes if committed within their territory. Furthermore, the international community may set up international tribunals and courts to prosecute and punish international crimes. Example: in response to international crimes, the Security Council set up the International Criminal Tribunals for the former Yugoslavia (ICTY) and Rwanda (ICTR). States also established the International Criminal Court (ICC). The ICC has jurisdiction to pursue international crimes committed in states that have accepted its jurisdiction (more than 120 countries so far) and in places that were referred to the ICC by the Security Council (examples: Darfur and Libya).

There are three major categories of international crimes that UN staff should know:

**War crimes:** Violations of fundamental rules found in the Geneva Conventions or other sources of IHL also entail war crimes on the part of the individuals who commit such crimes. As the name suggests, war crimes can only be committed in armed conflict.

**Crimes against humanity:** Where state authorities or armed groups commit inhumane acts such as murder, rape, torture in a systematic or widespread manner attack, with knowledge of this broader attack, this may entail crimes against humanity. Such crimes typically involve an underlying policy to commit crimes and an elaborate degree of planning at high levels.

**Genocide:** Following the 1948 Genocide Convention, killing, harming or imposing conditions of life calculated to bring about the physical destruction of a national, ethnical, racial or religious group in whole or in part amounts to genocide. The perpetrators must act with the “intent, to destroy, in whole or in part, the group, as such.” For example, it is not enough to kill some people because of their religion or race. There must be an intent to annihilate the entire group globally or in a specific area. Moreover, the crime of genocide does not contain a numerical requirement as it is the genocidal intent that matters when assessing whether the crime has been committed. The historical example that gave rise to the notion of genocide is the Holocaust, in which Nazi Germany tried to annihilate the entire Jewish population of Europe.

As noted above, sharing peacekeeping-intelligence with security forces engaged in international crimes can lead to legal complicity (soliciting or assisting crimes) if risks are not properly assessed before peacekeeping-intelligence is exchanged.

*The UN Photo shows the entrance to the International Criminal Court in The Hague, which has prosecuted international crimes committed in mission settings.*

Sources of International Law	
<b>International Human Rights Law</b> <ul style="list-style-type: none"> <li>• UN Charter</li> <li>• Human rights treaties</li> <li>• Universal Declaration of HRL</li> </ul>	<b>International Humanitarian Law</b>
	<u><b>International armed conflict:</b></u>
	Geneva Conventions Protocol I
	<u><b>Non-international armed conflict:</b></u>
<b>International Criminal Law</b> <ul style="list-style-type: none"> <li>• Int. criminal court</li> <li>• Customary Int. law</li> </ul>	Art. 3 Geneva Conventions Protocol II

Key message: The content of international humanitarian, human rights and criminal law is defined by international treaties that states have voluntarily signed and ratified. Many of the norms have also been practised and accepted by states to such a degree that they have become customary law that binds all states.

Apart from explicit mentioning human rights in the United Nations Charter, states have adopted nine major human rights treaties. They cover civil, political, economic, social and cultural rights and protect specific groups such as women, children, or persons with disabilities. Every state in the world has accepted several of these treaties. All states have also expressed their support for the Universal Declaration of Human Rights, which was first adopted by the UN General Assembly in 1948. Most, if not at all, of the rights in the Universal Declaration can be considered customary law.

International humanitarian law can be found notably in the four Geneva Conventions and their two Additional Protocols. For larger, multidimensional peacekeeping missions the norms applying in non-international armed conflict (NIAC) are most relevant: The most basic protections in NIAC are laid down in Common Article 3 of the four Geneva Conventions of 1949. Further details are set out in Geneva Protocol II. Fundamental rules of international humanitarian law have also become international customary law.

International criminal law emerged from the practice of the Nuremberg and Tokyo tribunals that prosecuted major crimes committed during World War II. The principles of international criminal law they developed have become customary law. The Rome Statute of the International Criminal Court has summarized that law in one treaty.

## International Refugee Law



- 1951 Refugee Convention:
  - Fear of **persecution** due to race, religion, political opinion
  - International protected status
  - Protected under UNHCR mandate
  - Refugee rights
- 1969 African Refugee Convention-  
Refugees also persons fleeing **armed conflict**
- 1984 Cartagena Declaration on Refugees-  
Persons fleeing internal conflicts & generalized violence



Key message: When governments are unwilling or unable to protect their citizens or persecute themselves, individuals may be at risk of such serious violations of their rights that they are forced to flee their country and seek safety in another country. Since, by definition, the governments of their home countries no longer protect the basic rights of refugees, the international community must step in to ensure that their basic rights are respected.

The 1951 Convention Relating to the Status of Refugees is the foundation of international refugee law. The term “refugee” under the Refugee Convention refers to persons who have to flee their country due to a “well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion”. Individuals suspected of crimes against humanity are excluded from refugee status.

Fleeing a country where an armed conflict is taking place qualifies a person only as a refugee if specific requirements are met (notably evidence of individual “well-founded fear of being persecuted”). However, regional instruments have expanded the scope of the refugee definition. Under the 1969 African Refugee Convention, refugees are also those who must flee “events seriously disturbing public order” such as armed conflict.

For Latin America, the Cartagena Declaration on Refugees expands the concept also to include persons who flee internal conflicts and generalized violence in their country.

Refugees are generally civilians, and the mission must hence protect them under its PoC mandate. Also, peacekeeping operations are often tasked with the creation of

conditions conducive to the voluntary, safe, dignified and sustainable return or local integration of refugees and Internally Displaced Persons (IDPs).

*Refugees exist around the world. The [UN Photo](#) shows refugees in the Balkans.*



### Case Study 5 – Refugees:

*JMAC obtains intelligence that the host government plans to force refugees to return to their home country where political oppression and armed conflict continues to persist. The JMAC chief wonders how that information is relevant.*

Are there concerns here and appropriate cause for action?



**Interactive.** Case Study to be discussed in group work or in plenary. Ask the students if there are concerns and if there is an appropriate cause for action. Here are points to consider for facilitating the discussions:

- Prohibition of non-refoulment under 1951 Refugee Convention and regional conventions
- Deportation of populations as a war crime or crime against humanity
- Responsibility to alert Protection of Civilians (PoC) coordination structures
- Responsibility to alert human rights component & UNHCR

The peacekeeping-intelligence obtained by JMAC points to refoulment, a grave violation of international refugee law. The country which plans to deport them is violating the fundamental principle of non-refoulment. Under the 1951 Refugee Convention, countries may not expel or return ("refouler") a refugee in any manner whatsoever to the frontiers of territories where their life or freedom would be threatened on account of their race, religion, nationality, membership of a particular social group or political opinion. Under regional conventions, it is also prohibited to send them back to a place where armed conflict persists. The forcible return of refugees, without a valid legal basis in international law, may even amount to the crime against humanity of deportation (if systematic) or deportation as a war crime (if done by a party to an armed conflict in the context of that conflict).




The JMAC chief should immediately bring this matter to the attention of the protection of civilians' coordination structures that every mission with a PoC mandate has. The JMAC chief must also alert the human rights component. Furthermore, the mission should bring the matter to the attention of the UN High Commissioner for Refugees, the agency with the specific mandate to protect refugees and their rights.

## Slide 23

### Rights of Refugees

- Prohibition of expulsion or return if real risk (“*Refoulement*”)
- Prohibition of discrimination for race, religion or country
- Freedom to practice religion
- Right to acquire property
- Access to courts
- Public education
- Freedom of Movement

The UNHCR logo is a circular emblem featuring a blue border. Inside, there is a white background with a blue silhouette of a person's head and shoulders. Below the silhouette, the text "UNHCR" is written in blue, and below that, in smaller blue text, "The UN Refugee Agency".

Key message: Refugees enjoy special status and related rights under international law. Since they have lost the protection of their home country, which has persecuted them, they are under the protection of the United Nations High Commissioner for Refugees.

Rights of refugees include, for instance:

- The right not to be subjected to refoulement (see the previous slide)
- No discrimination due to race, gender, religion, social origin or country of birth
- Freedom of religion
- Right to acquire property
- Access to courts
- Public education
- Minimum treatment and assistance
- Freedom of movement

*The illustration shows the emblem of the United Nations High Commissioner for Refugees (UNHCR). Not to be mistaken with the Office of the United Nations High Commissioner for Human Rights (OHCHR).*

## Internally Displaced Persons (IDPs)

- **Forced to flee** (due to war or natural disaster)
- Have **not crossed an international border**
- No special international status; Home state must protect
- Keep human rights & rights as citizens
- Protection reinforced by:
  - UN Guiding Principles on Internal Displacement
  - AU Convention on Internal Displacement in Africa

Key message: The protection of IDPs and other affected populations within their own country is primarily the responsibility of national authorities.

Internally displaced persons (IDPs) may have been displaced due to armed conflict, generalized violence, violations of human rights, natural or human-made disasters. But, unlike refugees, they have not crossed an international border, but remain in their own country.

Unlike refugees, IDPs do not enjoy a special legal status under international law. However, the international community has a role to play in promoting and reinforcing efforts to ensure protection, assistance and solutions for IDPs. UNHCR generally considers them to be of concern to its mandate and the mission will often make special efforts to protect IDP sites under its PoC mandate.

IDPs keep their human rights and also their rights as citizens of the country. For instance, IDPs maintain their citizen's right to vote in elections. Therefore, the state has to arrange that they can vote at the site of their displacement.

In 1998, the UN Representative of the Secretary-General on IDPs issued the Guiding Principles on Internal Displacement. The principles, which have been repeatedly endorsed by the international community of states, summarize binding legal obligations that can be found in international humanitarian and human rights law. The African Union has adopted the Kampala Convention on Internal Displacement in Africa, which further reinforces the protection of IDPs.

Displaced populations, IDPs and refugees, are typically civilians in a particularly vulnerable situation. Gathering PKI about threats facing them should be a priority.

## Take Away

- PKI personnel must assess how their work impacts on human rights and IHL. Compliance with the HRDDP ensures that they do not become complicit to violations of international law
- Like other civilians, refugees and internally displaced persons are of concern to the mission and hence its PKI priorities

## Summary

Key take aways for this lesson include the following. Let us review these topics:

- PKI personnel must assess how their work impacts on human rights and IHL. Compliance with the HRDDP ensures that they do not become complicit to violations of international law
- Like other civilians, refugees and internally displaced persons are of concern to the mission and are therefore a PKI priority

# Lesson

## 2.2



### Legal Framework for Peace Operations – Mission-Specific

#### The Lesson



Starting the Lesson

#### Overview

Apart from general international law, peacekeeping missions and their activities are also governed by a peacekeeping-specific legal framework that includes:

- Security council resolutions and mission mandates contained therein,
- Status of Forces or Status of Mission Agreements between UN and host state,
- Agreements between UN and troop- or police-contributing countries,
- Secretary-General and UN Department of Peace Operations (DPO) policies,
- Rules of Engagement and Directives on the Use of Force,
- Mission-specific SOPs and directives.

This legal framework shapes UN peace operations and their PKI activities. Peacekeepers are expected to carefully read and understand the mandates, agreements policies and directives relevant to their work. Compliance is mandatory for all peacekeepers, irrespective of whether they are military, police or civilians. PKI personnel must know about essential privileges and immunities that protect them in their work, while also being aware of the legal and policy framework governing the acquisition, use and sharing of PKI.

#### Slide 1



## Lesson 2.2

### Legal Framework for Peace Operations- Mission Specific

We will focus in this lesson on the mission- specific legal framework.

## Slide 2

### Learning Outcomes

- Describe the legal framework and UN policies for UN Missions
- Explain essential privileges and immunities and the legal framework to ensure their accountability, good conduct and discipline
- Explain the importance of protecting sources

Here are the learning outcomes for this lesson. Take a minute to read the slide.



### Slide 3

## Security Council Mandate

- Security Council Resolution:  
highest legal basis for the mission
- Outlines tasks  
and responsibilities
- What the Security  
Council expects  
Mission to accomplish



Key message: Every peacekeeping operation begins with the Security Council adopting a resolution that establishes the mission. The Council will seek to establish a mission with the consent of the host state to its deployment. Depending on the mission's mandate and role, it will also want the consent of the other parties to the conflict concerned.

The Security Council resolution sets out the mandate of the mission, i.e., the tasks assigned to it, including any explicit authorisation to use force. Mandates, or tasks, differ from mission to mission. The range of mandated tasks outlined in a mandate differs between peace operations, based on the conflict environment, the challenges on the ground and other factors. Security Council mandates may also set cross-cutting thematic tasks for all missions, e.g., the prevention of conflict-related sexual violence.

All PKI activities must be undertaken in line with the Security Council mandate of the mission. The PKI policy further specifies that the acquisition and management of information or peacekeeping-intelligence by United Nations peacekeeping operations will be conducted to enhance situational awareness and the safety and security of UN personnel and to inform operations and activities related to the protection of civilian's tasks of the Security Council mandates.

UN Photo shows a session of the UN Security Council, which authorizes every mission.

## Slide 4

### Observer mandates requiring PKI

- Observe and verify violations of ceasefires, armistices, withdrawal agreements
- Monitor security and humanitarian situation
- Monitor disarmament, demobilization and reintegration processes



Key message: The scope of PKI activities follows the scope of the mission's mandate. As the mandates and operating environments of UN peacekeeping missions have evolved, so too have the capabilities, processes and procedures required to gather and analyse information.

In the high-tempo complex and dangerous environments, where asymmetric and transnational threats pose serious dangers to peacekeepers and civilians, and negatively impact mandate implementation, there is a need for peacekeeping missions to understand their operating environments and contexts better, maintain a strategic overview of developments, and predict specific threats and opportunities to enable peacekeepers to execute their mandates effectively.

However, even very traditional observer mission may acquire PKI, which is often highly relevant to implement mandates such as: properly

- Observing and verifying violations of ceasefires, armistices, separation of forces and withdrawal agreements etc.
- Monitoring the security and humanitarian situation in the area of operation.
- Monitoring disarmament, demobilisation and reintegration processes.

*UN Photos show a ski patrol and an observer post of the United Nations Disengagement Observer Force (UNDOF), established by the Security Council in 1974 to maintain the ceasefire between Israel and Syria and supervise force disengagement.*

## Slide 5



Key message: Multidimensional peacekeeping missions are regularly assigned protection mandates.

Specialised civilian staff work on these mandates, including human rights officers, protection of civilian advisers, child protection advisers and women protection advisers. However, these mandates remain whole-of-mission responsibilities to which PKI processes must contribute. As all of the protection mandates are considered mission priorities, they also have to feature in the mission's Information Acquisition Plan as priorities. PKI provides the mission with early warning and situational awareness to deploy its assets to protect the most vulnerable populations from the worst type of threats. Protection mandates may overlap, as they complement and reinforce each other:

- The human rights mandate seeks to protect the entire population and the full range of human rights. The mission will use peaceful means such as reporting and other advocacy or capacity-building measures to advance this mandate.
- The protection of civilian mandate is narrower in that it is only concerned about physical violence and protects civilians only (as opposed to, e.g., detained fighters). However, it goes deeper than the human rights mandate because it authorises the mission to use force as a last resort to protect civilians.
- Child protection is focused on the six grave violations against children in conflict, namely killing and maiming of children, recruitment or use of children as soldiers,

sexual violence against children, abduction of children, attacks against schools or hospitals and denial of humanitarian access to children.

- Conflict-related sexual violence is being used as a tactic of war and as such requires a need to understand the connection between sexual violence and the conflict (e.g., domestic violence would typically not be covered).



**Interactive.** To help students develop an understanding of how the different protection mandates differ from one another while being mutually reinforcing, have them provide an example. Here are a few examples to help in the discussion:

- If state authorities ordered the closure of a newspaper for criticizing the government, this violates the human rights to freedoms of expression, media and information. However, in the absence of physical violence, the POC mandate is not triggered. However, if rogue state agents proceed to assault the journalists physically, the mission may intervene under its POC mandate, including by using force where necessary.
- If an armed group traffics underage girls for purposes of sexual exploitation, this amounts to abuse under the human rights mandate. The mission must exercise its POC mandate to protect the girls. Such sexual violence against children is of concern to both the child protection and CRSV mandates.

## Slide 6

### Host State Agreements (SOMA/SOFA)

- Legal document signed by UN and host state
- Privileges and immunities for UN mission / personnel
- Example: freedom of movement, customs exemptions, visa requirements
- Supplemented by special agreements  
(example-handover of persons detained by mission)



Key message: Before the deployment of a peace operation, the UN and the host Government sign a Status of Forces Agreement (for peacekeeping missions) or Status of Mission Agreement (for special political missions). The SOFA/SOMA establishes the legal framework that regulates the status of the mission and its members in the host state, including privileges and immunities for UN personnel (see above).

Notwithstanding their privileges and immunities, the peacekeeping operation and its members remain under an obligation to respect local laws and regulations. SOFA/SOMAs usually guarantee that:

- UN premises in the host country are inviolable and subject to the exclusive control and authority of the UN, which controls access to all its premises.
- UN equipment and vehicles are immune from search and seizure.
- The UN has the right to use UN-restricted communication throughout the host country.
- The UN may disseminate information on its mandate to the public which is under its exclusive control and cannot be the subject of any form of censorship.
- Mission personnel have functional immunity for official acts.
- Mission personnel enjoy the freedom of movement in the country.

The mission may conclude additional agreements with the host country. Example: A mission may conclude side agreements to regulate peacekeeping-intelligence sharing to mitigate any risks of its peacekeeping-intelligence being misused by recipients.

UN Photos show signing ceremonies of the UNMIS SOFA.

## Slide 7

### Important Privileges & Immunities under SOMA/SOFA

- Functional immunity from arrest, detention, seizure
- Immunity from legal process for official actions & words
- Inviolability of papers and documents
- Correspondence by code, courier & sealed bags
- Wear military uniform & fly UN flag
- Unhindered entry & departure (international staff)
- Freedom of movement within the mission area

For United Nations interest; not personal benefit.  
Can be waived by United Nations without prejudice

Beyond technical/financial issues like exemption from customs duties, the SOFA/SOMA provides privileges and immunities that are very relevant for personnel working on PKI:

- The host state cannot arrest and detain UN mission staff or seize any of their belongings concerning any functions they carry out in their official duties. They can also not prosecute or sue them for official acts or words spoken in an official capacity. This functional immunity is discussed below.
- Their documents are inviolable. The host state may not insist on seeing them.
- Mission personnel have the right to maintain confidential communications using codes or sealed diplomatic pouches.
- They may wear their military uniform and show the UN flag.
- They must be allowed unhindered entry and departure from the country (e.g., they do not need an exit visa). Their personal baggage enjoys the same comprehensive protection as those of diplomatic envoys.
- They enjoy the freedom of movement within the mission area.
- The same privileges are also guaranteed by the 1946 Convention on the Privileges and Immunities of the United Nations.

These privileges and immunities serve to allow the UN to work without obstacles. They are not for the personal benefit of individual staff. In particular, the UN may waive any of these immunities if it is in the interest of the organisation and the course of justice.



### Case Study 6 – Leaked Documents:

The mission obtained secret government plans to violently cleanse an area of a minority ethnic group. To contain the leak, the host government:

- Prosecutes the JMAC national officer who obtained the plans from a government official.
- Prohibits UN officials from leaving the country unless they agree to have their bags searched.
- Jams the mission's code cable correspondence.
- Declares the JMAC chief persona non grata.

Is the mission legally protected against these steps?



**Interactive.** Case Study to be discussed in group work or in plenary.  
Some SOFA/SOMA Immunities for discussion points:

- Freedom of movement
- Inviolability of papers
- Use of Code Cables
- Functional immunity from legal process

The mission may acquire PKI to inform activities related to the protection of civilians. Obtaining the secret government plans provides the mission with early warning about ethnic cleansing, a major threat to civilians that typically involves a combination of gross human rights violations and regularly entails crimes against humanity. Even though the ethnic cleansing plan is a confidential document, acquiring it also does not amount to a prohibited clandestine activity (defined as “the acquisition of information or peacekeeping-intelligence conducted in such a way as to assure secrecy or concealment of the activities, because they are illicit and are inconsistent with the legal framework, principles, policies and mandates of United Nations peacekeeping operations).

In any case, the privileges and immunities of the UN, as reinforced by the SOFA/SOMA, render most of the measures of the host government illegal under international law.

- UN officials, including national staff, enjoy functional immunity from host state legal processes such as prosecution concerning anything they say, write or do in pursuit of their official activities (see slide 29 for more details). The prosecution of the national JMAC staff is, therefore, a violation of international law. However, as a matter of good practice, the mission should not let have a national staff handle such a sensitive issue since national staff and their families are the most vulnerable to government reprisals.
- UN officials enjoy the freedom of movement throughout the host country. In addition, international officials may leave and enter the host country freely, without complying with requirements such as exit visas. When they travel, their documents and bags are inviolable. The host state may not deny them the privilege to freely leave the country unless they agree to having their bags searched.
- The SOFA/SOMA allows the mission to use codes and the host state may therefore not jam its code cable traffic.
- Under diplomatic law, the host state may declare a diplomat representing another state persona non grata, at any time and without having to explain its decision, may require that person to leave the country. However, as a matter of international law, the doctrine of persona non grata does not apply to, or in respect of, UN personnel. The mission enjoys the privilege to deploy whom it wishes within its mandate and staff ceiling. Although persona non grata declarations targeting UN personnel occasionally happen as a matter of practice, these are therefore not backed up by international law. The mission (and other concerned states) should protest at the highest level against this unlawful reprisal against the JMAC chief considering that the PKI activity conducted was in accordance with the mandate of the mission and the PKI Policy.



## Slide 9

### United Nations Functional Immunity

- Troop contingents under jurisdiction of their state, they may not be arrested, prosecuted etc. by the host state.
- UN civilians, UNMOs and all UNPOL have it for official acts:
  - Status of Forces Agreement/Status of Mission Agreement.
  - 1946 Convention on the Privileges & Immunity of the United Nations.
- Protects UN staff from intimidation and reprisals. Can be waived by Secretary-General in interest of UN.
- Actual misconduct (e.g., sexual exploitation and abuse) is always subject to disciplinary & criminal action.

**Immunity never means impunity for UN peacekeepers**

Key message: Even though following the mission's Security Council mandate, PKI activities may occasionally render UN personnel liable to accusations of "espionage" or the like. It is important to underline that all mission personnel have comprehensive protection under international law and the SOFA/SOMA against any host state prosecution or other legal measures linked to their PKI work.

As per the SOFA, troop contingents, including staff officers (e.g., in the U2/Military peacekeeping-intelligence), remain under the exclusive jurisdiction of the sending state. The host state has no jurisdiction to prosecute them or otherwise subject them to legal process.

UN Military Observers and UNPOL officers may also be involved in PKI. They are considered UN experts on mission. Like civilian UN staff, they are protected therefore by the SOFA/SOMA and the 1946 Convention on the Privileges and Immunity of the United Nations. They enjoy functional immunity from the legal process for any words spoken or written or actions taken in their official capacity. Example: In carrying out PKI work and improving the mission's situational awareness, UNMOs acquire information about a weapons cache that the host state tried to hide. Due to the UN personnel's functional immunity, the host government is prohibited from arresting and prosecuting them, e.g., under charges of espionage.

Functional immunity serves to protect the work of the UN from interference and reprisals. It does not guarantee impunity for actual criminal wrongdoing. In particular, the immunity of UN personnel can be waived by the Secretary-General in the interest of justice and

the United Nations. Example: UNPOL officers severely mistreat a suspected criminal until he reveals information about planned activities. By waiving their functional immunity, the Secretary-General allows their home state to prosecute them. Likewise, members of troop contingents can always be prosecuted by their own state.

The UN and troop- and police-contributing countries (T/PCCs) conclude legal agreements regulating the conditions of the contribution (T/PCC-MOU). Under these agreements, the contributing countries pledge to uphold discipline in case of misconduct and ensure accountability for any criminal conduct.

## DPO-DOS PKI Policies and Guidelines

- Human Rights Due Diligence Policy.
- Peacekeeping-Intelligence Policy Guidelines on Acquisition of Intelligence.
- Guidelines on the Exchange of Intelligence/Peacekeeping-Intelligence with Non-UN and Non-Mission UN Entities.
- PKI, Surveillance and Reconnaissance Staff Handbook.
- Military Peacekeeping-Intelligence Handbook.

**Compliance with UN policy is mandatory for all peacekeepers**

Key message: The Secretary-General has promulgated policies and regulations that bind the entire organisation, including all peace operations. HRDDP is the most relevant example in relation to PKI.

Additional policies have been adopted at the level of the Department of Peace Operations (DPO) and the Department of Operational Support (DOS). Beyond the Peacekeeping-Intelligence Policy, there is an evolving body of rules and regulations to implement the PKI Policy. These include:

- Peacekeeping-Intelligence Guidelines on Acquisition of peacekeeping-intelligence.
- Guidelines on the Exchange of peacekeeping-intelligence/Peacekeeping-Intelligence with Non-UN and Non-Mission UN Entities.
- Military Peacekeeping-Intelligence Handbook.
- UN Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook.

Compliance with these policy and guidance documents is mandatory for all peacekeepers.

## Slide 11

### **PKI legal limits**, as established or reaffirmed by DPO Peacekeeping-Intelligence Policy

- Full respect for human rights & international law
- No clandestine activities
- No exposure of sources to harm
- Independence of UN's peacekeeping-intelligence
- Cooperation with states subject to conditions

Key message: Gathering and sharing United Nations Peacekeeping-Intelligence is subject to legal limits.

Some limits follow directly from international human rights law and have been set out in lesson 2.1 Others are established by the PKI Policy to protect the independence and impartiality of our missions. Even though they are established through Policy, they are nevertheless binding on all UN personnel working on PKI.

Clandestine activities are outside the boundaries of PKI and shall not be undertaken because they undermine the reputation of the mission and may place our personnel at risk. UN policy defines clandestine activities as “the acquisition of information or peacekeeping-intelligence conducted in such a way as to assure secrecy or concealment of the activities because they are illicit and are inconsistent with the legal framework, principles, policies and mandates of United Nations peacekeeping operations”. For example, UN staff must never break into a government building or hack into a database of a non-governmental organisation to obtain information.

However, the limitation to non-clandestine means does not require the mission to reveal its methods and sources to the host state or others. On the contrary, all mission personnel are required to apply particular care not to expose any sources or potential sources of information to harm. This will often mean that all contact with a source (and materials and information gained from the source) must remain confidential so as not to expose the source to reprisals or intimidation. The identity of the source must also remain confidential.

UN PKI activities must be fully autonomous from and independent in all aspects of any national intelligence system or other operations and will maintain their exclusively international character. The mission's independence and perceived impartiality may be compromised if the mission is seen as being an intelligence arm of the host government or third states. Information may be shared with other state authorities, but subject to conditions and limits of international human rights law and the HRDDP that we covered in lesson 2.1.

## Case Study 7 – armed group

To obtain information on an armed group, the mission considers to:

- Pool its PKI resources with host authorities in a joint intelligence cell.
- Infiltrate UN language assistant into the armed group.
- Pay an armed group fighter for copies of the group's battle plans.
- Recruit as informants children who the armed group employs as cooks.

**What are relevant legal obligations?**



**Interactive.** Case Study to be discussed in group work or in plenary. Ask the students to bring out some relevant legal obligations. Here are the points for you to use in facilitating the discussions.

- Independence of PKI processes.
- Protect sources from harm.
- No covert action.
- The mission may share peacekeeping-intelligence with national peacekeeping-intelligence agencies, subject to compliance with human rights law and the related HRDDP. However, its PKI activities must remain independent, and the mission must therefore not pool its PKI resources with the host authorities into a joint peacekeeping-intelligence cell.
- Infiltrating a language assistant into an armed group is a clandestine activity not allowed under UN rules. It does not matter that a target is an armed group. The prohibition of clandestine activities also serves to protect us from accusations of “spying” that may undermine the mission’s reputation as impartial and place mission personnel at risk. Such infiltration would often also have to involve national staff (like the language assistant in this case) who are particularly vulnerable to reprisals.
- The UN prohibits providing payment or other incentives to human sources of PKI (see following slide and case study for details).
- Following the UN’s PKI principles, the mission must never recruit or otherwise develop children as sources of peacekeeping-intelligence, because they cannot give free and informed consent to assume the substantial risks involved in an informant’s role.

*Paying children for information on an armed group may also violate the human rights and IHL prohibition of not recruiting children for military activities.*

## Prohibition of incentives for human sources

- DPO guidelines on information from human sources for PKI:

‘The incentive approach implies trading something that the source wants for information. This method of acquisition is strictly forbidden under the Peacekeeping-Intelligence policy

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

13

Key message: Building on the PKI policy, the DPO Guidelines on Information from Human Sources for Peacekeeping-intelligence, stipulate that no amount of money will be paid, nor gifts offered, to human sources, or their relatives, in remuneration for information.

It is strictly forbidden to trade something that the source wants for information. However, logistical expenses to facilitate meetings and debriefing a source are not considered incentives.

The no incentive rule helps ensure that sources do not provide the UN with fabricated information for personal gain and thereby protects the credibility of the entire PKI process. Other components such as the human rights component have long followed a policy of not paying or otherwise incentivising sources of information. In cases of doubt about borderline cases, MIO staff officers should turn to the human rights component for advice on how the prohibition of incentives has been handled in the local context to ensure a uniform approach by the mission.



## Case study 8: keeping a human source

To facilitate meetings with an important human source who lives far from the mission, the mission's PKI cell wants to:

- Provide her meals on the day of her debriefings
- Reimburse the source for the transport costs, ideally through a 150 USD lump sum for every meeting
- Offer to hire her brother as a cafeteria assistant
- Pass on a request for a quick impact project (building of a well) in her village to the military's engineering company

**Which of these measures would be prohibited incentives?**



**Interactive.** This case study provides typical examples of borderline cases. Course participants should discuss them in small groups or plenary considering the rules just presented.

*It is acceptable, and in many cultural settings of peacekeeping missions expected, to provide a source with drinks or meals to facilitate a meeting, especially in this case where the source must travel far.*

*The mission can also reimburse for actual transport costs, but funds provided should match actual expenses. It should be verified in this case, whether 150 USD is excessive and would be understood as a form of payment in the dire socioeconomic realities of many peacekeeping mission settings. In that case, the lump sum would amount to a hidden incentive. peacekeeping-intelligence officers can check with human rights officers or others that know the local context well on what type of travel expenses are appropriate.*

*Incentives must not be given to relatives or other persons close to the source. It would clearly not be in line with the rules to hire the source's brother as a quid pro quo for information provided. The case of Quick Impact Project is less clear cut. A peacekeeping-intelligence officer could agree to pass on the request to the relevant staff in the mission. But the peacekeeping-intelligence officer should make it clear to both the source and the colleagues that the request should be entirely evaluated on its merits,*

*like any other request, and that doing the source a favour would not be a factor in the eventual decision.*

## Slide 15

### Source protection- Information Acquisition Plan

- 1. Who faces protection risks?**
  - Sources and persons suspected to be sources
  - Family members; others close to sources
  - Mission staff, national staff
- 2. What protection risks must be considered?**
  - Reprisals and intimidation
  - Prosecution of sources
  - Community stigmatization
- 3. How can protection risks be mitigated?**
  - Individual risk assessment before source contact
  - No recruitment if risks too high
  - Confidentiality of all contact with source
  - If exposed: advocacy, relocation, physical protection, coping mechanisms

A mission that does not protect its sources, will not have sources

Key message: UN Policy requires the mission to take particular care not to expose any human sources or potential sources of information to harm.

Owing to its status and values, the UN is bound to apply source protection standards that may be more onerous than what peacekeeping-intelligence officers apply in their national context.

Source protection cannot be ensured in an ad hoc manner but requires careful assessment and planning by the HPKI cell. Individualized protection assessments must complement this general protection assessment for every human source the mission intends to contact and develop.

Three questions should guide protection planning:

### Who faces protection risks?

Not only human sources face risks, but also anyone suspected of being a PKI source. Mere contact with a person, if observed, can, therefore, expose the person to risk even if s/he declines to be a source. Furthermore, family members and others close to the source are often at risk of collective reprisals. It is also important that, in its outside communication, the mission strictly distinguishes its PKI processes from the information

gathering from other civilian staff such as human rights, child protection, humanitarian or civil affairs officers. The latter's work becomes more dangerous and complicated if they are providing inputs into PKI processes, especially if these link to situational awareness on the military situation.

#### What protection risks must be considered?

If exposed, human sources may face reprisals and intimidation from state authorities or armed groups. These can take the form of violence, including death in the most extreme cases. They can also involve more subtle but not fewer effective forms such as removing persons from their job, imposing travel bans, denying essential public services or smearing their reputation. Unlike UN personnel, sources also do not enjoy immunities and are liable to prosecution for charges of espionage or similar offences. Depending on the reputation the mission enjoys in communities, a person may be subject to social stigma and ostracised by their own community if s/he is seen as a "traitor" who shares peacekeeping-intelligence with the UN.

#### How can protection risks be mitigated?

Before any potential source is contacted, an individual risk assessment must be carried out. The source must not be recruited/developed if protection risks are deemed too high. Contact with the source must be organised (in terms of time, place, circumstances, etc.) to ensure confidentiality. If a source is nevertheless exposed, the mission must take all feasible steps to counter protection risks. This can take the form of advocacy interventions by the mission or its partners, but also concrete measures such as relocating or physically protecting a source. PKI personnel should seek the views of the source on the best course of action since most sources will already have coping mechanisms to deal with protection risks. These can be further reinforced by appropriate mission action.

## Handling of detention in PKO: DPO Standard Operating Procedures (2020)

- Detention powers based on Security Council mandate and ROE.
- Humane treatment in detention. Mission responsible for water, food, hygiene, medical care, etc.
- Mission's detention focal point must be immediately notified.
- Due process: inform person about reason for detention, inventory of items taken from detainees, notification of their family. ICRC notified within 36 hours and given access.
- Foreigners may demand their consulate is alerted.
- Temporary detention (96hr) only. Then handover to authorities or release.
- No handover if risk of persecution, torture/ill -treatment, disappearance, summary execution or death penalty. Mission must assess risk prior to handover and monitor handed -over persons.

Complemented by mission specific guidance, appropriate orders and training for all concerned staff

Key message: the UN has imposed strict procedures on detention, which are laid out by the DPO Standard Operating Procedures on the Handling of Detention. They set out a process on how the UN can temporarily detain persons with a view to handing them over to the host state authorities or releasing them again, as appropriate.

A mission's mandate and its Rules of Engagement may give a peace operation the power to apprehend and temporarily detain individuals.

Staff Officers are responsible for familiarising themselves with the SOPs and mission-specific rules. Every mission will also nominate a detention focal point (a civilian who is neither military nor police) who will monitor compliance with the SOP under the overall responsibility of the head of mission and who can provide advice as needed.

The SOPs apply once the UN has the target person/s under its effective control, even for very short periods. Once the UN mission has effective control over a person, the SOPs set out detailed guidance on how to proceed. They must inform the detainee about the reason for the detention, make an inventory of any items temporarily taken or seized from the detainee, give the person the option to inform their family or third parties etc. Furthermore, the Detention Focal Point must be immediately notified. The SOPs also require the notification of the International Committee of the Red Cross (ICRC) within 36 hours. As per the SOPs, the ICRC has a right to get access to detainees and conduct confidential interviews with them. Foreign nationals may demand that their consulate is alerted (the choice is with the detainee).

Anyone detained by the UN must be treated humanely and torture or ill-treatment is strictly prohibited. The mission must plan to ensure that detainees are kept in adequate holding cells, receive water, food, hygiene facilities, medical care as required by international standards (these are detailed in an international document called the Mandela Rules, named after the famous Anti-Apartheid campaigner, political prisoner and later South African President).

If any UN personnel receives any allegations of detainees being subjected to torture or ill-treatment such concerns should be immediately transmitted to the Detention Focal Point and the mission's conduct and discipline team.

The SOPs envisage that the UN will only hold detainees for 96 hours. After 96 hours, the person must be handed over to state authorities (usually the host state authorities, although exceptionally a handover to a third state presence may be carried out). If no handover is possible or appropriate, the person must be released.

The UN is prohibited from handing over a person to the host state if there is a real risk of that person being subjected to persecution, torture or ill-treatment, disappearance or summary execution. Consistent with the UN policy of opposing the death penalty, a person must also not be handed over if there is a real risk of the person being subjected to the death penalty.

In order to implement these non-refoulement guarantees, every mission must strike a legal agreement on handover and related guarantees with the host government. In addition, the mission must carry out an individual risk assessment before any handover and closely monitor the subsequent treatment of the person who was handed over.

## Case study 9: debriefing a detainee

- A patrol apprehends a man as he is planting an improvised explosive device (IED) on a road that is regularly used by civilian and UN vehicles. Several UN staff have been killed and maimed by IEDs in recent weeks
- The mission wants to debrief the man about the other IEDs that he or others have planted and the source of the bombs. The interrogation plan foresees to:
  - To keep him detained without contact to any other persons
  - Question him for 8 hours per day over the next 7 days
  - Provide him with food as soon as he starts providing information
  - Promise to release him if he fully cooperates – instead of handing him over to the host state authorities, which regularly torture suspected terrorists

Does the interrogation plan comply with international standards and UN rules?



**Interactive.** A case study discussion should bring out the following key points:

- The mission could apprehend and temporarily detain the man in line with its power to exercise self-defence and, assuming the mission has such a mandate, also in line with protection of civilian's mandate. He can also be questioned in pursuance of these mandates since there is an imminent threat to the life of civilians and UN staff due to possible other IEDs being planted.
- However, it cannot keep the detention secret or keep the detainee incommunicado. His family must be informed about the detention. Family visits can have certain temporary restrictions, e.g., if there is real concern that the man channels information through his family that would subject civilians or UN staff to further risk. However, the ICRC must be informed and given access in all circumstances.
- The man can only be held for a period of 96 hours (four days) so on that ground alone the interrogation protocol does not comply with UN rules. Furthermore, the man cannot be compelled to respond to questions. In line with the general obligation to treat the man humanely, he must be provided with food, water and medical care and withholding any essential needs to induce cooperation would amount to prohibited inhumane treatment.
- Similarly, the promise of release instead of handover implies a veiled threat of torture, which is strictly prohibited. Instead, the UN must immediately institute a handover risk



*assessment and if there is a real risk that the man will be tortured by host state authorities, he must be released regardless of whether he cooperates or not.*

## DPO detention SOPs: questioning of detainees

- UN personnel may question detained persons within ambit of their protection of civilians and self-defence mandates.
- Record must be kept of UN personnel present and detainee responses.
- Detainees may not be compelled to answer, but must be informed about that right.
- No torture, inhumane treatment or other methods of questioning that would violate international law.
- Questioning of children only in the presence of a Child Protection Advisor.

While not explicitly mentioned in the DPO Detention SOPs, the UN may question a detained person in pursuance of their protection of civilians and self-defence mandates. However, a record of all interrogations must be kept, including who was present and what responses were provided.

The detainee must be informed that UN rules state that s/he may not be compelled to answer questions. Any questioning must abide by international law.

As a matter of policy, the UN uses and promotes techniques of non-coercive interviewing, which have been successfully used in law enforcement and intelligence work of many national agencies. The details are summarized in the UNPOL/OHCHR/UNODC policy/guidance on Non-coercive Interviewing [forthcoming, link to be inserted later].

If children (i.e., anyone under 18 years) are to be questioned, one of the mission's Child Protection Advisers or child rights focal points must be present.



## Take Away

- Protection mandates rely on good PKI and must be made a PKI priority, as per UN policy.
- PKI personnel enjoy privileges and immunities protecting them from any host state reprisals related to their official duties.
- Protecting PKI sources from harm is a priority from a legal, policy, ethical & operational perspective. Protection must be ensured before sources are approached.

## Summary

Key take away regarding the Peacekeeping Specific Legal Framework include:

- Protection mandates rely on good PKI and must be made a PKI priority, as per UN policy.
- PKI personnel enjoy privileges and immunities protecting them from any host state reprisals related to their official duties.
- Protecting PKI sources from harm is a priority from a legal, policy, ethical and operational perspective. Protection must be ensured before sources are approached.

# Module

## 2



### Legal Framework

Take away from Module 2 includes:

- International and national humanitarian legal frameworks impact and guide peacekeeping in the field.
- Bodies of international law provide special protection for members of the most vulnerable communities, women, children, refugees.
- Peacekeepers must monitor and report violations of human rights and international humanitarian law.
- Peacekeepers do not have impunity from laws and are held accountable for unlawful activities.
- Peacekeepers and MIO/PKISR officers can ask their command, Legal Officers, Human Rights staff officers, POC Officers for assistance.
- Legal frameworks govern human rights, IHL and peacekeeping generally.
- Peacekeepers must comply with IHRL and IHL themselves, and monitor/report abuses by others. Peacekeepers will be held accountable for individual actions. Turn to command or legal advisors for help.
- Protecting PKI sources from harm is a priority from a legal, policy, ethical and operational perspective. Protection must be ensured before sources are approached.
- The DPO policy on PKI is a good start to review the UN PKI legal framework.

# Module 3



## Operational Framework for MPKI

### Module 3 at a Glance

#### Aim

The objective of this module is for individuals to better understand the key operational framework to conduct PKISR as military staff officers in a UN peacekeeping mission.

#### Overview

Module 3 provides an overview of the operational framework and skills related to conducting PKISR staff functions. This includes understanding the different PKISR disciplines, how they support the PKISR process, and the staff skills required to plan, task and execute PKISR activities.

## Slide 1



### Module 3 Military Peacekeeping- Intelligence, Surveillance and Reconnaissance Operational Framework

Module 3 provides an overview of the operational framework and skills related to conducting PKISR staff functions.



**Note to Instructor:** *The instructor should be familiar with the United Nations MPKI and PKISR handbooks and have an understanding of ISR.*

## Slide 2

### Module 3 Content

- PKISR Disciplines
- PKISR Process
- PKISR Key Roles
- RFI Management
- Requirements Management and Prioritization
- Analysis and Dissemination
- PKISR Planning
- PKISR Operations
- Unmanned Aerial Systems Unit
- Human Peacekeeping-Intelligence
- Long Range Reconnaissance Patrol

Module 3 contains lessons on these subjects.



## Peacekeeping-intelligence disciplines

### The Lesson



#### Starting the Lesson

All peacekeeping-intelligence staff must have a good knowledge of the intelligence disciplines, in order to make the information acquisition process and the MPKI cycle as effective as possible. A thorough knowledge of the strengths and limitations of each discipline will help PKISR personnel determine how best to employ them in a UN peacekeeping operation.



## Lesson 3.1

### The Peacekeeping- Intelligence Disciplines

## Lesson Contents

- Peacekeeping-intelligence disciplines
- Geospatial Peacekeeping-Intelligence (GPKI)
  - Imagery Peacekeeping-Intelligence (IPKI)
- Signals Peacekeeping-Intelligence (SPKI)
- Human Peacekeeping-Intelligence (HPKI)
- Open Source Peacekeeping-Intelligence (OPKI)



Here are the subject areas we will be covering in this lesson.



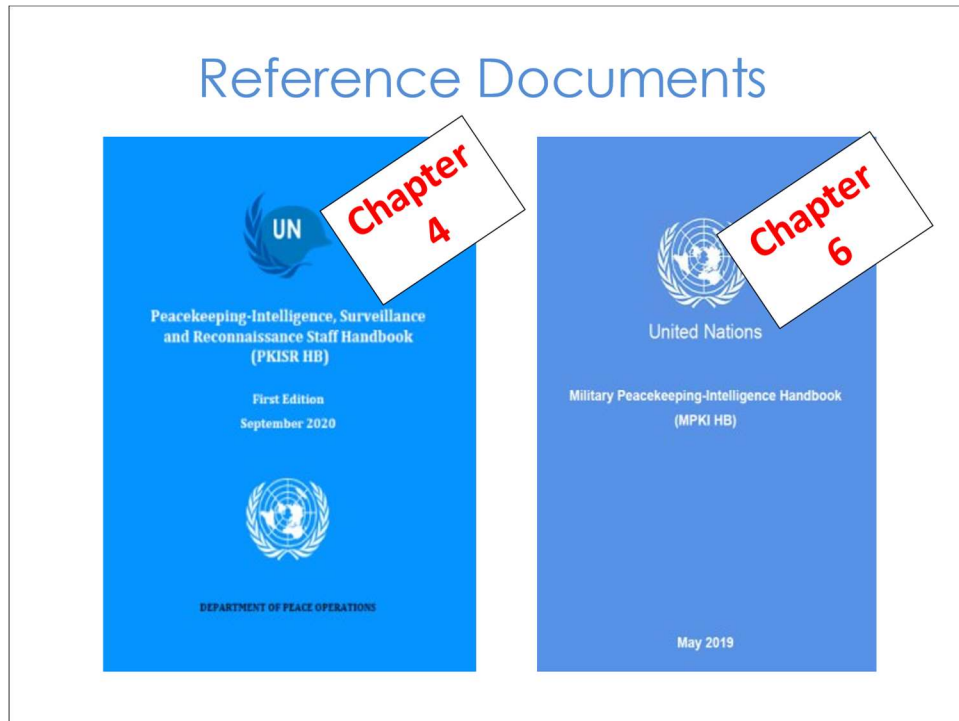
## Learning Outcomes

- Describe the key PKISR intelligence disciplines
- Understand the strengths and weaknesses of intelligence disciplines in relation to PKISR



Let us take a look at the learning outcomes before we start this lesson. Please take a moment to read and understand what you are expected to be able to do at the end of the lesson.

## Slide 6



For your information, additional details on this topic can be found in the following reference documents. First, Chapter 4 of the Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook and second, Chapter 6 of the Military Peacekeeping-Intelligence Handbook.

## Slide 7

### Peacekeeping-Intelligence Disciplines

- It is important to know the strengths of the individual disciplines, and which is most appropriately tasked against an intelligence requirement.
- A UN mission will not necessarily have access to a wide variety of acquisition capabilities and must make the best use of those intelligence disciplines available.
- MPKI capabilities should be operated with the respect of the legality of the host nation, the UN mandate and international law.

Key message: Specialised MPKI capabilities will be deployed to some UN peacekeeping operations; what is available will depend on the mission and its' mandate. Often, such capabilities will be provided alongside a specialized Troop Contributing Country's unit or a civilian contractor.

To make the information acquisition process and the MPKI cycle as effective as possible, all PKI staff must have a good knowledge of the kind of acquisition units that are present in the mission and the respective strengths and weaknesses of employing them.

As a UN mission does not have access to a wide variety of acquisition capabilities, it is critically important to make the best use of those peacekeeping-intelligence disciplines available.

Lastly, 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 international and national legal norms.

## Peacekeeping-Intelligence Disciplines

- Geospatial Peacekeeping-Intelligence (GPKI)
  - Imagery Peacekeeping-Intelligence (IPKI)
- Signals Peacekeeping-Intelligence (SPKI)
- Human Peacekeeping-Intelligence (HPKI)
- Open source Peacekeeping-Intelligence (OPKI)

We will consider the following peacekeeping-intelligence disciplines during this lesson. It is worth noting that this lesson will only provide a general introduction to the different disciplines – a more detailed look into selected fields will be provided later in the course.



**Note to Instructor:** *The instructor should ask the students if they have any experience using the various peacekeeping-intelligence disciplines. Use the students' experiences throughout the lesson to complement your instruction.*

## Slide 9

# Geospatial Peacekeeping-Intelligence (GPKI)

- The GPKI discipline refers to the PKI gained through the analysis of:
  - Geographic imagery
  - Geospatial data
- Imagery Peacekeeping-Intelligence (IPKI)



Key message: Geospatial peacekeeping-intelligence (GPKI) is peacekeeping-intelligence derived from the analysis and exploitation of imagery and geospatial information that describes, assesses, and visually depicts physical features and geographically referenced activities on the earth.

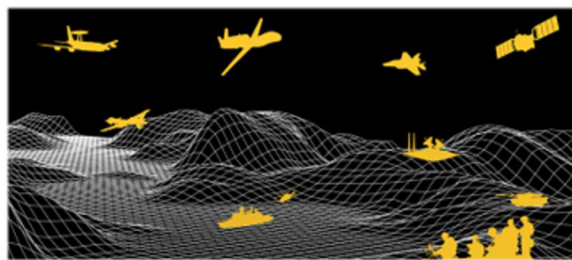
The fundamental difference between GPKI and imagery peacekeeping-intelligence (IPKI) is that an IPKI product will only use imagery to provide the assessment; once geospatial information is incorporated into the product, it becomes GPKI.



**Interactive.** *The instructor should ask the students if they have any experience using GPKI and what kind of products they produced.*

## Various Imagery Platforms for GPKI

- Satellite platforms
- Closed-Circuit Television (CCTV) cameras
- Airborne platforms, both manned and unmanned



Key message: There are 3 main imagery platforms. These are satellite platforms, close circuit television cameras and airborne platforms. Imagery can be acquired by other means such as handheld, however are less frequent. Let us look at each in turn.

First, satellites can provide pattern of life over time of strategic areas of interest such as border crossings or refugee camps. The sensors can be Electro-optical (EO), Infra-Red (IR) and Synthetic Aperture Radar (SAR).


Second, CCTV can provide an excellent overview of an area of interest and are common in almost every city around the world.

Lastly, airborne platforms can provide surveillance and reconnaissance over areas of interest, for example areas occupied by known armed groups. Smaller unmanned aircraft systems are better used for more tactical tasking such as overwatch of a convoy or IED emplacement activity. The sensors can be Ground Moving Target Indicator (GMTI), EO, IR and SAR. Airborne platforms will be covered later in the course and therefore will not feature as much in this lesson.



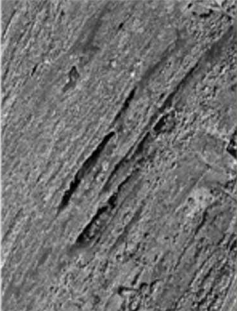


**Interactive.** *The instructor should ask the students if they have any experience using imagery provided by satellite, airborne or CCTV platforms before, and ask them to share their experiences.*

## Slide 11



### Satellite Platforms

- What is a satellite/sensor
- Strengths and weaknesses in relation to PKISR



EOIRSAR

Key message: Imagery can be obtained through military and commercial/civilian satellites.

Almost all the world's satellites operate at an altitude of between 300 km – 36,000 km above the earth. These include TV, communications, weather and military satellites.

The resolution of satellite images can be a challenge: high resolution is expensive and may not always be available to a UN peacekeeping mission. A 30 cm resolution can detect what kind of a car you are looking at from an altitude of 600 km.

Let us take a bit of time to consider the benefits of the three sensors highlighted on the slide:

#### **Electro-optical (EO):**

- Can cover a lot of area.
- It is a “normal” picture to look at.

#### **Infra-Red (IR):**

- Can locate radiation concealed under a camouflage net or in houses and vehicles.

**Synthetic Aperture Radar (SAR):**

- Can cover a large area.
- Not depending on weather or time of day.
- Possibility for Ground Moving Target Indicator (GMTI).

The **limitations** aligned to satellite imagery include:

- It is not always available to a UN peacekeeping mission.
- Imagery from a commercial satellite is very expensive.

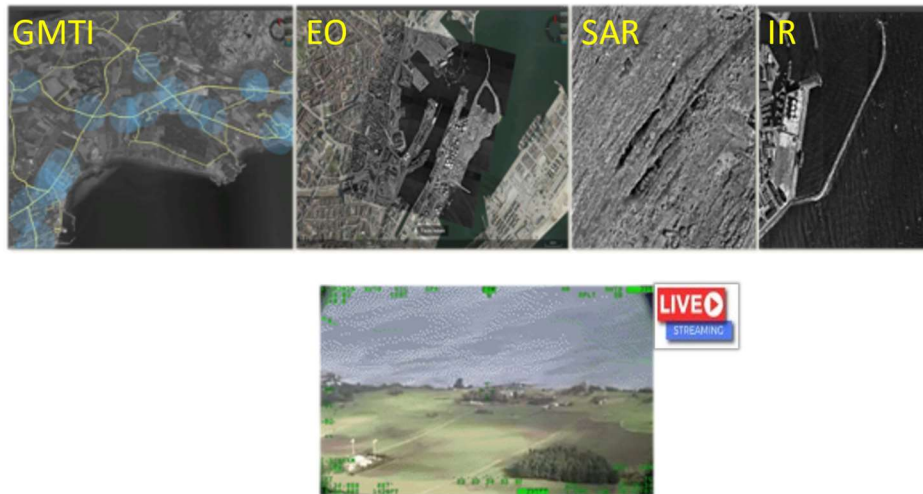


**Interactive.** Ask the students if they have ever worked with satellite platforms before. Ask them to share their experiences.



## Slide 12

### Airborne platforms - manned and unmanned



Key message: The three space-based sensors mentioned in the previous slide are also available on airborne platforms. The capabilities of the sensors are the same, although the type of airborne platform will vary, for instance, whether the platform is manned or unmanned. Factors, such as platform speed and range, will determine how best to use the asset and the associated sensors.

The additional sensor for manned and unmanned is GMTI (Ground Moving Target Indicator). GMTI is a specific capability of SAR, which can identify moving objects. The GMTI sensors are particularly useful at highlighting new and existing routes/paths through open areas and, when used in a surveillance mode over a period of time, can provide indicators of certain activity.

Details regarding manned and unmanned airborne platforms will be covered later in the course, as separate lessons.

## Strengths and limitations of GPKI

- **Strengths:**

- The ability to detect and identify activity or individuals at long range.
- Mitigates the loss of human life and detection during acquisition.

- **Limitations:**

- A requirement for highly trained, specialist personnel to interpret obtained images.
- Weather and climate might limit the use of technical equipment for IPKI and/or GPKI.

Key message: You should be aware of the strengths and limitations aligned to GPKI, details of which will help you determine which assets to use to acquire information.

Some of the **strengths** of GPKI include:

- The ability to detect and identify activity or individuals at long range.
- GPKI mitigates the risk to human life and detection during acquisition.

Some of the **limitations** of GPKI include:

- There is a requirement for highly trained, specialist personnel to interpret obtained images.
- Weather and climate might limit the use of technical equipment for IPKI and GPKI.

## Slide 14

### Closed-Circuit Television (CCTV) cameras

- What is CCTV
- Strengths and limitations in relation to PKISR



Key message: CCTV is the use of video cameras to transmit signal imagery to a specific place, on a limited set of monitors.

Many of you will be familiar with CCTVs (also known as video surveillance). You will have often seen them in towns/cities for security purposes.

The **strengths** of CCTV include:

- Ability to conduct surveillance of public spaces.
- The system can be operated continuously.
- The possibility to record data.

The **limitations** of CCTV include:

- Video surveillance has generated significant debate about an individual's right to privacy even when in a public area.
- The resolution is not always that good.



**Interactive.** *Does anyone have any experience in using CCTV? Ask them to share their experiences.*

## Signals Peacekeeping-Intelligence (SPKI)

- What is SPKI?
- Benefits of using SPKI in UN peacekeeping missions
- Strengths and limitations in relation to PKISR



Key message: The PKISR Staff Handbook acknowledges signals peacekeeping-intelligence (SPKI) as an important and valuable discipline, but specific guidance on how to manage this capability will only be developed once the policy and the framework to facilitate the legal process is in place.

It is important to note that there will always be a need to engage with the host nation to determine the boundaries of what can and cannot be acquired to support implementation of the mandate.

SPKI is peacekeeping-intelligence achieved by intercepting signals, whether it is related to communications between people or from electronic signals not directly used in communication. SPKI involves acquiring peacekeeping-intelligence from communications and information systems. SPKI sources include communication, radar and other electronic systems. It includes COMINT (communications peacekeeping-intelligence - communication between people) and ELINT (electronic peacekeeping-intelligence - signals from radars or navigation systems).



**Interactive.** Have the students used Signal peacekeeping-intelligence before? What is the students' experience? Ask them to share their experiences.

## Strengths and limitations of SPKI

- **Strengths:**

- It provides a 24hr, all-weather capability.
- The system is passive.

- **Limitations:**

- SPKI can only work when a threat actor is radiating and providing signals.
- Depending on the range of the system, it might need to be deployed near the object, thereby increasing the risk of compromise.
- There may be Host State concerns regarding the use of SPKI.

[Key message:](#) You should be aware of the strengths and limitations aligned to SPKI, details of which will help you determine which assets to use to acquire information.

Some of the **strengths** related to SPKI include:

- It provides a 24hr, all-weather capability.
- The system is passive and therefore, inherently non-detectable by an actor's electronic warfare (EW) capability.

**Limitations** of SPKI include:

- SKPI can only work when a threat actor is radiating and providing signals that can be intercepted.
- Depending on the range of the system, it might need to be deployed near the object, thereby increasing the risk of compromise.
- There may be Host State concerns regarding its use, as SPKI is likely to pick up all communications on its frequency, not just those of threat actors.

## Slide 17

### Human Peacekeeping-Intelligence (HPKI)

- HPKI is information acquired and provided by human sources
- The use of HPKI in peacekeeping can only be used in a non-clandestine manner. For this reason, Mission personnel may not operate based on a covert or false identity to acquire peacekeeping-intelligence
- The safety of a HPKI source and their family is paramount and therefore it is essential that any HPKI capability is carefully managed



Key message: Human peacekeeping-intelligence (HPKI) is peacekeeping-intelligence gathered by means of interpersonal contact, as opposed to the more technical peacekeeping-intelligence gathering disciplines.

In other words, information acquired and provided by human sources. Human sources can provide a wealth of timely, accurate, and specific information. It is important to ensure that HPKI is acquired by both men and women to:

- provide a balanced gender perspective on the situation, and
- to facilitate better interaction with female sources.

There are strict guidelines governing HPKI, which are captured in UN policy and guidelines. Under no circumstances should a mission recruit or otherwise cultivate children as HPKI sources given that they cannot provide the necessary free and informed consent to engage in such sensitive activities. Likewise, no amount of money will be paid, nor gifts offered to HPKI sources or their relatives, as remuneration for information.

A HPKI source must be managed by specialist teams, whose responsibility is to provide the interaction between the Mission and the source to reduce any risks to the identity and their safety and security.

You will receive a more in-depth overview of HPKI later in the course.



**Interactive.** *Has any of the students worked as a HPKI (sometimes referred to as HUMINT) operator? Ask them to share their experiences.*

## Strengths and limitations of HPKI

- **Strengths:**

- Information is more readily available than from other acquisition capabilities.
- HPKI operations are cost effective.

- **Limitations:**

- The credibility of your source and the information he/she gives you.
- It takes time to develop a HPKI network.
- Communication with potential sources is likely to require interpreter support. Local interpreters must be vetted; otherwise, there is a risk of bias in interpretation or operational security lapses.

Key message: You should be aware of the strengths and limitations aligned with HPKI, details of which will help you determine which assets to use to acquire information.

Some of the **strengths** related to HPKI include:

- Information is more readily available than from other acquisition capabilities.
- HPKI operations are cost effective when compared to other sophisticated, technological acquisition platforms.

**Limitations** of HPKI include:

- The credibility of your source and the information they give you.
- HPKI is not precise; operations may take time to develop and to shift emphasis to new peacekeeping-intelligence requirements.
- Communication with potential sources is essential, and 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 lapses.



## Open Source Peacekeeping-Intelligence (OPKI)

- OPKI is data that is accessible in publicly available sources to be used in an intelligence context. This includes:
  - Media
  - Internet
  - Publicly available government data
  - Professional and academic publications
  - Commercial data
  - Grey literature



Key message: Open source peacekeeping-intelligence (OPKI) is a multifactor methodology for acquiring, analyzing and making decisions about data accessible in publicly available sources to be used in an peacekeeping-intelligence context.

'Open' means publicly available sources. As you can imagine, OPKI generates a significant volume of data that needs evaluating to determine its usefulness. Different open sources include:

**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 this source comes from an official source, they are 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.

## Open Source Peacekeeping- Intelligence (OPKI)

- An OPKI analyst will be more efficient using specific tools
- All Missions should consider a dedicated OPKI analyst within the U2



Key message: To allow for the rapid sorting and prioritisation of Publicly Available Information (PAI) such as Twitter, YouTube and Facebook feeds, an OPKI analyst acts in a passive way by gathering the PAI to analyse attitudes, behaviours or perceptions.

It is possible to task OPKI with key indicators and warnings (I&W), for example, alerting the Mission to videos produced by armed group leaders suggesting future attacks against civilians or UN peacekeepers.



**Interactive.** Have any of the students worked with OPKI? Ask them to share their experiences.

## Strengths and Limitations of OPKI

- **Strengths:**

- Internet is widely available
- Use of is accessible to all
- Normally cheap, easy to use and can produce results quickly.
- Is easy to share

- **Limitations:**

- It is difficult to verify the credibility regarding the information you can find on the internet
- Deception can be employed to encourage dis/misinformation
- Can be mis-used

Key message: You should be aware of the strengths and weaknesses aligned to OPKI, details of which will help you determine which assets to use to acquire information.

Some of the **strengths** related to OPKI include:

- Internet is available almost all over the world.
- The use of OS is accessible to all, though for best results personnel should receive specialised training. It is normally cheap, easy to use and can produce results quickly.
- OS is easy to share.

**Limitations** of OPKI include:

- It is difficult to verify the credibility regarding the information you can find on the internet.
  - Deception is easily possible in OS.
  - OPKI capacity can be mis-used.

## Learning activity

- Time – 5-10 mins
- Mini group task
- Name the different PKISR disciplines
- What are the strengths and limitations in relation for PKISR: GPKI, SPKI, HPKI, OPKI
- Be prepared to discuss your answers



**Interactive.** Split the participants into four groups. Give each group one peacekeeping-intelligence discipline to consider. Ask students to highlight the strengths and limitations of each peacekeeping-intelligence discipline and be prepared to share their thoughts.

## Slide 23

Matrix PKISR Strengths and limitations		
PKISR Disciplines:	Strengths:	Limitations:
GPKI	<ul style="list-style-type: none"><li>- Able to detect and identify activity or individuals at long ranges.</li><li>- Mitigates the loss of human life and detection during acquisition.</li></ul>	<ul style="list-style-type: none"><li>- Requires highly trained, specialist personnel to interpret obtained images.</li><li>- Weather and climate might limit the use of technical equipment for IMINT and/or GPKI.</li></ul>
SPKI	<ul style="list-style-type: none"><li>- Provides a 24hr, all-weather capability.</li><li>- The system is passive and therefore inherently non detectable by an actor's Electronic Warfare (EW) capability.</li></ul>	<ul style="list-style-type: none"><li>- SPKI can only work when a threat actor is radiating and providing signals that can be intercepted.</li><li>- Depending on the range of the system, it might need to be deployed near the object, thereby increasing the risk of compromise.</li></ul>

Use the slide to summarise the strengths and limitations of the different peacekeeping-intelligence disciplines. Use the lesson to assess whether students have assimilated the information during the lesson.



**Note to Instructor:** If possible, provide each student with a hard copy handout of this slide.

## Slide 24

Matrix PKISR Strengths and limitations		
PKISR Disciplines:	Strengths:	Limitations:
HPKI	<ul style="list-style-type: none"><li>- Information is more readily available than from other acquisition capabilities</li><li>- HPKI operations are cost effective when compared to other sophisticated, technological acquisition platforms</li></ul>	<ul style="list-style-type: none"><li>- HPKI is not precise; operations may take time to develop and to shift emphasis to new IRs</li><li>- Communication with potential sources is essential, and interpreters with the knowledge of local language and dialects might not be accessible when needed</li></ul>
OPKI	<ul style="list-style-type: none"><li>- The use of OS is accessible to all, though for best results personnel should receive specialised training. It is normally cheap, easy to use and can produce results quickly</li><li>- OS is easy to share</li></ul>	<ul style="list-style-type: none"><li>- The credibility regarding the information you can find on the internet/ Source evaluation and verification is difficult.</li><li>- Deception can be employed for mis/disinformation</li></ul>

Use the slide to summarise the strengths and limitations of the different peacekeeping-intelligence disciplines. Use the lesson to assess whether students have assimilated the information during the lesson.



**Note to Instructor:** If possible, provide each student with a hard copy handout of this slide.

## Take Away

All PKI staff must have a good knowledge of the types of intelligence disciplines available in the mission area and how best to use them.



## Summary

Once deployed onto a UN peacekeeping operation, students should make sure they familiarise themselves with the different types of UN intelligence disciplines that are available for tasking in the mission area. Understanding the ISR disciplines, including the strengths and limitations of each, will help PKISR staff officers when it comes to assigning ISR assets against specific information requirements.



# Lesson 3.2



## UN PKISR Process

### The Lesson



#### Starting the Lesson

The purpose of the PKISR process is to acquire information as part of the acquisition step of the MPKI cycle.

In the last lesson, we learned the different key PKISR intelligence disciplines and their strengths and limitations.

With limited resources and with the understanding of their capabilities as well as the ever-evolving need for information, the mission will need to define a clear PKISR process that enables all the information requirements to be addressed in order of their priority.

Slide 1



## Lesson 3.2

### UN PKISR Process

## Lesson Contents

- PKISR purpose
- PKISR steps in the process
- Relationship between PKISR and the MPKI cycle
- UN PKISR command and control (C2)



**Note to Instructor:** The instructor should recap the MPKI cycle by asking the students to describe the cycle. Inform students that elements of this lesson will be revision, to ensure they have a firm grasp of PKISR terminology. A clear understanding of the terms at this stage of the course will provide a solid foundation for the remainder of Module 3 as well as the final course staff exercise.

## Learning Outcomes

- Explain the PKISR process
- Explain PKISR steps in the process
- Explain the relationship between PKISR and the MPKI cycle
- Describe UN PKISR command and control (C2) structure

At the end of the lesson, the participants should be able to explain the PKISR process, including its steps. They should also be able to explain the relationship between PKISR and the MPKI process. Furthermore, they should be able to describe the PKISR command and control structure that enables efficient tasking of resources while at the same time affording some degree of flexibility to the PKISR resource managers.

## Slide 4



### UN PKISR Process



## Slide 5

### PKISR Purpose

- Seeks to answer PKI questions
- Allows U2 to address all PKI requirements, including the mission Information Acquisition Plan (IAP), Requests For Information (RFIs) and Indicators and Warnings (I&Ws)
- Allows tasking prioritization
- Ensures efficient tasking of PKISR assets

Key message: The purpose of the PKISR process is to ensure that all PKI questions are answered.

The PKISR process is the means by which the mission's PKI requirements are addressed within the capabilities of the available PKISR resources. In the mission environment, various entities and individuals will seek peacekeeping-intelligence from the U2. Therefore, PKISR tasking can come from any of the following sources:

- The mission Information Acquisition Plan (IAP) – the core tasking source.
- Request for information (RFI).
- Indicators and warnings (I&W).

All information requirements will need to be prioritised depending on their importance and urgency. It is the U2's responsibility to ensure that the available PKISR assets are used efficiently in order to ensure that all taskings are addressed.



**Note to Instructor:** The instructor should emphasize the importance of having a well-defined process that ensures no tasking is overlooked or duplicated.

## PKISR Terms - Group activity

- In your sub-groups, discuss the following terms, covered in lesson 1.2.
- Time allocated - 10 minutes.
- Be prepared to discuss your answers with the rest of the group in an open forum.



**Interactive.** The next slide lists PKISR terms which have been covered in lesson 1.2 'Fundamentals of PKISR'. To gauge the participant's understanding of the terms, split the group into two sub-groups. Give the groups 10 minutes to consider 5 terms each. The participants should be prepared to discuss their results with the rest of the class in an open forum. Their responses should include the importance of understanding the component parts of the PKISR process and the role each plays.



**Note to Instructor:** Slides 8 and 9 should be displayed as the groups discuss each term – you will be able to confirm student responses or fill in any knowledge gaps based on the notes provided in each slide.

Slide 7

## PKISR Terms - Group activity

### Group A

- IR
- CCIR
- PIR
- SIR
- EEI

### Group B

- RFI
- I&W
- NAI
- IAP
- IAL



**Interactive.** Assign each group 5 terms each.



## Slide 8

### PKISR Terms – Group activity

- Peacekeeping-Intelligence Requirement (IR)
- Commander's Critical Information Requirement (CCIR)
- Priority Peacekeeping-Intelligence Requirement (PIR)
- Specific Peacekeeping-Intelligence Requirement (SIR)
- Essential Elements of Information (EEI)

Key message: The instructor should use this slide to confirm the participant's understanding of the different terms and clarify any areas that are not clear. Spend as little time as possible on this slide, noting that these terms have already been covered earlier in the course.

**Peacekeeping-intelligence Requirement (IR).** peacekeeping-intelligence requirements are determined during the planning process by reviewing what needs to be known to fulfil the mission. When there is a gap in knowledge, a question is posed which forms the basis for a peacekeeping-intelligence requirement.

**Commander's Critical Information Requirements (CCIR).** CCIRs will be broad and not necessarily limited to PKI and hence the U2 must determine those relevant to PKI and define them on behalf of the leadership. The leadership can then endorse the CCIRs as appropriate.

**Priority Peacekeeping-intelligence Requirement (PIR).** PIRs are drawn from the CCIRs or any other guidance that the mission leadership may deem necessary. PIRs form the basis for acquisition for the Force and should therefore be thoroughly thought out and reflect the Force's priorities.

**Specific Peacekeeping-intelligence Requirement (SIR).** SIRs are in essence PIRs broken down to allow the U2 to focus the PKISR assets to more specific requirements.

**Essential Elements of Information (EEI).** EEI is the final step in the PIR relationship. These are the specific questions that will be assigned to the acquisition asset.

All this information will be displayed on the Information Acquisition Plan (IAP).

## PKISR Terms – Group activity

- Request for Information (RFI)
- Indicators and Warnings (I&W)
- Named Area of Interest (NAI)
- Information Acquisition Plan (IAP)
- Information Acquisition List (IAL)

Key message: Use this slide to confirm participant's responses. Spend as little time as is needed to ensure student understanding of the different terms.

**Request for Information (RFI).** An RFI is basically a question asked by anyone within the Mission, that needs to be answered and should be prioritised against the EEIs to allow for effective tasking of PKISR assets.

**Indicators and Warnings (I&W).** I&W is an observable behaviour or event that points towards a particular outcome, or that confirms or denies a relevant actor's course of action. These events or behaviours will be observed at specific areas called named areas of interest (NAI).

**Named Areas of Interest (NAI).** NAIs are geographical areas or points where the required information is expected to be observed or acquired.

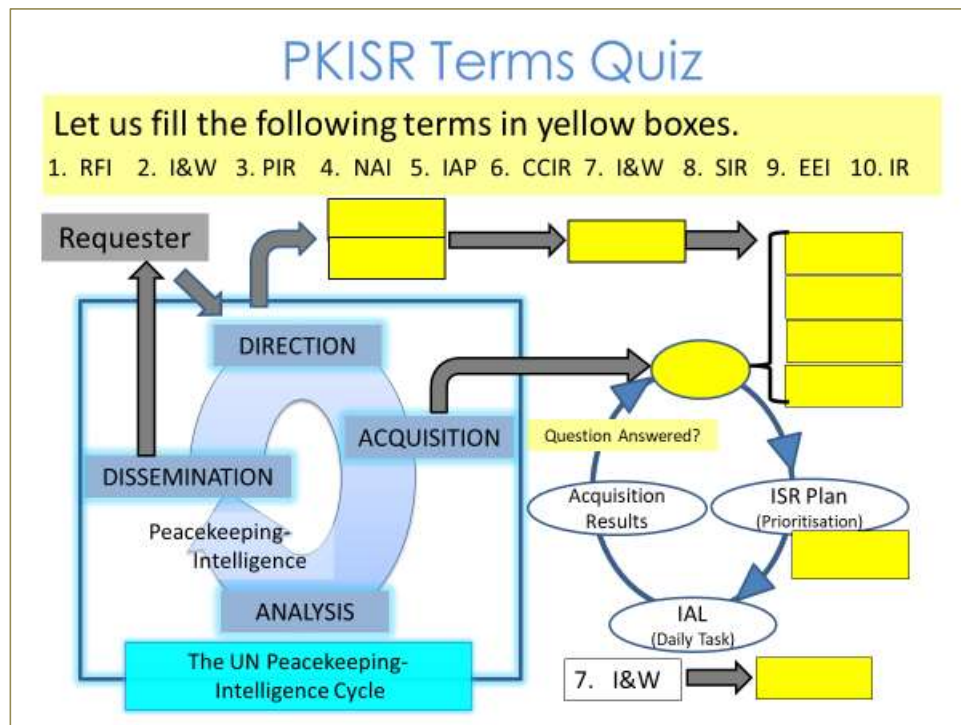
**Information Acquisition Plan (IAP).** The IAP is a living document showing all PIRs, SIRs and EEIs, with corresponding assets (discipline) that can answer the EEI, and the time limit by when an answer to an information requirement is needed. There could be several IAPs within the same mission. The IAP should be routinely reviewed and updated.

**Information Acquisition List (IAL).** The IAL is a list of information requirements (IRs) that are planned for acquisition by PKISR units for a given day. The IAL also prioritises the IR to enable easy planning for tasking.



**Note to Instructor:** *Remind the course participants that one PIR can have as many SIRs and subsequently EEs as possible. The more the requirement is broken down, the more specific the question is, and the easier it will be to focus the acquisition effort. The IAP must be regularly updated so that assets can be reallocated to other tasks. Also inform students that the abbreviation IR is often used in different ways – first as a means of direction from the mission leadership (peacekeeping-intelligence requirement) and as a means of tasking acquisition assets (information requirement). Students should remain flexible regarding this term and expect to hear it in different contexts.*

## Slide 10



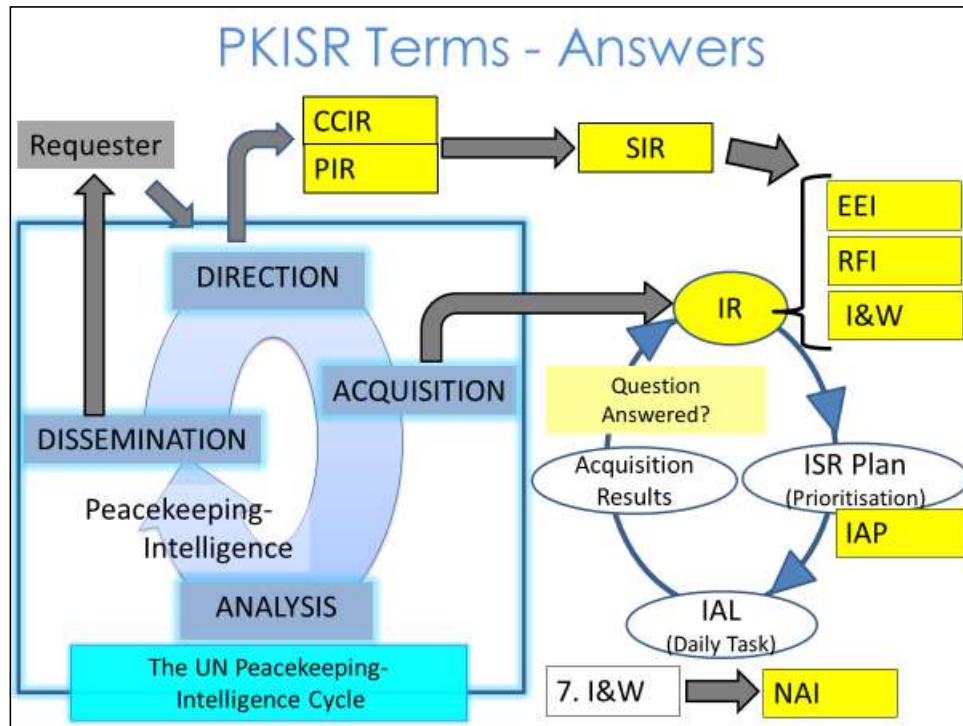
**Interactive.** Provide students with a printed copy of the slide. Ask each student to work alone to fill in the boxes with the PKISR terms highlighted at the top of the slide. Give students 10 minutes to consider the requirement. Use the time to assess student understanding. Interact with the students to see where they think the terms sit within the schematic - use the next slide to confirm their answers.



**Note to Instructor:** In terms of this slide, IR refers to information requirement. Note that I&W is mentioned twice at the top of the slide, however, one is already included in the slide (No7).

References: MPKI Handbook and PKISR Staff Handbook.

Slide 11



**Note to Instructor:** The instructor should use this slide to confirm the participant's understanding of the PKISR terms.

References: MPKI Handbook and PKISR Staff Handbook.

## PKISR Terms

- Pre-Planned Tasking
- Dynamic Tasking

Key message: PKISR acquisition assets continually get tasked and re-tasked depending on the evolving peacekeeping-intelligence situation. Hence the need for flexibility.

**Pre-Planned Tasking.** Pre-planned tasking are the information requirements (IR) in the Information Acquisition List (IAL) that are scheduled for acquisition the following day. Any tasks from the IAL that are not completed on the given day will form part of the pre-planned tasking list for the subsequent day. This may be necessitated by dynamic tasking.

**Dynamic Tasking.** It may be necessary to re-task a PKISR asset when a high priority incident that was not in the IAL occurs. Before re-tasking a PKISR asset, it is important to ensure that the asset is not already involved in a higher priority engagement. This explains why proper prioritisation in the IAL is crucial.



**Note to Instructor:** Inform the students that they will receive a further lesson on tasking later in the course.

## Information Acquisition Plan

- Captures PIRs, SIRs, EEIs and the PKISR unit capable of answering the EEI questions.
- Each mission level should have its own IAP.
- Managed by IAP manager at the Force HQ.
- Addresses 4W and 2H: 'who, what, where, how, when and how'.
- A complex tool, used for management and not for tasking ISR assets.
- The mission can have more than one IAP.

Key message: The Information Acquisition Plan (IAP) is the living document that captures all PIRs, SIRs and EEIs, and identifies which PKISR unit can answer the questions within the EEIs. There could be several IAPs designed to meet the peacekeeping-intelligence needs of the mission leadership, for example, one held by the Joint Mission Analysis Centre and one at the Force HQ.

At the Force level, the IAP is managed by the IAP manager who answers to the U2. At sector and battalion level, the IAP will be managed by the G2 and S2 respectively. In cases where a sector or battalion does not have sufficient PKISR assets, they can raise an RFI to the Force HQ or another sector/battalion. In a mission, due to operational aspects, the IAP Manager could also be called CCIRM Manager.

The IAP answers the following questions (referred to as '4W and 2H')

- **Who** would acquire the information?
- **What** information needs to be acquired?
- **Where** to acquire the information – NAIs?
- **How** are the sources and sensitive information going to be protected and kept confidential?
- **When** is the information required (no later than (NLT)/latest time of peacekeeping-intelligence value (LTOIV)?
- **How** is the acquisition unit to disseminate the acquired information?



The IAP should be used as a management tool rather than a tasking tool – tasking of ISR assets is achieved through the Information Acquisition List (IAL), which will be discussed later in another lesson.

Maintaining a complete IAP helps the mission to understand where gaps exist in acquisition capabilities and assets.

## Slide 14

# IAP – Interactive Session

## IAP Example

What?

Who?

How?

Where?

When?

How?

PIR	SIR	EI	Acquiring Unit			Source protection Considerations	NAI	NLT	LTIOV	Dissemination
			OPKI	UAS	UN Ob					

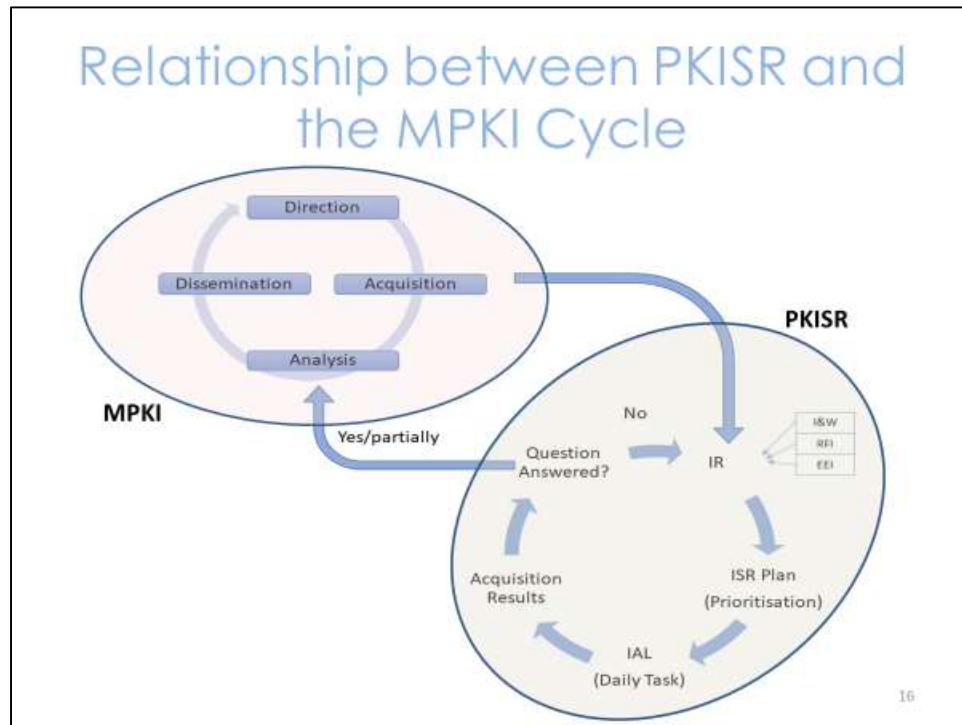


**Interactive.** The table shows suggested IAP headings. Ask the students to identify where the 4W and 2H are listed on the table. The last column is not included in the PKISR handbook but will be important since it answers the 'how' to disseminate the information.



**Note to Instructor:** Following the student discussion, build the slide to show where the various questions are addressed in the IAP.

## Slide 15



Key message: PKISR is the tool used to achieve the acquisition step in the UN MPKI cycle.

PKISR could be used to mean the entities used to acquire information or the process of managing the acquisition. For the purpose of this course, PKISR refers to the latter. That said, the two processes are closely interlinked. MPKI seeks to enhance situational awareness, maintain the safety and security of UN personnel and to inform operations and activities related to the protection of civilians (POC). PKISR is the enabler for providing these functions. The following applies to both PKISR and MPKI:

- Provide situational awareness and predictive PKI products to enable military peacekeeping planning and decision-making.
- Provide early warning of threats to the security of UN personnel (uniformed and civilian).
- Provide early warning of threats of physical violence to the local population in support of protection of civilians.
- Enhance the mission leadership's understanding of shifts in strategic and operational landscape through the early detection and identification of relevant trends and threats.

PKISR is just one component of the MPKI process that contributes towards the development of the PKI picture. Therefore, MPKI is broader than PKISR in that it involves the analysis stage to provide situational awareness. Hence the MPKI entity responsible for information acquisition manages the PKISR assets in order to satisfy all the requirements.

## Slide 16

# UN PKISR Command and Control (C2)

We will now consider the C2 arrangements regarding PKISR.

It is important to have a clear understanding of command and control within PKISR and the ability to task PKISR capabilities at the different organisational levels.

## UN PKISR Command and Control (C2)

- **Centralised Command** - responsibility and accountability for effective utilization of UN PKISR assets
- **Decentralised Execution**– assigning of effective tasking at appropriate levels depending on the task
- UN PKISR C2 can be delegated as appropriate

Key message: The most effective way to manage PKISR assets is to have a centralised command and decentralized execution structure.

A clear understanding of the PKISR C2 structure as well as the ability to task PKISR capabilities is crucial. In mission set up, the Chief/ Director of Mission Support Services (D/CMS) is responsible and accountable for effective utilization of Mission Level UN PKISR assets (civilian contracted and military). To support this, the Chief PKISR, on behalf of U2 is responsible for assigning effective tasking for those PKISR assets.

C2 can be delegated as appropriate. For instance, the Force commands the mission assets on behalf of the D/CMS. The Force can delegate control of these assets to lower levels, for instance, a sector. Effective delegation of C2 frees the mission leadership up from being involved in routine decision making on how PKISR is tasked. Some assets will be controlled at the sector level or below, especially if they are organic to units.

This system should allow for transparency and minimizes the complexities and bureaucracies imposed on various entities and individuals making information requests. This can be possible when there is effective command and control.



**Note to Instructor:** The instructor should emphasize the importance of having a clear understanding of the C2 when arriving in mission – this will help in the effective management of PKISR assets.

## Take Away

- The PKISR process begins with direction, from which gaps will be identified and PKISR assets tasked accordingly.
- The PKISR C2 structure must allow for efficient tasking while at the same time avoiding unnecessary constraints on the Mission leadership and acquisition units.
- This requires prioritization and a well defined IAP.

## Summary

The PKISR process begins with direction from the mission leadership since the process revolves around closing PKI gaps.

Finite PKISR resources should be appropriately managed against clear priorities as set out in the IAP. All missions must be traced back to an IR. CCIRs provide the U2 with clear direction and guidance on what the Force leadership considers to be important.

# Lesson 3.3



## PKISR Key Roles

### The Lesson



#### Starting the Lesson

There are a few key roles which are essential in the management of PKISR. It is important for students to understand the different roles and responsibilities and how they work together to acquire information.

Slide 1



## Lesson 3.3

### PKISR key roles



## Slide 2

### Content

- PKISR management
- PKISR key roles and responsibilities

The lesson will focus on these main areas.

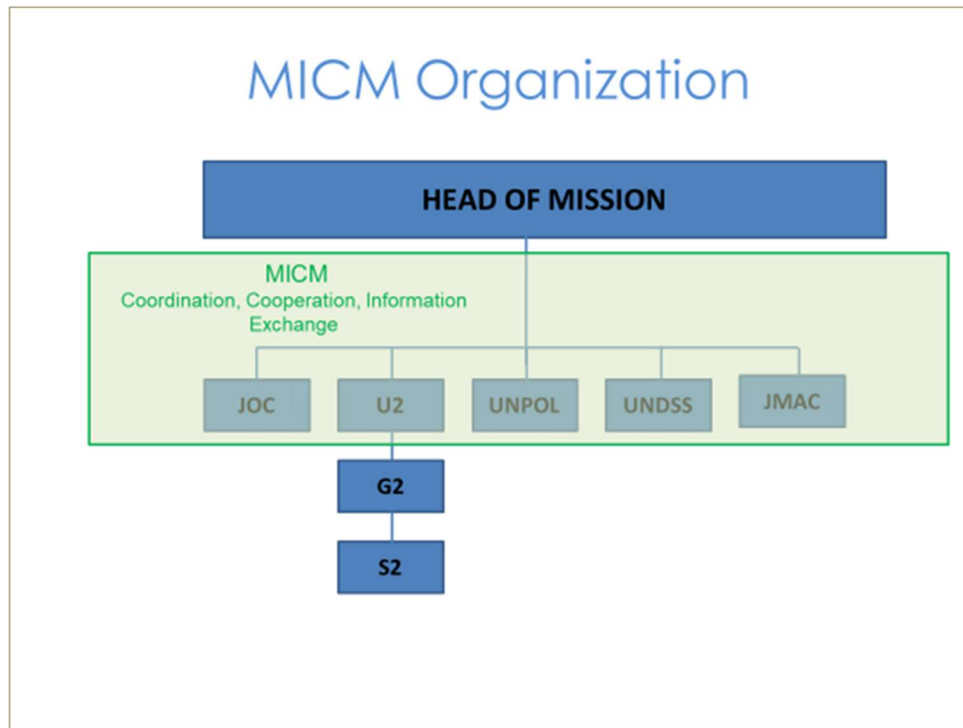
### Slide 3

## Learning Outcomes

- Explain the key roles in the management of PKISR.
- Describe how the key roles fit into the PKISR process.

At the end of this lesson, we expect you to be able to understand and explain the PKISR key roles and describe how they fit into the PKISR process.

## Slide 4



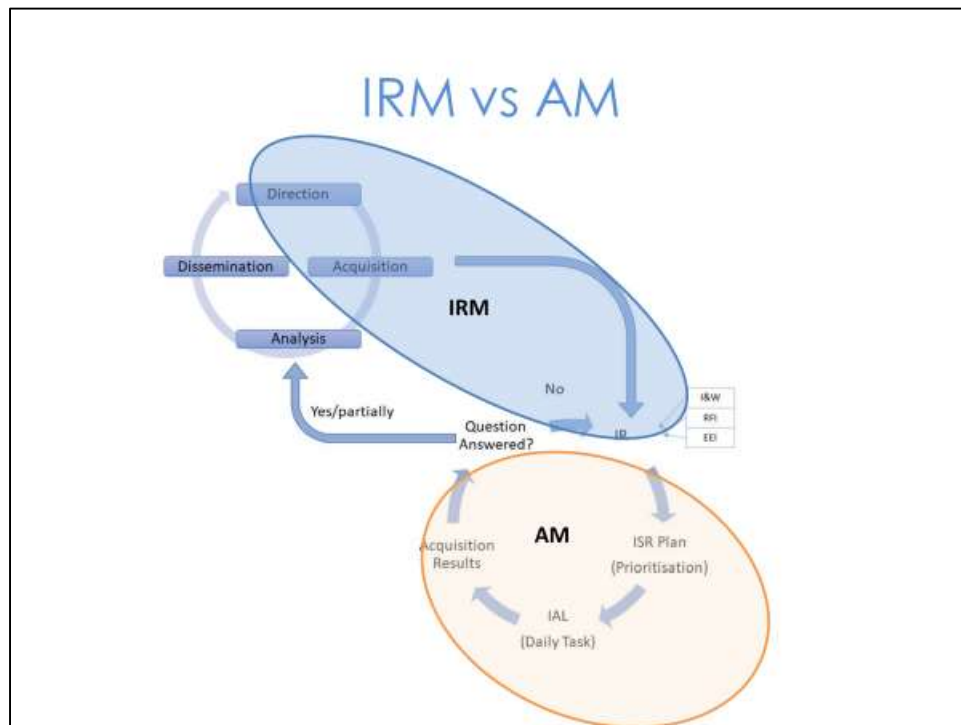
Key message: The prioritisation of peacekeeping-intelligence requirements starts with direction from the Mission leadership.

**The mission leadership holds a key role in directing the PKISR process.** The use of Commanders Critical Information Requirements (CCIRs) in this process cannot be overstated - all activity associated with PKISR must lead back to answering a CCIR.

The Mission Peacekeeping-intelligence Coordination Mechanism (MICM) provides a forum where Mission leadership can articulate their peacekeeping-intelligence requirements, all of which need to be answered to inform decision making. This process is essential if peacekeeping-intelligence activity is to be focused on mission priorities.

Without clear direction from the Mission leadership, ISR acquisition could become inefficient, meaning ISR assets tasked against an activity that is not important to the implementation of a Mission's mandate.

## Slide 5



Key message: There are two teams within an ISR cell to ensure the management of PKISR: the Information Requirements Management (IRM) team and the Acquisition Management (AM) team.

**Information Requirement Management (IRM):** IRM is the part of the PKISR process that ensures the Mission leadership's Priority peacekeeping-intelligence Requirements (PIRs) are satisfied. This entails collating peacekeeping-intelligence requirements and determining peacekeeping-intelligence gaps. The first step would be to see whether peacekeeping-intelligence requirements can be answered with information already stored on file by the mission (information management) or whether the information would have to be acquired.

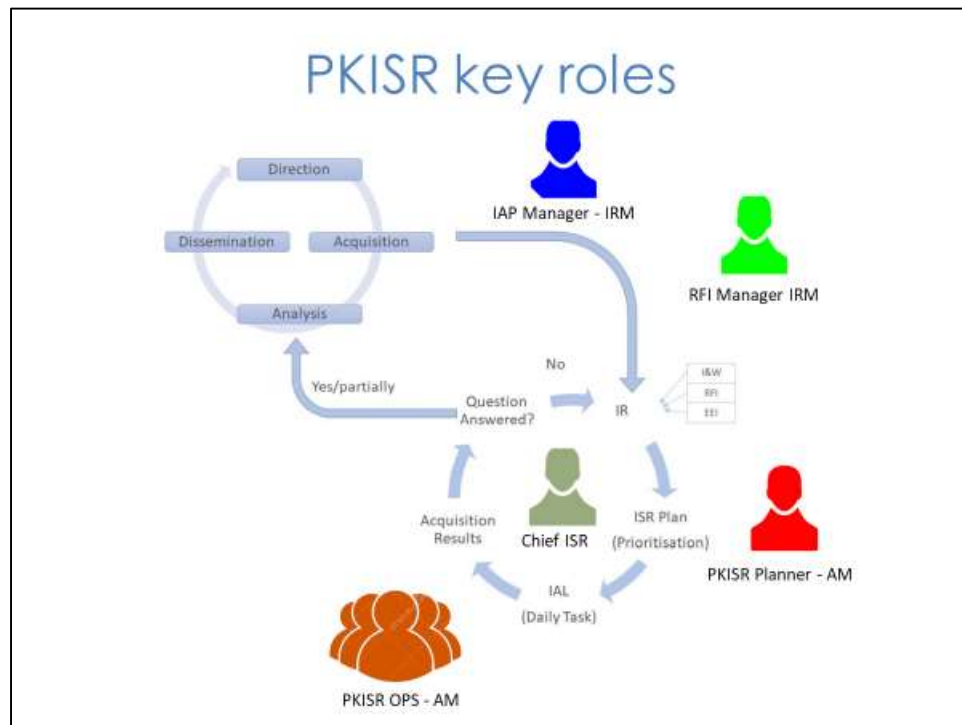
The IRM team often needs to be in close communication with those functions that understand the capability of ISR acquisition assets and to ensure the effective use of ISR resources. Therefore, IRM should maintain a strong relationship with the AM team.

**Acquisition Management (AM):** AM is the part of the process that deals with the planning and tasking of operations. This involves the management, tasking and coordination of acquisition units or assets, monitoring results (incoming reports) and re-tasking assets as required.



**Note to Instructor:** Some of the information mentioned in this slide has been addressed in earlier lessons and therefore could act as a means of revision.

## Slide 6



Key message: The PKISR process is reliant on several key personalities.

The key roles and responsibilities are shown here on the slide. Let us go through a quick summary of each role, before focusing on their specific responsibilities in the PKISR cycle.

**Chief PKISR:** The Chief PKISR, on behalf of U2, is responsible and accountable for the day-to-day oversight of PKISR management.

**IAP Manager (IRM):** The IAP Manager is responsible for ensuring the IAP is up-to-date and reflects the priorities peacekeeping-intelligence requirements remain aligned to the Mission leadership's direction. In a mission, IRM Manager can also be called the CCIR Manager.

**RFI Manager (IRM):** The RFI Manager is the point of contact for anyone outside the PKISR team that has a peacekeeping-intelligence requirement. All RFIs must go through the RFI Manager for quality control, registration and prioritisation.

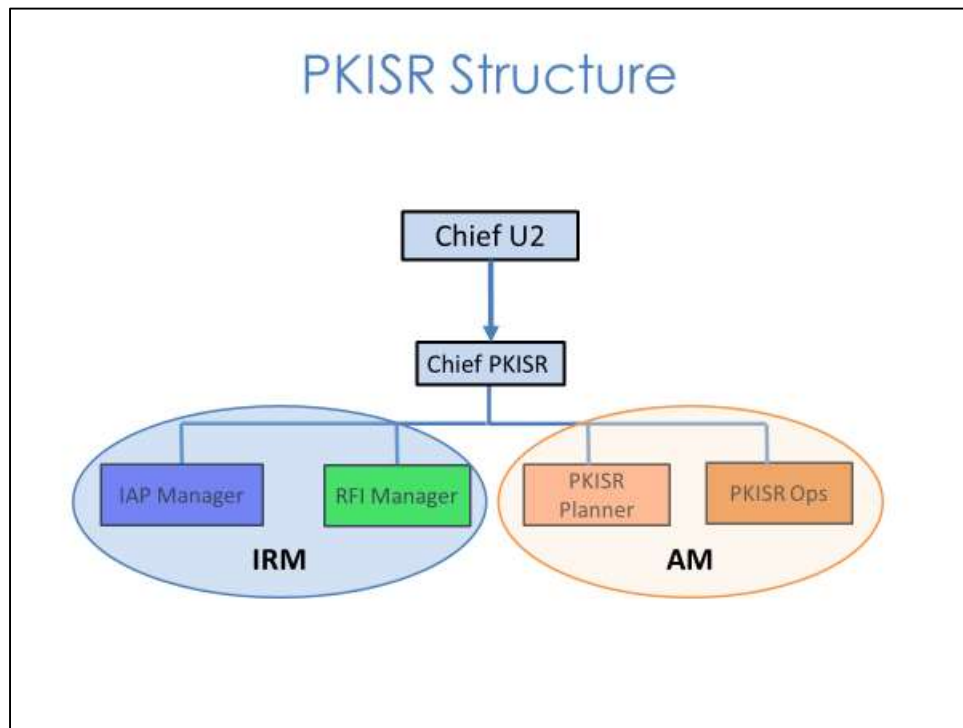
**PKISR Planner (AM):** The PKISR Planner plans for short to medium term PKISR coverage, taking into consideration the priority of the IRs, sensor capability and capacity, operational plans and external factors like weather and terrain.

**PKISR OPS (AM):** The PKISR OPS is responsible for the daily tasking of the acquisition assets.



**Note to Instructor:** *Stress the importance of communication and interaction between the different roles. Although they have different tasks and responsibilities, mission success is everybody's responsibility, and communication is key to a smooth process.*

## Slide 7



Key message: The exact composition and structure of the U2 will depend on the size of the military component and its mandate.

For the purposes of this presentation, I have split the PKISR cell into four component parts: the IAP Manager, the RFI Manager, PKISR Planner and the PKISR Operations. You can see in this slide how the different roles support the Information Requirements Management team or Acquisition Management team.

It is important for these individuals to work closely together to ensure the PKISR process is effective and efficient. This structure will be used as a framework to go through each role in turn.

## Slide 8

### Chief PKISR Responsibilities

On behalf of Chief U2:

- Manage and oversee Force-level PKISR activities
- Support CCIR validation
- Advise on RFIs/IR de-confliction



Key message: Chief PKISR oversees the management of both Information Requirements Management (IRM) and Acquisition Management (AM).

The nature of the mission will determine if this function is held by a military or civilian person. In practice, whilst the mission leadership - Director/Chief of Mission Support (D/CMS) and Force Commander - is responsible and accountable for the effective utilization and tasking of UN commercial or military PKISR assets, the process of assigning tasking to those assets should be managed by Chief PKISR cell on behalf of the Chief U2.

Chief PKISR supports CCIR validation by confirming the priority peacekeeping-intelligence requirements from the Head of Mission and Force Commander. Chief PKISR should attend the relevant PKISR meetings, e.g., the Mission peacekeeping-intelligence Coordination Mechanism (MICM), as well as meetings with the Force Commander, to ensure a credible understanding of mission priorities.

Chief PKISR will provide oversight of all PKISR activities and will provide final arbitration over the prioritisation of information requirements.

Chief PKISR's role does come with some challenges (next slide).



## Chief PKISR - Challenges

- Receiving clear direction from the Mission leadership.
- Understanding tasking authority for ISR assets.

Key message: Earlier in the course, you heard that direction from the Mission leadership drives the PKISR cycle – this cannot be overstated as all Mission activity associated with PKISR and MPKI must lead back to answering the commander's critical information requirements (CCIRs).

However, there might be occasions when this does not happen, due to the commander's busy work schedule. In such circumstances, the U2 / Chief PKISR will have to arrange a time to ask the mission and/or Force Leadership for their direction to ensure PKISR activities are continually aligned to mission priorities and are acquiring the information needed to inform high-level decision making.

In some instances, the U2 / Chief PKISR might have to suggest priority peacekeeping-intelligence requirements to the commander for their approval. This approach might act only as a catalyst to a dialogue between the commander and the U2 / Chief PKISR resulting in an agreed set of peacekeeping-intelligence requirements. To support this dialogue, the U2 / Chief PKISR must have a clear understanding of the mandate, mission priorities and the commander's intent to ensure their suggestions are credible.

Another challenge is understanding the tasking authority for PKISR assets in the Mission area. Occasionally, there may be an unclear understanding of who provides tasking authority for PKISR assets, such as UAS. The UN's policy on 'Authority, Command and Control' provides the C2 arrangements regarding PKISR assets. However, Mission standard operating procedures will dictate local tasking arrangements. Having a clear

understanding of these procedures early on in your assignment is key to the effective management of PKISR, especially during times of crisis management.

## Slide 10

### IAP Manager - responsibilities

- Support PIR validation.
- Develop indicators and warnings.
- De-conflict RFIs vs IRs of MPKI cycle – support breakdown of active and new IRs.
- Highlight, track and support evaluation on incoming reports from units/assets.



The role of the IAP Manager is outlined on this slide. The role includes:

**Supporting PIR validation:** It is important for the IAP Manager to keep track of what information requirements (IRs) have been answered to avoid repeated tasking. A good metric to track is the percentage effort of acquisition against EEs, RFIs and I&W that are answered. This will assist in determining if the weight of activity is appropriately based on the ongoing situation in the mission, and if the requirement has been met by the U2.

**Acquire I&W:** The IAP Manager should have responsibility for monitoring the I&W process and feeding the IRs generated into PKISR Plans for acquisition. There is often a close link between the I&W and the IAP and therefore the IAP Manager should oversee both aspects.

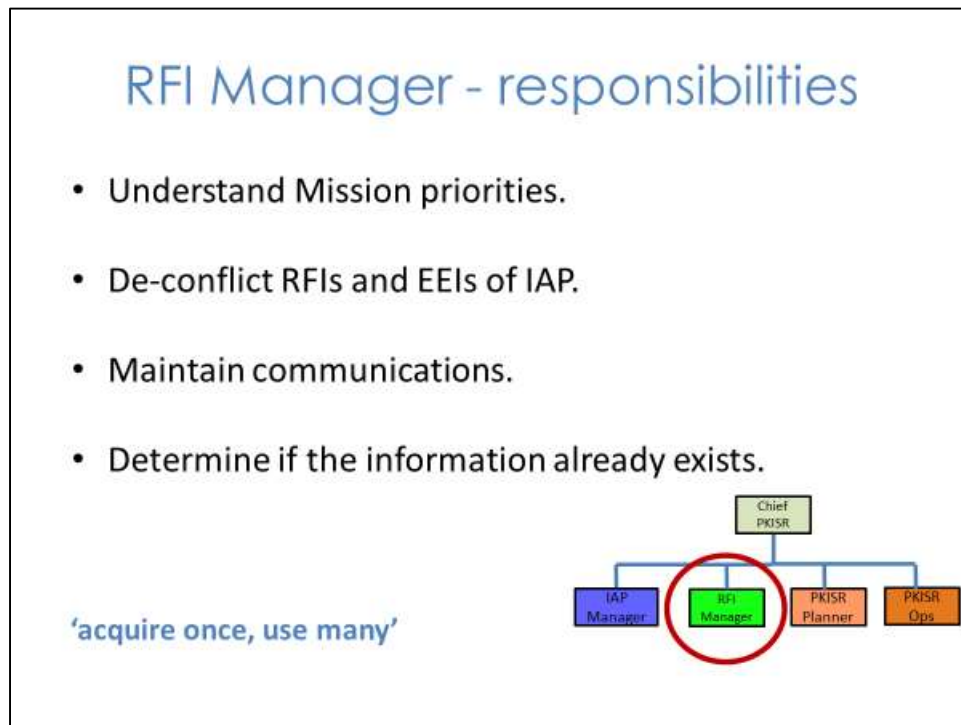
**De-confliction of RFIs.** To ensure the most efficient management of IRs and a seamless process for handing over the IRs to the AM section for acquisition, the IAP Manager should also take the IRs developed by the RFI Manager and compile all active IRs with new ones, into a prioritised list.

**Support evaluation:** It is important to evaluate performance over a period of time to see whether PKISR assets are being effectively utilized or not. This will normally involve a period longer than just one 24-hour Information Acquisition List tasking. They can acquire part of the answer on one day and complete it later on another tasking.



**Note to Instructor:** *Inform students that they will hear more on the IAP later in the course.*

## Slide 11



**Key message:** ‘Acquire once, use many’ refers to effective information / data management, where information requirements can often be answered by information already acquired and stored on a mission database.

**Good understanding:** Determining the priority of operational RFIs requires a good understanding of what the mission leadership is focused on.

**De-confliction:** If the information does not already exist, the RFI Manager should consult the IAP to determine if the RFI relates to any of the current EEIs. If the RFI is a PKI request that does not directly relate to an EEI then the topic should be recorded.

**Close communications:** Regardless of the origin of the RFI, good communication to any requester is required throughout the process to ensure that there is an accurate picture of the acquisition to be planned and executed. This is essential to ensure that there is clear understanding on the priority of the acquisition, so tasking is not repeated unnecessarily.

**Existing information:** Once the RFI has been accepted by the manager, the next task should be to determine if the information already exists. One of the fundamental principles of PKISR is to “acquire once, use many”, meaning that instead of acquiring new information for every request, if the answer already exists then this should be sent to the customer to determine if it meets their needs.

One of the challenges facing the RFI Manager is having to send RFIs back to the originators since the request forms lack the detail required to incorporate the requirement into the IAP. It is in the interest of the RFI Manager and U2 as a whole that Mission components understand how to fill out an RFI form correctly in order to avoid prolonging the process. This is especially important if RFIs are submitted very late in the planning process, which can often be the case.


## Slide 12

## RFI Tracker - example

[illegible]

Key message: An RFI tracker is used by the RFI Manager to capture and manage all RFIs requiring ISR support. This slide highlights an example of a real-time 'RFI Tracker'.



 **Note to Instructor:** The purpose of this slide is to provide an overview of an RFI tracker and not to go into the detail. Therefore, inform students not to try and read the detail, but instead listen to your explanation of the document. More detail on RFIs will come in the next lesson. You will need to build the slide as you progress through the notes (prompts are provided in the notes).

Let us take a look at the example tracker to understand its value in the PKISR process. Starting at the left-hand side of the table, the document captures who is requesting the information, when the information is required and in what format. Importantly, it also captures why an RFI has been submitted, which helps the RFI Manager when it comes to prioritising information requirements. Having a good understanding of mission priorities and the Commander's intent will help to ensure information requirements are prioritised correctly.

The RFI Manager, working closely with the IAP manager, considers all RFIs to see whether they can be answered by using information already stored in a PKI or PKISR database (remember, 'acquire once, use many'). If an RFI cannot be answered using the database, then the RFI Manager will have to determine whether the RFI is related to other EEs already on the Force's Information Acquisition Plan (IAP). This ensures that ISR tasking is coordinated to avoid the duplication of effort, i.e., two assets acquiring the same information twice.

In this example, you can see that a number of the RFIs at the top right are aligned to an operation that the Force Commander has deemed his or her highest priority. As such, these RFIs are likely to be included in the IAP. There are other RFIs whose EELs are the same as the major operation already mentioned. As such, this RFI can be merged with the other RFIs rather than tasking a separate PKISR asset. Next, you will see an RFI circled at the bottom right of the spreadsheet that can be answered using information already stored in the ISR database and as such does not need to appear on the IAP. Finally, some RFIs will be low priority and may not be actioned unless there are sufficient ISR assets available to task, due to de-confliction of assets availability.

All RFIs should be submitted with sufficient time to enable deliberate tasking. However, on occasion the RFI Manager will need to request dynamic tasking in response to a request (more of which in a later lesson).

Note the status against each RFI, allowing the RFI Manager to have oversight of those RFIs that are planned, tasked or have been completed. This ensures assets are not tasked more than once against the same requirement and are removed from the list once the originator is content that their request has been answered.



## Slide 13

### PKISR Planner - responsibilities

- **PKISR asset capabilities:** Good understanding of asset capabilities, in order to task several acquiring units at the same time.
- **Operational perspectives:** Responsible for prioritisation of longer-term planning requirements vs current dynamic requests.
- **Blending:** Able to handle and blend in on unplanned events or any new circumstances.



**Asset capabilities:** The role of the PKISR Planner is to have several views on what PKI gaps or RFIs need closing and which PKISR capabilities are best placed to answer them. This includes considering geographical locations of acquisition assets as well as whether the asset is physically capable of answering the question.

**Operations perspectives:** The PKISR Planner must maintain a close link with the Force U5 Plans and Chief PKISR to ensure an understanding of upcoming operations. For example, if there is a future planned operation, the PKISR planner must factor in PKISR support to that operation in advance of its execution. This could include acquiring pattern-of-life information or answering related RFIs. This would ensure that appropriate PKISR assets were available to support the operation, assuming the tasking was considered a high enough priority.

**Blending:** The PKISR Planner would also have to focus on the current situation and any change in tasking; unplanned events such as poor weather or a changing operational plan would affect planned ISR activities and may require another unit or assets to be tasked with an additional tasking line. The PKISR Planner must minimize the impact of such events to the Information Acquisition List (IAL) while maximizing any acquisition opportunities.



**Note to Instructor:** Inform students that they will hear more on PKISR Plans later in the course.

## Slide 14

### IAL - example

FBQ U2 IAL to Forces											
Ref: U2 in case		This IAL is dated 13/02/2019									
Ref: U2 in case		Approved Tasking: 2019									
SERIAL	WP REF	REQUEST	INDICATOR	NH	Phase	A City	B City	C City	Secured	SSP	IA
1	PKISR 1.1	Sign of armed group presence?	Camps of about 200 x 100 m with trees in the background, armed PV and/or offensive weapon in the center, a kitchen area, and a place where IAC together. Several / Full storage in the area.			X					X
2	PKISR 1.1	What are the main areas of interest, most problematic areas, etc.?	Check and measure are identified in villages destroyed villages. Check and measure are checked. Government and regional administration centers checked. Several of the most important areas of interest of electricity, water, and other services are checked. Several.						X		X
3	PKISR 1.1	Where are schools affected with security issues?	No teaching. Schools closed because of no power or no internet service.						X		X

(information extracted from the IAP and RFI  
tasker)

**Key message:** The IAL is a living document and can be updated up to 24 hrs prior to operational execution.



**Note to Instructor:** You should re-acquaint the students to the IAL and its different headings. The purpose of this slide is to provide an overview of IAL and not to go into the detail. Therefore, inform students not to try and read the detail, but instead listen to your explanation of the document. More detail on the IAL will come later in the course.

This slide shows an extract from an Information Acquisition List (IAL). You will be familiar with the format, which highlights those priority acquisition requirements that are being planned to support the mission. The PKISR Planner uses this tool to manage the acquisition, making sure the most appropriate ISR assets are assigned to acquire the information listed in the IAL. To enable this, the planner must have a thorough understanding of the capabilities of the different PKISR assets within the mission area, as well as the location of each asset and whether it is available for tasking, e.g., a UAS might be undergoing maintenance.

The PKISR Planner will maintain communication with the Force U3/5 cell to ensure the acquisition requirements have not changed and also with the PKISR units to ensure they are available and able to acquire the information as planned. The 24-hour IAL will be handed to the PKISR Ops the day before the PKISR missions are due to be executed. The planner will ensure PKISR Ops fully understands the acquisition requirement before the IAL is formally handed over.

Lastly, the planner may become involved during the day of the PKISR execution if there are any last-minute or time sensitive PKISR requirements that qualify for dynamic tasking. If this is the case, the PKISR Planner working with PKISR ops will help determine which PKISR asset is best placed to conduct the dynamic tasking, and based on the asset's capabilities, the planner's understanding of current operations and the Mission / Force's priorities, so that any re-tasking has a minimal impact on the IAL.

Communications between PKISR Plans/Ops and the PKISR acquisition units can be challenging at times, especially if the unit is not forthcoming on issues of capability, availability of assets and its own activities. It is important for the PKISR Planner to maintain regular communications with such units to build up a professional and effective relationship.

## PKISR OPS - responsibilities

- Tasking PKISR assets
- Enabling dynamic tasking
- Evaluation and dissemination



Key message: The PKISR Ops function focuses on the 24-hour period before and after the point of acquisition.

**Describe tasking:** The Information Acquisition List (IAL) is handed over to PKISR Ops 24 hours before execution. PKISR Ops should check the plan to make sure it is achievable and liaise with the acquisition elements to ensure they understand the tasking, including reporting requirements. This ensures the acquisition unit can implement the mission knowing the priority requirements, should communication be lost, or a mission is cut short.

**Dynamic tasking:** PKISR Ops manages dynamic tasking, although will work alongside the PKISR Planner. For example, if the Force HQ receives reporting notifying them of an imminent attack against village X, PKISR Ops must react to this as a matter of high priority to divert acquisition assets to determine any action to be taken. It is the PKISR Ops' job to determine which asset is most appropriate to support the dynamic tasking and to liaise with the respective unit to ensure that the new tasking is understood. This could be an PKISR asset that happens to be in the area or the activation of another PKISR asset that can deploy to the area at speed. Once the urgency of the situation has subsided, PKISR Ops should then clarify with the unit what tasking was not completed and liaise with PKISR Plans to ensure the missed tasking is incorporated into future plans or IALs.

**Dissemination:** It is the PKISR Ops' job to ensure that a report is analysed and disseminated to the customer of the RFI or to the IAP Manager in the case of tasking against the IAP or I&W. The PKISR Ops must also evaluate the tasking of the PKISR plan (IAL) for that day, in

close consultation with PKISR analysts and PKISR units. This is a very important function, most notably to ensure that PKISR assets are not tasked against gaps that no longer exist.

## Slide 16

### Tasking Line - example

NAI	GRID	OBJECT	TASK	WHEN	PRI	COMMENTS
A and T	55673346	Forested area	Pattern of life - Phase 4 reporting	after scan MSR	1	Share message with U2ISR

**Transit time task**  
Follow the track and report on overall activity, follow the main support route DOUENTZA - HOMBORI and report on visible signature in accordance with the main supply route indicator list

**Task:**  
Scan the main supply route (MSR) against the request: "Sign of armed group X presence?"  
  
Describe how IDPs are living in the DOUENTZA area – tented areas?  
  
Describe visible activity in NAI A and T. Is there activity or any public infrastructure within the forested areas? IDP-flow on MSR? Outline of the village. Phase 3 imintrep on following indicators to be provided to U2 PKISR.

**Indicators**

- Temporary camps in the vicinity of villages.
- Check points present on roads.
- Camps of about 200m x 300m with fires, armed individuals and/or weapon caches.
- Large cooking areas. Barrels / fuel storage in forested areas.
- More people than expected in villages.
- Public infrastructure.
- Armed PAX or vehicles with mounted weapons.
- Bonfires in vicinity of villages.
- Wells and water tanks / pumps.

Key message: PKISR Ops must ensure acquisition units understand the tasking so that they are able to complete or prioritise activities.



**Note to Instructor:** The purpose of this slide is to provide an overview of a PKISR asset tasking line and not to go into the detail. Therefore, inform students not to try and read the detail, but instead listen to your explanation of the product. More detail on tasking lines will come later in the course.

A tasking line is best practice to make sure a PKISR unit has a detailed description of what is expected from the activity – the document would be attached to an IAL or communicated directly to an acquiring unit/asset.

The slide is an example of what a tasking line might look like in a UN Peacekeeping Mission. In this example, a UAS has been tasked (blue box) to observe activity in a specific area, namely NAIs 'A' and 'T'. The focus of the mission is to observe pattern of life in these two areas, as well as to observe any possible activities that could affect an upcoming operation (orange box). The tasks (red box) relate directly to the information requirements contained in the IAL, including the reporting requirement. To assist the unit, the tasking line also includes a series of indicators (green box) that would help to answer the information requirement. Such indicators, all of which might not be included in the IAL, help the PKISR unit answer the information requirement.

The PKISR Ops' role in this process is to produce the tasking line and ensure the PKISR unit fully understands the requirement. As such, PKISR Ops will discuss the details of the tasking

line with the PKISR unit. This ensures the PKISR unit can execute the order and react to uncertainties without relying on further guidance from the HQ, especially in times of crisis, such as a failure in communication with Force HQ.

Once the acquisition period is over, it is the PKISR Ops' job to ensure that the acquisition unit disseminates the product back to PKISR IRM, for further distribution to U2 analysis or the originator of the request. The outcome of the PKISR activity will determine whether the IR has been answered or it needs further tasking.

## Take Away

The PKISR cycle relies on a team of PKISR staff, all working towards a common goal, using agreed procedures that ensure an effective and efficient acquisition process

### Summary

The PKISR cycle relies on individuals performing their duties to ensure the process is effective and efficient. Everyone needs to understand their role and how they interact with other actors involved in the process.



# Lesson 3.4



## Request for Information (RFI) Management

### The Lesson



#### Starting the Lesson

As a PKISR Unit member, you must keep in mind that RFI Management is essential in making the information acquisition process efficient.

This lesson will cover the following topics:

**Initially**, it will address the definition of the 'request for information', or RFI as it is termed, before listing and explaining the PKISR assets' tasking sources.

**After** that it will explain the process of managing peacekeeping-intelligence requirements (IRs), before going through the RFI Manager's tasks, the RFI prioritisation process and the dissemination of information.

**Finally**, it will describe how to complete and scrutinize a RFI form and the life of the information request.

Slide 1



Lesson 3.4  
Request For  
Information Management

## Slide 2

### Learning Outcomes

- Explain the RFI management process.
- Demonstrate how to write and manage RFIs.



**Note to Instructor:** *The instructor can take a minute to discuss the outcomes with the students.*

Upon completion of this lesson, you will be able to explain the UN PKISR's RFI management process and you will be able to write and manage RFIs within a PKISR unit.

## Slide 3

### Content

- RFI definition
- PKISR assets' tasking sources
- Management of intelligence requirements
- RFI Manager's tasks
- RFI prioritization process
- Dissemination of information
- Life of an RFI
- Writing an RFI

Key message: Understanding how RFIs are initiated and managed is important so that you all can contribute effectively to a PKISR Unit, especially one with limited resources.

## Slide 4

### RFI definition

- An RFI is an intelligence related question to be answered by PKISR capabilities.
- **In general, within the UN Mission:**
  - Initiated by any UN staff member (civilian or uniformed) or entity in the Mission
- **Specifically, within the MPKI network:**
  - An external request to another part of the MPKI architecture, made when the military entity does not own the "required assets to acquire the needed information".



**Note to Instructor:** The instructor should be aware of the definitions given in the PKISR Handbook and in the UN MIO RTP courseware. They should also encourage the participants to raise questions and enhance student interaction.



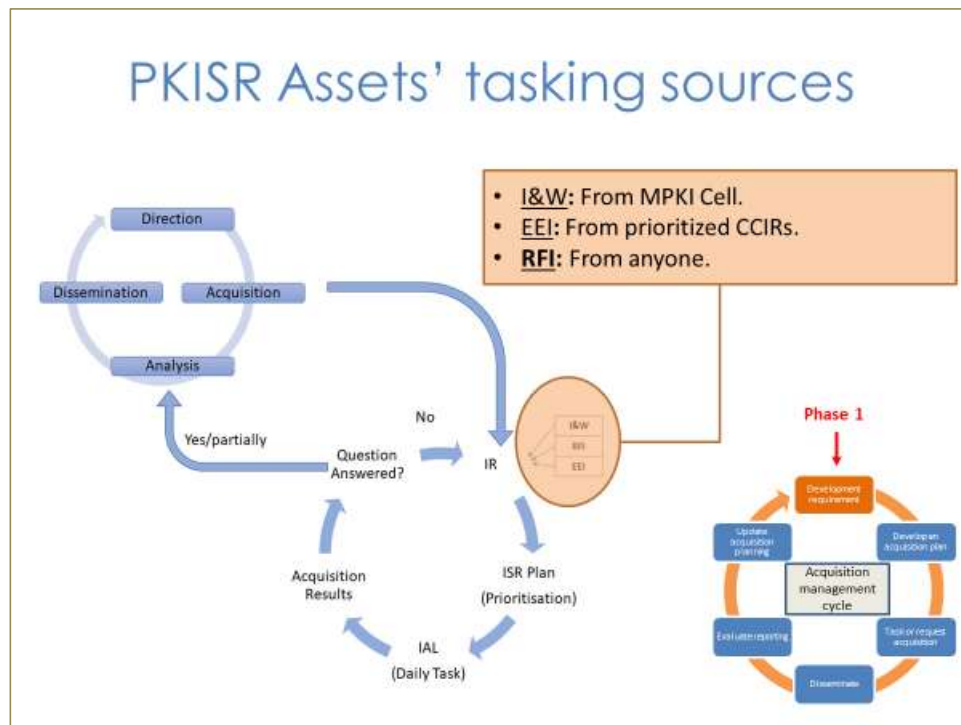
**Interactive.** Ask the students when they think a Request for Information (RFI) is initiated.

**In general:** An RFI is a peacekeeping-intelligence related question asked by any UN personnel (civilian or uniformed) or entity in the Mission, that needs to be answered by using PKISR capabilities. For example, a request for information from the Joint Mission Analysis Centre (JMAC).

**But within the MPKI network:** An RFI is made when the MPKI entity does not own the assets required to acquire the information, and thus must send an external request to another part of the MPKI architecture in the form of an RFI. For example, a request from one Sector HQ to a neighbouring Sector HQ or Force HQ.

All RFIs must receive a response, even if it is a nil response.

## Slide 5



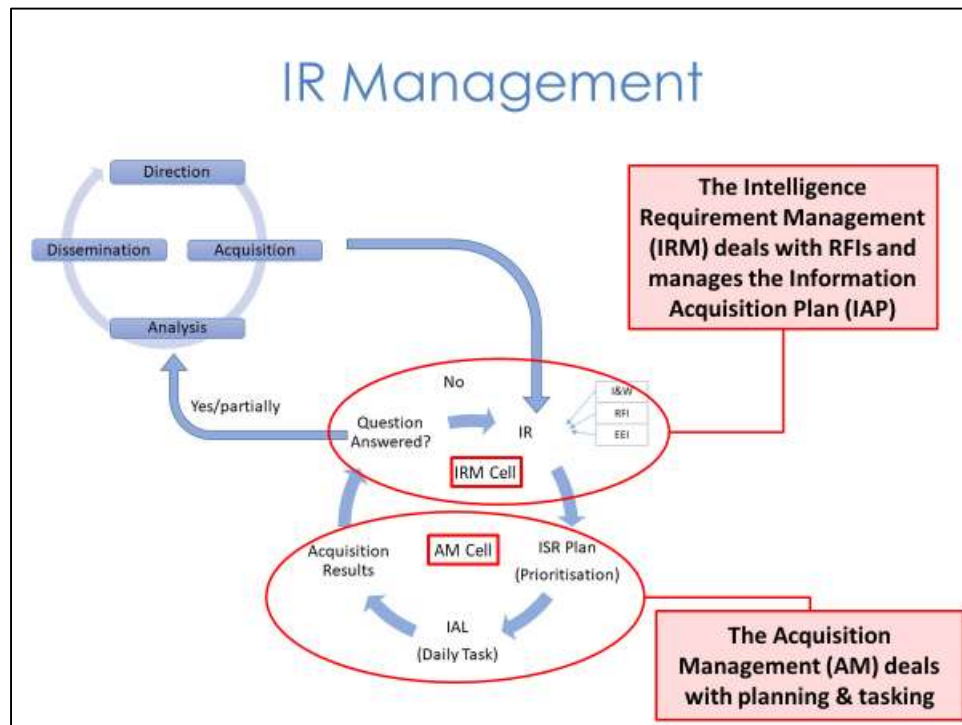
Key message: It is important to set up a process that allows anyone within a UN Peacekeeping operation to initiate a RFI and for the PKISR unit to answer it, using available resources.

This slide shows the PKISR process alongside the acquisition management cycle. You should recall that the three core sources of a peacekeeping-intelligence requirement are:

- Indicators & Warnings (I&W).
- Essential Elements of Information (EEI) obtained from prioritised Commander's Critical Information Requirement (CCIR), and
- Requests for Information (RFIs).

So, RFIs should also be answered by prioritising the request against the other tasking.

## Slide 6



Key message: Communication between peacekeeping-intelligence Requirement Management (IRM) and Acquisition Management (AM) is essential to ensure the most effective employment of what are finite ISR resources.

As highlighted in an earlier lesson, there are two parts to the management of PKISR, the peacekeeping-intelligence Requirements Management (IRM) and the Acquisition Management (AM):

- IRM deals with the management of RFIs and the Information Acquisition Plan (IAP).
- Whereas AM deals with the planning and tasking of the acquisition operation.



**Interactive.** Does anyone have experience working in an ISR position in your home country? Please tell the group about how you would manage RFIs.

## Slide 7

### RFI Manager's Tasks

- Review all RFIs.
- Crosscheck databases - "*Acquire once, use many*".
- IAP consultation (if RFI relates to any EEI).
  - RFI recording as an IR.
- Information review (IAP properly reflecting intelligence requirements).

[Key message:](#) "*Acquire once, Use many*". Students should recall the earlier lesson on data and information management.

The RFI Manager is part of peacekeeping-intelligence Requirement Management (IRM). The RFI Manager's role includes reviewing each RFI to ensure that the request has been filled out correctly by the customer. We will look at the RFI form later in the lesson so that you are aware of the information that is needed to be included in the request.

**RFIs without the necessary information must be rejected and returned to the originator / customer to be updated.**

Once a RFI has been accepted by the RFI Manager, the next task is to determine if the information already exists. In fact, one of the fundamental principles of PKISR is to "*Acquire once, use many*". This means that you should not acquire new information for every request. Instead, you should search databases to see if the information already exists and check whether this information meets the customer's needs. It is recognized that in some missions it will be a challenge to know if the information already exists since databases may not be used or up to date.

If the information does not already exist, the next step for the RFI Manager will be to consult the IAP to determine if the RFI relates to any of the existing EEIs. This will assist in the prioritisation process. If the RFI does not relate directly to an EEI, then the RFI Manager has to raise the request as a new peacekeeping-intelligence requirement (IR). Finally,



when the IAP is updated, the RFI Manager must review the information to determine if the IAP properly reflects the IR.

## RFI Prioritisation process

Effective prioritisation relies on:

- A close working relationship between the RFI and IAP Managers.
- A good understanding of the Mission priorities.

Key message: RFIs need to be prioritised alongside other peacekeeping-intelligence requirements. This requires the PKISR management team to work closely together and have a credible understanding of the mission's priorities to be effective.

Sometimes, a single RFI can contain multiple questions, each of which should be developed into an information requirement (IR) that can be answered. It is the RFI Manager's job to develop these IRs and to ensure that the indicators are appropriate to the topic. Once the RFI has been broken down into individual IRs, they should be passed to the Information Acquisition Plan (IAP) Manager who will then prioritise them against other IRs.

Upon receipt of the IRs from the RFI Manager, the IAP Manager will assign a priority to each IR. This will be straightforward when the RFI relates directly to the IAP. If the RFI does not relate to the IAP it becomes more challenging to assign an appropriate priority to the RFI. Prioritisation is essential as without it, there is no way to ensure that the critical aspects of the mission are being covered.

## Slide 9

### Dissemination of Information

- Ensure RFIs are closed after being answered.
- Ensure that the information goes to the right organisation at the right time.

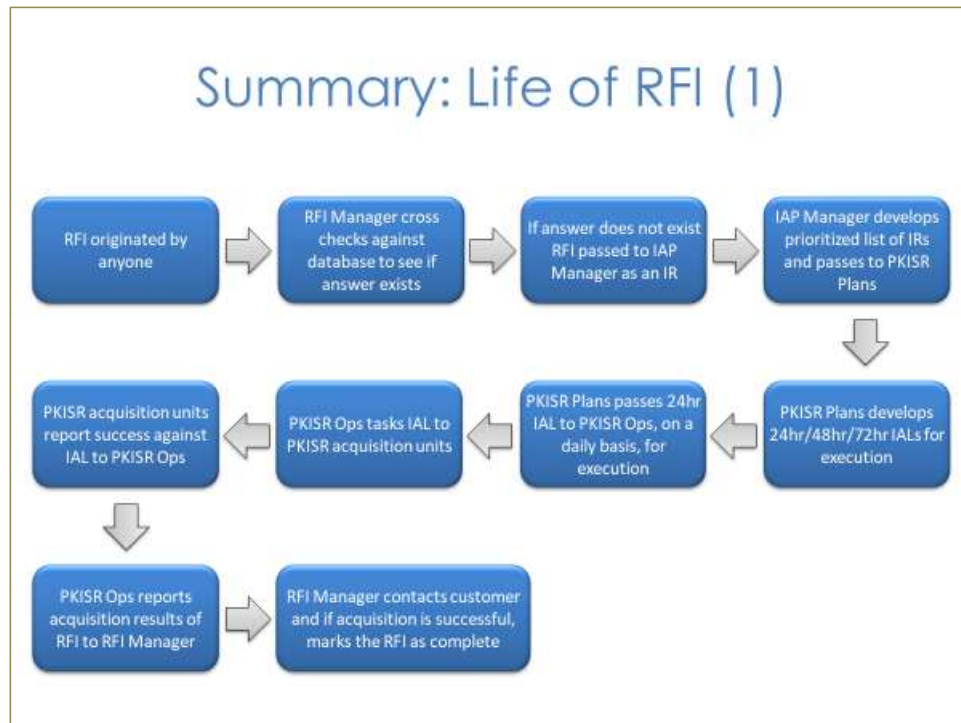
Key message: Once a RFI has been answered in accordance with the Information Acquisition List (IAL), the next step within the process is to receive a report from the acquisition unit.

Once the information requirement (IR) relating to the RFI is successfully answered, the acquisition management team must inform the RFI Manager, who is responsible for disseminating the response to the customer. This is to ensure that a response is disseminated to the customer at the right time. Regarding this particular task, other PKISR unit members could disseminate the product, especially when there is a time-sensitive aspect to the RFI response. The response should also be stored in a database in case the information can be used again in the future, by other U2 cells or wider mission entities.

In all circumstances, it is very important to ensure that RFIs are closed once they have been answered to maintain the IAP and daily IAL.

Finally, the handling of reporting and the dissemination of peacekeeping-intelligence requires oversight to ensure the product only goes to those that need to see it.

## Slide 10



Key message: Within a PKISR unit, a RFI cycle of life starts and finishes with the RFI Manager.

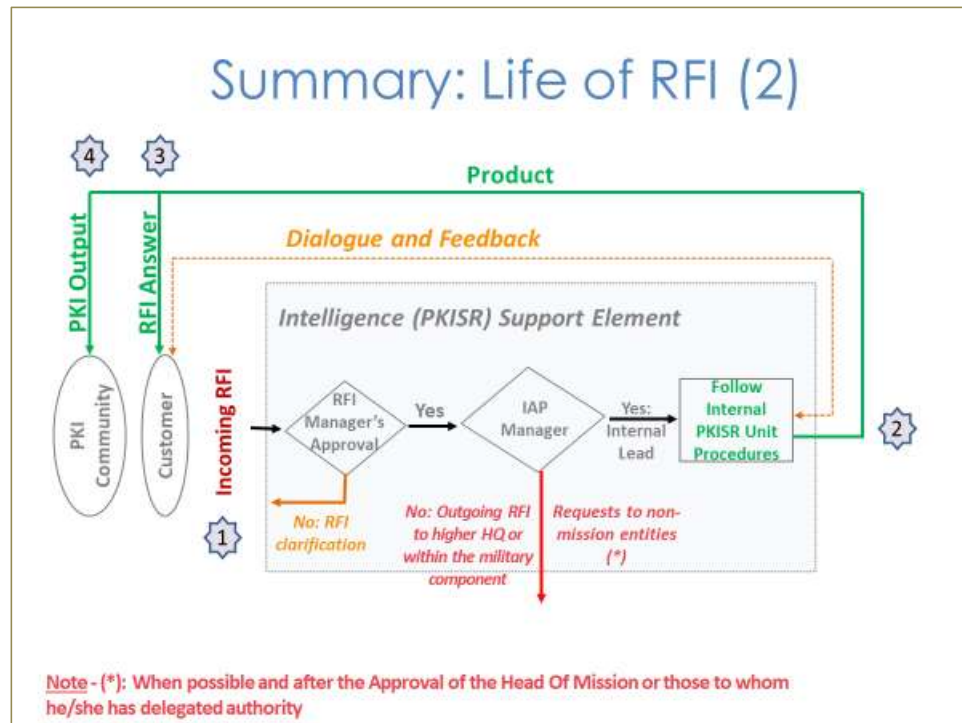


**Note to Instructor:** In many cases, depending on a mission's mandate, tempo of activity and level of resources, the RFI and IAP Manager, ISR Plans and ISR Operations may be the same person. You should use the diagram to talk through the life of an RFI. Inform students that the figure is available on the PKISR Handbook, page 18.

This diagram explains the life cycle of the RFI and reflects what we have already discussed. Starting at the top left of the slide, you can see that once the RFI has been received by the RFI Manager, the first step is to check if the answer already exists in the database. If not, the RFI is then passed to the IAP manager as an information requirement (IR). The IAP Manager then develops a prioritised list of IRs and passes it to the ISR Plans.

After developing 24hr/48hr/72hr Information Acquisition List (IALs) for execution, the ISR Plans passes daily, the 24-hour IAL to the PKISR Ops and tasks this list to the ISR acquisition units. The units will acquire the information, as tasked, and report back to the PKISR Ops the success against the IAL. PKISR Ops will then report the acquisition results to the RFI Manager who contacts the customer having originated the RFI and marks the RFI as complete if the acquisition is successful.

## Slide 11



Key message: This slide outlines the life of an RFI in a slightly different format, highlighting some of the decisions / responsibilities of the RFI and IAP Managers during the process. This process is fundamentally the same for any MPKI organization.

In the case of a PKISR unit, the RFI Manager reviews and approves all RFIs at first. To this end, the RFI Manager will coordinate with the customer to clarify the RFI has been filled out effectively, get the customer to amend it, if necessary, explaining their decision to approve/disapprove the RFI, and keep the customer informed about the RFIs status throughout the entire process.

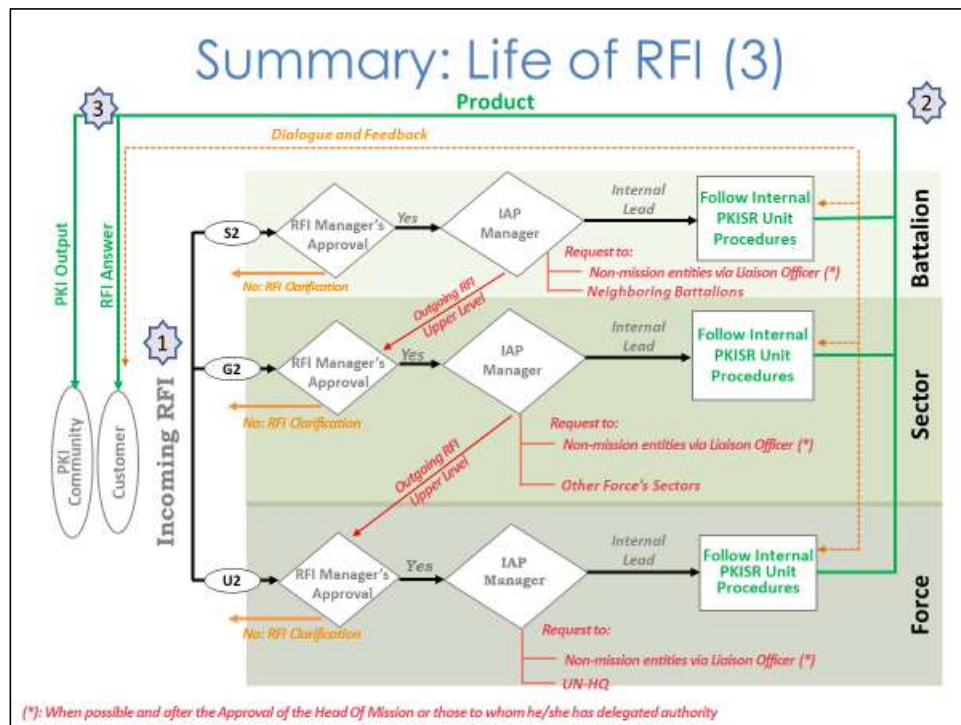
If approved, the IAP Manager determines whether the PKISR unit has the capability to answer the RFI. If yes, the RFI is assigned to the PKISR unit, as explained in the previous slide. If no, the RFI will be submitted to the next appropriate external peacekeeping-intelligence structure for consideration, either to another military organisational or to non-mission entities when possible and authorized.

When the answer to the RFI is obtained, the RFI Manager provides it to the customer as an answer to his question. The RFI Manager will also share the final answer with the peacekeeping-intelligence community of the Mission, as a peacekeeping-intelligence output.



**Note to Instructor:** Consider printing the next 2 slides for students before the lesson. Explain that the numbers on the slide help to guide the students around the process.

## Slide 12



So, within the Mission, the RFIs' process will be the same at the three organizational levels: battalion, sector and Force HQs.

## Slide 13

**Writing RFI (1)**

RFI Form		
1 Priority	<input type="checkbox"/> Immediate <input type="checkbox"/> Routine	2 Security Classification <input type="checkbox"/> Strictly Confidential <input type="checkbox"/> UN Confidential <input type="checkbox"/> Unclassified
4 Reference Number		3 DTG of Request
5 Type of situation	<input type="checkbox"/> Life threatening <input type="checkbox"/> Mission critical <input type="checkbox"/> Mission essential <input type="checkbox"/> Mission desirable	6 Subject
8 Request	7 U2 Reference	
9 When required	<input type="checkbox"/> No later than: Date <input type="text"/> Time <input type="text"/>	
10 Format	<input type="checkbox"/> Verbal <input type="checkbox"/> Written <input type="checkbox"/> Graphic	
11 Dissemination information	Contact details, email, radio call sign, telephone	
12 Location	Region <input type="text"/> Name of village/area <input type="text"/> Grid reference <input type="text"/>	
13 Point of contact	<input type="text"/>	
14 Remarks	Safety and security issues? <input type="text"/> 15 Intent to share? With whom? <input type="text"/>	

Key message: You must be fully aware of the type of information that is needed to fill out the RFI form. This will allow you to provide advice to other mission entities that wish to submit RFIs and ensure you are able to scrutinize incoming RFIs, all of which are crucial in responding to a peacekeeping-intelligence requirement.

The RFI form is required to be filled in with extreme precision. An incomplete RFI will be returned to the customer. The lack of precision can cause one of the following outcomes:

- it takes longer to answer the RFI.
- the requirement is misunderstood, resulting in an incomplete or irrelevant answer.

So, let us talk through the RFI form, box by box, to see what is expected from the originator of an RFI:

- Item 1: The priority given to the RFI by the customer: it could be either 'Immediate', or 'Routine' based on how urgent the request is.
- Item 2: Indicate the desired security classification based on UN policy for security classification (strictly confidential, UN confidential or unclassified) based on ST/SGB/2007/6.
- Item 3: Reports the date-time-group when the request is made.
- Item 4: Provides a reference number to facilitate the dissemination of the answer. This would be filled out by the RFI Manager.
- Item 5: Indicates a clear statement of the subject of the RFI.

- Item 6: Describes the type of the situation for which the RFI is needed to be answered (life threatening, mission critical, mission essential or mission desirable) – items 5 and 8 should reflect the situation.
- Item 7: Any U2 reference that has been used in relation to this tasking if one exists.
- Item 8: Gives the clear statement outlining the nature of the requirement – this statement must align with information contained under 'priority', 'classification' and 'type of situation'.
- Item 9: Specifies the date and time by which the information is required. In other words, the latest date-time-group after which the information will be of little value, in other words, some RFIs will be time sensitive.
- Item 10: The format in which the customer wants the RFI to be produced and disseminated.
- Item 11: The contact details of the person designated to receive the response to the RFI. This is particularly important when the RFI is time sensitive.
- Item 12: Provide the details of the affected area/location.
- Item 13: Identify by name and contact details who is the originator or responsible for handling the RFI (the point of contact for the request).
- Item 14: Any remarks that will assist in clarifying the request or any safety and security issues.
- Item 15: The persons or entities with whom the customer intends to share the response to the RFI. This relates to the 'need to know' principle.

Note: Items 1 and 6 will help to prioritise the request.



## Slide 14

**Writing RFI (2)**  
**Example of a correct filling**

RFI Form	
1 Priority	Immediate <input checked="" type="checkbox"/> Routine <input type="checkbox"/>
2 Reference Number	23
3 Security Classification	Strictly Confidential <input checked="" type="checkbox"/> UN Confidential <input type="checkbox"/> Unclassified <input type="checkbox"/>
4 DTG of Request	180920Z May 21
5 Subject	Main threat to the population security in our AOR
6 Type of situation	Life threatening <input checked="" type="checkbox"/> Mission critical <input type="checkbox"/> Mission essential <input type="checkbox"/> Mission desirable <input type="checkbox"/>
7 U2 Reference	455
8 Request	Identify personnel carrying weapons. Identify hot or cold spots on the ground. Identify enemy force presence.
9 When required	No later than: Date: 19 May 2021 Time: 0830Z
10 Format	Verbal <input checked="" type="checkbox"/> Written <input type="checkbox"/> Graphic <input type="checkbox"/>
11 Dissemination Information	Contact details, email, radio call sign, telephone Maj Xxx Yyy - xxx_yyy@un.org - Radio Call Sign: Bravo 21. - Phone: +1813 425 3802
12 Location	Region: Bangley Village Name of village/area: Down Town Grid reference: 15km Radius around N36°39'03" – W115°39'53"
13 Point of contact	Email: xxx_yyy@un.org Phone: +1813 425 3802
14 Remarks	Safety and security issues? Risk of Manpads
15 Intent to share?	With whom? U2 – G2 – S2 – JOC

Key message: Filling in the RFI form correctly in the first instance saves critical time, especially when the request is time critical.



**Note to Instructor:** It is highly recommended that you talk through each item on the form to emphasize the type of information required. Allow the students to question the content so that they are confident with the requirement.

Now, let us complete a learning activity to see whether you are content with the RFI format and detailed requirements.

## Learning Activity - RFI

- Time 10 minutes
- Consider the following RFI request
- Confirm whether the form has been filled out correctly
- Be prepared to discuss any concerns you have and how you would rectify any errors



**Note to Instructor:** Students should now be confident in the completion and scrutinization of the RFI form. Use this activity to confirm understanding.



**Interactive.** Split the participants into small groups. Hand out a copy of the completed RFI (next slide) to each student (without the corrections on it). Give the groups 10 minutes to consider the completed RFI and to identify any issues regarding its content. Participants should be prepared to discuss their thoughts in open forum.

Use the next slide to confirm some of the discrepancies in the RFI, noting it should be returned to the originator for amendment. Note that the PKISR should assist this process, especially if the originator is not familiar with the RFI process and is requesting information at speed.

## Slide 16

### Learning Activity

RFI Form			
1 Priority	Immediate Routine	2 Security Classification	Strictly Confidential Confidential Unclassified
2 Reference Number	23	3 DTG of Request	180930Z May 21
5 Type of situation	Life threatening Mission critical Mission essential Mission desirable	4 Subject	Main threat to the population security in our AOR
6 Request	Confirm/deny enemy activities. Identify patterns of life area. Identify defensive fighting positions.	5 U2 Reference	455
9 When required	No later than	Date	19 May 2021
10 Format	Verbal Written Graphic	Time	0830Z
11 Dissemination Information	Contact details, email, radio call sign, telephone	Maj Xxx Yyy - xxx_yyy@un.org - Radio Call Sign: Bravo 21. - Phone: +1813 425 3802	
12 Location	Region	Bangley Village	
	Name of village/area	Down Town	
	Grid reference	15km Radius around N36°39'03" – W115°39'53"	
13 Point of contact	xxx_yyy@un.org	Phone number missing	
14 Remarks	Safety and security issues?	Risk of Manpads Rebels	
15 Intend to share?	With whom?	U2 – G2 – S2 – JOC	

**Non compatible** (points to Priority and Type of situation)

**Lack of precision** (points to Request)

**Does it make sense to request a written answer when the situation is time sensitive?** (points to Format)



**Interactive.** You should allow the students time to provide feedback on their findings and any subsequent discussions. Once complete, build the slide to highlight some of the errors, many of which will have been identified by the students.



**Note to Instructor:** Build the slide as described above. You will see that:

- Item 1 (Priority) and Item 6 (Type of situation) are not compatible. A life-threatening situation is likely to be aligned to an immediate priority.
- Item 8 does not contain the necessary precision. This could cause the answer to take longer if PKISR asks the originator / customer for more information or could affect the accuracy of the answer.
- It is likely that item 10 would request a verbal response since the requirement is time sensitive – a written product is likely to take longer to prepare.
- Considering the situation, it would be more helpful if the phone number (Item 15) of the point of contact was included in the request.

## Take Away

- RFIs are 1 of the 3 core sources of tasking PKISR assets.
- There are 2 sources of RFIs:
  - one requested by a non-military Mission entity;
  - one requested within the MPKI architecture.
- RFI can be initiated by anyone within the UN mission (civilian and military)
- The management of RFIs requires an effective and informed process.
- Precision in filling an RFI form is crucial in receiving timely the right answer.
- *"Acquire once, Use many"* relies on an effective database.

## Summary

Students should now feel confident to explain the RFI management process and to write, manage and scrutinize an RFI.

# Lesson 3.5



## Requirements Management and Prioritisation

### The Lesson



#### Starting the Lesson

Welcome to the lesson on Requirements Management and Prioritisation of the PKISR.

## Slide 1



### Lesson 3.5 PKISR Requirements Management and Prioritisation



**Note to Instructor:** Set the scene by sharing some of the challenges that the U2 would face when managing and prioritising PKISR requirements:

- The commander and their staff will rarely seek a dialogue with the peacekeeping-intelligence staff, which seeks to determine what the commander's information and peacekeeping-intelligence requirements are; what the commander and their staff need and want to know. Therefore, it is up to U2/S2 to ensure that the meeting with leadership is scheduled to ensure the PKISR process is command led.
- The commander will rarely frame requirements as Priority peacekeeping-intelligence Requirements (PIRs). Rather, they will outline their concerns and operational priorities. It is the responsibility of the U2/S2 to draw PIRs from what is discussed in the meeting.
- MPKI cells and units have limited acquisition assets, and limited time to acquire information. Therefore, IRs must be prioritised. For instance, IRs relating to POC and UN Force Protection will always be in the top two PIRs. They will always be mission-critical, which means that a mission will fail unless the mission has access to information and peacekeeping-intelligence about them.

## Slide 2

### Content

- PKISR requirements management process
- Key components of the requirements management process
- Prioritisation of PIRs
- Translating PIRs into SIRs into EEIs
- Indicators and warnings (I&W)

Here is the lesson content. This presentation extends from requirements management process to indicators and warnings (I&W). In addition, there will be a couple of learning activities for interaction with students.



**Note to Instructor:** Steer students to the following references.

1. PKI policy (2019)
2. MPKI Handbook (2019)
3. PKISR Staff Handbook (2020)
4. UN MIO RTP (2020)

### Slide 3

## Learning Outcomes

- Explain the PKISR requirements management and prioritisation process
- Describe the key components of the requirements management process
- Demonstrate translating PIRs into SIRs into EEIs
- Describe indicators and warnings (I&W)

By the end of this lesson, students will be able to explain the requirements management process and principles for prioritisation and describe the key components of the requirements management process. Students will also be able to create Priority Peacekeeping-intelligence Requirements (PIRs) and understand how to break these PIRs down into sets of smaller questions, which can be used to acquire detailed information. Furthermore, students are expected to understand Indicators and Warnings (I&W).



## Slide 4

### Key Terms

- Peacekeeping-Intelligence Dialogue (ID)
- Priority Peacekeeping Intelligence Requirements (PIR)
- Specific Peacekeeping Intelligence Requirements (SIR)
- Essential Elements of Information (EEI)
- Named Area of Interest (NAI)
- Indicators & Warnings (I&W)



**Interactive.** Use this slide as revision from Lesson 1.2. Ask students to explain what they think each term means. Only spend a few minutes going through the different terms. Notes below provide the instructor with a brief explanation.

Key terms prevalent in the lesson:

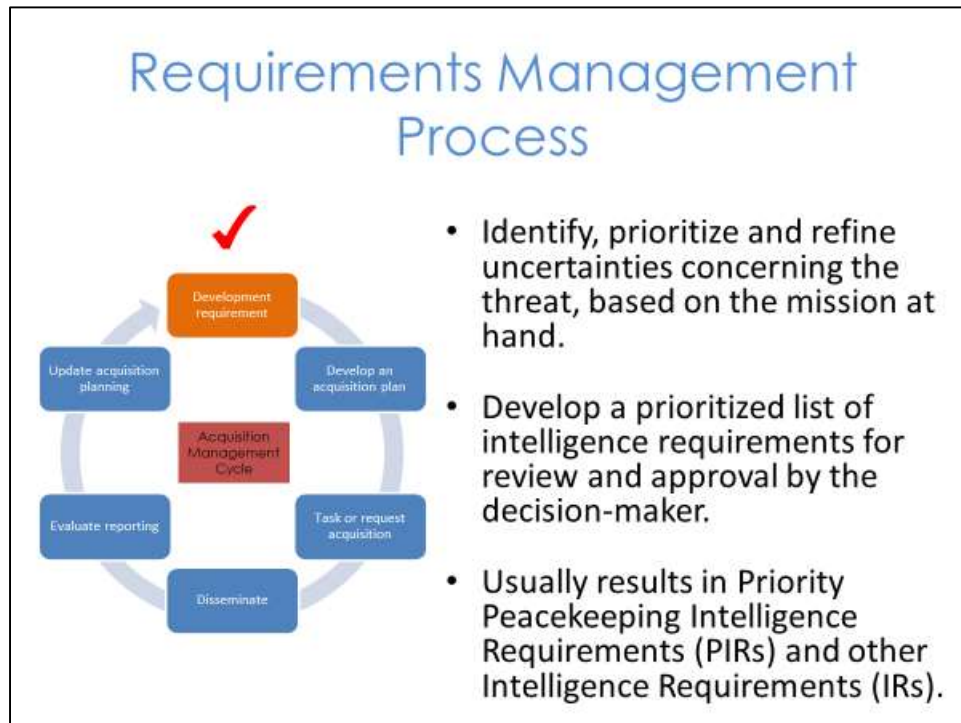
- **The peacekeeping-intelligence dialogue** is a continuous dialogue between the U2 and the Force leadership group (the commander and their staff), which seeks to determine what the commander's information and peacekeeping-intelligence requirements are and what the commander and their staff need and want to know.
- **Priority Peacekeeping-intelligence Requirements** (PIRs) are those requirements raised by a commander to support their decision making.
- **Specific Peacekeeping-intelligence Requirements** (SIRs) come from breaking down PIR's into sub-questions, which can provide partial answers to the PIRs.

Often the SIR is a broad question for acquisition assets and will need to be further broken down into several sub-questions called Essential Elements of Information (EEIs), which can be responded to.

**Named Area of Interest (NAI)** are geographical areas or points where the required information is expected to be observed or acquired. For example, if the commander is interested in locating smuggling locations, then border crossing points could be NAIs.

An **'indicator and warning'** refers to observable behavior or an event that points towards a particular outcome, or that confirms or denies a relevant actor's course of action. We will go into each term in more detail later in the lesson.

## Slide 5



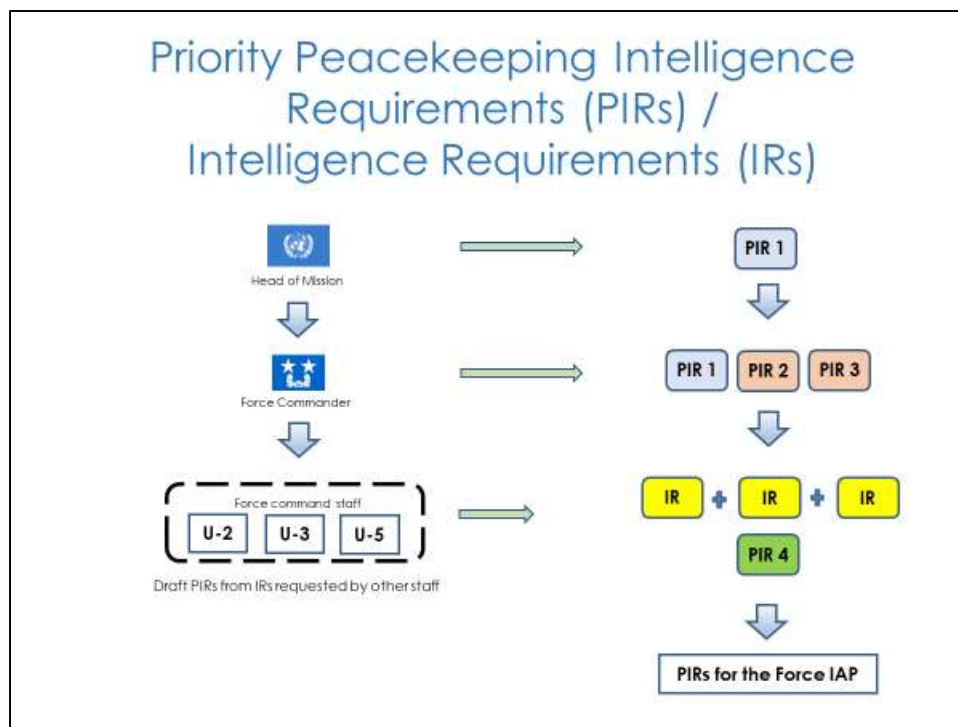
Key message: The requirements management of PKISR is a complex process. It requires good judgement to make decisions on priorities and a clear understanding of a mission's mandate and activities.

- Define the peacekeeping-intelligence requirements (IRs) (in other words, what does the commander want to know); it is essential that the U2 should identify, prioritise and refine uncertainties that should be answered concerning the threat, based on the mission at hand. Upon receipt of the mission, uncertainties are confirmed and broken down into information requirements. The U2 then searches its databases to find out what is already known and whether these requirements can be immediately responded to.
- Prioritise those requirements (in other words, which are most important to the commander's mission and mandate); the U2 will be able to develop a prioritised list of information requirements for review and approval by the decision-maker; this process results in Priority Peacekeeping-intelligence Requirements (PIRs) and other peacekeeping-intelligence Requirements (IRs).
- Break broad PIRs into smaller SIRs and, when necessary, into Essential Elements of Information (EEIs), on which sensors can reasonably be expected to report.



**Interactive.** Ask the students what they would do if their HQ did not own the assets required to acquire the information. They would need to send an external request in the form of an RFI to a neighbouring unit and/or higher HQ.

## Slide 6



Key message: It is the responsibility of the U2 to draft PIRs from what is discussed in the meeting with the commander.

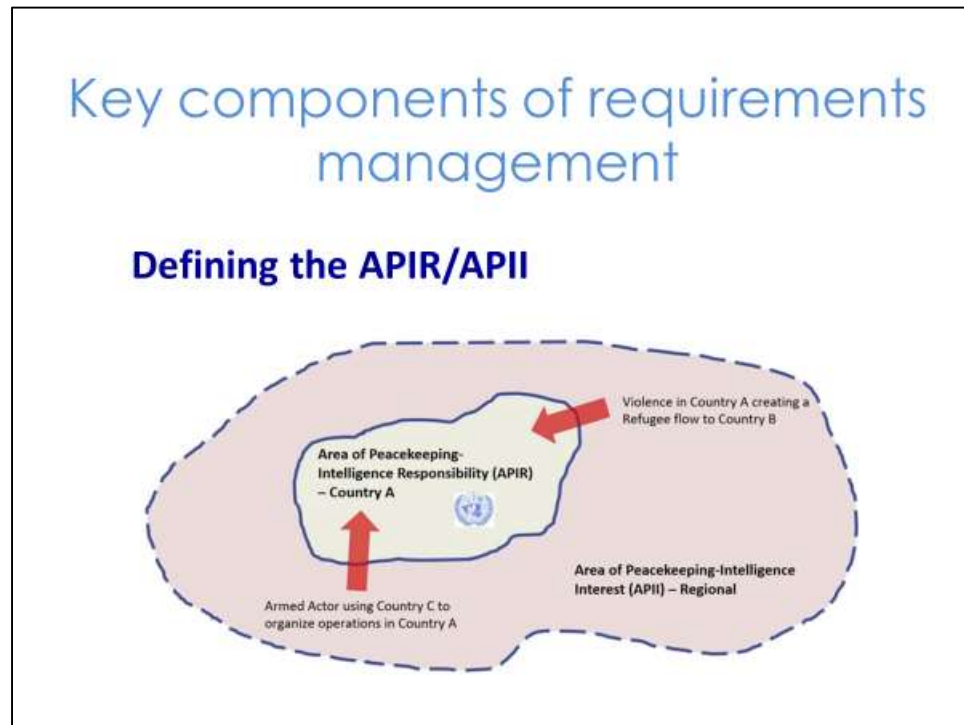
The U2 is responsible for drafting the Force Priority Peacekeeping-intelligence Requirements (PIRs) on behalf of the Force Commander based on their direction, the mission's mandate, military concept of operations and other less formal peacekeeping-intelligence-oriented meetings. In addition, the U2 may receive PIRs from the mission leadership (Head of Mission or Mission Chief of Staff) that require MPKI support. These PIRs are likely to be communicated via Mission leadership meetings, the Mission Peacekeeping-intelligence Coordination Mechanism (MICM) or the Mission IAP. Such PIRs will be incorporated into the Force's IAP.

In addition, the U2 prioritises peacekeeping-intelligence requirements requested by other Force HQ staff functional areas. All PIR/IRs will be prioritised and approved through the peacekeeping-intelligence dialogue with the Force Commander.



**Note to Instructor:** *Remind students that there can be more than one IAP in the mission area, e.g., at Mission HQ level as well as Force HQ level. Sometimes, Mission level PIRs may be included in the Force's IAP due to the PKISR assets under control of MPKI.*

## Slide 7

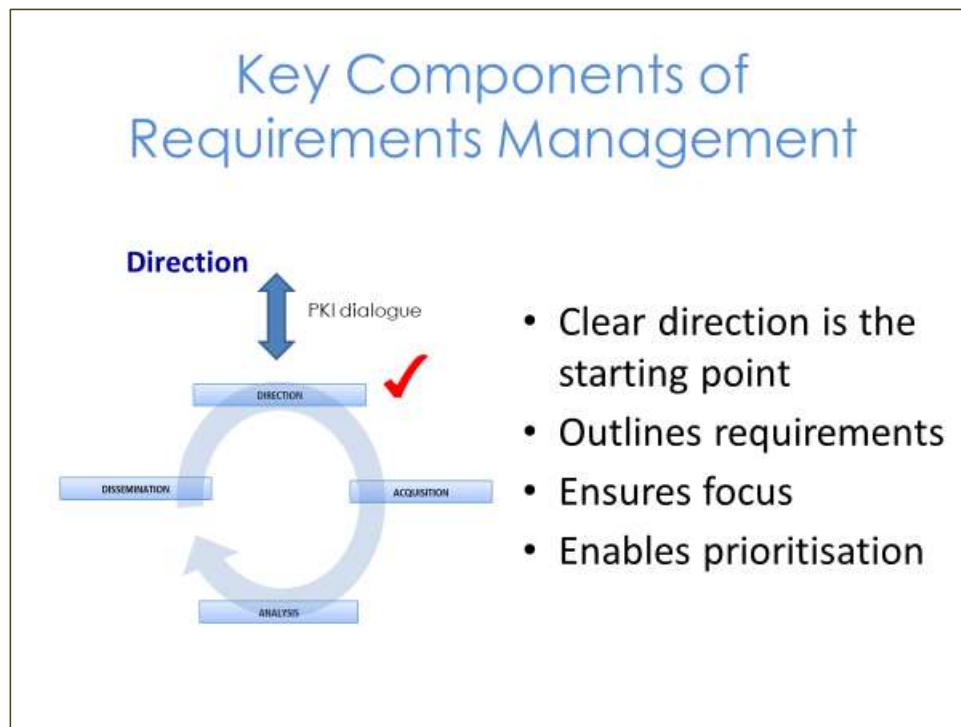


Key message: To deconflict and understand the focus areas for information acquisition, there is a requirement to identify and stipulate the military unit's area of Peacekeeping-intelligence Responsibility (APIR).

The APIR is the geographical domain where commanders are responsible for the acquisition of information and production of PKI using their own resources. There may be a larger area outside of this APIR where a commander wants to understand what is happening now / in the future but is not responsible for 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 own APIR.

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 mandate implementation, even if this would be outside their APIR. This larger area is called an Area of Peacekeeping-intelligence Interest (APII). The U2 could ask for information about its APII. If the APII is a Mission Operating Area, then the U2 should send an RFI to a neighbouring unit to satisfy peacekeeping-intelligence requirements. If the APII is in a neighbouring country, then the U2 will often have to rely on open sources to acquire information.

## Slide 8

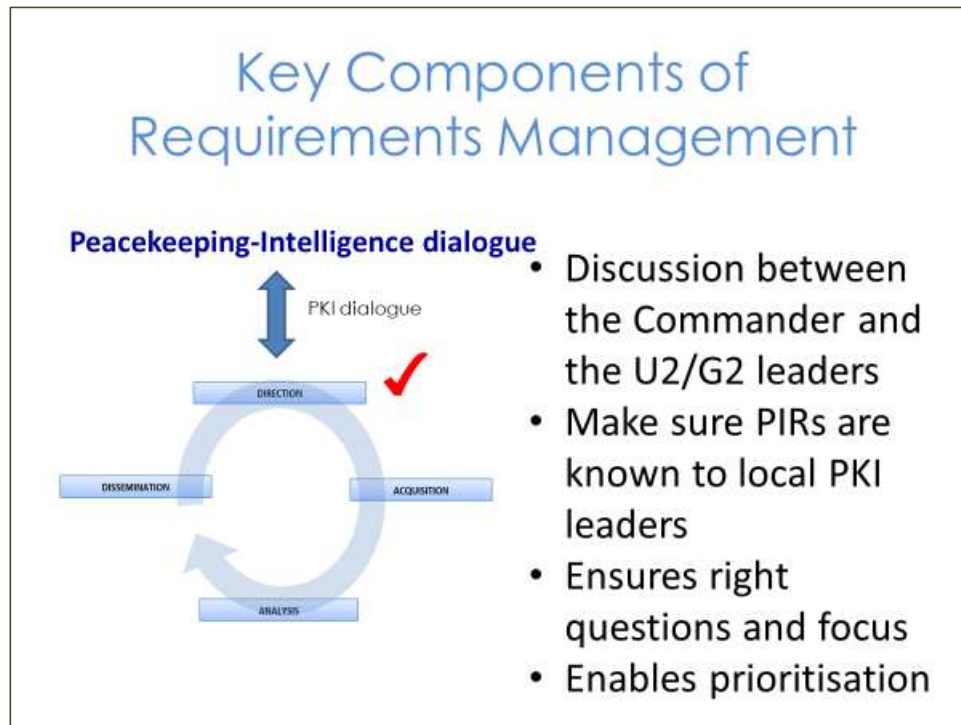


Key message: Clear direction from the commander, at all levels, is the start point of requirements management. The direction outlines to the U2/G2 what the commander wants/needs to know and ensures that the U2/G2 has a clear focus for their efforts. It is also important to understand that MPKI assets are usually limited, and therefore direction should ideally include prioritisation.

The direction is heavily reliant on the input from the commander who is being supported in order to ensure that the entire MPKI efforts are focused on underpinning the overall mission. If clear direction is not given, the U2 must ask for it. In some instances, the U2 might have to educate commanders and users regarding this input, to the point where the MPKI function might deliver proposed direction and guidance for approval from the commander in question. The direction and guidance received from the commander (and the staff) are vital in focusing MPKI efforts on the important issues, thus utilizing the often-limited resources in the best possible manner.

The U2 must not wait on the commander and their staff to give a set of Priority Peacekeeping-intelligence Requirements (PIRs) to work with. Rather, the U2 must often propose the PIRs for the FC's approval. There are several sources of direction, for example the mandate and military concept of operations, which the U2 must use in order to deepen its understanding of what the commander and their staff need to know. The U2 should study the commander's intent so it is aware of the commander's operational priorities. In this case, the U2 works to decide what information and peacekeeping-intelligence the commander needs to ensure their intent is achieved.

## Slide 9



Key message: There must be a peacekeeping-intelligence dialogue with the Commander. The U2 should engage the commander and his or her staff in the peacekeeping-intelligence dialogue to discuss their specific peacekeeping-intelligence requirements. This discussion should take place between the local peacekeeping-intelligence staff and the commanders or users of the PKI products.

The PKI dialogue, often as part of the decision-making process, ensures that the right questions are asked, that PIRs are prioritised, thereby ensuring that the subsequent information acquisition and production effort is prioritised and focused. Plus, the decision-makers (from HoM/FC to company commanders) should make PIRs known to their local PKI staff to ensure that peacekeeping-intelligence requirements relate to their specific mission and mandate and cover all relevant thematic tasks.



## Slide 10

### Peacekeeping-Intelligence Dialogue

- Commander, U2/G2/S2 representative and any other necessary staff
- Why is it important?
  - To fully understand the Commander's intent
  - To understand how your cell can be most useful
  - To generate 'buy-in' to the intelligence process
  - To manage expectations
- Types of questions that could be asked:
  - What geographical areas do you require acquisition coverage?
  - What do you want or need to know?
  - What are your intelligence priorities?
  - When, where, and how do you need the reporting?

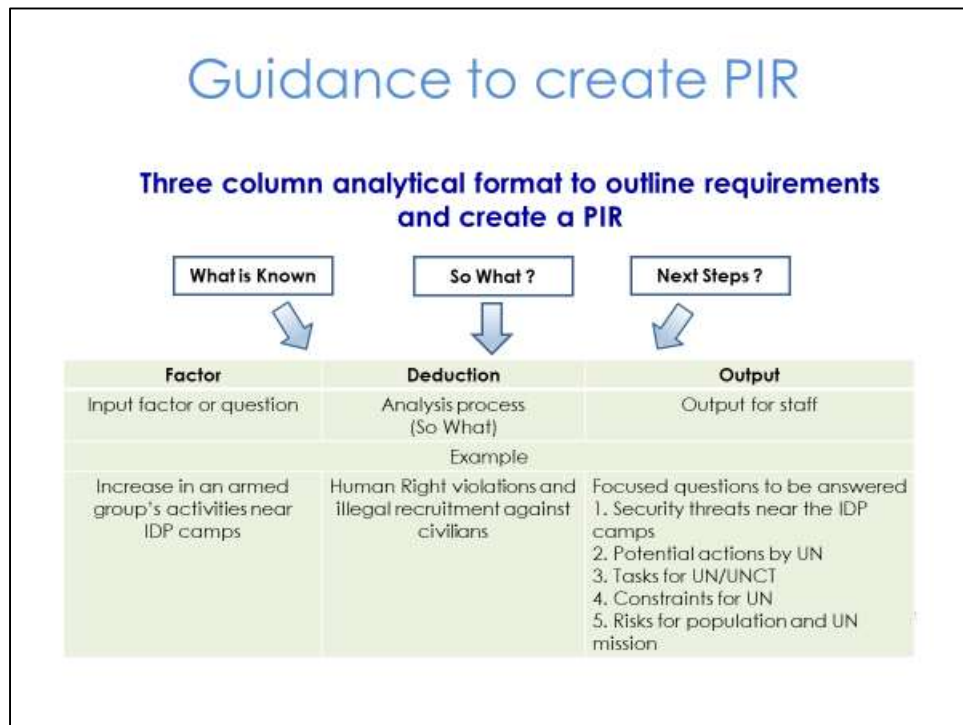
Key message: peacekeeping-intelligence dialogue is vital for the direction of peacekeeping-intelligence requirements.

The U2 must meet their commander when they are fully prepared. It is necessary to have the peacekeeping-intelligence dialogue after the U2 has drawn up a coherent and complete set of draft Priority Peacekeeping-intelligence Requirements (PIRs) and add to them or subtly change them based on the commander's guidance. This means that the U2 uses all tools available to it to ascertain PIRs before the dialogue takes place.



**Interactive.** Ask students what they should study to ascertain direction? Responses should include: operating environment; commander's intent; mission and mandate; and specified and implied tasks. It is also important during the dialogue to manage the commander's expectations of peacekeeping-intelligence. Outline any limitations the entire MPKI cell has. For example, is it fully staffed with qualified personnel? The U2 can also speak about the shortcomings of some PKISR assets, such as UAS. Often commanders believe that UAS are the answer to everything. This is clearly not the case. A UAS' capability is based on its range and sensors. A UAS cannot ascertain, for example, the exact location where an IED is buried but could provide indicators, such as disturbed ground. The kinds of questions the U2 should ask the commander during the dialogue are suggested on the slide.

## Slide 11



Key message: Factors like 'What is Known' can be worked through as part of the UN military planning process, specifically mission analysis.

One way of identifying information gaps is by using a three-column analytical format methodology, which will subsequently create several deductions from each factor. These deductions should uncover peacekeeping-intelligence requirements.



**Interactive.** Ask students about how to create a PIR. The final step to identifying a Priority Peacekeeping-intelligence Requirements (PIRs) is grouping these requirements thematically in consideration of the UN mission, especially risks to the civilian population. For example, if there are several peacekeeping-intelligence requirements relating to various threats to the population, it would be logical to deduce that at least one PIR should be linked to the protection of civilians. A suitable PIR, in that case, would be 'What are the threats to the civilian population?'.

## Prioritisation of PIRs/IRs

- Important to make the acquisition effort more efficient and focused
- A PIR/IR may be prioritised as:
  - Mission Critical (MC). A PIR critical to success of mission; will not succeed unless PIR is answered
  - Mission Essential (ME). A PIR deemed essential to assist in mission success
  - Mission Desirable (MD). A PIR / IR is important to know but not essential to the success of the mission

Key message: MPKI cells and units will have limited acquisition assets, and limited time during which to acquire information. Therefore, PIRs and IRs must be prioritised.

- Prioritisation is the ordering of Priority Peacekeeping-intelligence Requirements (PIRs) /Intelligence Requirements (IRs). One way of doing this is by determining whether they are mission-critical, essential, or desirable.
- Students should be aware that peacekeeping-intelligence requirements relating to the protection of civilians and the protection of UN personnel will always be in the top two PIRs / IRs. They will always be mission-critical, which means that the mission will fail unless we have access to information and peacekeeping-intelligence about them.



**Interactive.** Which priorities should the MPKI cell focus most effort on? The response is MC, followed by ME, followed by MD. Who prioritises these PIRs? The response is that the commander should, but if they do not react, then the MPKI cell should work jointly with the operations cell to do this.



**Note to Instructor:** The MPKI and PKISR handbooks do not identify a process to prioritise peacekeeping-intelligence requirements. This slide highlights one possible method to do this. Inform students that this may not be the case in all situations, and certain UN peacekeeping missions may have their own methodology. The students should be prepared to adapt to the specific mission SOPs.

## Prioritisation of PIRs/IRs

- EEIs can be time sensitive, and often include a 'Not Later Than' (NLT) or 'Latest Time Information of Value' (LTIOV) label
- A review process that assesses the degree of fulfillment of the requirement
- Establish NAIs to deconflict sensors and EEIs.

Key message: EEIs can be time-sensitive, and often include a 'Not Later Than' (NLT) or 'Latest Time Information of Value' (LTIOV) label. Information that does not meet a deadline is useless, leading to a waste of time and resources. LTIOV also helps the PKMI cell to focus its acquisition effort.

There should be a review process that assesses the degree of fulfilment of the requirement. A NAI is a geographical area or point where the required information is expected to be acquired. NAIs should be established to focus acquisition effort and deconflict sensors and EEIs.

## Slide 14

## Prioritised as MC, ME, MD

Status	Priority	PIR	SIR	EELs	Indicators	Collecting unit	NAI	NLT	LTI/IV				
Has it been fulfilled?			What information needs to be acquired??			A SS Y	B SS Y	C SS Y	Re ss #	Unit MP SS	Who will acquire the information ?		

Here is an example Information Acquisition Plan (IAP) with text boxes to explain the categories. Note that mission critical (MC), mission essential (ME) and mission desirable (MD) ratings are put beside the questions – SIRs that the MPKI cell acquire information on.

Points to note regarding the IAP are:

- PIRs should be regularly reviewed to ensure that they are still relevant. If fulfilled, they can be removed from the list.
- The ratings can be put beside an SIR or an EEL. In the first example, an SIR is rated as being mission critical.
- The IAP should include:
  - Who could acquire the information?
  - What information needs to be acquired?
  - Where to acquire it: (normally a named areas of interest - NAIs)?
  - When is the information required (No Later Than/Latest Time peacekeeping-intelligence of Value)?
  - Although not shown on this slide, it should also include:
    - How are sources and sensitive information going to be protected and kept confidential?
    - How should the acquisition unit disseminate the acquired information?



**Interactive.** Ask the students what does mission critical mean. Response - It is important to know, critical to the success of the mission; will not succeed unless PIR is answered. In the second example, an SIR is rated as being mission desirable. Ask the students what does mission desirable mean. Response - It is important to know, but not critical or essential to mission success.

## Learning Activity 1 – Prioritise PIRs

- Time 5 minutes.
- Syndicate work.
- Using the 7 PIRs given to you, decide which are mission critical, essential and desirable.
- Be prepared to justify your responses in your back brief to the instructor.



**Note to Instructor:** Hand out 8 PIRs to the students.

- What challenges are there to the Force's freedom of movement?
- What is the capacity of national partners?
- What are the threats to UN Forces?
- What hazards are in the UN AO?
- What is the capacity of international organizations?
- What are the threats to the civilian population?
- What are the threats to mandate implementation?



**Interactive.** Ensure that the back brief takes place in front of the whole class to encourage debate. Select a few students to brief the class on the PIRs. They should NOT describe all PIRs as MC or ME; instead, have them choose at least one that is MD.

Possible responses are:

- What challenges are there to freedom of movement? (ME)
- What is the capacity of national partners? (MD)
- What are the threats to UN Forces? (MC)
- What hazards are in the UN AO? (MD)
- What is the capacity of international organizations? (MD)
- What are the threats to the civilian population? (MC)

- *What are the threats to mandate implementation? (MC)*



## Translating PIRs into SIRs into EEIs

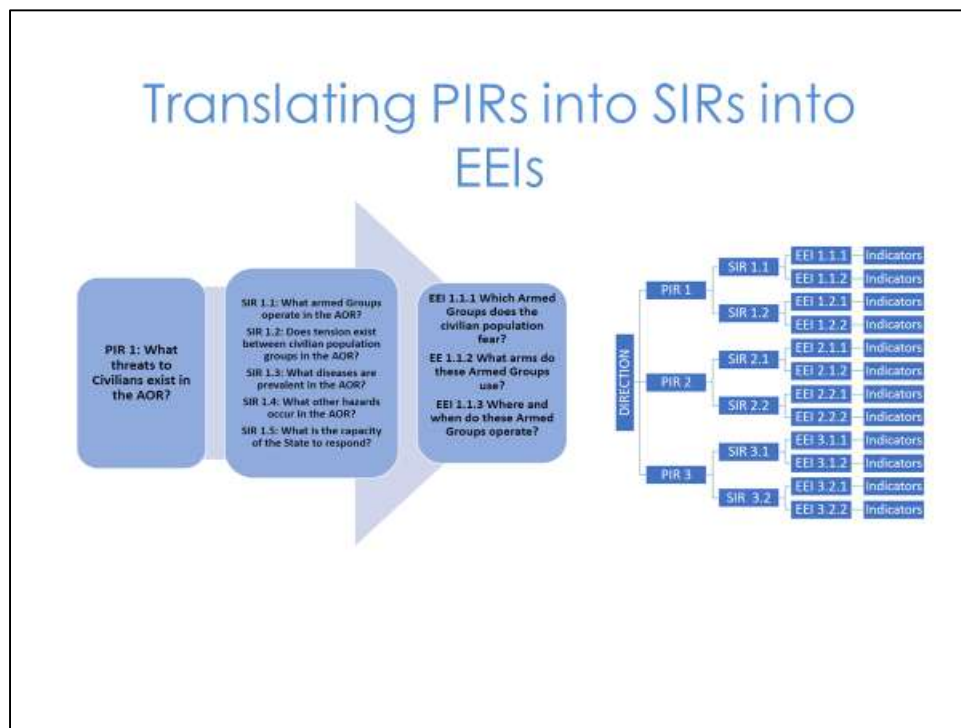
- A PIR is an intelligence requirement
- Intelligence is comprised of multiple sources of information
  - Specific Peacekeeping Intelligence Requirements
  - Essential Elements of Information
- PIRs are too broad
- Often your sensors will NOT understand:
  - What to look for
  - What kind of question to ask
  - What to report

Key message: A significant amount of data is required to produce a valid response to a peacekeeping-intelligence requirement. This data is acquired by gathering responses to numerous Priority Peacekeeping-intelligence Requirements (PIRs) and Essential Elements of Information (EEIs), each of which links back to one PIR.

Typically, PIRs are broad, vague questions, which are not designed for acquisition assets. Rather, a PIR is designed to be broken down into sub-questions. Because PKISR sensors will not understand what to look for, what kind of questions to ask or what to report.

Also, the MPKI cell will decide where these EEIs can be found by location. These are known as named areas of interest (NAIs). Next, the MPKI cell will liaise with the operations section, which should then task acquisition assets to acquire information based on these requirements.

## Slide 17



Key message: Priority Peacekeeping-intelligence Requirements (PIRs) and Essential Elements of Information (EEIs) can relate to specific areas and actors. SIRs/EEIs are always connected to a PIR and posed in specific questions like granular details and specific actor's geographical areas.

Here is an example of how one PIR is broken into several Specific Peacekeeping-intelligence Requirements (SIRs). Each SIR is then broken down to several EEIs. Each SIR relates to the parent PIR, while each EEI relates to an SIR. As you can see, there will be many EEIs for each PIR. Generally, EEIs are what acquisition assets will be tasked to deliver on. For example, 'what armed groups operate in the AOR' is not a good SIR in this context as the MPKI cell needs much more details, such as 'what arms and ammunition do the group have', and other questions relating to its capabilities and intent.

It is important to note that while SIRs will generally be broken down to EEIs, this will not always be the case. For example, 'Have the activities of militant group 'Al-Shabaab' increased in the last month? Then it does not need to be broken down further. Meanwhile, SIRs can be further broken down into more specific questions. These can be termed EEIs or I&W. For example, SIR 1.1 What armed groups operate in the AOR? It can be broken down into EEI 1.1.1, EEI 1.1.2 and EEI 1.1.3.

## Learning Activity 2 – Breaking down PIRs

- Time 10 minutes.
- Syndicate work.
- Using a PIR given to you, break down it into SIRs relating to the relevant actor's intentions and capabilities.
- One method of breaking down PIRs into information requirements (IRs) is to consider the equation:  
$$\text{THREAT} = \text{INTENTION} \times \text{CAPABILITY}$$
- If a PIR relates to a threat, it can be broken down into subordinate IRs relating to the relevant actor's intentions and capabilities.



**Interactive.** One of the typical PIRs in a UN mission will be 'What security threats exist in the UN area of operations?' Now you will learn how to break down the given Priority Peacekeeping-intelligence Requirements (PIRs) into Specific Peacekeeping-intelligence Requirements (SIRs) in terms of the relevant actor's intentions and capabilities.

Consider the equation:  $\text{THREAT} = \text{INTENTION} \times \text{CAPABILITY}$  when breaking down the PIR into information requirements (IRs).

Keep in mind that if a PIR relates to a threat, it can be broken down into subordinate IRs relating to the relevant actor's intentions and capabilities.

## Learning Activity 2 – Breaking down PIRs

### 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?

### 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?
- EEL 2.20.1 How does the group prepare to conduct attacks?
- EEL 2.20.2 What patterns of activity does Group X engage in prior to an attack?



**Note to Instructor:** Talk through the example of the slide using the notes below. It is important for the instructor to be familiar with the slide before briefing against it.

Here is an example of a typical PIR, broken down further into SIRs for a threat group. In the case of PIR 2 'What security threats exist in the UN area of operations?' the PIR can be broken down into 20 SIRs applying the 'threat equation' with two categories of intent and capability. This can be repeated for many threat actors. But this is not an exact science; it is more of a logical exercise where the MPKI personnel break down the overall PIRs into subordinate information requirements (IRs), the answers to which the PIRs to be answered.

If necessary, SIRs can also be further broken down into more specific questions. These can be termed Essential Elements of Information (EELs) or indicators and warnings (I&W). For example, PIR 2 - What security threats exist in the Area of Operations? It can be broken down into SIR 2.20 and into EEL 2.20.1 and EEL 2.20.2.

## Indicators and Warnings (I&W)

- An indicator & warning: An observable behaviour or event that points towards a particular outcome, or that confirms or denies a relevant actor's course of action.
- Generally, MPKI always ensures that indicators are linked to a NAI (Named Area of Interest), where such behaviours and events can be observed.

An indicator & warning is an observable behaviour or event that points towards a particular outcome, or that confirms or denies a relevant actor's course of action. Generally, MPKI always ensures that NAIs are properly set up in the area of peacekeeping-intelligence area of responsibility/ interest (APIR/APII) and indicators are linked to a NAI (Named Area of Interest), where such behaviours and events can be observed with proper PKISR assets. Indicators, once observed, could prompt analysts to a particular warning that a specific event is to take place.

## Types of Indicators and Warnings (I&W)

- Alert/warning indicator
  - Indicators that reflect the intention of a group to initiate hostilities; they relate to preparations for aggression.
- Tactical/combat indicator
  - Indicators that reveal the type of operations a group is about to undertake.
- Identification indicator
  - Indicators and signature equipment that enable the nature of a formation, unit or installation to be determined.
- Gender early indicator
  - Indicators specific to genders can inform requirements for information acquisition.

The slide highlights some examples of how indicators could be broken down into categories, based on historical behavioural patterns in a specific peacekeeping mission.

- **Alert/Warning indicators** reflect the intention of a group to initiate hostilities; typically, they relate to preparations for aggression.
- **Tactical/combat indicators** reveal the type of operations a group is about to undertake.
- **Identification indicators** and signature equipment enable the nature of a formation, unit or installation to be determined.
- **Gender early indicators.** Here we have some examples:
  - Increased incidence of men and women having to pay for additional security.
  - Women notice new actors in their community.
  - Boys and girls are not attending school.
  - Women and children avoid public areas.
  - The placement of a military base/encampment in close proximity to schools, markets, IDP/refugee camps and other civilian centres, particularly those frequented by women and girls.
  - Indicators of women's empowerment.
  - Indicators of restrictive laws for women.
  - Indicators of gender-based violence.



## Slide 22

## How indicators are captured in the IAP

- Transmissions on frequency utilized by armed group X
- Presence of signature equipment
- Local population display fear/no fear for armed group X
- Statements (posters/leaflets) in area from group X

Updated DTG: U2 DIRECTION				Signed by: Date:		LEGEND			
PH	GR	ED	INDICATOR	LEAD	ACQUIRING UNITS	PH	NAO	REMARKS	FORMAT
1. What is the threat to the local population?	1.1 What armed group operates in this area?	1.1.1 What armed group's presence?	INDICATOR on frequency utilized by armed group & Presence of signature equipment.						
	1.2 What is the attitude armed group towards the population?	1.2.1 What an armed group demonstrated intent?	LOCAL population's display behavior fear for armed group & Statements (oral letters) to area threat group &						
WHAT I NEED TO KNOW			OBSERVATION #PHO	TASKING		WHERE TO ACQUIRE		HOW TO REPORT	

### Example of an Information Acquisition plan

You might wonder how indicators are captured in an Information Acquisition Plan (IAP). You learned how a PIR is translated into SIRs into EEIs. Once observed, an indicator warns us to expect a particular outcome related to SIRs and EEIs. For example, under PIR 1 'what are the threats to the local population? ', there will be several indicators related to EEI 1.1.1 and 1.2.1. These are:

- Transmissions on frequency utilized by armed group X.
- Presence of signature equipment.
- Local population display fear/no fear for armed group X.
- Statements (posters/leaflets) in area from group X.

## Take Away

- Define and prioritise the requirements
- Draft PIRs and other information requirements
- Break down PIRs into smaller SIRs into EEIs to be moved into an IAP
- Key components of the requirements management process
  - Defining the APIR/APII
  - Direction and PKI dialogue

## Summary

The instructor should go through the slide which captures the key learning points from the lesson.



# Lesson 3.6



## Analysis and dissemination

### The Lesson



#### Starting the Lesson

Military PKI supports the UN decision-making process. Analysis is the discipline that turns information into Peacekeeping-intelligence and dissemination is the process that ensures that the decision-makers are timely informed about changes in the operating environment and threats to the force or to civilians.

Slide 1



Lesson 3.6  
Analysis and  
Dissemination

## Slide 2

### Lesson Contents

- Analysis and dissemination in the intelligence cycle
- Analysis
  - Concept and definition
  - Process and methodologies
  - PKISR analysis
- Dissemination
  - Principles
  - Formats
  - Challenges
- Conclusion and take away

These are the subject areas we will be covering in this lesson.

### Slide 3

## Learning Outcomes

- Explain the levels of analysis available for PKISR assets
- Describe the dissemination processes and typical products




The PKI process is driven through the four stages of the peacekeeping-intelligence cycle: Direction – Acquisition – Analysis – Dissemination.

Upon completion of this lesson, students will be able to explain the levels of analysis available for PKISR assets and describe the dissemination processes and typical products.


## Slide 4

# Analysis and Dissemination




**Military Peacekeeping-Intelligence Handbook (MPKI HB)**

Chapter 7: Analysis 46  
Chapter 8: Dissemination 66



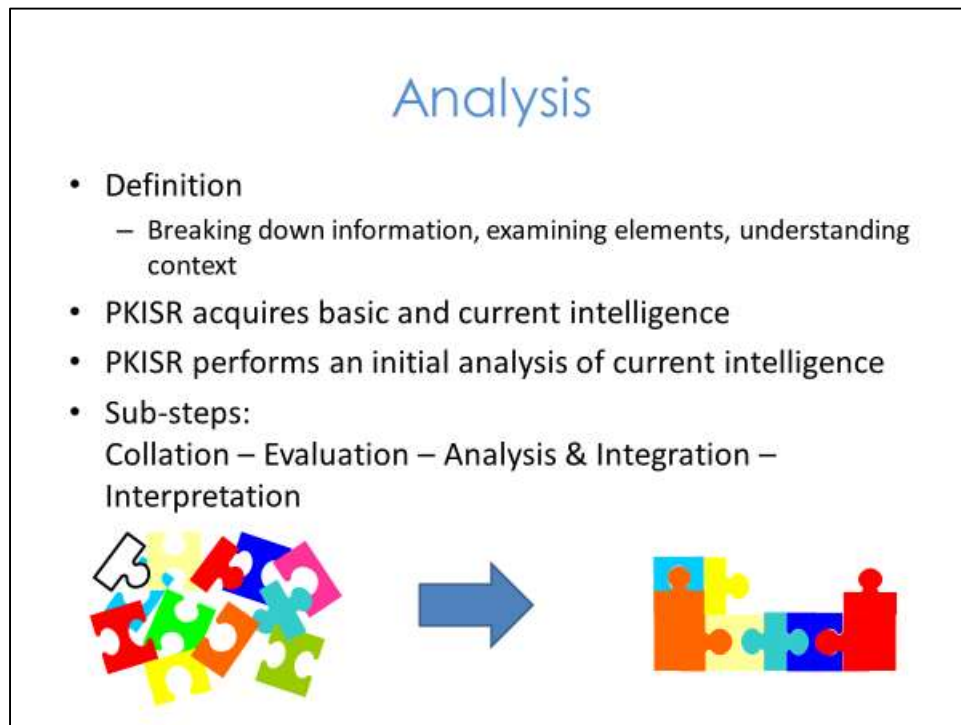
**Peacekeeping-Intelligence, Surveillance, and Reconnaissance Staff Handbook (PKISR HB)**

Chapter 3: PKISR in practice 12  
- 3.7 Phases of analysis 19  
- 3.8 Dissemination 19



The reference documents for this lesson are the Military Peacekeeping-Intelligence Handbook (MPKI HB) and the Peacekeeping-Intelligence, Surveillance, and Reconnaissance Staff Handbook (PKISR HB). Specific page references are listed on the slide should you wish to read more about analysis and dissemination.

## Slide 5



Key message: The analysis phase answers the following questions: So What? Why is the information important? How to identify and register each piece of information? Analysis transforms information to peacekeeping-intelligence.

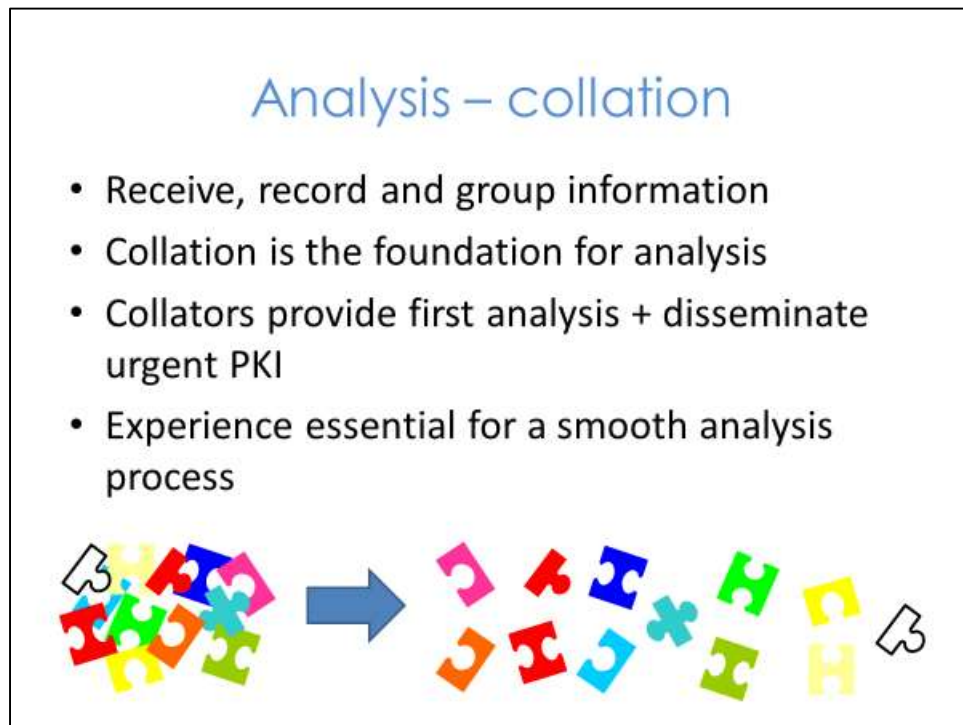
Over the next five slides, I will go through the basic principles of analysis and try to relate them to PKISR and emphasise those that are commonly used.

Analysis is the act of breaking down complex pieces of information to examine and understand the elements thereof to understand the information better. Analysis is also acquiring a series of pieces of information and arranging them into a system to understand a bigger problem set.

Analysis can be broken down into four sub-phases: Collation – Evaluation – Analysis & Integration – Interpretation. In principle, the four phases are conducted in Military PKI as well as in PKISR. But the difference is that Military PKI often analyses a multitude of sources and pieces of information whereas PKISR often only analyses data and information from a single acquisition asset. PKISR must understand the strengths and limitations of PKISR assets in order to critically assess the credibility of the peacekeeping-intelligence. In a larger Military PKI Cycle, multiple sources are used to confirm or deny peacekeeping-intelligence whereby enhancing the overall quality of the end-product.

In the following slides I will go more in depth with the four phases of analysis.

## Slide 6



Key message: Collation is the act of organising and systematising information.

Once data or information is acquired by a PKISR asset, it will be conveyed to the collator(s) of the unit. When the analysts receive data or information this kicks off the first step of analysis: Collation.

Collation consists of:

- The assimilation of a large volume of information.
- Identifying and registering each piece of information without compromising the security of the source.
- Recording the reliability of the source. We will see how to do this in a few minutes.
- Categorising each piece of information in a way to retrieve it with ease in support of future acquisition.

Collators also store information so it can be retrieved at a later point to answer future peacekeeping-intelligence requirements. If this is not done properly, then the information will be lost.

## Slide 7

### Analysis – evaluation

- Every item of information is examined
  - Reliability of source and credibility of information
- Verification (validity, credibility, relevance)
- Comparison (cross-check, coherence, assessing conformity)

Source Reliability	
Rating	Evaluation
A	Reliable
B	Usually reliable
C	Fairly reliable
D	Not usually reliable
E	Unreliable
F	Cannot be judged



Credibility of Information	
Rating	Evaluation
1	Confirmed
2	Probably true
3	Possibly true
4	Doubtfully true
5	Unprobable
6	Cannot be judged

Key message: Evaluation is the thorough examination of each piece of information to determine its credibility.

Evaluation is defined as the step of the analytical process where every piece of information is examined regarding the reliability of its source and the credibility of its content. It is then graded as such using the ratings shown in this slide. For some acquisition disciplines the information is also graded based on the source of information, by grading the reliability of the source. This is primarily done for human sources and it is done by evaluating the motivation of a source and by looking at previous pieces of information provided by that source. Grading credibility often requires more acquisition disciplines – for instance, a picture of a person talking on the phone and a transcript of the phone conversation. If the conversation reveals hostile intent the individual can be identified as a person you want to watch out for in the future.



## Slide 8

### Analysis – Evaluation - example

- Example 1: Source X was told by the police chief that criminals plan to attack a humanitarian convoy tomorrow. Source Y was cleaning the office of the police chief as the conversation took place. One HPKI team talks to source X and another team talks to source Y. The two reports deceptively confirm each other, but in fact the information comes from one source only: the police chief.
- Example 2: IPKI (IMINT) provides a picture of a SAM site. This poses a threat to UN aircraft flying in supplies. To mitigate the risk the flights are cancelled. SPKI (SIGINT) shows no emission from the SAM site over a period of more than a week. After analysis, the intelligence assessment is that it is **LIKELY** that the SAM site is a harmless decoy. The military decision-maker weighs up the risk against the urgency of getting supplies delivered. Do they accept the risk?

As just mentioned, HPKI grades the individual who provided the information and the credibility of the information - the only means to validate the information is by other sources. MPKI strives to confirm information through other acquisition disciplines, for instance SPKI (also referred to as SIGINT in other organisations) or IPKI (IMINT). It is important to understand the source of information and preclude that information that has been derived from the same source.

We will look at 2 examples.

Example 1: Source X was told by the police chief that criminals plan to attack a humanitarian convoy tomorrow. Source Y was cleaning the office of the police chief as the conversation took place. One HPKI team talks to source X and another team talks to source Y. The two reports deceptively confirm each other, but in fact the information comes from one source only: the police chief.



**Interactive.** Does anyone know what it is called when information or peacekeeping-intelligence is repeated and seemingly confirms itself? Answer: Circular reporting – one of the deadly sins! One of the best ways to avoid circular reporting is by always mentioning the (true) source of a piece of information or peacekeeping-intelligence and never analysing just the finished peacekeeping-intelligence product.

As mentioned, Military PKI will strive to validate the credibility of information and peacekeeping-intelligence by using different acquisition disciplines.

Example 2: IPKI provides a picture of a SAM site. This poses a threat to UN aircraft flying in supplies. To mitigate the risk the flights are cancelled. SPKI shows no emission from the SAM site over a period of more than a week.

After analysis, the peacekeeping-intelligence assessment is that it is **LIKELY** that the SAM site is a harmless decoy. The military decision-maker weighs up the risk against the urgency of getting supplies delivered. Do they accept the risk?

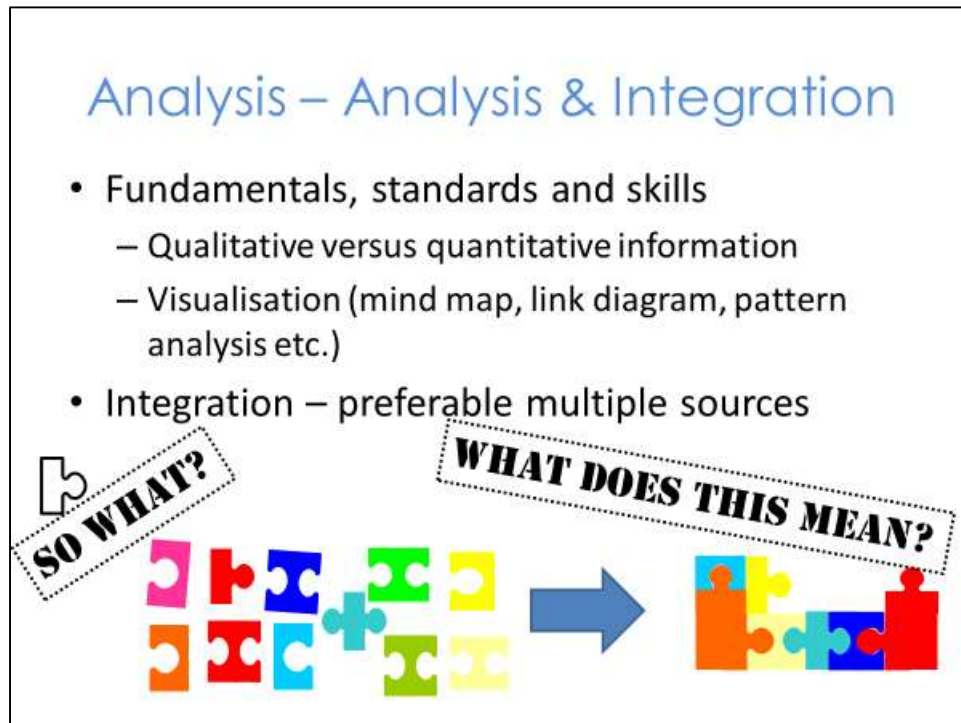


**Interactive.** Ask students, would you accept the risk? Why / why not?



**Note to Instructor:** SAM – Surface-to-Air-Missile. The qualitative statement “**LIKELY**” will be explained in two slides.

## Slide 9



Key message: Analysis follows a deliberate, structured process or processes that integrate information to enhance our understanding of the operational environment. Applying analytical principles ensures that the quality and timeliness of PKI effectively aids the achievement of mission goals.

Analysis and integration is an art in itself. This is done by highly trained individuals often specialised in different fields of expertise depending on the source of information, complexity, nature, etc. Different techniques are used (for example, statistics and graphic visualisation for quantitative information and mind maps and link diagrams for qualitative information). Quantitative information is items, incidents, actions, etc., that can be counted, whereas qualitative information is non-countable information.



**Interactive.** Can anyone give an example of quantitative information? Possible answer: Population counts, number of attacks, number of food rations delivered. If, for example, 67 out of 100 food rations were delivered, this gives a success or delivery rate of 67 %. When measuring this over a longer period of time one can see an upward trend, a neutral trend or a downward trend.

Can anyone give an example of qualitative information? Possible answer: Religion - it is not measurable, but it may determine whether Friday or Sunday is a prayer day/day off. Children are showing up in school may indicate a perception of safety. Parents would keep children at home if there was a threat of them being kidnapped.

Analysis and integration are done to a lesser degree during the PKISR cycle, depending on which discipline we are talking about. At least some shallow analysis is conducted based on experience and common sense. Throughout the process the analyst strived to answer the questions "So what?" and "What does this mean?" to extract all relevance and significance of the information. For PKISR, the purpose is to identify time-sensitive information that could identify a threat that needs to be addressed immediately.

## Analysis – Interpretation

- Interpretation turns information into PKI
- Placing the result in the context of a prediction  
Not simply telling what is happening, but why it is happening and what will happen next
- Communicate uncertainty

Qualitative statement	Associated probability range
Remote or highly unlikely	Less than 10 %
Improbable or unlikely	15-20 %
Realistic Possibility	25-50 %
Probable or likely	55-70 %
Highly probable or highly likely	75-85 %
Almost certain	More than 90 %



Key message: All PKI analytical products are expected to be prepared in a way that supports the UN decision-making process.

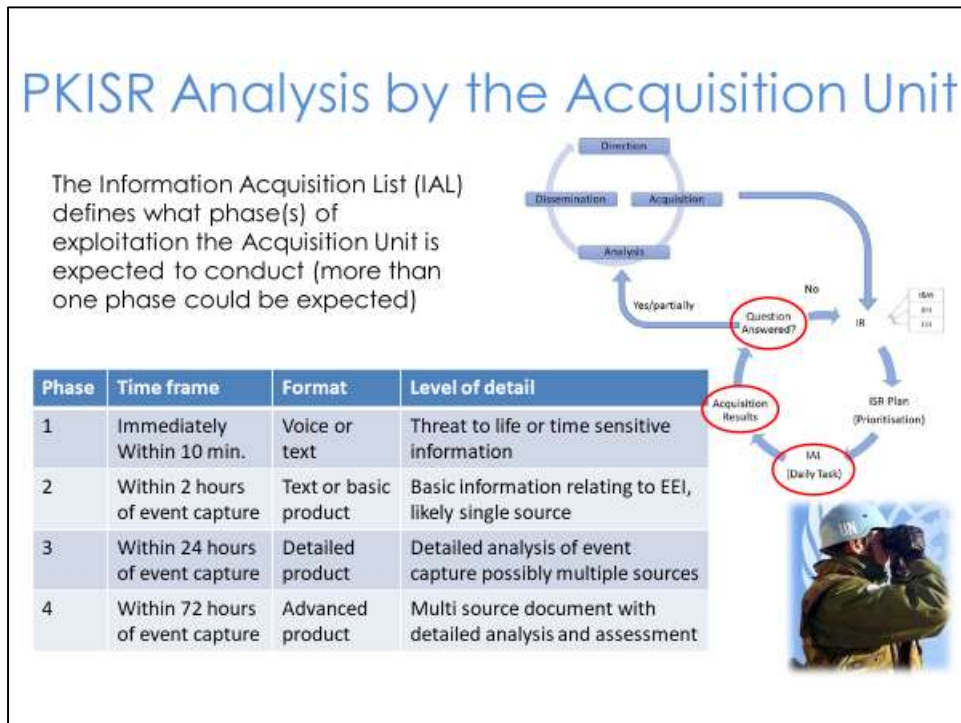
Interpretation is the final step of the analysis. Interpretation places the result of the analysis and integration into the context of a prediction. The significance to the commander must be clear and ideally, predict what is going to happen.



**Interactive.** Remember the SAM site (two slides back)? What was the prediction? (That the site was a decoy and hence would not pose a threat). You may tell the commander what has happened, but only as a lead-in to explaining why it happened and what is **LIKELY** to happen next.

Note the word **LIKELY**. This is an expression of probability – a qualitative statement. peacekeeping-intelligence assessments are always encumbered with uncertainty and this uncertainty must be communicated. The qualitative statements depicted on the slide must be included in all peacekeeping-intelligence products and should stay the same throughout a mission.

## Slide 11



**Key message:** Acquisition units must perform one or more phases of analysis.

As mentioned, the acquisition unit must conduct a 'first-level analysis' of acquired information to determine whether information is urgent or time-sensitive. Urgency is often related to threats to lives, material or installations and some pieces of information (urgent or not) are only relevant within a short time window.



**Interactive.** Can anyone give an example of urgent and/or time-sensitive information?

- **Urgent:** A criminal group plan an attack on a refugee camp (next week).
- **Time-sensitive:** A sandstorm will hit the (refugee) camp within the next 30 minutes.
- **Both:** A Vehicle-Borne Suicide Bomber is headed towards HQ right now.

As you can see on the table on the slide there are four phases of analysis. The Information Acquisition List (IAL) defines what phases of exploitation is expected from each acquisition unit and more than one could be expected. As an example, a unit could be tasked to generate a Phase 2 product to support immediate planning whilst a more detailed product is awaited too (Phase 3). This would require more work and correlation with other products, whereby the quality will be higher and the result might even be different from the Phase 2 product. Even so the Phase 2 product was time-sensitive and

had to be delivered within a two-hour timeframe for it to be included in a planning process.

Phase 1 products are those posing a (possible) threat to life or time-sensitive information. These must be conveyed back to HQ in the fastest way possible.



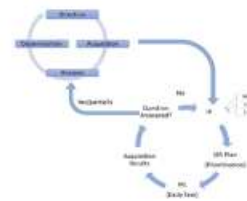
**Note to Instructor:** *inform students that the reporting phases will feature in the final staff exercise.*



## Slide 12

### Dissemination

- Dissemination starts when an IR is answered
- This concludes the PKISR process
- PKI that is not disseminated has no value!
- PKI that cannot be understood has no value!
- Timely – relevant – brief – standardised



Key message: Dissemination is the process of conveying PKI to mission decision makers and other relevant mission personnel.

Dissemination starts as soon as a peacekeeping-intelligence requirement is answered. The purpose of dissemination is to get the answer to the individuals or entities that need to know the answer. The PKI reporting must be presented to “the customer / originator”. If PKI is not disseminated, it has no value! If PKI cannot be understood, it has no value!

Therefore, PKI should be disseminated with certain principles in mind: timeliness, relevance, brevity, interpreted and standardized

- Timeliness because outdated peacekeeping-intelligence has no value.
- Relevance because irrelevant peacekeeping-intelligence has no value.
- Brevity to limit the time and avoid blurring the message.
- Interpreted to ensure all facts are correctly evaluated and interpreted before being disseminated.
- Standardised because this eases comparison and quick identification of relevant parts of the PKI report.

MPKI reporting to commanders and decision makers are generally finalised products in the form of reports or briefings. PKISR reporting may undergo further analysis and provide the single pieces of the jigsaw that makes up the MPKI report.



PKI disseminated outside the time window may be too late to save civilian and UN lives at risk.

## Slide 13

### Dissemination

- Dissemination Formats
  - Verbal
  - Written
  - Graphical
- UN Reporting Formats
  - Peacekeeping-Intelligence Report (INTREP)
  - Peacekeeping-Intelligence Summary (INTSUM)
  - Picture Peacekeeping-Intelligence Summary (PICINTSUM)

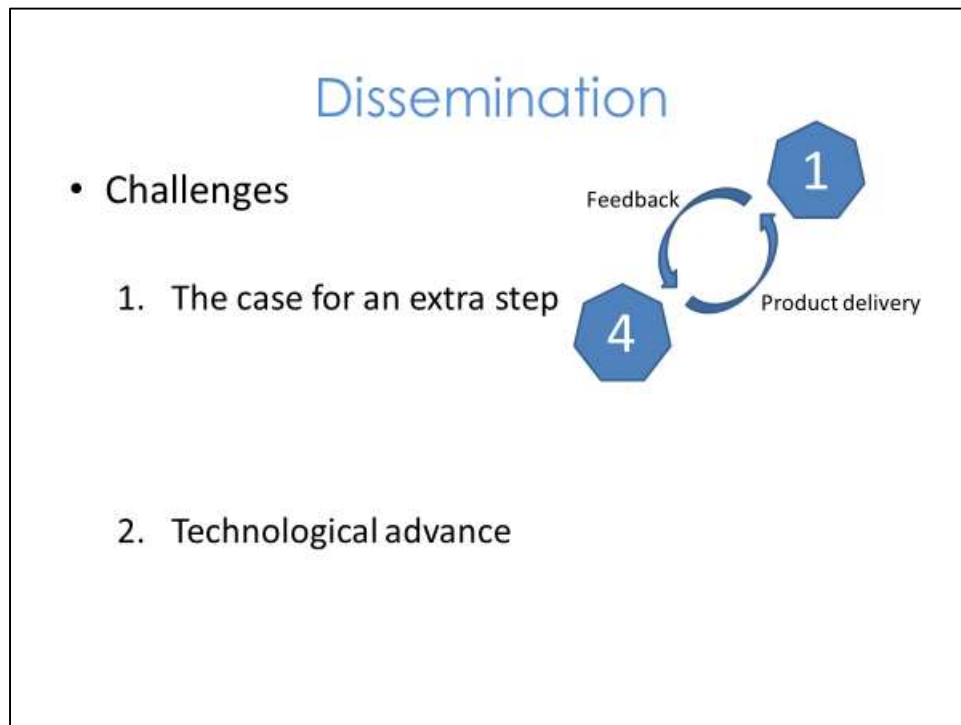
Key message: There are three combinable dissemination formats: Verbal, written and graphical.

- Verbal dissemination is typically used for time-sensitive and/or urgent information. Such dissemination could be constrained due to language, security related restrictions over the use of certain communication systems, the security clearance of the recipient, etc.
- Written dissemination is typically INTREPs and INTSUMs and is useful over a larger area or between several dispersed entities.
- Graphical dissemination is typically (part of) a reoccurring status briefing or report. Such products can be presented as a PICINTSUM, sketch map, an overlay or link chart.

As I mentioned on the previous slide, PKISR differs from MPKI in that MPKI is informing commanders and decision makers whereas PKISR generally is used within the MPKI community. There are exceptions to this rule in case of urgent reporting like for instance threat warnings.

For written dissemination commonly agreed templates should be used. These are often defined by each mission. Templates for such reporting can be found in the MPKI Handbook.

## Slide 14



Key message: There are several challenges associated with the implementation of peacekeeping-intelligence.

These challenges have the potential to negatively impact on the performance of the PKI function as a whole. Arguably, dissemination is the step in the cycle where these challenges become visible to others – as this is the step where the producer meets the client for the delivery of the product. It is important to understand two most important shortcomings regarding dissemination – this is important because it will help you to understand your own role in a better way.



**Note to Instructor:** ask the students what is meant by ‘the case for an extra step’. Perhaps the students can explain this particular case in their own words and if so, you can use the time to discuss instead of explaining what is written at 1. You can take a similar approach with the second point.

1. The case for an extra step. The PKI cycle implies that it is finished after a product has been disseminated. This would be wrong. The case for the extra step is the need to gain feedback from the customer, as to understand if the customer has received what has been requested – in the right format and at the right time? We cannot just assume that the cycle is finished after a product has been disseminated. It often happens that a customer receives a product that does not quite answer to the needs or does not meet the expectations. Thus, to improve the PKI function and to shape it into a ‘learning-organization’ – and improve the producer-customer relation – it would

be useful to add an extra step to your cycle (or just create an option for feedback when you disseminate a product).

2. The challenges with technology. UN missions are currently not capable to fully support the analytical process behind the acquisition of bulk amounts of raw data and information. This means that priorities need to be made to prioritise analytical capacity or to limit the acquisition in accordance with the analytical capacity available. This also impacts the dissemination step as the IT backbone and limited bandwidth available will prevent certain output to be delivered to a customer. For instance, a customer could request a full motion video (FMV) output from a specific UAS but if – and this is often the case – the IT does not support the delivery of FMV, PKISR will not be able to 'disseminate' and will therefore not be able to meet a customer's expectations and demands. PKISR officers need to understand the possibilities and limitations of their supporting IT platform and need to continually strive for optimization of the IT platform in order to disseminate as widely, as fast and as efficient as possible.

## Take Away

- Analysis transforms information into intelligence.
- Analysis supports decision making.
- Intelligence that is not disseminated has no value.

## Summary

Analysis is the act of breaking down complex pieces of information to examine and understand the elements hereof to better understand the information. Analysis is also acquiring a series of pieces of information and arranging them into a system to understand a bigger problem set.

Analysis that does not support decision making is of no value. Therefore, an analyst's job is to provide the best possible assessments to decision makers in time to have a positive effect on the protection of civilians and mission personnel, and on enhancing situational awareness.

# Lesson 3.7



## PKISR Planning

### The Lesson



#### Starting the Lesson

The next lesson is about PKISR planning. During this lesson you will understand the basics and learn to describe the key elements and considerations of PKISR planning.



**Note to Instructor:** *It is advised that you have a basic understand of military planning in general and military ISR planning in detail. Also, this lesson contains a level of interaction with the students. It is suggested you think about different examples (based on real events perhaps) to maximize the level of interaction.*

Slide 1



## Lesson 3.7

### PKISR Planning

## Slide 2

### Lesson contents

- The basics of PKISR planning
- The key elements of PKISR acquisition planning
- Key considerations and factors affecting PKISR plans

PKISR planning is crucial in balancing resources with results. Planning can make it possible to get the information you need, with the best possible sensor and at the right time. It is therefore an important part of the PKISR cycle.



**Note to Instructor:** When showing this slide, you can either verbally repeat what is depicted on the slide or let the students read the contents themselves.



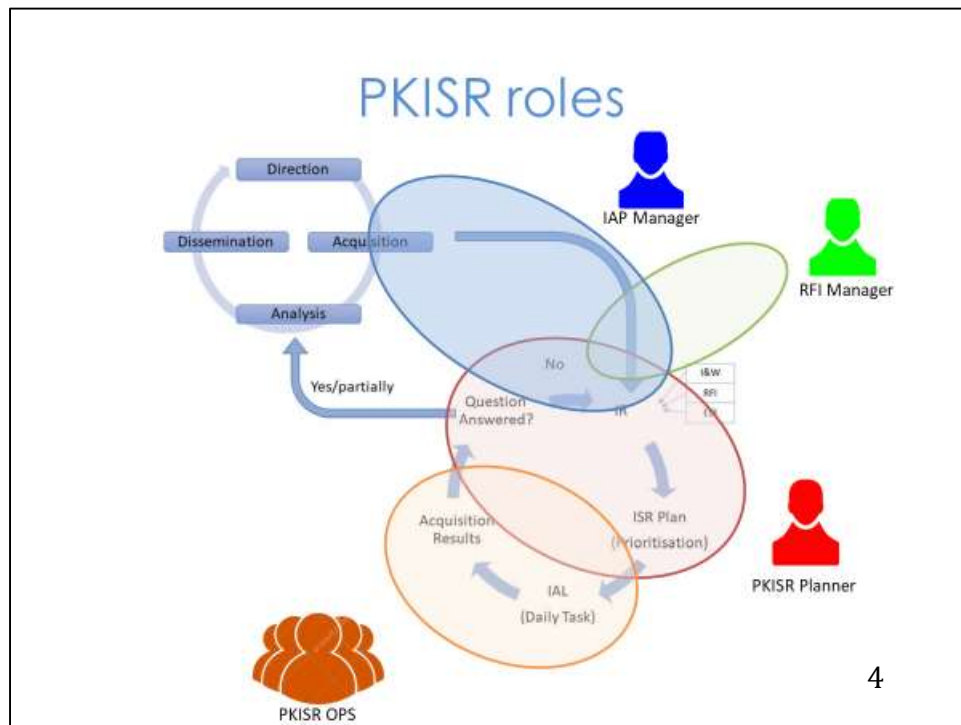
### Slide 3

## Learning Outcomes

- Understand the basics of PKISR planning
- Describe the key elements of PKISR acquisition planning
- Explain the key considerations and factors affecting PKISR Plans

At the end of this lesson, you will understand the planning function within a PKISR cell. You will understand the basics of PKISR planning, be able to describe the key elements of PKISR acquisition planning and will be able to explain the considerations and factors affecting PKISR plans.

## Slide 4



Key message: The PKISR process involves several roles and responsibilities. Understanding these roles (and associated functions) is important for the lessons on PKISR planning and operations.



**Interactive.** Use this slide for revision purposes. Students will have been introduced to all the PKISR key roles in a previous lesson. Ask students to explain the different roles within the PKISR process. The notes below can be used by the instructor if students cannot remember the information.

**IAP manager:** The IAP manager is responsible for all peacekeeping-intelligence and information requirements (be it U2, sector or battalion staffs). The IAP contains all Priority Peacekeeping-intelligence Requirements (PIRs), Specific Peacekeeping-intelligence Requirements (SIRs), Essential Elements of Information (EIs) as well as the PKISR unit most suited to answer the questions. The IAP manager is also responsible for merging information requirements (IRs) from indicators and warnings (I&W) and requests for information (RFIs - from the RFI manager) with the IAP and for conveying the IAP to the PKISR planner. The IAP is a management tool for the peacekeeping-intelligence staff. The IAP manager needs to be informed about all ISR asset capabilities, availability and reporting to keep the planning tool updated.

**RFI manager:** The RFI manager is the point of contact for anyone outside the PKISR team that has information requirements. All RFIs must go through the RFI manager for quality control, registration and prioritisation. If the answer to the RFI does not already exist within

the peacekeeping-intelligence staff, the RFI manager will coordinate with the IAP manager to merge RFI IRs into the IAP and prioritise them in relation to the other requirements. The RFI manager must always be informed about RFIs that have been answered.

**PKISR Planner:** The PKISR planner plans for ISR coverage, taking into consideration the priority of the IRs, sensor capability and capacity, operational plans and external factors like weather and terrain. The PKISR planner's current Information Acquisition List (IAL) is handed over to PKISR OPS as "daily tasking". The PKISR planner(s) are responsible for what is called the Information Requirement Management (IRM) part of the PKISR cycle; this is the planning and prioritizing part of the cycle.

**PKISR OPS:** The PKISR OPS is responsible for the daily tasking of the acquisition assets. PKISR OPS will make sure that acquisition is achievable, contingency plans are in place, and products are disseminated as planned. The PKISR OPS is responsible for the Acquisition Management (AM) part of the PKISR cycle; this is the operations and acquisitions part of the cycle.



**Note to Instructor:** *You should stress the need for communication and interaction between the different roles to ensure successful tasking. Although they have different tasks and responsibilities, mission success is everybody's responsibility, and communication is key to smooth processes. You may also clarify that is depending on the size of the Mission, a single person may have at the same time more than one role (IAP and RFI Manager – PKISR Planner and Operations).*

## Slide 5

### The basics of PKISR planning

- The planning environment
- The resources available

**Key message:** The planning environment of PKISR depends on which level (of military operations) the activity is conducted (i.e., tactical / operational / strategic).

The planning environment will also define the resources available for this activity. Meaning that if you are a G2 at a Sector HQ, your resources are limited and most of the planning will be done by a few individuals. However, the U2 branch at the Force (operational) level has a PKISR cell with specific planning capacity, and a battalion S2 often is one person.



**Note to Instructor:** Inform the students about the basics by delivering the Key message. Also, add the following information to ensure that they understand the difference between the various levels of military operations: Force HQs often have specialised capabilities and capacities for specific functions such as analysis. At the battalion level, this often comes down to 1 or 2 individuals.



**Interactive.** Let a student explain who they think is performing PKISR planning duties at the battalion level. (Often it is the S2, as there is no specialised capacity to perform these duties).

## Slide 6

### The key elements of PKISR acquisition planning

- Short term planning overview
- Acquisition strategy
- Avoid redundancy

Key message: Best practice for PKISR acquisition planning focuses on a time span of between 72 hours and 24 hours. This is referred to as short term planning.

For the purpose of this course, everything beyond 72 hours is referred to as either medium- or long-term planning.

Everything shorter than 24 hours is seen as current operations and is the responsibility of PKISR Operations (Ops). Note that battle rhythms may differ between mission's, dependant on internal planning processes.

PKISR planning needs an acquisition strategy. An acquisition strategy is a systematic plan to optimize tasking and requesting of all capable, available and appropriate acquisition assets and/or resources against requirements.

Lastly, and this speaks for itself, as it is part of the acquisition strategy too, it is essential to avoid redundancy.

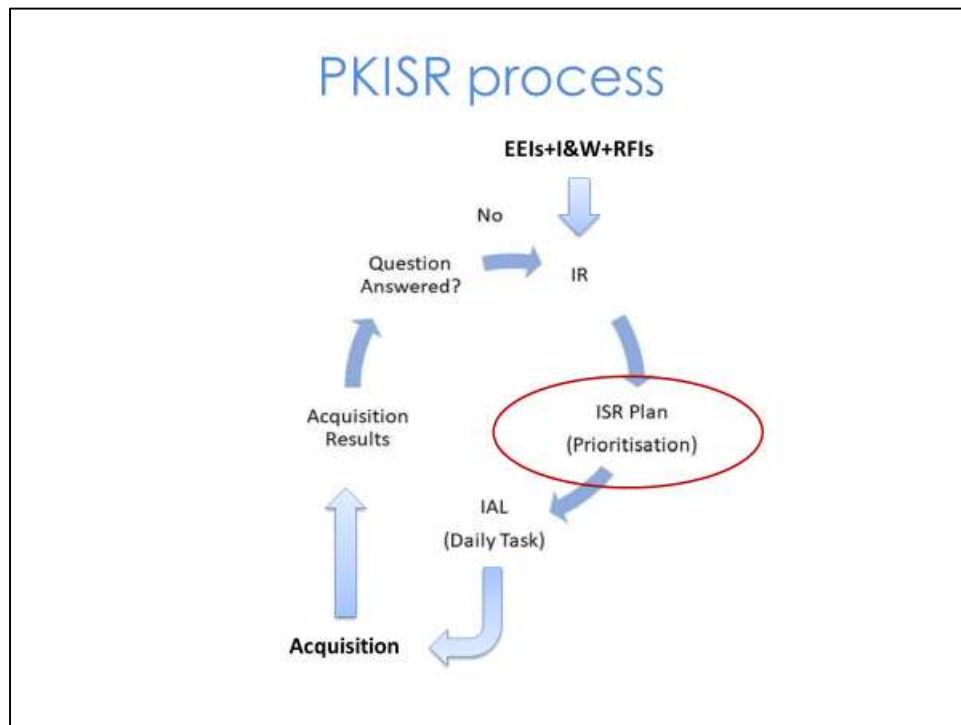


**Note to Instructor:** Highlight the key elements and inform the students that all bullet points will be developed in more detail in the following slides.



**Interactive.** Ask one of the students to explain in their own words why they think an acquisition strategy is important. Also, ask them why close cooperation between PKI analysts and PKISR assets is necessary.

## Slide 7



Key message: The PKISR process is designed with flexibility and robustness; it should create an efficient tasking and reporting environment.

The Information Acquisition Plan (IAP) helps the PKISR planner to create a PKISR plan. As said in the previous slide, the PKISR plan is a planning product beyond 24 hours, which determines which assets have the best prerequisite for successful acquisition by matching the prioritised Information Requirements (IRs) with acquisition assets capabilities and availability. At any time, some of the mission's acquisition assets will be 'out of service' due to technical issues, planned service time, personnel on leave, etc. Based on the PIRs within the IAP, and the PKISR plan, an Information Acquisition List (IAL) is made. This list contains all the IRs, independent of origin, together with information about who is to acquire the information, and by whom it is required.

If the IR is answered by acquisition, the report is sent to the requiring unit and to the IAP manager, so that the IAP can be updated. If an IR is only partially answered, or not answered, it stays in the PKISR process, for a new round of prioritisation and possibly more acquisition.

## Slide 8

### Example of an IAP

PIR	SIR	EEL
1 Threats against an IDP Camp	1.1 Ethnic/tribal dynamics	1.1.1 What is the ethnic breakdown in the IDP camp?
		1.1.2 Are there any conflicting ethnic groups/tribes within the IDP camp?
		1.1.3 Is there any evidence of changes in the ethnic groups/tribe's laydown within the IDP camp?
		1.1.4 What is the size of the ethnic groups/tribes in the immediate vicinity of the IDP camp?
		1.1.5 Has the size of the ethnic groups/tribes in the immediate vicinity of the IDP camp changed?
		1.1.6 Who are the local ethnic groups/tribes' leadership in the vicinity of the IDP camp?
	1.2 Armed group activity in the area	1.2.1 What armed groups are operating in the local area?
		1.2.2 What are the known armed groups' TTPs?
		1.2.3 What are the size of the armed groups in the local area?
		1.2.4 Do any of the armed groups have relations with the local community/UN/other nation?
		1.2.5 What weapons capability do the armed groups have?
		1.2.6 Are there any combat indicators associated with the armed groups in terms of uniform or clothing?
	1.3 Weather considerations	1.3.1 Where are the armed groups based?
		1.3.2 When is the rainy season?
		1.3.3 How long does the rainy season last for?
		1.3.4 In what way is the IDP camp at risk of flooding?
	1.4 IDP relationship with UN and national institutions	1.4.1 What are the road conditions into and out of the IDP camp?
		1.4.2 Is there any evidence of propaganda/media directed at the IDP camp (positive or negative)?
		1.4.3 Are the IDPs supportive of the UN and national institutions?
		1.4.4 Is there any national security provided for the IDP camp?
	1.5 Key leadership within IDP camp	1.4.5 Is there any NGO activity within the IDP camp or in the local area?
		1.5.1 Are there any identifiable leaders within the IDP camp?
		1.5.2 Is there evidence of any formal meetings taking place within the IDP camp?
		1.5.3 Do the leaders have any obvious political connections?
		1.5.4 What is the media outlook of the IDP leadership?
		1.5.5 Do the leaders have any stated agendas or goals?
	1.6 Freedom of movement	1.5.6 Is the leadership connected to armed groups in any way?
		1.6.1 Are there any restricted areas within the IDP camp?
		1.6.2 Who is controlling the restricted areas?
		1.6.3 Is there evidence of illegal taxation within the IDP camp?

Key message: The IAP contains the PIRs, SIRs and EEL. The IAP is a living document managed by the IAP manager.

This slide shows an example of an Information Acquisition Plan (IAP). The IAP captures PIRs that need to be answered. The SIRs are analytic questions, broken down from PIRs, needed by analysts to answer the PIR. And the EEL are detailed questions needed to answer an SIR.

## Short Term Planning Overview

1. The IAL (information Acquisition List) planning horizon is 72 hours. This IAL planning must be flexible enough to accommodate new time-sensitive tasking.
2. The PKISR Plans uses the IAP and 3 "living" IALs:
  - one at the 72-hour point
  - one at the 48-hour point
  - one at the 24-hour point
3. At the 24-hour point the plan is passed to the PKISR Ops role to execute.

Key message: The Information Acquisition List (IAL) is a dynamic copy of the Information Acquisition Plan (IAP) but limited to the information requirements between 72 hours and 24 hours.

As said, PKISR acquisition planning focuses on a time span between 72 hours and 24 hours. For planning purposes, Information Acquisition List's (IAL) are used to cover this period. At the 72 hour point a broad review of where the PKISR assets will be tasked is considered against what should be established. This is communicated to the units to determine feasibility. As the time frame closes, the plan should become more mature and at the 24-hour point the plan is passed to the PKISR Ops role for execution.

The PKISR Planner has three "living" IALs: one at the 72-hour point, one at the 48-hour point and one at the 24-hour point. The planner uses the IAP for planning activities beyond the 72-hour mark. The planner must be able to deal with the impact of dynamic tasking and adjust the plans to ensure that deadlines are met. Notwithstanding dynamic tasking, the closer the IAL gets to the 24-hour point the more accurate and refined it becomes. The PKISR Planner's job is never complete. There are always unknowns within the Mission and when there are no RFIs or operational tasks to complete, emphasis must be on the IAP and answering the EEIs. The PKISR Planner must have a very good understanding of the IAP and routinely assign tasks to the PKISR assets to fill in the gaps.



**Interactive.** Ask the question why the 24-hour IAL will be more refined (answer: The information and understanding about the next 24 hours is more precise than the



understanding about a moment in time that is further away). Everything shorter than 24 hours is seen as an ongoing activity and is the responsibility of PKISR Ops.



**Note to Instructor:** The students need to understand the planning horizon of PKISR Plans. Ensure that they understand the timeframe and the difference (in time) between plans and operations. The planning horizon reduces in time for subordinates of the Force HQ, i.e., a battalion would not have such a planning horizon, nor would it have a handover between plans and operations.

A living document means a document that is constantly changed and edited.

## Slide 10

## Example of an IAL

[illegible]


**Note to Instructor:** Talk through the IAL to familiarize students with its contents.

This slide provides an overview of an Information Acquisition List (IAL). At the top, it highlights references pertinent to the IAL, including the IAP, Operation Order (OPORD) and the Mission Peacekeeping-intelligence Coordination Mechanism. Moving from left to right, the document provides an IAP reference showing where the PIR originated from, the specific information requirement, and indicators or warnings as well as the named area of interest. It then highlights when the information is needed, and which assets have been assigned to acquire the information. Finally, it provides details on the start and finish time of the task as well reporting information.

While PIRs, SIRs, EEs and IRs are prioritised in the IAP by mission leadership, the priorities in the IAL are set by the PKISR planner(s). However, by using the IAP as a foundation for the IAL, the PKISR acquisition will be done according to mission priorities.

## Acquisition Strategy

1. A systematic plan optimizing effective and efficient tasking and requesting of all capable, available and appropriate acquisition assets.
2. Consisting of:
  - a) Tasking own acquisition PKISR assets.
  - b) Requesting adjacent and higher level for PKISR assets.
  - c) Requesting other available sources.



Note: Developing an acquisition strategy needs close cooperation between PKI analysts and PKISR assets

Key message: PKISR planning needs an acquisition strategy.

Let us take time to dive into the importance of an acquisition strategy and highlight the key elements.

Without an acquisition strategy you will not be able to optimize your tasking of PKISR assets. Your IALs are the core product of this strategy. An acquisition strategy that integrates tasking / requesting of multidisciplinary assets consists of the following three elements:

- Tasking HQ acquisition PKISR assets, i.e., the assets the HQ has control over.
- Requesting adjacent and higher-level entities for support from their PKISR assets, i.e., when working at Sector Level you could request support from a Force Level UAV asset.
- Requesting other available sources, such as NGO's or the Host Nation.

The strategy consists of an approach as to how the HQ thinks it can acquire information requirements, i.e., which questions will be answered by HPKI, or HPKI and UAV, or solely by NGOs, etc.

When developing your strategy, you need to ensure that very close cooperation exists between PKI analysts and PKISR assets. This close cooperation improves the understanding of the acquisition assets as to what to acquire.



**Note to Instructor:** Inform the students about the need to develop an overarching acquisition strategy that is based on the bullets depicted on this slide. The aim is to be as effective and efficient as possible – tapping into sources as often as possible in order to maximize their output.



**Interactive.** Ask one of the students to explain in their own words why they think an acquisition strategy is important. Also ask them why close cooperation between PKI analysts and PKISR assets is necessary.

## Avoiding Redundancy

Always try to avoid **redundancy** in tasking PKISR capabilities on PKI gaps.

Aspects to consider:

- Convergent
- Sequential
- Swarm
- Probing
- Queuing

Key message: Avoiding redundancy is one of the key elements of PKISR planning.

Redundancy has a direct connection to your acquisition strategy, which needs to be effective and efficient in its tasking and requesting of assets. As such, you should ensure that your plan is free of redundancy. An example of redundancy is when you task 2 assets when you could acquire the information with just one.

The following aspects are important to consider:

- **Convergent** Conduct acquisition operations with different types of sensors to acquire different types of information.
- **Sequential** Trigger a sensor to start acquisition by the information that is acquired by another sensor.
- **Swarm** Use all means available for a period of time in order to intensively cover one or more NAI (good for countering-actor/counter-intelligence measures).
- **Probing** Trigger "target" behaviour to allow acquisition on a "target".
- **Queuing** Plan multiple sensors subsequently to ensure continuous coverage of a NAI.



**Note to Instructor:** Inform the students about the need to prevent redundancy. Redundancy is a risk for the timeliness of acquiring against other prioritised information requirements. When preparing the lesson, come up with a few examples of redundancy yourself – this will allow you to respond to the answers of the students. Also, explain the aspects until they understand what they mean and why they are important. An example

could be: A High Value Individual needs to be followed with a UAV to establish a pattern for future operations. HPKI is tasked to identify the High Value Individual. The planner could decide to keep the UAV on standby while HPKI tries to identify the High Value Individual – the planner could also decide to task the UAV to acquire a different requirement and allow dynamic re-tasking after the High Value Individual is identified. This prevents redundancy.



**Interactive.** Ask one of the students to explain in their own words about an example of redundancy in PKISR operations.

## Key Considerations and Factors affecting PKISR Planning

- Which IRs need to be answered?
- Which PKISR capabilities to use?
- Where are my PKISR capabilities?
- Are those PKISR capabilities able to answer my question?

**Key message:** The PKISR planner needs to have a short- and medium-term view on what PKI gaps or RFIs need closing.

First, the planner must have a close working relationship with the Information Acquisition Plan (IAP) Manager. The IAP Manager will provide them with an understanding of the existing gaps and RFIs. A PKISR planner also needs to have a good understand of what Force / Sector HQs is planning for the future and therefore needs to maintain a close working relationship with the MPKI Plans officer. This will provide the PKISR planner with a broad view of the priority requirements.

Secondly, which PKISR capabilities are available. For this, you need to understand the availability of your capabilities – are they available, when will they be available, how long will they be available for, and what are their limitations?

Thirdly, you need to know where your assets are. On some occasions particular assets are stationed at location A and only have a limited range – and thus will not be able to physically get to location B (where acquisition needs to occur).

Fourthly, are those assets able to answer the question in a timely, relevant and efficient manner? If you need to know if a particular building is in use, you could decide to send a UAV to observe activity in and around the building, but it might be easier to task a HPKI cell with access to a source in that area - which would only cost a quick telephone call to answer the question.

## Take Away

- PKISR plans needs to have a short and medium-term view on what PKI gaps or RFIs need closing.
- The IAL is a dynamic copy of the IAP.
- PKISR planning needs an acquisition strategy.
- Avoid PKISR asset redundancy.

## Summary

You should understand the plans function within a PKISR cell, including the key elements of PKISR acquisition planning and the considerations and factors affecting PKISR Plans.

- PKISR Plans needs to have a short- and medium-term view on what PKI gaps or RFIs need closing.
- The IAL is a dynamic copy of the Information Acquisition Plan (IAP) but limited to the information requirements between 72 hours and 24 hours.
- PKISR planning needs to be based on an acquisition strategy.
- Avoiding redundancy is one of the key elements of PKISR planning.



# Lesson 3.8



## PKISR Operations

### The Lesson



#### Starting the Lesson

The PKISR process and tasking routines may seem complex – but it is less daunting once you have broken down the roles, responsibilities and products, which is what we will do during this lesson.

Slide 1



## Lesson 3.8

### PKISR Operations

## Slide 2

### Lesson Contents

- Deliberate tasking
- The basic principles of PKISR operations
- Key elements of PKISR operations execution
- Dynamic tasking

These are the subject areas we will be covering in this lesson.

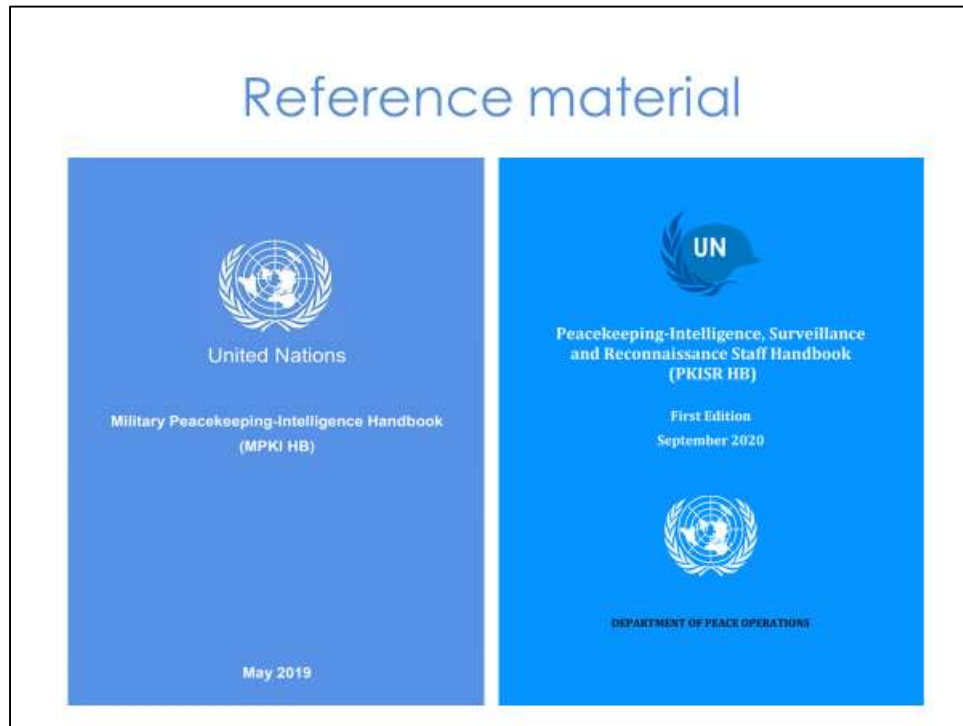
### Slide 3

## Learning Outcomes

- Explain the deliberate and dynamic tasking processes
- Describe typical mission specific tasking frameworks and authorities

Let us review the desired learning outcomes before we start this lesson. Please take a moment to read what you are expected to be able to do at the end of the lesson.

## Slide 4

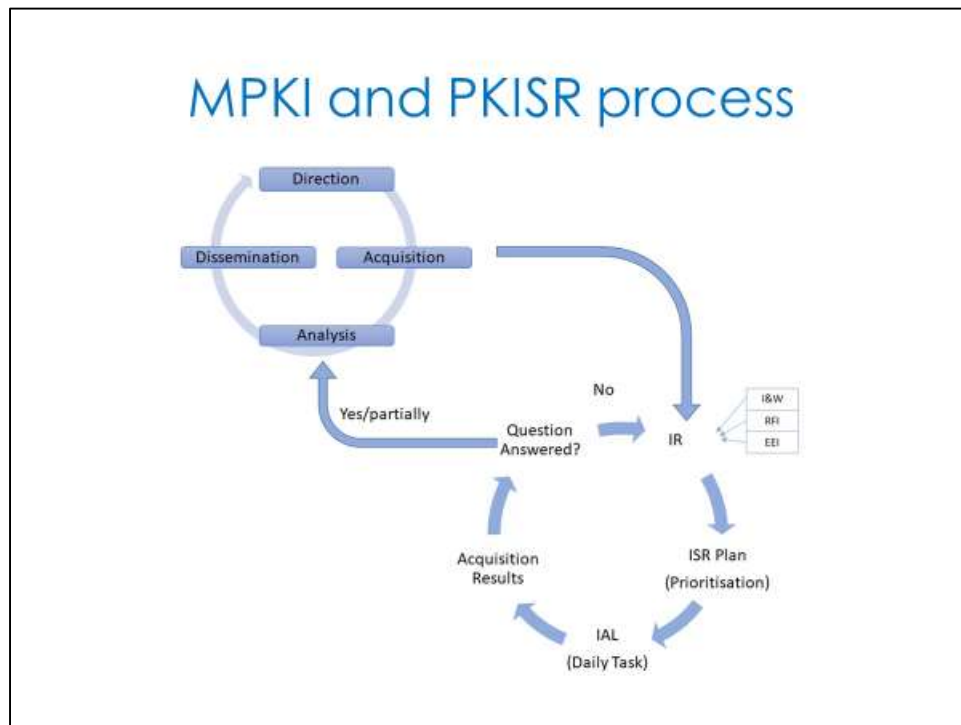


This lesson is based on the United Nations Military Peacekeeping-Intelligence Handbook (May 2019) and the Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (September 2020).



**Note to Instructor:** Inform students that each peacekeeping mission will have its own standard operating procedures that will provide detailed information and guidance on mission ISR tasking and reporting.

## Slide 5



Key message: the PKISR process is tightly connected to the MPKI process.



**Interactive.** Students will have already been introduced to the MPKI and PKISR processes in lesson 3.2. As such, use the time to assess students' knowledge by asking them to list the different steps in the MPKI process. Ask them specifically, who generates EEIs and who is responsible for the Information Acquisition Plan (IAP)?

The PKISR process is tightly interconnected with the MPKI process. The main input to PKISR acquisition are the EEIs and the Indicators and Warnings (I&W) from the Force IAP converted to information requirements by the IAP Manager. In addition to the input from the IAP, there may also be other mission requirements for operations or decision making, such as Requests for Information (RFIs).

## Slide 6

### Asset tasking

- PKISR OPS tasks acquisition units based on 24h IAL
- U2 responsible for tasking, U3-5 has authority to approve operations.



Key message: PKISR OPS tasks the assets, usually through the Force HQ U3/5.

The PKISR OPS creates the acquisition unit tasking from the ISR Planners 24 hours' Information Acquisition List (IAL). The 24-hour IAL should reflect the daily priorities and main objectives, but in real life this is highly influenced by dynamic taskings and changes in the situation.

Although the PKISR OPS creates the tasking, the formal tasking authority lies with the Force HQ U3/5 Cell the staff function responsible for operations, unless OPCON is given to the U2 for the acquisition assets.

## Slide 7

### PKISR OPS tasking

- Execution order:
  - **Who** could acquire the information?
  - **What** information needs to be acquired?
  - **Where** to acquire it?
  - **How** are sources and sensitive information going to be protected?
  - **When** is the information required?
  - **Why** is the information required?
  - **How** the acquisition unit is to disseminate the acquired information
- Based on the IAP and focused on a 24 hour period

[Key message:](#) Correct tasking is important to get the right answers.

The IAP is the basis for execution orders to PKISR units. It may be written and published in the operation order format in accordance with the mission's SOP.

PKISR units are usually not tasked with the IAL directly. Parts of the 24-hour IAL is rewritten as orders to the different PKISR units. As a minimum the execution order should contain:

- **Who** could acquire the information?
- **What** information needs to be acquired?
- **Where** to acquire it (NAIs – named area of interest)
- **How** are sources and sensitive information going to be protected and kept confidential?
- **When** is the information required?
- **Why** is the information required?
- **How** the acquisition unit is to disseminate the acquired information.

The orders format, and details, will differ between different types of acquisition units, for example, UAS, Human Peacekeeping-intelligence, and Long-Range Reconnaissance Patrol.



## Slide 8

### Indicators

- Observable phenomena or objects for the acquisition units to base their reporting on.
  - Damaged portions of road / asphalt / bridges.
  - Potential obstacles, debris on road, water flooding, fallen objects
  - Check points established on route
  - Width of road going from double to single lane

Key message: Indicators help the acquisition unit decide what to look for and include in its report.

When creating tasking for an acquisition unit, the PKISR OPS should not only give PIRs or IRs but also observable indicators for the acquisition unit to look for and include in its reporting. It is likely that such indicators will have already been determined by the IAP Manager and PKISR plans, however these can be constantly refined. For example, if the acquisition unit is a UAS system and the mission is to conduct a route search, the indicators might look like those listed on the slide.

## Slide 9

# Tasking formats

### TASK OVERVIEW

The task is:

- To support the Birtlett convoy with a route scan.
- To support Intel Collection in pre-planning of intel led operations

Several villages have experienced hostile action from unidentified assailants. The goal of this mission is to ascertain the suitability of the surrounding environment for AG presence/support base. The overall purpose is to increase situational awareness in order to help inform protection of civilian activities, security risks in the area and to assess freedom of movement for UN personnel. Thus, this type of mission will likely be re-tasked several times from now on.


Flight Time: 0400Z09DECNOV – 1900Z09DEC - 2018

### TASK #1-2

Conduct the ISR mission in the following sequential support the SA and answer the questions raised by HRD and U2 Prod

Sequence:

- Villages along the LOC to KORD
- GMTI scan Area of BAKASS - KORD



Task	Priority	Timing	Reporting
Transit time task	High	0400Z-1900Z	U2ISR

**Transit time task**

Follow the track east of KORD along the border and report on overall activity, from border to KORD follow the main LOC and report any visible signatures and LOC indicators.

Human Rights division provided a named area of interest west of KORD. From their assessment, due to the events and inter communal clashes in the last week they have reported that at least up to 1500 displaced persons are present in the area. No information on whether they are living in a special IDP camp or just are housing in the area.

Main effort is to provide KORD with a SA on the activity in the AGI west of KORD and the villages along the tracks / LOCs.

Scan the villages for IEDs and the indicators.

**Rough indicator list:**

- Tents/camps in the outline of the villages?
- Armed group presence
- Reduced amount of activity/gathering on LP in the villages in the AGI with special focus on the two mentioned above.
- Assessment on the IDP situation with regard to how are people living in the area – tent areas? Huts? More people than expected in a village of that size?
- Any public infrastructure visible?
- Any signatures of armed PAX or PU with mounted weapons?
- Camps / huts in IDP villages.
- LP gathering, wells and water tanks / pumps.

Key message: Different units use different tasking formats, adapted to their specific needs.

The example you see on the slide is a UAS tasking from MINUSMA, where a UAS unit was tasked to conduct a route scan in direct support of a UN unit, and a GMTI (Ground Moving Target Indicator) scan to aid mission planning.

On the top left slide, the two tasks are stated, with a brief description of the mission intent and intended outcome. Also stated is the timeframe for the mission.

The top right slide gives guidance concerning the geographical area, with the sequence of the mission execution.

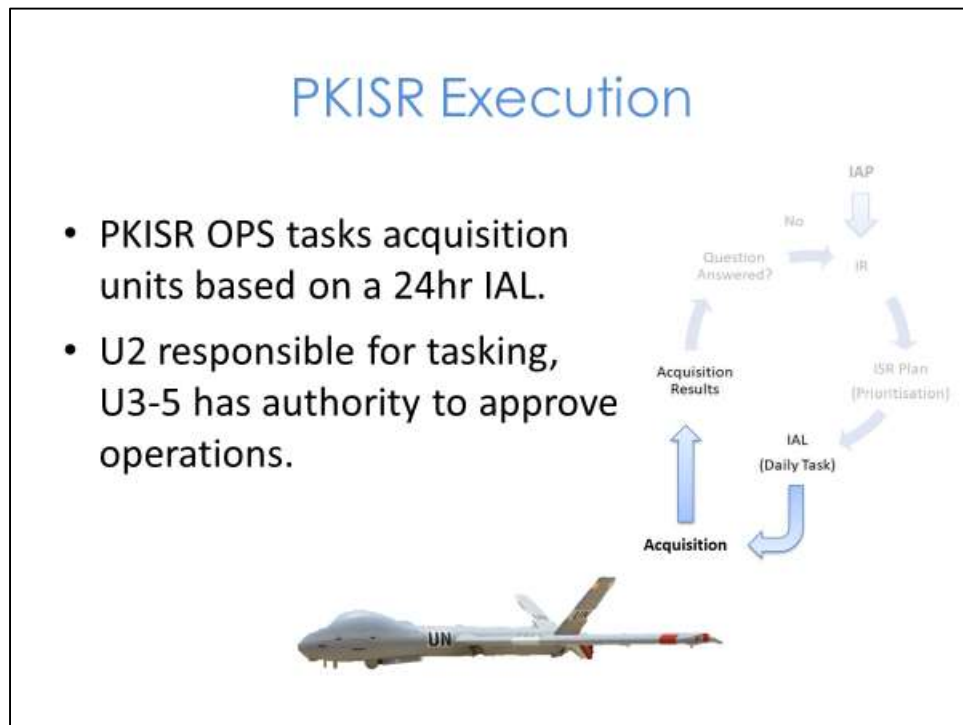
The bottom slide gives more details about the mission. There might be several slides like this in a single tasking. The top matrix states NAI in which the mission is to be executed, the task (PoL = pattern of life), timings (in this example the mission is sequential) and how to report (e-mail to U2ISR). While the blue text box describes the mission, the red box describes the situation and mission intent, and the green box contains indicators. The indicators are reporting criteria related to the intended outcome of the mission. If the UAS unit observes any object or activity on the indicator list, this is to be reported according to the tasking.



**Note to Instructor:** GMTI means 'Ground Movement Target Indicator'. A radar system usually mounted to an airborne platform that is able to monitor all movements in

*an area. GMTI is not used to track single moving targets, but rather to map all movement in an area within a timeframe of hours to days (depending on the platform). Inform students that they will be expected to complete a tasking line as part of the final staff exercise at the end of the course.*

## Slide 10



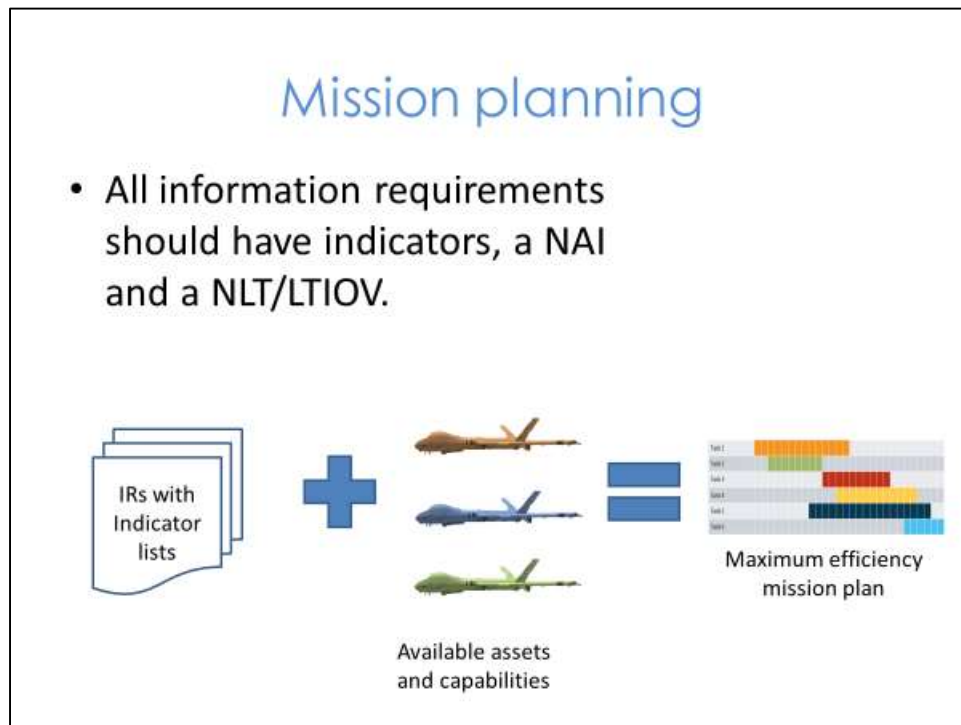
Key message: PKISR OPS tasks the PKISR acquisition units based on the 24-hour Information Acquisition List (IAL), in other words, a daily tasking list.

PKISR operations is what happens between the tasking from PKISR OPS and the return of a PKISR product from a PKISR unit.

When the PKISR unit, exemplified in the slide by a UAS unit, receives the tasking from the PKISR OPS, their own mission planning begins.

You should be aware that the tasking process may vary for different acquisition units, more on which will follow later in the course. UAS is used for the purposes of this lesson only.

## Slide 11



Key message: Mission planning is to match available assets and capabilities against information requirements (IRs) and indicators in the most efficient way.

First, the PKISR unit will look at the IRs and their indicators and decide which sensors are needed to answer them. Maybe normal camera footage is enough, or maybe infrared or thermal is needed, for instance, to observe the presence or movement at night, or vehicles in garages.

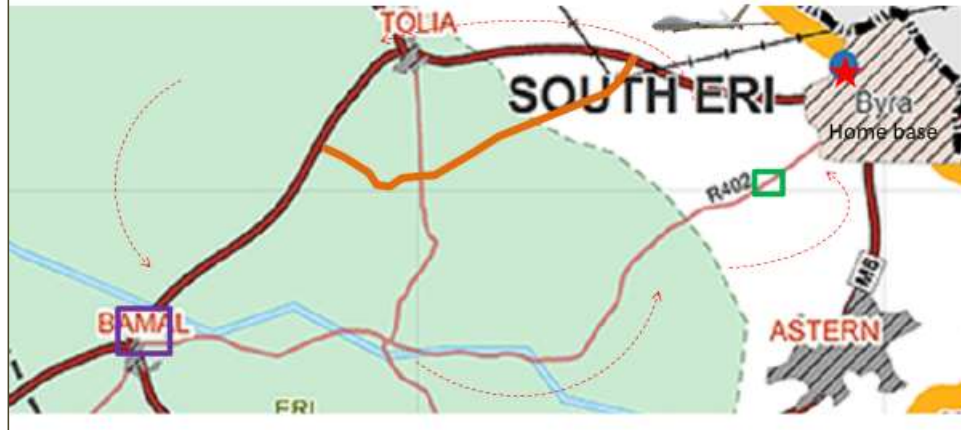
Based on sensor requirements and platform availability, the UAS unit will try to stack missions for maximum effect. One flight might support several IRs; first, a recce to answer one IR, followed by direct support to an ongoing operation before returning to base, while answering any possible IRs along the way. The key to maximising sensor efficiency is always to include a named area of interest (NAI) (the area where the IR will probably be answered) and necessary timings like NLT (no later than) or LTIOV (latest time information is of value) to allow time for the analyst to process the information required. This enables the UAS unit to maximise sensor usage in planning.

## Slide 12

## Mission Execution

**Flight mission task list:**


1. 08:00 – 09:30 Route search on R400 (medium priority)
2. 09:30 – 10:30 Direct support to distribution of humanitarian aid in Bamal in order to establish situational awareness and deliver early warning indicator list (high priority)
3. 10:30 Return to base for refuel, confirm status of bridge on R402 on the way (medium priority)



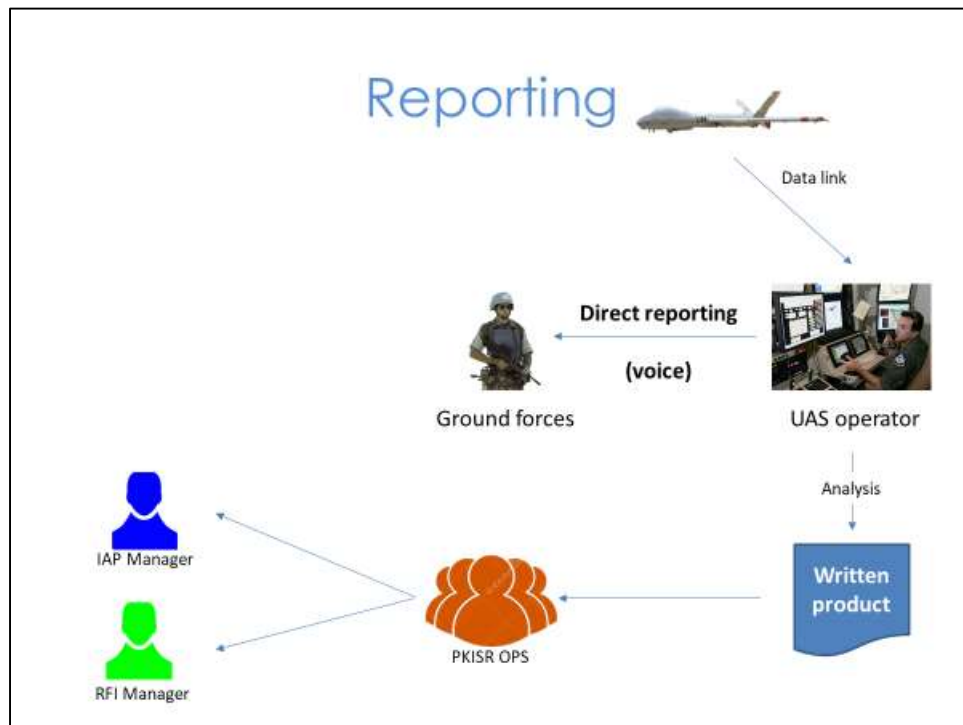
Key message: The UAS combines as many information requirements (IR) as possible on the same flight.

This slide provides an example to show how one UAS flight mission might be carried out. First, a route search between two known locations to answer one IR, then direct support to a humanitarian operation to establish situational awareness, before returning to base and assessing the state of a bridge along the way.



 **Interactive.** Question to students regarding reporting: which of these missions needs direct reporting from the UAS asset to the ground force, and which demands a written product? The answer would be the second task – high priority support to the distribution of humanitarian aid.

## Slide 13



Key message: As students have already heard in a previous lesson, sometimes reporting needs to be direct and provided as soon as possible. On other occasions, the report can be written and supplemented with analysis.

As we have seen, the expected products from each mission will vary. This slide depicts the reporting lines. In the figure above the data is relayed to the UAS operator, who will disseminate products based on the Information Acquisition List (IAL) or re-tasking orders.

Some missions, like direct support to ground operations, requires the possibility of near real-time reporting from the UAS operator to the ground force commander. For instance, it may be necessary to give a warning about ambushes or other immediate threats. Other times, for example, while conducting a road recce missions, or answering analytic questions (e.g., pattern of life information about a village), a written product is required. Such a report will be channelled through PKISR OPS and onto the relevant information manager.

We will now move on to consider some of the types of products available in a UN peacekeeping environment.

## Slide 14



Key message: most UAS systems can provide a still image, which is one that only includes raw data.

Written products come in many forms. Different PKISR units will have different technical and analytical capabilities, and hopefully, they will provide a guide to the different products they may provide. A still pack provides only imagery of a point, area or structure with little or no annotation or analysis. As there is no analysis involved, this will not take long to produce and disseminate.

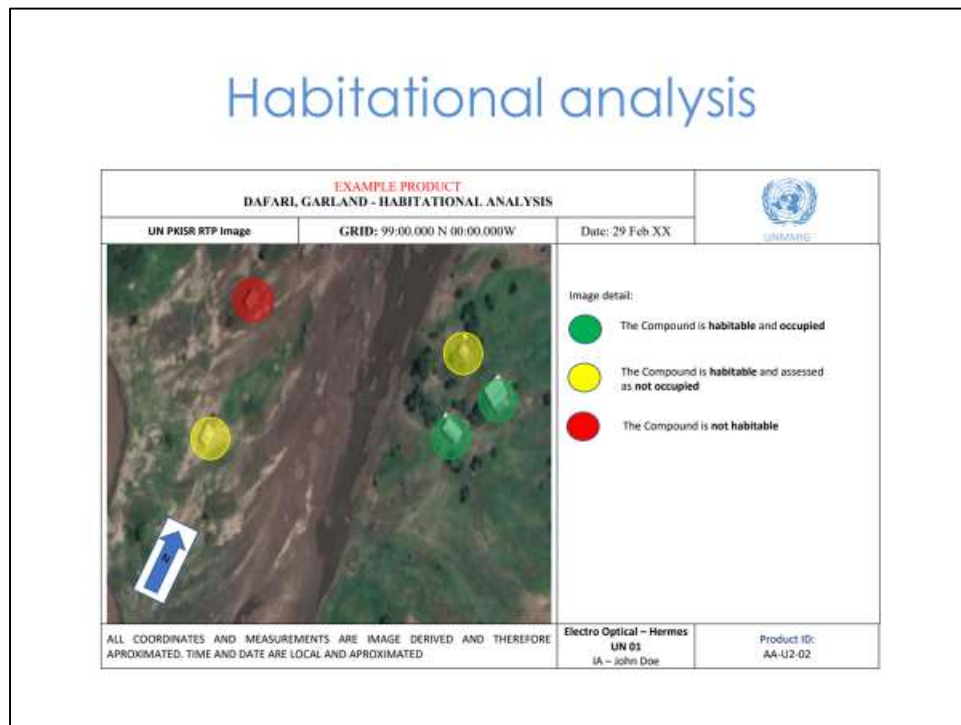


**Interactive.** Ask students: When can a product like this be useful? Are there any disadvantages to this type of product?

A still package like this can be very useful in planning operations, for instance, it could indicate cleared routes, the unusual presence of vehicles, heavy weaponry, etc. The disadvantage is that the image represents a single point in time, which could change immediately after the image is taken.



## Slide 15



Key message: the imagery analyst can produce several types of analytical products.

A PKISR unit contains single discipline analysts. In a UAS unit, imagery analysts are specialists in interpreting imagery and video. They can assess what we see in an image, and what in most likely means.

The imagery analysts produce/deliver/provide several analytical products, for example:

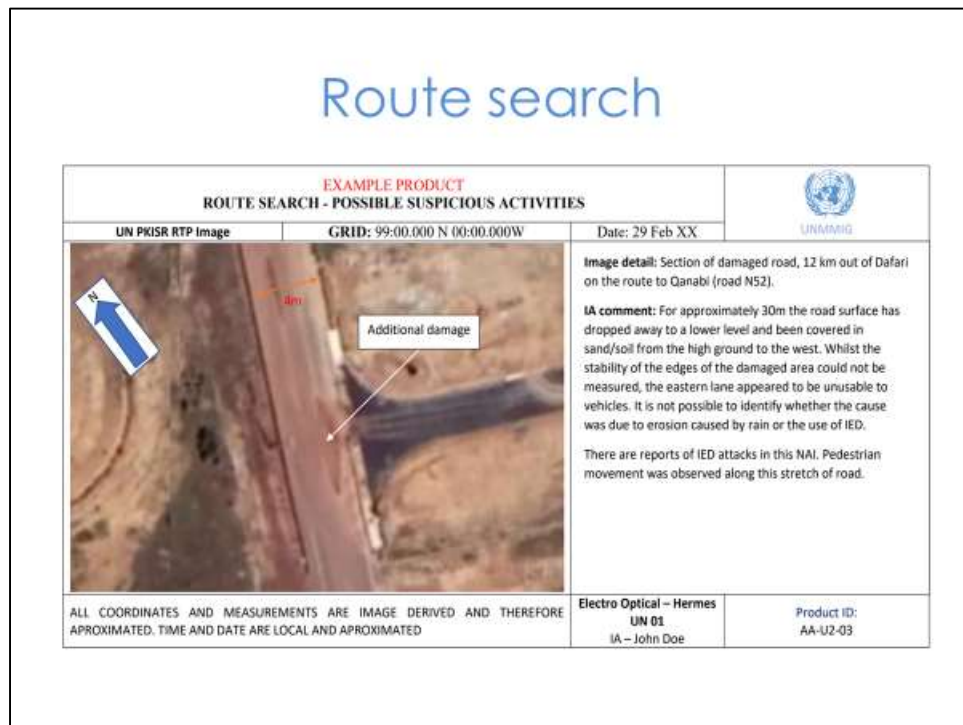
- Habitation analysis.
- Activity analysis.
- Pattern of live products.

This example in this slide is a habitation analysis. Here the imagery analyst has interpreted which compounds in a village are occupied, not occupied or not habitable at all. It is important to note that analytical products might take some time to produce as they are time-consuming for analysts.



**Interactive.** Ask the students: When and why do we want a product like this (habitational analysis)? A possible answer would be to establish a pattern of life. Why is the “pattern of life” so important to understand? A possible answer would be to help decision-makers understand the habits or behaviours of persons in a specific area of interest. Changes to these habits could indicate a warning that something is about to happen.

## Slide 16



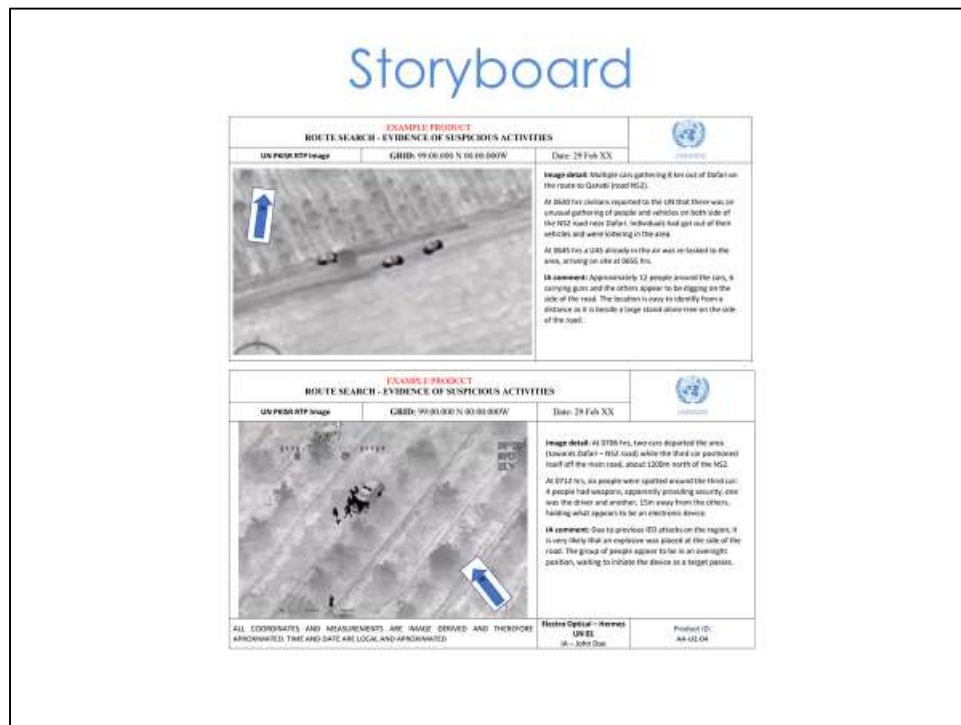
Key message: A route search is intended to study a particular route to identify vulnerable points and vulnerable areas.

Sometimes there is the need to identify vulnerable points or areas along a route. A UAS PKISR unit is usually able to provide this product, with details such as

- Vulnerable points
- Route width
- Route length
- Bridges, crossing points and culverts
- Surface types
- Maintenance or signs of damage
- Traffic density and types of traffic
- Checkpoints
- Roadside facilities
- Alternate routes

This slide provides an example of such a report. You will see how detailed it is and the benefits over a still image. This information would be very useful in mission planning or risk management. Unfortunately, this kind of product is very time and resource consuming. There are many details contained in the image, which requires human effort to analyse what each means.

## Slide 17



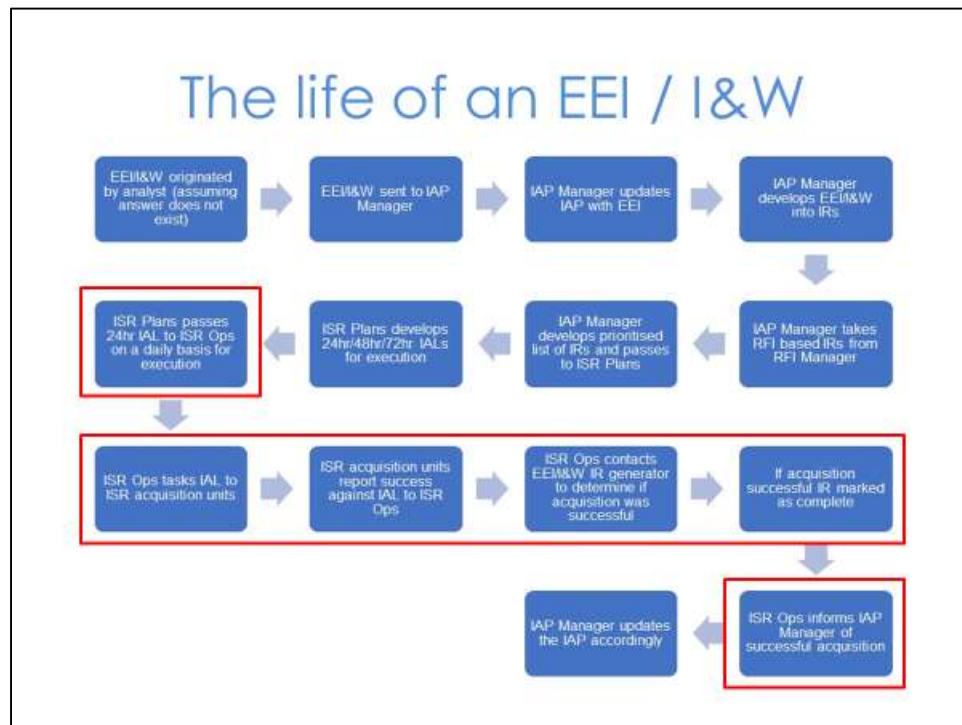
Key message: The storyboard is useful for understanding a chain of events, and could be compared with operations logs, or other sources, to give the U2 a better understanding of the situational dynamics.

A storyboard might highlight certain indicators, which may be a prerequisite for a certain activity. A storyboard could take some time and resources to produce as it is done manually by the UAS analysts.

A storyboard is a chronological reporting of monitored events, usually with still pictures and descriptions. This may be for planned events, for instance, the civilian or hostile forces reactions to UN operations. Or it may be the result of dynamic tasking, where an event occurs while PKISR units are available, and they are re-tasked to cover the event (for example an attack, demonstration or accident).

The slide shows an example of a storyboard. You will see the text beside the image, providing a description of the image along with an analysis of what it could mean.

## Slide 18



Key message: PKISR tasking is based on EEIs and I&W.



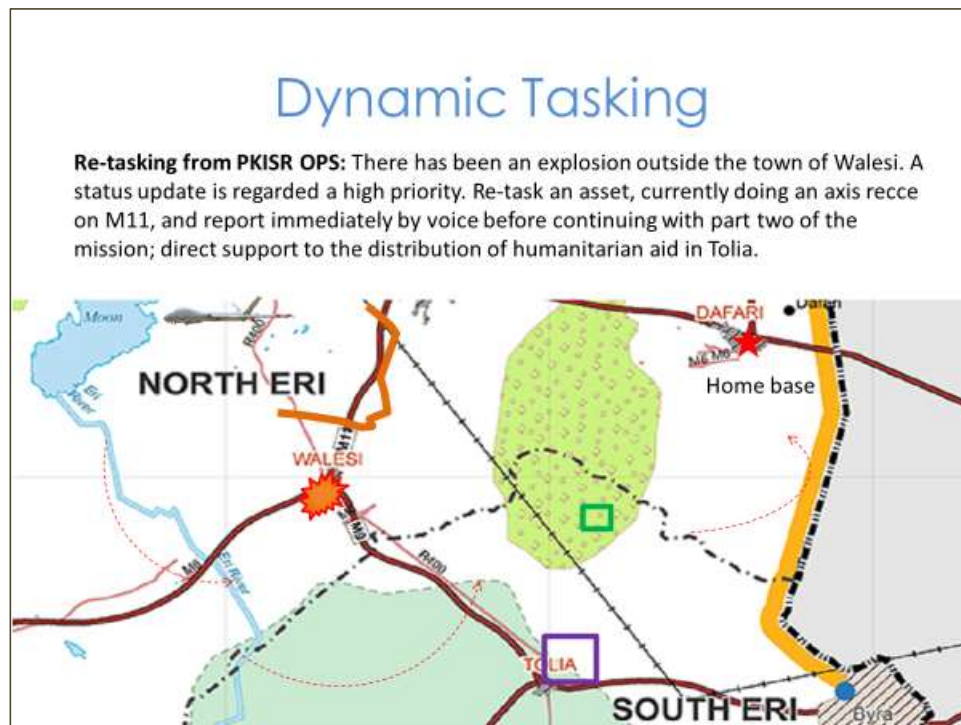
**Note to Instructor:** You should work your way around the slide starting at the top left. Those steps of the process that are highlighted by the red box refer to the tasking process.

EEIs and indicators for I&W originate from the analysts, as they are pieces of information needed to answer the overarching PIRs.

The analysts send them to the IAP manager who processes them into IRs and updates the IAP. The IAP is also updated with IRs originated from RFIs (these are handled by the RFI manager) and all the IRs are then prioritised.

The ISR Plans take the prioritised IRs and develop the 24-, 48- and 72-hour IALs. The 24-hour IAL is passed to PKISR Ops who tasks the PKISR acquisition units. The acquisition units send answers to IAL questions back to PKISR OPS who then forwards them to the EEI originator (the analyst), as well as to the IAP and RFI managers. If the analyst or the RFI originator agrees that their requirement is met, the IR is marked as "complete" and the IAP or RFI manager removes it from the IAP.

## Slide 19



Key message: Unplanned incidents will occur in a UN peacekeeping mission and must be dealt with in a timely manner. But dynamic tasking is not an excuse to avoid PKISR planning!



**Note to Instructor:** Explain the slide to the students by reading the scenario. Use this example to explain dynamic tasking.

What we have seen so far is pre-planned PKISR; the acquisition of information answering questions from the daily IAL. However, sometimes unexpected incidents occur, making it necessary to shift plans and re-task PKISR assets at short notice. When this occurs, it is the PKISR OPS, in close consultation with the Force U3-5, who decides to re-task, based on their situational understanding, the urgency of the dynamic requirement and the priority of ongoing pre-planned IAL acquisition tasks.

Using this slide as an example, a UAS asset might be re-tasked while it is flying a deliberate mission, especially if the new task is of a higher priority. Sometimes this is not possible due to, in this example, flight distance or remaining fuel. In which case, another asset must be considered. A dialogue between the PKISR unit and PKISR OPS is therefore needed to see what options are available.

When re-tasking, the PKISR OPS is also required to disseminate the results of the dynamic acquisition and one of the major challenges in such cases is to disseminate these results to the appropriate recipient. This requires experience at the PKISR OPS level.

Finally, the PKISR OPS communicates to the PKISR planner if any pre-planned tasking was not completed, so that these tasks can be re-scheduled into the next 24-hour IAL.

## Take Away

- PKISR OPS and U3/5 have roles and responsibilities for PKISR tasking.
- IALs and EEIs are essential to the PKISR tasking process.
- Tasking can be pre-planned or dynamic.

## Summary

Tasking is prepared by PKISR OPS, but tasking authority is usually at U3/5 as they are the Force HQ's staff function responsible for operations.

An effective IAP and IAL is essential to ensure effective taskings. These must be updated, relevant and prioritised.

Acquisition units need a high level of detail to achieve the necessary results. This entails indicators for reporting, and information about NALs, when reporting is needed and type of report.

# Lesson 3.8a



## UAS Unit

### The Lesson



#### Starting the Lesson

As a military intelligence officer, working in PKISR, you must be familiar with the PKISR assets available to you in the mission area so that you can employ them to full effect. This lesson will focus on **unmanned aircraft systems (UAS)**.



Slide 1



Lesson 3.8a  
UAS Unit

## Slide 2

### Contents

- Terminology
- Characteristics and capabilities.
- Strengths and limitations.
- Deployment Considerations.
- Tasking and Employing.



**Note to Instructor:** Ask the participants if anyone has experience working with UAS or other reconnaissance operations.

### Slide 3

## Learning Outcomes

- Describe UAS characteristics, capabilities, acquisition and analysis at Force, Sector and Battalion level.
- Explain the strengths and limitations of employing UAS units.
- Demonstrate how UAS units receive tasking, operates and are employed at FHQ and Sector level.
- Explain the differences between UAS and manned aircraft

Please take a moment to read what you are expected to be able to do at the end of the lesson.

## Slide 4



Here are the subject areas we will be covering in this lesson.

## Slide 5



This lesson is mainly based on the United Nations UAS Guidelines (2019), the Military Aviation Unit Manual (2021) and the Aviation Manual (2021). A deeper explanation about the subject can be found in these three publications.

## Slide 6

### Terminology

The following are the recognized terms used in the UN

• Unmanned aircraft (UA)	• Remotely piloted aircraft (RPA)
• Unmanned Aerial Vehicle (UAV)	• Remotely piloted aircraft system (RPAS)
• Unmanned Aircraft System (UAS)	• Aviation Safety

Key message: As UAS are widely employed across a variety of national and coalition operations, the terminology around the capabilities and the way in which they are described are relatively broad. It is important to make use of UAS terminology for the purpose of creating a clear, unambiguous UN picture when discussing the subject.

The following definitions are the basis for understanding UAS operations in a UN peacekeeping mission:

**Unmanned aircraft (UA).** The overall term for all aircraft that do not carry a human operator and can be operated remotely using varying levels of automated functions.

**Unmanned Aerial Vehicle (UAV).** A UAV is an unmanned aircraft that is remotely controlled by a UAV operator who is tasked with the overall responsibility for the operation and safety of the UAV but does not need to be trained and certified to the same standards as a regular pilot of a manned aircraft. This is typically the case for small and tactical UAS operated for military purposes or for commercially available quad copters employed for main operating base security and surveillance (such as ScanEagle, Shadow 200, etc.).

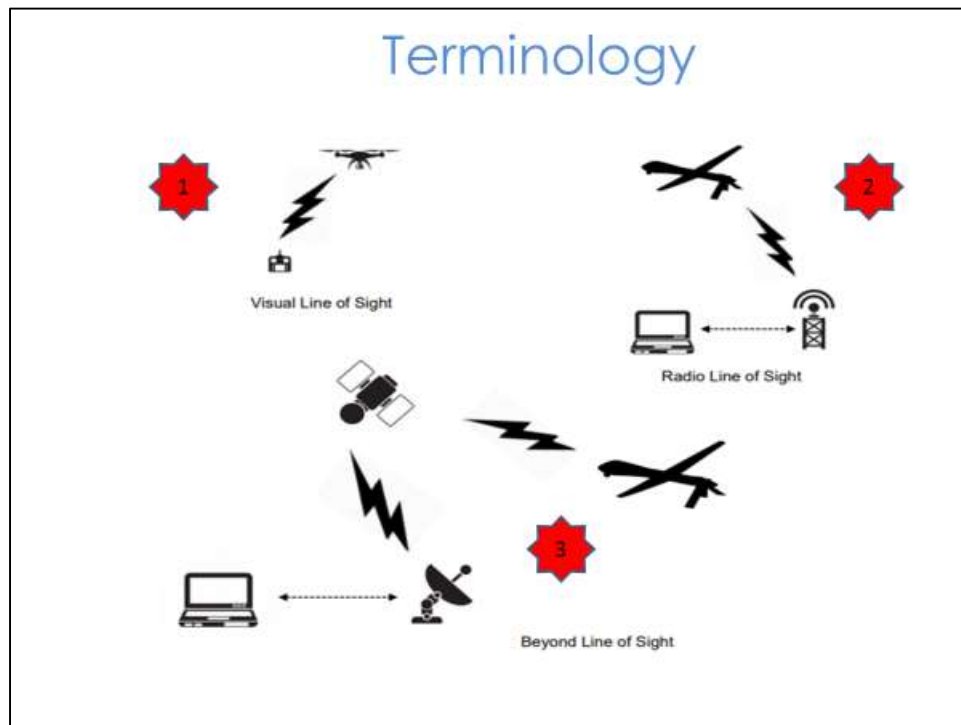
**Unmanned Aircraft System (UAS).** The overall term for a system whose components includes one or more unmanned aircraft, the supporting network and all equipment and personnel necessary to control the unmanned aircraft.

**Remotely piloted aircraft (RPA).** An unmanned aircraft that is controlled from a remote station by a pilot, who is tasked with the overall responsibility for the operation and safety of the RPA and who has been trained and certified to equivalent standards as a pilot of a manned aircraft as per civilian or military regulations. This is usually the case for all medium and high altitude / long-endurance RPA (e.g., MALE/HALE).

**Remotely Piloted Aircraft System (RPAS).** A UAS whose components include one or more RPA, the supporting network and all equipment and personnel necessary to control the RPA.

**Aviation Safety.** In the context of aviation, safety is the state in which the possibility of harm to persons or property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.

## Slide 7



Key message: There is additional terminology that requires clarification in the context of the UN's use of UAS. When discussing the ability to control the aircraft the term line of sight (LOS) is often used.



**Note to Instructor:** Some students might question the accuracy of the technical information below. Please note that technological advancements in ISR mean that some of the information provided below might be out-of-date. Remain flexible, and when necessary, ask the students to share their knowledge of any recent changes to the information being discussed.

Let us start explaining the differences between the various types of control. The term line of sight (LOS) refers to the way a Ground Control Station (GCS) communicates with a UAV to provide directional input and to receive any feed from the sensors. There are 3 types of 'line of sight' control depicted on the slide.

- First, 'visual LOS' is used to describe most Class I UAS as the aircraft pilot must be able to see the UAS at all times to safely control the asset and avoid collisions with other aircraft, people, buildings and terrain.
- Next, 'radio LOS' is used to describe a UAS that can go beyond the visual operator range, but is limited by terrain obstacles, just like a common radio station that we tune in our car.



- Finally, 'beyond LOS (BLOS)' refers to the need to use satellite uplinks and downlinks to communicate with the UAS and is almost exclusively used to refer to Class III UAS.

## Slide 8

### Characteristics

Class	Category	Recommended Employment	Normal Aprox Recommended Altitude (AGL)	Range	Examples
Class III	HALE	Strategic/National	< 65,000 ft	Unlimited (BLOS)	Global Hawk
	MALE	Operational/Theater	< 45,000 ft	Unlimited (BLOS)	Heron/Hermes 900
Class II	Tactical	Tactical Formation	< 18,000 ft	< 150 km (LOS)	Hermes 450/Falco Sperwer
Class I	Small	Tactical Unit	< 1,000 ft	< 50 km (LOS)	Scaneagle/Shadow 200 Luna
	Mini	Tactical Subunit (manual or hand launch)	<1,000 ft	< 25 km (LOS)	Raven/Aladin Puma/Skylark Heidrum V1
	Micro	Tactical Subunit (manual or hand launch, tethered)	< 400 ft	< 5 km (LOS)	WASP III/MICADO DJI Phantom 4, DJI Mavic Pro Hovermast 100

Key message: UAS are categorized to acknowledge certain characteristics.



**Note to Instructor:** Some students might question the accuracy of the technical information on this slide. Please note that technological advancements in ISR mean that the distinctions between different classes of UAS might not be as clear cut as outlined here. Remain flexible, and when necessary, ask the students to share their knowledge of any recent changes to the technical data on the slide.

We will go through each, in turn, using this slide, starting at the bottom with Class I.


- Class I UAS are small, mini and micro in size, and are only operated up to a limited altitude of not more than 1,000ft above ground level (AGL). Normally they weigh between 1-25kg and are operated within radio line of sight (LOS) of the operator. They have a maximum range of up to 50km. The main purpose of these UAS is to support operations at a tactical unit level, normally platoon or company, and up to a battalion level in case of the small UAS.
- UAS Class II UAS/RPAS normally have a maximum take-off weight of between 150-600kg and are equipped with a LOS data link. They are normally operated up to 18,000ft AGL, with a maximum range of 200km. Payload limitations and airworthiness restrictions may limit these systems to operations in restricted or special use airspace. Class II systems are normally used at the Sector level.

- Finally, UAS Class III UAS, typically MALE (Medium Altitude Long Endurance) and HALE (High Altitude Long Endurance), normally weigh more than 600kg and operate up to 65,000ft AGL. Theoretically, they have a greater range since they operate under a 'beyond line of sight' (BLOS) control system, however, they are limited by the satellite footprint. These systems are normally used at the Force level.

## Slide 9

### Sensor capabilities

- Full Motion Video (FMV)
- Synthetic Aperture Radar (SAR)



Key message: UAS cannot carry weapons while serving on a UN peacekeeping operation.

The overwhelming majority of UAS available in UN peacekeeping missions, whether commercially provided or as part of a TCC commitment, have imaging sensors as a core capability. Where operational requirements dictate, more complex sensors can assist in enhancing the peacekeeping-intelligence picture. Two specific sensors are full-motion video and synthetic aperture radar. Let us look at both capabilities.

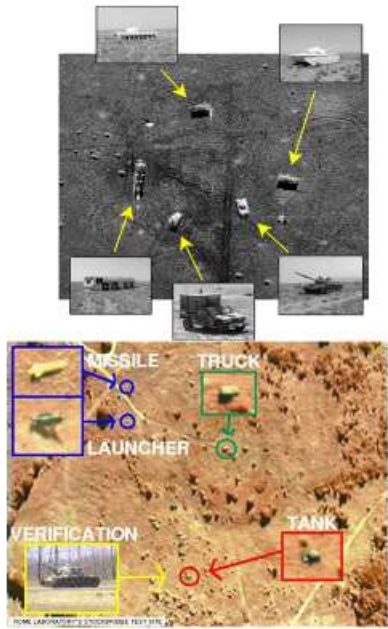
A **Full Motion Video** (FMV) sensor suite will likely have electro-optical (EO) for use during daylight and infra-red (IR) capabilities for day and night, which further enhances situational awareness as the IR sensors will highlight activity that is not visible to the human eye. Both sensors will be affected by adverse weather conditions such as cloud, dust and moisture, regardless of whether they are fitted to manned or unmanned platforms.

A **Synthetic Aperture Radar** (SAR) can operate in all weather. It provides a day/night imaging capability and in its more basic employment can support disaster relief through covering large areas, for example, by detecting flooding and assisting in prioritising humanitarian relief. More advanced techniques can highlight changes not detectable by the human eye, for example, dirt displaced by tyres or digging, potential improvised explosive device placements and changes in dispositions of forces.

## Slide 10

### Sensor capabilities

- Ground Moving Target Indicator (GMTI)
- Multi/hyper Spectral Imaging (MSI/HSI)



Other sensor capabilities are:

**Ground Moving Target Indicator (GMTI):** a specific capability of SAR, the GMTI provides a scanning mode to identify moving objects. The GMTI sensors are particularly useful at highlighting new and existing lines of communication through open areas and, when used in a surveillance mode over a period of time, can provide indicators of a certain activity, for example, possible smuggling routes.

**Multi/Hyper Spectral Imaging (MSI/HSI):** MSI and HSI sensors can exploit data across the entire electromagnetic spectrum. These advanced sensors can be particularly useful in UN peacekeeping missions by detecting chemical spills, gaseous effluent and objects concealed by artificial camouflage techniques. These more advanced sensors generate considerable volumes of data and therefore specialists and data storage infrastructure will be needed - this must be considered as part of the approach in procuring these capabilities.

## Slide 11





Moving onto the strengths and limitations of UAS.

## Slide 12

### Strengths

- Long endurance
- Enhancing situational awareness
- Supporting the protection of forces
- Reducing footprint in dangerous environments
- Verifying reports on displaced people



Key message: Students need to have a good understanding of the strengths and limitations of all ISR assets to help them determine which ones to use to acquire information. We will now look at some of the strengths that support the employment of UAS over other ISR assets.

**Endurance.** UAS tend to have a significantly longer endurance than manned aerial systems. They can provide uninterrupted support with a single asset by changing crew at a ground station mid-mission.

**Enhancing situational awareness.** A UAS can provide a prolonged presence over a target area. This continual presence can provide significant pattern-of-life assessment, including the movement of displaced civilians or the activities of an armed group.

**Supporting the protection of forces.** UAS can support the protection of forces by monitoring hostile areas, tracking the movement of armed groups, surveillance of critical infrastructure and reconnaissance of suspicious routes. The presence of a UAS could also provide an element of deterrence against an armed group that is considering conducting a violent activity if that group believes it is being monitored.

**Reducing footprint in dangerous environments.** UAS allows commanders to acquire information without putting UN personnel at risk.

**Verifying reports on vulnerable people.** UAS could be used to verify reports on IDP movements or the situation on IDP camps.

## Slide 13

### Limitations

- Cost
- Meteorological effects
- Constraint: operating near international borders



The diagram on the left illustrates the operational components of a UAS system. It shows a 'Control Station' on the ground connected via a 'Radio Link' to a 'UAS Aircraft' in flight. The aircraft's 'Operating Area' is defined by a green cube. Other labeled elements include 'Terminal Response', 'Transition Controller', 'RTE (Route)', 'Control Link', and 'Ground Station/Control Link'. The photograph on the right shows a white UAS aircraft with 'UN' markings on its fuselage, parked on a tarmac next to a hangar.

Now we will look to some limitations that must be considered before deciding to employ UAS.

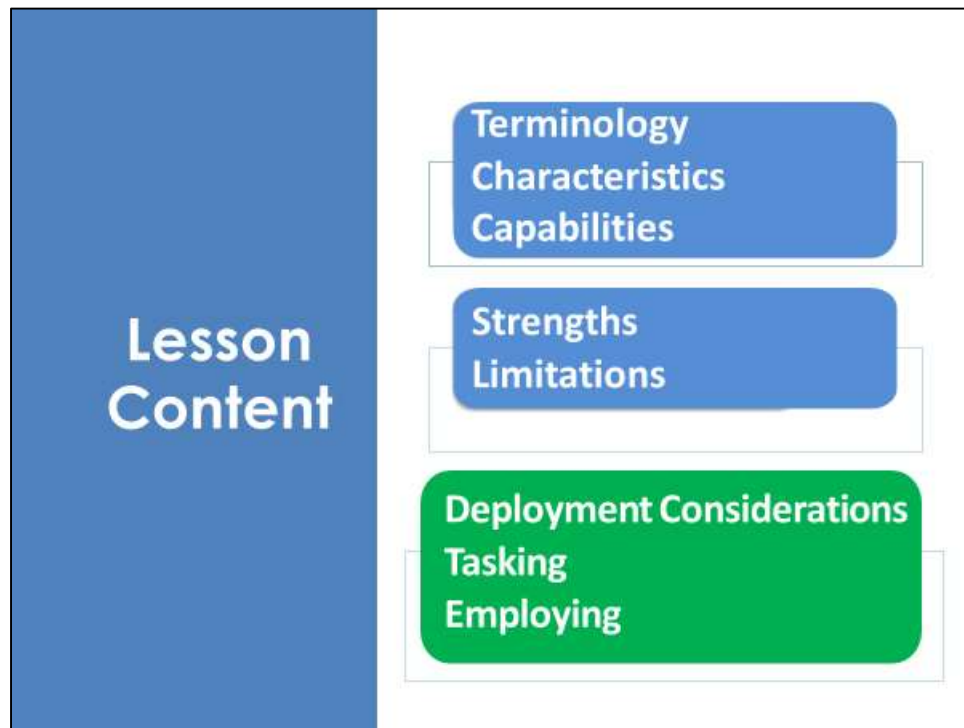
**Cost.** A Class III UAS is expensive and can come with up to 100 support personnel and equipment, which will probably include a ground control station, and possibly launch equipment and a recovery element. The cost of a UAS will inevitably impact on how many assets are available in a UN mission and how quickly they can be repaired or replaced following an incident due to mission operating budgets. As such, a UAS will probably be a scarce resource that must be managed to ensure efficient and effective employment.

**Meteorological effects.** Poor weather conditions have a greater effect on UAS since they tend to be smaller, lighter and slower than manned aircraft. High winds can affect take-off and landing as well as increase fuel consumption, thereby reducing the asset's time on task.

**Constraint - International Border Proximity Operations.** UAS are constrained from flying within 0.5 nautical miles of an international border without authority to do so. This is a constraint since a considerable number of the countries where UN peacekeeping missions are deployed have active borders, meaning that they experience activity that could affect mandate implementation, e.g., flow of refugees, movement of armed groups, transnational criminality, etc. Other proximity restrictions may also be in place, requiring specific authorisation for Mission leadership, e.g., up to 5 nautical miles from an international border.



## Slide 14



We will now move on to consider deployment considerations.

## Deployment Considerations

- Operational context
  - Understanding the task.
- Airspace considerations
  - Adherence to international and national rules.
- Command and control
  - Maintain high-level command, while delegating control.
  - Supported by CAVO and Chief PKISR.
- Endurance
  - Distance to the NAI will affect time on task.
- Range
  - Range can be affected by UAS command and control mechanism.



Key message: A variety of factors can impact the ability to successfully employ a UAS to meet the operational requirements of the mission.

The following should be considered when determining if the UAS is able to meet the needs of the mission.

**Operational Context.** You need to understand the context in which the UAS will be employed. The context is important as it lays the foundation for many of the following considerations. Therefore, understanding why a UAS is being deployed is important for information acquisition and reaching the intended outcome of the mission.

**Airspace Considerations.** UAS tasking will be regulated by the host nation and international bodies. For example, the host nation will dictate airspace considerations, including whether the UAS will be operating in segregated or unsegregated airspace. Likewise, international bodies such as the International Civil Aviation Organization (ICAO) maintain guidance materials, standards and recommended practices for the use of UAS, including operating near to international borders (as discussed earlier). The rules and regulations surrounding the use of UAS in a Mission area will be managed by the Mission's Aviation Section.

**Command and Control.** The overarching principle of command at the highest appropriate level and control at the most effective level should guide UAS planning. For example, UAS will be commanded at mission level and controlled at Force level, with tasking and control being delegated to lower formations when appropriate to do so.

However, there is no reason why a Class III UAS could not be employed to support a company level operation. In these circumstances, control of the tasking and sensors must be delegated to the battalion level to gain maximum benefit. UAS command and control will be supported by the Chief Aviation Officer (CAVO) and Chief PKISR. The C2 relationship is likely to be different for contracted UAS assets and those provided by TCCs.


**Endurance.** In general terms, the further the UAS launch site is from the area of operations, the less time the aircraft will have on-task over a named area of interest (NAI). This is due to the fuel it uses to fly the asset to the NAI. Different assets will have different endurance times.

**Range.** The tasking range of a UAS will be largely influenced by its command and control means. A UAS operating on 'Visual Line of Sight' has a much shorter range than one operating at 'Radio Line of Sight', and both are surpassed by 'Beyond Line of Sight' operations.

## Slide 16

### Deployment Considerations

- **Launch and recovery**
  - Time taken to launch and recover will vary between aircraft.
- **Communications**
  - Interference with other systems.
- **Logistic footprint**
  - Moving UAS can be difficult.
- **Data storage**
  - Data must be accessible.
- **Aircraft safety**
  - Adhering to national and/or international rules.



(Continuing on from the previous slide).

**Launch and Recovery.** Class I UAS usually can be hand-launched or operated using vertical take-off and landing techniques, whereas larger UAS will need more space to the extent that Class III UAS will require a prepared runway. Class II UAS sit somewhere in the middle, with some simply requiring a catapult system. Time taken to launch, recover and re-task will vary between aircraft.

**Communications.** The frequency range used must be taken into consideration during the deployment process because it is essential that frequency deconfliction occurs. For example, Class II and III use VHF radio communications that can interfere with other land and air operators, including civilian activities from the host nation.

**Logistic Support.** The class of UAS will tend to dictate the deployment footprint required to support the capability; from Class I UAS being organic to a military infantry company (and therefore all logistical support will be embedded within the unit) to a Class III UAS demanding up to 100 support personnel and airport level infrastructure. This is an important consideration should a UAS need to be moved to support operations elsewhere in a mission area – moving a larger UAS will take time and result in the asset being 'non-operational' for a period of time.

**Data Storage.** Data should be retained, stored and archived in such a way that it is possible to identify and retrieve the data at a future point in time. Any TCCs or

commercial companies that seek to introduce proprietary standards that cannot be integrated to the common database should be rejected at the earliest opportunity.

**Aircraft Safety.** UAS must meet the minimum aviation safety requirements relevant to the mission's airspace as demanded by the host nation. Therefore, Class II and III UAS must be fitted with a Traffic Collision Avoidance System. Tactical systems (typically Class I) must operate within a Restricted Operating Zone to limit the risk of collision between UAS and other flying platforms, for example, helicopters.

## Slide 17

### Tasking

- UAS mission management:
  - Mission Air Operations Centre (MAOC), led by the Mission's Chief Aviation Officer.
- Class II and III UAS/RPAS – U2 (ATO)
  - The ATO is a MAOC responsibility
- Class I UAS – U2 (ATO) or SOPs



Key message: Most UN peacekeeping missions will have a civilian/military coordination system to manage aviation resources, including UAS effectively; this is achieved through the Mission Air Operation Centre (MAOC).

The Chief Aviation Officer (CAVO) is responsible for all aspects of air operations, including the overall management of aircraft (including UAS) assigned to the Mission.

All operations of the Class II and III UAS/RPAS will be conducted in direct response to tasking by the U2 and subsequently by an Air Tasking Order (ATO) through the Mission chain of command. The issuance of an ATO will authorize the flight and provide confirmation of airspace/air traffic management arrangements.

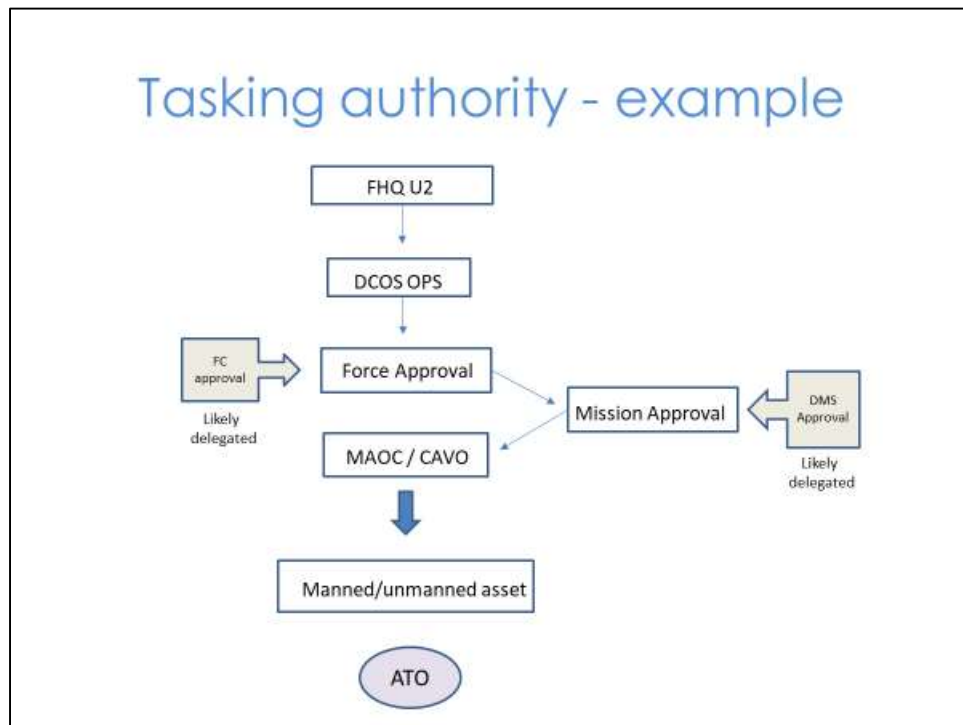
Therefore, an information requirement from an Information Acquisition List (IAL) to be acquired by a Class II/III UAS/RPAS must be linked to an ATO. A process / standard operating procedure must be in place to ensure coordination between the Force HQ and the MAOC so that the tasking can be achieved effectively. Mission Air Ops has the overarching authority regarding the tasking and flight patterns of UAS/RPAS and the PKISR operator must work within that framework.

The range, endurance and sensor suite will make mini and micro UAS only suitable for battalion-level operations.



**Note to Instructor:** *The air tasking order contains the task and flight information for all tactical, combat or surveillance missions.*

## Slide 18



Key message: This slide depicts how a mission **might** approve the tasking of aerial assets, either manned or unmanned. In other words, steps through which the tasking request should go before an ATO is issued.

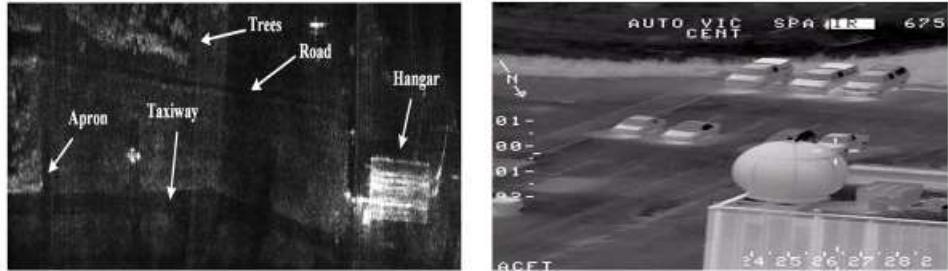
The Information Acquisition List (IAL) will inform the daily tasking of UAS in a mission area. Within the IAL, certain acquisition requirements will have been assigned to UAS units. Those requests will be passed to Force DCOS (Deputy Chief of Staff) Ops who will provide an initial filter to ensure the effective tasking of UAS assets and that they support current and future military operations as well as other mission priority acquisition requirements.

The tasking request will then be sent for approval to the Force Commander before being sent to the Director of Mission Support (DMS). Both individuals are likely to delegate this responsibility to a subordinate. For the Force Commander, this is likely to be the DCOS Ops. For DMS, it is likely to be the Mission's Civilian Aviation Officer (CAVO). Finally, once approved, CAVO will include the task in the daily ATO.



## Tasking

- Commander's intent (mission goals)
- Clear reporting lines
- Command and control



Key message: Certain information is essential when tasking a UAS - the following three pieces of information are mandatory:

**Commander's intent** (mission goals). The ISR objective of the mission must be clear to the operator. If possible, a briefing on the situation and real-time communication should be provided to assure that the UAS controller understands the PKISR analyst's needs. For example, surveillance on UN Base Villa perimeter from 1800 to 0400 between D+1 and D+3, identify mooring points on the riverbank between the villages of Mai and Jio on the Apu River, etc.

**Clear reporting lines.** The situation can change during the mission and communication between UAS operator and PKISR analyst may not be possible. Therefore, dissemination of the information must be explicit in the ATO, for example, reporting that the base perimeter, from the previous scenario, is secure.

**Command and control.** The chain of command and equipment available should be defined before the mission. For example, contact between U2 and UAS operator is going to be primarily by mobile, using TETRA radio as an alternative. If communication fails, the UAS operator should proceed as per the ATO as the situation allows. There can be no doubt who has control of the asset.

## Employment of Class II / III UAS

- Tasking, by U2, is through an Air Tasking Order (ATO).
- Flights operate under UN aviation standards.
- Understand the command and control measures associated to the employment of UAS.
- The Mission is responsible for the overall airspace management coordination plan.



Key message: The management and employment of UAS/RPAS within a peacekeeping mission will be done in accordance with UN Military Aviation Unit Manual, the UN Department of Operational Support's Aviation Manual, the UN Department of Safety Aviation Manual, the UN Aviation Safety Manual and the Aviation Risk Management Policy.

Class II and III UAS/RPAS aviation units will be tasked by the U2 following the mission air assets tasking procedures, coordinated by the Mission's Air Operations Cell (MAOC - Air Ops). So, although the U2 has operational authority over the UAS, its operation must occur inside a broader environment with specific rules and regulations; it is the Air Ops' job to ensure the UAS flight operates under UN Aviation Standards.

Ensure that you understand the C2 arrangements for all UAS assets. Direction will be found in the UN Authority, Command and Control in UN Peacekeeping Operations policy as well as individual Mission standard operating procedures. Aspects that might determine where the responsibility lies, including whether the UAS is available for military and/or civilian use and the conditions agreed between UN HQ and the UAS provider, which could be a military unit or a civilian contractor.

Finally, the mission is responsible for overall airspace management, including aviation safety. A close relationship between the Force HQ and the MAOC is essential for seamless UAS operations. The mission will coordinate all airspace management with the host nation authorities.

## Slide 21

### Employment of Class I UAS

- Operations within 8 Km from an airfield or heliport are restricted.
- Operational altitude is restricted to 400 feet above ground level.
- Visual Line of Sight (VLOS) operations only.
- Night operations need coordination with the Mission's Aviation Section
- Must not be flown close to other aircraft



Key message: All UAS operators, civilian and military, are required to abide by existing requirements, coordinating all UAS operations with the mission aviation authorities.

These are the main recommendations concerning tasking and employment of Class I UAS (deployed at the lower tactical level, i.e., battalion):

- Operations within 8 Km from an airfield or heliport are restricted. Operations are only allowed with prior coordination with the Mission Aviation Section. If the operations are conducted within the area of an airfield/heliport with no Aviation Section presence, Local Air Traffic Control authorization will be required (if available in the Mission area). However, military mini/micro UAS may continue to operate close to airports and heliports under urgent operational requirements.
- Class I UAS have a maximum operating altitude of 400 feet above ground level (AGL) unless a different Restricted Operating Zone (ROZ) has been previously arranged with the mission authorities.
- Class I UAS can only operate under Visual line-of-sight (VLOS).
- Night taskings are to be coordinated by the Mission's Aviation Section.
- Finally, Class I UAS must not be flown close to an aircraft, in any case yield right of way to other aircraft.

## Differences between UAS and manned ISR aircraft

- Same sensors – EO and SAR
- Endurance
- Response time - speed over distance
- Human engagement allows more flexibility over target areas
- Detection



Key message: UN military aviation PKISR assets consist of three types of units: rotary wing, fixed wing (both manned) and UAS.

This slide considers the similarities and differences between UAS and manned aircraft.

- **Same sensors.** regarding to payload, manned aircraft can use the same payload as UAS, mainly EO and SAR equipment's.
- **Endurance.** This characteristic is related to the inability of aircraft to fly indefinitely, as they need to refuel more often than UAS and change crews. UAS can change the operator without landing, the same is not possible with Manned Aircraft.
- **Response Time.** in general terms, a manned aircraft can travel faster than a UAS. However, this parameter can be affected by the time it takes to prepare a manned aircraft to be launched. As such, the deployment time of a manned aircraft needs to be known before such assets are considered for dynamic tasking.
- **Human Engagement.** Manned aircraft have more flexibility on the mission than UAS, due to the presence of a pilot on board the asset. A UAS will always be dependable on communication with a ground station to perform its mission, whereas a manned aircraft can operate on radio silence / loss of communication once a crew is briefed on the mission objectives.
- **Detection.** It is more difficult for those on the ground to perceive that they are being observed by a UAS compared to a manned aircraft, as they emit less noise and are generally smaller than manned aircraft.

In summary, and in general terms, the main difference between manned and unmanned systems are speed (in favour of the manned) and endurance (in favour of UAS). The PKISR Plans team should take this into account when assigning tasking as they are both equally suited to the same tasks.

## Take Away

- PKISR payload can vary
- Assign the most appropriate ISR asset to the information requirement
- Coordination between Force HQ and MAOC is essential
- Understand the different types of manned and unmanned aircraft – this will help dynamic tasking

## Summary

Students should take away the following key points:

PKISR aircraft can carry different payloads that will produce diverse products. It is important to define first what information is needed in order to demand the correct PKISR manned or unmanned asset.

Manned/unmanned aircraft will not be the best solution for every mission – it is important to understand the strengths and limitations compared to other ISR assets.

Although the U2 has operational authority over the UAS, it is the Mission's Air Operations Cell (MAOC - Air Ops) that oversees the flight authorization. Close coordination in mission is essential for effective tasking and employment.

Understand the different types of unmanned and manned aircraft and their associated strengths and weaknesses – knowing which assets to be tasked during times of crisis will speed up response times.

# Lesson 3.8b



## Human Peacekeeping-intelligence

### The Lesson



#### Starting the Lesson

As an MPKI officer, working in PKISR, you must be familiar with the PKISR assets available to you in the mission area so that you can employ them to full effect. This lesson will help you get acquainted with the **Human Peacekeeping-intelligence (HPKI)** unit.

## Slide 1



### Lesson 3.8b Field HPKI Unit



## Slide 2

### Contents

- Terminology, characteristics and capabilities.
- Strengths and limitations.
- Tasking and employment considerations.



**Note to Instructor:** Ask whether any of the students have been involved with human peacekeeping-intelligence (in a UN Mission) or human intelligence (in their national context) in general. See whether they would be willing to share their experiences with the class throughout the lesson.

## Learning Outcomes

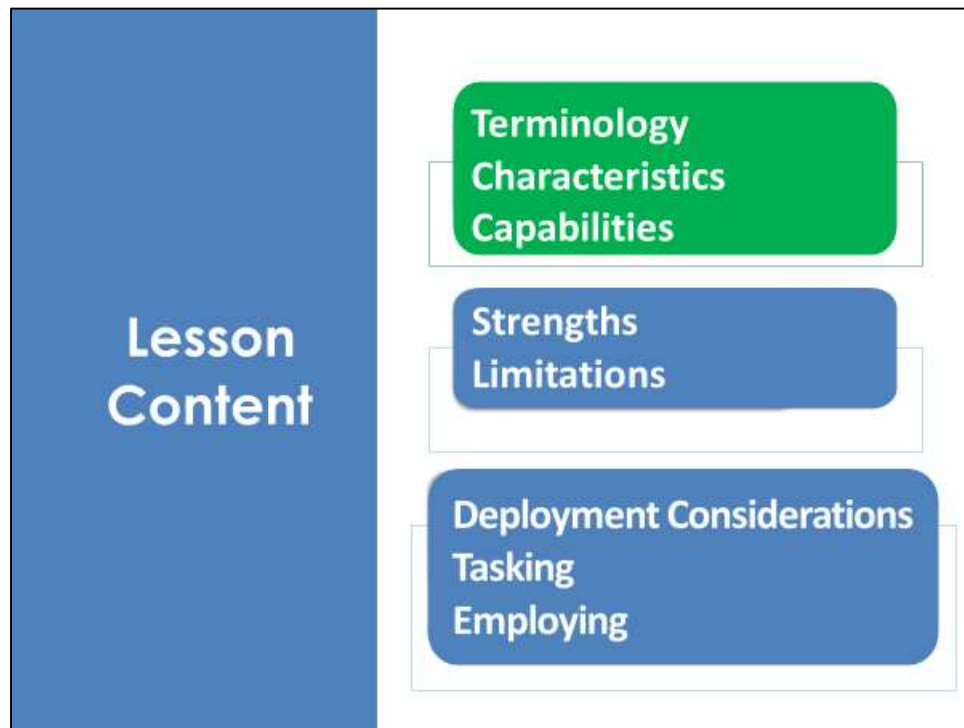
- Explain the characteristics and capabilities of Field HPKI Units.
- Explain the strengths and limitations of employing Field HPKI Units.
- Demonstrate how Field HPKI units receive tasking.



**Interactive.** *Ask the students to explain what human peacekeeping-intelligence is.*

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

## Slide 4



Here are the subject areas we will be covering in this lesson.

## Slide 5



This lesson is mainly based on the UN's Acquisition of Information from Human Sources for Peacekeeping-Intelligence (HPKI) Guidelines and the Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff handbook (PKISR HB). The purpose of the HPKI guidelines is to provide a legal and operational framework for and to facilitate the safe acquisition of information from human sources for peacekeeping-intelligence (referred to as "HPKI").



**Note to Instructor:** Students should be aware that UN HPKI may differ significantly to their national practices. The UN's approach to HPKI will be outlined during this lesson, based on the reference documents shown on this slide. It is important that the correct terminology be used at all times.

## Slide 6

### HPKI terminology (1)

- **HPKI** is the process in which information is acquired from human sources in a structured, lawful and non-clandestine manner.
- A **Component HPKI cell** refers to a military, police or civilian HPKI cell that is the mission's focal point for the planning and implementation of HPKI operations.
- A **human source** refers to an individual who is willing to share information with UN HPKI personnel.

Key message: It is important to know the main terminology used by the UN in HPKI, which might differ from your national experience of employing human intelligence (HUMINT).

Let us go through each term listed on the slide:

- **HPKI** is the process in which information is acquired from human sources in a structured, lawful and non-clandestine manner.
- A **Component HPKI cell** refers to a military, police or civilian HPKI cell that is the mission's focal point for the planning and implementation of all HPKI operations.
- A **Human source** refers to an individual who is willing to share information with UN HPKI personnel. Potential HPKI sources include hostile, neutral, and friendly individuals. Categories of HPKI sources may include refugees and Internally Displaced Persons, the local population, friendly forces, non-state actors, other mission partners and non-governmental organisations.

## HPKI terminology (2)

- **Human source handlers** are qualified civilian or uniformed UN personnel trained in HPKI techniques, specifically deployed for and tasked with the acquisition of information from human sources.
- **Human source protection** refers to the necessary measures to ensure the human source's physical safety and security before, during, and after a meeting or contact, and maintaining the confidentiality of the human source's personal details and of the fact that the source provided information to the United Nations.

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

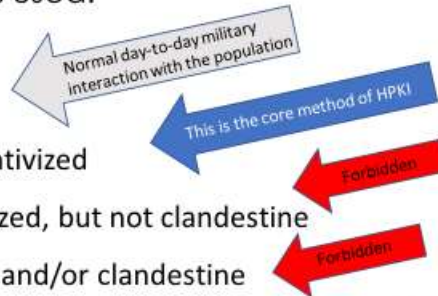
**Human source protection** refers to the necessary measures to ensure the human source's physical safety and security before, during, and after a meeting or contact, and maintaining the confidentiality of the human source's personal details and of the fact that the source provided information to the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

## Slide 8

### Characteristics (1)

The acquisition of information from human sources can be generally divided into four categories, based on the acquisition methods used:

- Undirected, casual
- Directed, but un-incentivized
- Directed and incentivized, but not clandestine
- Directed, incentivized and/or clandestine



Key message: The acquisition of information from human sources can be generally divided into four categories, based on the acquisition methods used. **Only the directed un-incentivised method is used and permitted in PKISR.**

Let us go through each in turn:

- **Undirected, casual.** Casual, undirected acquisition refers to the gathering of information from human sources, but not in response to specific information requirements (IRs). Examples would include information gained from casual interactions with the local population by UN military units on patrol. **This is not HPKI** and is performed by any UN personnel on a daily basis while they are engaging with any interlocutor.
- **Directed, but un-incentivized.** This category refers to the same type of acquisition methods as above but conducted as part of the mission's PKI cycle. In other words, information is acquired in response to peacekeeping-intelligence requirements developed at the mission level. This acquisition method requires a more active role in order to direct the source to acquire the needed information. **This is the core method of HPKI.**
- The bottom two methods shown on the slide for acquiring HPKI **are forbidden in UN peacekeeping operations** since they do not align to PKI principles. You will recall from Module 2 of the course that UN forces do not use incentives to acquire information, nor do they undertake clandestine operations.

Mission entities shall not resort to HPKI to acquire information, unless exceptionally authorized to do so by the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM).



## Characteristics (2)

- A mission-level HPKI coordination cell.
- HPKI only considered if acquisition requires human interaction to answer an IR.
- HPKI operations are not single actions.
- HPKI operations are conducted in a non-clandestine manner



Key message: All HPKI operations will be planned, managed and coordinated by a single HPKI cell at the mission level, to avoid, for example, the duplication of efforts, having undesired multiple contacts with the same source from different human source handlers. You might find that some UN peacekeeping missions will not initiate a HPKI cell until they have the assets available to them.

HPKI activities should only be considered if acquisition from other sources has proven impossible or inconclusive, due to the risks involved with conducting HPKI, both for UN personnel, and human sources and their families. It is worth noting that information acquired through HPKI operations is not inherently more valuable than other sources of information.

HPKI operations are never carried out by an individual operating alone. The basis for HPKI operations is that a minimum of two people are required for HPKI operations within a permissive environment. This requirement would need to be supplemented by interpreters and force-protection forces from an assigned UN military unit. You should always consider female operators within a HPKI team since they will provide a different perspective on gathering information, plus they might be able to engage better with female human sources.

As discussed, and reflecting PKI principles, HPKI is to be conducted in a non-clandestine manner, which is likely to be different from national human intelligence characteristics.

## Slide 10

### Capabilities

- Set up networks of human source.
- Interaction with multiple entities.
- HPKI operations are sensitive and require a high-degree of operational security.



Key message: The HPKI Team's capabilities must be understood by PKISR personnel so that the Acquisition Management Cell is able to suggest employing the asset to its maximum potential.

First, HPKI will develop a number of human sources to cover all required thematic and geographic areas. The team can establish interpersonal contact to obtain data about the threats to the population, as well as the intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities of armed or criminal groups operating in their area.

Secondly, HPKI provides access to multiple kind of sources (from the civilian population, and NGOs, to members of armed and criminal groups).

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

## Slide 11



Moving onto the strengths and limitations of HPKI.

## Slide 12

### Strengths

- Direct engagement with human sources.
- Can acquire information about intentions, morale and relations between actors.
- Low profile.
- Low cost compared to other ISR disciplines.



Key message: It is important for PKISR staff officers to know the strengths and limitations of ISR disciplines to acquire information.

We will now look at some of the strengths of employing HPKI over other PKISR capabilities.

HPKI teams can engage directly with human sources to acquire specific information. Physical interaction allows HPKI to gauge a source's body language, temperament, etc. which can help to determine the reliability of the information. Such interaction cannot be achieved by other PKISR assets. For example, a UAS unit can show the locations of a convoy, but HPKI can acquire information on the individual leading the convoy, the contents of the convoy, etc.

HPKI teams are difficult to be monitored by hostile actors due to their low profile. This profile allows teams to meet sources without drawing undue attention to their activities.

Finally, HPKI is a low-cost capability compared to other more technical PKISR assets.

## Limitations

- It takes time to develop a network of human sources
- Reliant on others for force protection
- Language and cultural barriers
- Rarely able to react to time sensitive acquisition
- Limited resource

We will now look at some of the limitations of employing HPKI over other ISR capabilities.

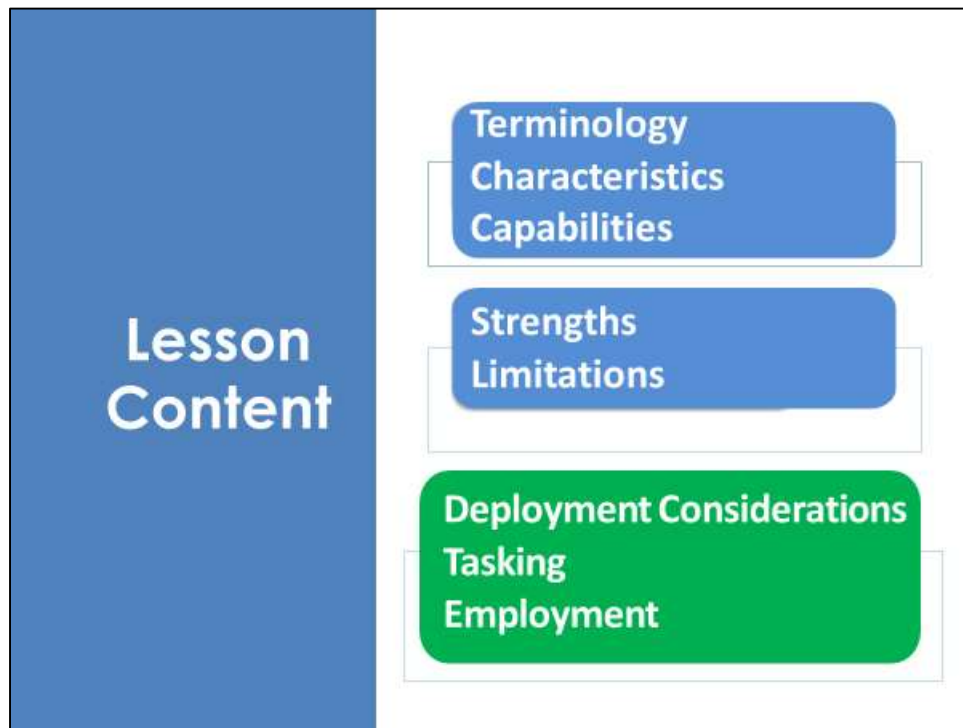
Developing a network of human sources takes time – identifying the sources to determining their credibility and reliability will often take months to achieve. As such, HPKI units need more time in a mission area than other PKISR assets to be fully operational. There will also be a need to double check the continuous reliability and credibility of human sources after a period of time as they could act as double agents.

HPKI activities are limited by a series of factors including force protection and language capabilities. HPKI teams are often unable to provide the necessary force protection to perform their duties and therefore rely on others for this capability. Likewise, HPKI will often require interpreters to engage with their sources. Such support needs to be planned and coordinated, which adds to the time it takes to task HPKI assets.

As already said, it can take considerable time to develop sources with access to the sort of information required by the mission, and therefore HPKI should not be considered a quick answer to acquiring information. Often HPKI teams will not be able to respond to short notice tasking (and immediate reporting) and therefore it is better to align their activities around thematic issues, for example, trends associated with the protection of civilians. That said, a mature, confident source might be able to react to time-sensitive tasking and could respond to specific questions. The HPKI cell would be best placed to advise on such issues.

Finally, HPKI is a finite resource. Currently, there are no functioning HPKI teams in UN PKO – the intent is to generate such teams for peacekeeping missions; however, this will take time and will likely only be in certain mission areas.

## Slide 14



We will now move on to consider the tasking and the employment of HPKI units.



**Interactive.** Before showing the next slide, ask students what they think HPKI units could be tasked to do. Use the next slide to share some possibilities.

## Slide 15

### Possible tasks

- Monitoring
- Screening
- Contact Operations
- Operational Recruitment
- Document exploitation

Key message: HPKI operations refer to the planning and safe execution of an operation in a peacekeeping mission to elicit information from human sources.

HPKI Teams could be tasked with:

- **Monitoring** and **screening** areas, facilities, materials, equipment or personnel of interest in an operations area.
- Conduct **contact operations** with sources to gather information.
- Perform **operational recruitment** of interpreters in languages of interest to the mission.
- Perform **document exploitation** to contribute to the acquisition of targets and manage the risk of search actions and/or an operation.



## Tasking Considerations (1)

- Employed when other assets have failed to acquire information or the information is inconclusive.
- Strictly to support Information Acquisition Plan and Intelligence Support Plan.
- Security of UN personnel and sources.
- Gender requirements.



Key message: Students should consider certain operational considerations before deciding to use HPKI to acquire information.

HPKI activities should only be considered after careful determination by the Mission Peacekeeping-Intelligence Coordination Mechanism that the acquisition of the necessary information needs to be acquired by this capability. In other words, HPKI should only be considered when other options have failed.

All HPKI operations should only be conducted in support of the IAP and in accordance with the Mission Peacekeeping-Intelligence Support Plan, which will include adherence to UN principles and rules.

HPKI planning must always prioritise the safety and security of mission personnel (including HPKI personnel) and their human sources. You may recall from Module 2 that UN policy requires the mission to take particular care not to expose any human sources or potential sources of information to harm. The HPKI cell will consider this issue when planning HPKI operations.

An HPKI unit must have the capacity to deploy both men and women handlers. Some human sources may only like to engage with men, others only with women. As such, HPKI teams should be configured in such a way to acquire the necessary information.

## Tasking Considerations (2)

- Non-clandestine manner.
- Structured to ensure that source coverage exists in all information gaps.
- HPKI sources cannot be Host State employees or affiliated personnel.
- No amount of money will be paid, nor gifts offered, to HPKI sources, or their relatives, in remuneration for information.



In line with the DPO PKI Policy, all HPKI operations must be conducted in a non-clandestine manner. HPKI personnel should neither conceal the fact that they work for the UN, nor, under any circumstances, operate under fake identities. In particular, information requests to national peacekeeping-intelligence contacts must be carefully examined to ensure that they do not risk instigating any national human rights violations, notably by requesting information that is likely to be gained from torture or other human rights violations.

HPKI must be structured in a way to ensure that source coverage exists in priority thematic and geographic areas to support the Mission's decision making.

HPKI sources cannot be Host State employees or affiliated personnel.

Finally, PKI policy stipulates that no amount of money will be paid, nor gifts offered, to human sources, or their relatives, in remuneration for information. It is strictly forbidden to trade something that the source wants for information.

## Employment (1)

Prior the employment, the HPKI Cell must ensure that:

- Operation aligns to the IAP.
- Threats and risks are understood.
- Deconfliction with other Mission actors.
- The engagement is planned.
- Possible contingencies are prepared and rehearsed.



During the employment, the HPKI Cell must ensure that:

- The engagement (conversation) achieves the planned goals and adheres to UN policies.
- The safety of the UN personnel and the sources.

Key message: The concept of planning, implementing and reporting on HPKI activity is like that of other PKISR assets. However, it is useful for students to understand some of the considerations considered when employing HPKI assets.

PKISR Plans should coordinate closely with the HPKI Cell to review the prioritised information requirements to identify which acquisition topics could be supported by the HPKI teams. The HPKI Cell will manage the detailed tasking of HPKI assets.

Some of the issues that need to be considered are listed on the slide.

**Prior to employment, the HPKI Cell** must ensure that:

- The threat in the area is fully understood.
- A full operational risk assessment is carried out.
- The operation is deconflicted with other UN elements.
- Adequate protection or safety/security measures are in place.
- The engagement (conversation) is planned in line with best practices.
- The information acquisition is in line with the applicable IAP.
- All possible contingencies are prepared and rehearsed.

**During the employment, the HPKI Cell** must ensure that:

- The conversation elicits, as much as possible, the required information (based on the IAP).

- UN policies are adhered to, and the source is always treated with dignity and respect.
- The safety of UN personnel and sources is maintained.

## Employment (2)

After deployment, the HPKI Cell must:

- Collate data using a dedicated HPKI system.
- Grade the source.
- Disseminate information according:
  - timeliness, relevance, brevity and interpretation.

Source Reliability		Credibility of Information	
Rating	Evaluation	Rating	Evaluation
A	Reliable	1	Confirmed
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtfully true
E	Unreliable	5	Improbable
F	Cannot be judged	6	Cannot be judged

Information acquired during HPKI operations should be collated on a stand-alone HPKI component collation system, which will be separate from the peacekeeping-intelligence regular collation system, due to the sensitive nature of HPKI.

All human sources will be graded for reliability and information, for credibility, using an agreed UN chart shown on the slide. Every item of information must be rated in the form of an alphanumeric code whereby the 'letter' indicates the reliability of the source (the table on the left) and the 'number' indicates the credibility of the information (Table on the right). Such grading helps decision-makers determine how useful the information is to support decision making.

HPKI handlers should not grade their own sources. They tend to grade too high. For this reason, HPKI cells should have an impartial mechanism in place to ensure the impartial grading of sources.



**Interactive.** Ask students to discuss their thoughts on information that had been graded as D,3. How would the information be used by decision makers? What could decision makers do to confirm the information?



**Note to Instructor:** Highlight those ratings of 'F' for the source reliability and 6 for the credibility of Information should not be dismissed without consideration. New sources may attract such grading since their credibility and reliability may not have been determined at that point.

Information acquired by a HPKI cell should be disseminated in the same way as other peacekeeping-intelligence is disseminated. The following dissemination principles should be adhered to whilst protecting the source:

- **Timeliness.** Acquired information must be delivered in a timely manner so planners and decision makers can act rather than react.
- **Relevance.** Is determined by the needs of the recipients as defined in the Information Acquisition Plan.
- **Brevity.** Reports must be kept as brief as possible, but at the same time include everything that the recipient needs to know.
- **Interpretation.** Wherever possible, all facts must be correctly evaluated, and their significance interpreted before dissemination.

## Take Away



- HPKI is a directed, non-clandestine and un-incentivized activity
- HPKI can fill information gaps that other sensors cannot acquire.
- HPKI Cell must ensure the safety of UN personnel and sources throughout operations



It is important that you understand how HPKI can be employed, including the strengths and limitations of employing such assets, and the rules governing the use of such assets.

## Summary

It is important that you understand how HPKI can be employed, including the strengths and limitations of employing such assets, and the rules governing the use of such assets.

# Lesson 3.8C



## Long Range Reconnaissance Patrol

### The Lesson



#### Starting the Lesson

The Mission will not necessarily have access to a wide variety of acquisition capabilities and must make the best use of those available. This lesson will concentrate on the long-range reconnaissance patrol.

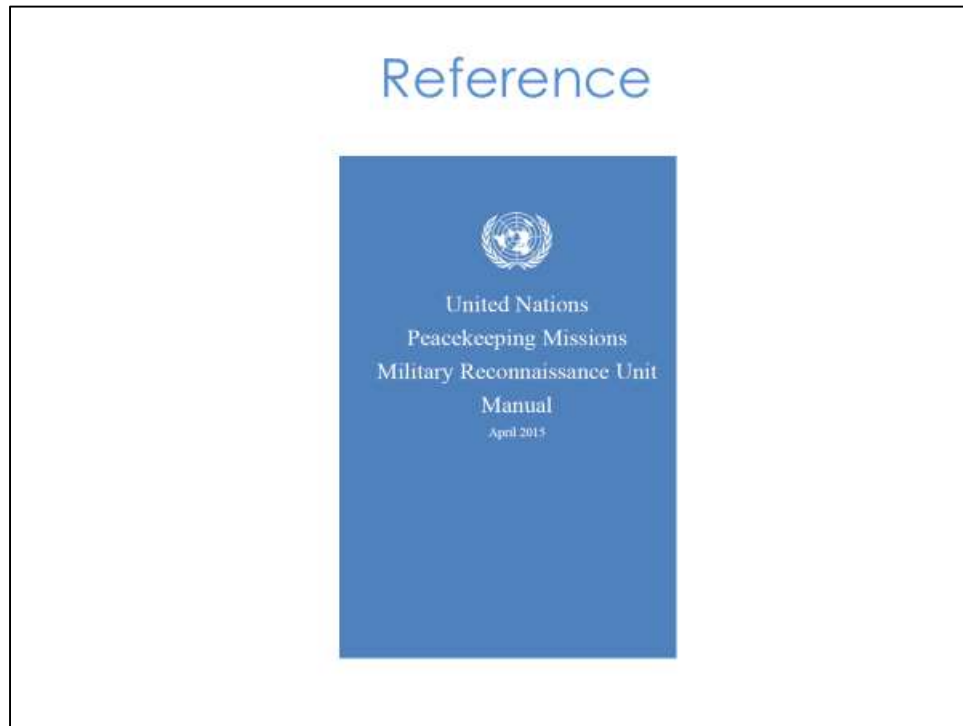


Slide 1



Lesson 3.8c  
Long Range  
Reconnaissance Patrol  
(LRRP)

## Slide 2



The main reference for LRRP is the UN Peacekeeping Missions Military Reconnaissance Unit manual presented in this slide.

### Slide 3

## Contents

- Characteristics and capabilities.
- Strengths and limitations.
- Employment considerations and tasking.



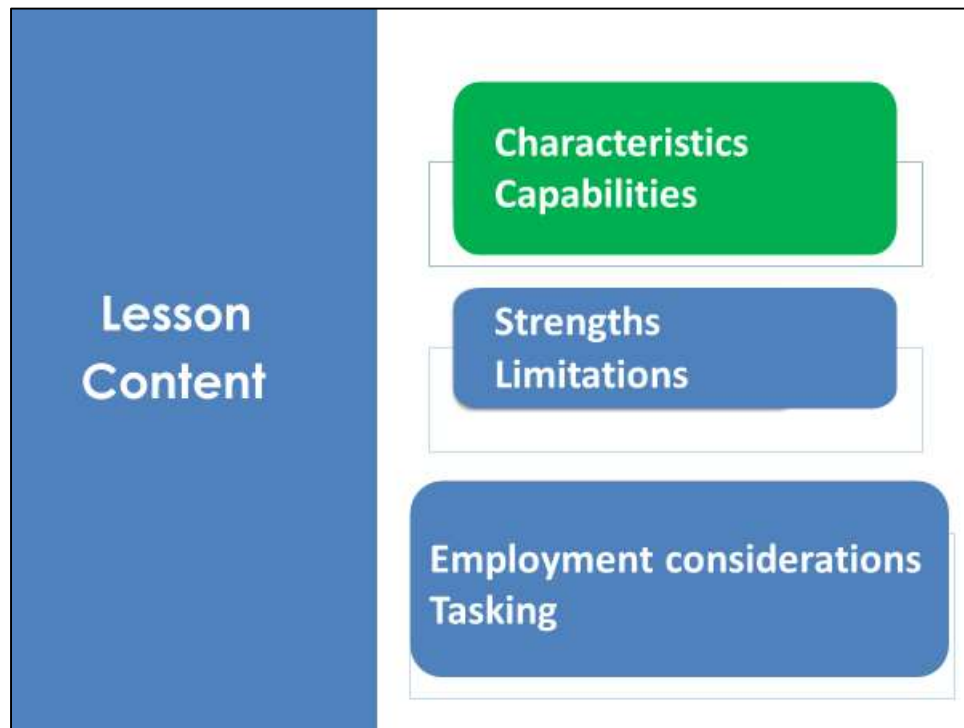
**Interactive.** Ask whether any of the students has experience working with an LRRP – use any local expertise to support the lesson content.

## Learning Outcomes

- Describe Long Range Reconnaissance Patrol (LRRP) unit characteristics, capabilities, acquisition and analysis at FHQ, Sector in Battalion Level.
- Explain strengths and limitations of employing LRRP units.
- Demonstrate how LRRP units receive tasking, operate and are employed.

Let us review the learning outcomes before we start this lesson. Please take a moment to read and understand what you are expected to be able to do at the end of the lesson.

## Slide 5



I will break the lesson into 3 component parts as shown here on the slide.

## Slide 6

### Characteristics

- Lightly armed.
- Operate in small packets.
- Task organized for specific missions.

LRRP units tend to have the following characteristics:

**Typically, light-armed.** An LRRP is not designed to conduct offensive operations in the UN peacekeeping context. It is a unit designed to acquire information. That said, the unit would be sufficiently armed to provide force protection and, if necessary, protect civilians that it might encounter that are facing a physical threat (based on the UN mandate).

**Operate in small packets.** An LRRP should be a mobile and flexible unit that is able to move across an area of operations acquiring information in support of the IAP. The patrol should not be too large, especially when conducting surveillance operations or other discrete tasks. Packets should maintain good communication among themselves.

**Task organised.** An LRRP unit comprises various capabilities, which can be grouped together in different ways to meet the acquisition requirements. An LRRP's configuration would depend on the task at hand.

## Slide 7

### Capabilities (1)

- Acquisition, collation and dissemination of information.
- Situational awareness and reporting.
- Command, control and communications.
- Organic firepower.
- Mobility.



Key message: The UN LRRP is an efficient and versatile organisation with a multifaceted capability due to its task-oriented composition of specialized personnel and equipment. The unit accomplishes its tasks through a combination of dismounted, mounted and aerial reconnaissance operations, including the use of tactical UAS.

LRRP capabilities are:

- **Acquisition, collation and dissemination of information.** Using its technological capabilities, an LRRP is able to provide timely responses to information requirements as a result of its acquisition, staff processing and ability to disseminate information rapidly.
- **Situational awareness and reporting.** The LRRP can provide the commander with a greater understanding of the operational environment, thereby supporting the decision-making process. The unit is also capable of providing early warning by means of timely, accurate and relevant information. Such reporting relies on the unit maintaining effective voice and data communications with the HQ.
- **Command, control and communications.** The LRRP tailors its task organisation by deploying modular and scalable assets in response to the mission requirement. Therefore, the unit must be capable of deploying a tactical headquarters to ensure clear channels of command and control for all subordinate elements.

- **Firepower.** An LRRP employs its organic and attached weapons to protect itself and, where necessary and mandated to, civilians.
- **Mobility.** The unit can move tactically and non-tactically, to conduct robust reconnaissance tasks throughout the mission area of operations.



## Slide 8

### Capabilities (2)

- Force protection.
- Sustainment.
- Interoperability.
- Civil interaction.



(Continuing with the capabilities associated to the LRRP).

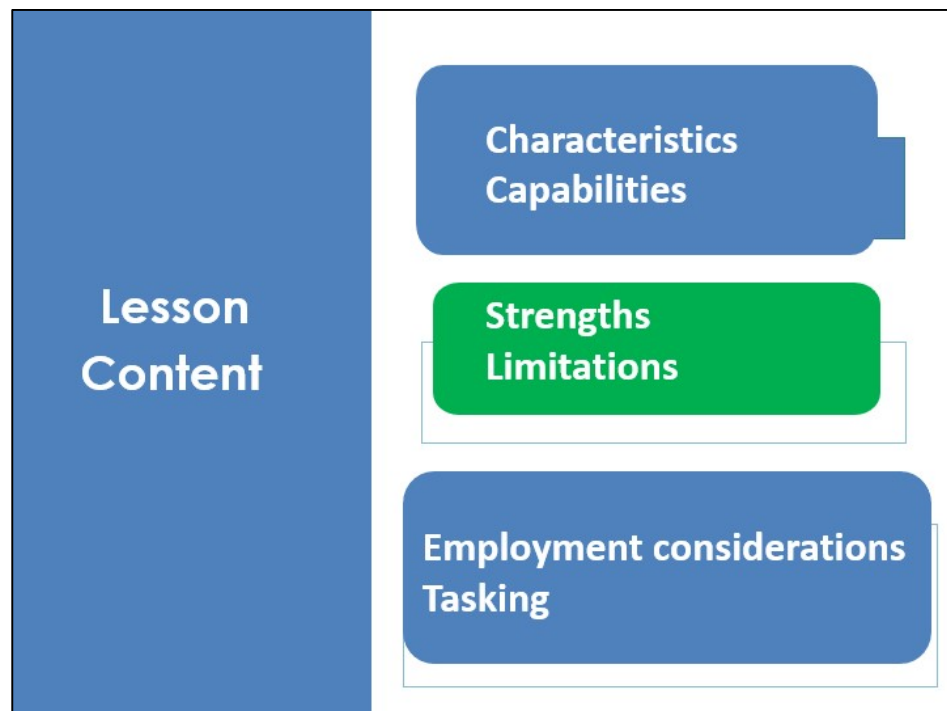
**Force Protection.** An LRRP can provide its own protection as well as protection for the wider UN mission. It does this by providing a deterrent presence against those entities wishing to attack UN personnel or its infrastructure. In addition to its weapons capability and physical presence, it establishes protective measures by providing situational awareness to the commander.

**Sustainment.** An LRRP is self-sufficient in terms of logistic and administrative support for a specific period of time. This includes a sufficient supply of food, water and ammunition, organic vehicle maintenance and recovery capabilities, and medical support. Sustaining independent deployment of reconnaissance platoons or task organised detachments is typically for periods not exceeding 30 days.

**Interoperability.** An LRRP must operate in accordance with UN policies and SOPs. A LRRP should be able to operate under a common UN C3 arrangement involving numerous nationalities beyond its contingent.

**Civil interaction.** An LRRP must be capable of interacting with the local population and other UN and non-UN entities active in the mission area. Language ability or the use of interpreters facilitates engagement with the civilian population enabling the unit to acquire and collate against information requirements. Civil interaction helps to build trust between the population and UN forces.

## Slide 9



Moving onto the strengths and limitations of the LRRP.

## Slide 10

### Strengths

- Direct engagement with civilians.
- Modular composition.
- Larger operating area.
- Sustained operations usually planned up to 30 days.



Key message: LRRP operate in all types of terrain and environments.



**Interactive.** Based on the capabilities mentioned in the previous slides, ask the students to consider the strengths and limitations of the LRRP.

*Possible response:*

- An LRRP can be in direct contact with civilians. Such interactions can provide updates on the general situation, including security concerns, that help develop the situational awareness of the HQs.
- Given the modular and scalable nature of the LRRP, planners can alter the structure of each patrol to meet a specific requirement. The LRRP is likely to comprise multiple reconnaissance platoons, a specialist platoon with specific acquisition technologies, e.g., UAS, and a logistics support platoon. This means that the LRRP can launch multiple patrols at any one time.
- The unit can deploy across a larger operating area compared to other UN military ground units since it does not have to return to its base every day.
- An LRRP can conduct self-sustaining operations for a prolonged period, usually planned, in the UN Mission, to 30 days. Such a unit can provide the Force Commander with an enduring presence in a specific area of operations.

## Slide 11

### Limitations

- Require additional support.
- Finite resource.
- Limited reaction time.



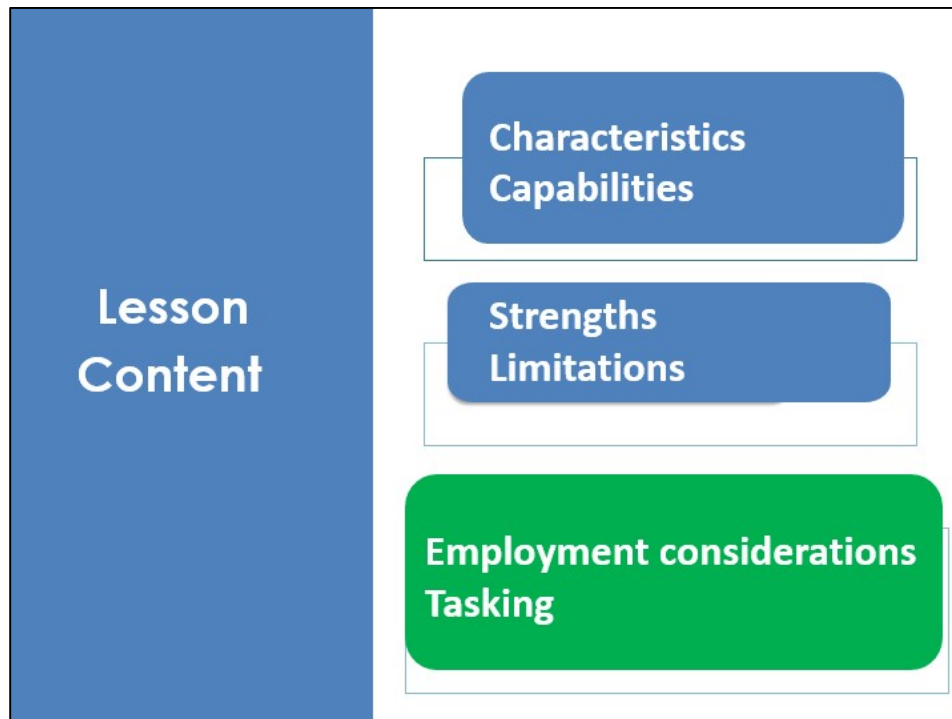
There are some limitations associated with the employing of an LRRP. These include:

**Require additional support.** Although relatively independent, an LRRP is reliant on support during any long-term deployment, for example, logistic support from sector HQs as it operates across the mission area of operations. Likewise, since the unit can operate at distance and could be relatively isolated, it requires dedicated CASEVAC and reinforcement support as part of its contingency planning. Such support needs planning and coordination to ensure the unit can operate effectively.

**Finite resource.** Few UN peacekeeping missions have LRRP units. If they do have them, it is likely to be only one or two units. As such, the employment of such units is restricted and therefore would probably be focused on priority operational tasking only.

**Limited reaction time.** Due to the LRRP's capacity and the nature of its operations, it would be very difficult to task an LRRP without considerable planning and preparation. Therefore, an LRRP is not a reactionary acquisition asset. Re-tasking would be possible, but only if the unit was already operating within or near to the specific area of interest.

## Slide 12



We will now move onto the third part of the lesson: employment considerations and tasking.

## Employment concept

The size of the UN LRRP depends on the following types of operations to be conducted:

- Area reconnaissance
- Route reconnaissance
- Surveillance
- Determine population disposition
- Security operations



Key message: The UN LRRP acquires information needed for the planning and conduct of Mission operations.

The LRRP is a highly mobile unit and can play a vital role in the protection of civilians by offering situational awareness in remote areas not otherwise covered by UN personnel. The size and capabilities of an LRRP will be determined by the types of operations it has been generated to do. These could include:

**Area Reconnaissance.** Area reconnaissance provides awareness of a general area's terrain and geographic characteristics. Area Reconnaissance objectives may be a small village or town; facilities such as water treatment plants or a weapons storage site.

**Route Reconnaissance.** Route reconnaissance analyses the conditions of roads / tracks, terrain features, general security conditions and the capacity to achieve operational capability along a specified route and its immediate surroundings. Route reconnaissance can be performed as either a standalone mission, or as an additional task during a larger area reconnaissance mission.

**Surveillance.** Surveillance is the systematic and continuous observation of a designated area, place or person by using its organic acquisition equipment. Surveillance operations provide the commander information to prevent surprise, provide reaction time, and allow the commander to make informed decisions for planning and action.

**Determine Population Disposition.** These are tasks aimed at the acquisition of information about the local population and its disposition towards UN and negative forces. Determining the population disposition helps commanders understand the threats against the local population and develop countermeasures to mitigate that threat and other negative factors affecting the community.

**Security Operations.** Security operations are conducted to provide early and accurate warning of activities posing a threat to protected groups or areas. Security operations provide the Force with the time and operating space within which it can react to negative forces. Security operations are not distinctly separate from reconnaissance missions and therefore should be considered in the overall IAP. Security operations include observation posts, border monitoring, convoy security and evidence collection.

## Employment considerations

A detailed deployment plan, including:

- Purpose of the mission.
- Acquisition requirements.
- External support.
- Command, control and communication measures.

Key message: The deployment of an LRRP must be based on a robust plan to ensure it is able to function effectively for up to 30 days.

Let us look at some of the issues that should be considered when planning an LRRP (this is the same at Force, Sector or battalion level).

There are several factors that need to be considered during the planning process, since the patrol might be operating at a distance from its operating base. These factors include:

- What is the purpose of the LRRP mission – reconnaissance, surveillance, etc.? This will determine the composition of the patrol.
- What information requirements will the patrol be expected to acquire during its deployment (based on the IAP)?
- What is the threat to the patrol in its area of operations?
- How will the patrol be logistically supported, especially during longer missions?
- How will the patrol communicate and what means of alternative communications must be employed?
- What is the casualty evacuation (CASEVAC) plan, and who would provide support should the patrol become isolated and require reinforcement?
- What is the C2 status, especially if the unit is operating across multiple sectors?
- How will the terrain affect the operation?
- What other UN and host troops are operating in the specific area of operations? (To avoid fratricide).



## Slide 15

### Tasking



PKISR should:

- Plan sufficiently in advance in close coordination with LRRP liaison element to ensure the LRRP is employed efficiently for the duration of its patrol.
- Prepare IRs, taken from the IAP.
- Conduct detailed briefing for the LRRP commander.
- Coordinate with LRRP commander, U/G/S3 and U/G/S4 regarding support requirements.

Key message: The success of an LRRP will depend on the coordination and peacekeeping-intelligence preparation of the mission and a detailed briefing to the LRRP commander.

In preparation, the PKISR cell should:

- Be aware of where the unit will be operating ahead of time to provide information requirements for the patrols to answer. The IAP should be used as the basis for this tasking. The U2/G2 should liaise with their corresponding U5/G5/S5 and U3/G3/S3 in time to ensure that the tasking matches the intended patrol area and timeframe for deployment.
- Provide a detailed briefing for the LRRP commander so that they are fully aware of the task in case communication is lost, or so the LRRP can exploit opportunities that enhance the acquisition effort. As well as confirming the methods of dissemination information during the operation.
- Coordinate with LRRP commander, U/G/S3 and U/G/S4 to ensure sectors and ground units are aware of the LRRP's activity and their role in supporting the task.

## Tasking

- Obtain data.
- Specialized reconnaissance.
- Monitoring.
- Surveillance.
- Provide situational awareness.



An LRRP could be assigned with the following tasks:

- **Obtain, confirm or refute data** on: armed groups - their facilities and personnel; the physiographic characteristics of a defined area; structures relevant to operations; population and civil considerations.
- Perform **specialized peacekeeping-intelligence reconnaissance** in hostile, denied or sensitive environments to seek or verify data of strategic or operational importance.
- **Monitor** areas, facilities, materials, equipment or personnel in the area of operations, through electronic, photographic, optical or acoustic means.
- Conduct **surveillance** in areas normally not visible.
- Detect, record and report negative force activities, in a specific place and period, in order to provide timely data for operations (**situational awareness**), even under adverse weather and luminosity conditions.

Slide 17

## Take Away

- LRRPs can cover large operating areas for up to 30 days.
- External support to a LRRP is key to its success.
- LRRP activity must be coordinated among mission staff and the unit commander.

## Summary

It is important that you understand how an LRRP can be employed, including the strengths and limitations of employing such an asset. Not many missions have an LRRP and therefore, if available, planning is essential to ensure the asset is tasked and employed effectively.

# Module 3



## Operational Framework Wrap Up

At the conclusion of Module 3, some key elements should be emphasised:

- A general understanding of the key operational framework covering PKISR in UN peacekeeping operation can be found in the UN PKISR handbook.
- The PKISR process begins with direction from the mission leadership since the process revolves around closing PKI gaps. CCIRs provide clear direction and guidance on what the Force leadership considers to be important.
- MPKI cells and units have limited acquisition assets, and limited time to acquire information. Therefore, IRs must be prioritised.
- Understanding the ISR disciplines, including the strengths and limitations of each, will help PKISR staff officers when it comes to assigning ISR assets against specific information requirements
- PKISR planning needs to be based on an acquisition strategy.
- Tasking is prepared by PKISR OPS, but tasking authority is usually at U3/5 as they are the Force HQ's staff function responsible for operations. An effective IAP and IAL is essential to ensure effective tasking.
- The PKISR cycle relies on individuals performing their duties to ensure the process is effective and efficient. Everyone needs to understand their role and how they interact with other actors involved in the process. The PKISR staff exercise will allow you to practice many of these staff skills so that you can be confident in these procedures when you deploy to a UN peacekeeping operation.

# R e f e r e n c e s



## Glossary and Annexes

The following annexes and references can be found in separate folders to aid in the delivery of the modules:

- **Annex A:** PowerPoint Slide Lesson Presentations
- **Annex B:** Staff exercise (TTX)
- **Annex C:** Supporting reference material

### Glossary (acronyms and abbreviations)

APII	Area of Peacekeeping-Intelligence Interest
APIR	Area of Peacekeeping-Intelligence Responsibility
AM	Acquisition Management
ATO	Air Tasking Order
BLOS	Beyond Line of Sight
C2	Command and Control
CAVO	Civilian Aviation Officer
CCIR	Commanders Critical Information Requirements
CCIRM	Commanders Critical Information Requirements Manager
CCTV	Closed-Circuit Television
CMS	Chief of Mission Support
COIST	Company Peacekeeping-Intelligence Support Team
CPKI	Communications peacekeeping-intelligence
CRSV	Conflict-Related Sexual Violence
DMS	Director of Mission Support
DOS	Department of Operational Support
DPO	Department of Peace Operations
EEI	Essential Elements of Information
EO	Electro-Optical
FC	Force Commander
FHQ	Force Headquarters
FMV	Full Motion Video
FTS	Field Technology Section
G2	Sector Level peacekeeping-intelligence Staff
GCS	Ground Control Station

GPKI	Geospatial Peacekeeping-Intelligence
GMTI	Ground Moving Target Indicator
HCT	Humanitarian Country Team
HPKI	Human Peacekeeping-Intelligence
HRDDP	Human Rights Due Diligence Policy
HSI	Hyper Spectral Imaging
I&W	Indicators and Warnings
IAL	Information Acquisition List
IAP	Information Acquisition Plan
ICRC	International Committee of the Red Cross
IDP	Internally Displaced Personnel
IED	Improvised Explosive Device
IHL	International Humanitarian Law
IM	Information Management
INTREP	Intelligence Report
INTSUM	Intelligence Summary
IPKI	Imagery Peacekeeping-Intelligence
IR	Peacekeeping-Intelligence Requirement
IR	Information Requirement
IR	Infra-Red
IRM	Information Requirements Management
ISP	Peacekeeping-Intelligence Support Plan
ISR	Intelligence, Surveillance and Reconnaissance
JMAC	Joint Mission Analysis Centre
JOC	Joint Operations Centre
LOS	Line of Sight
LRRP	Long-Range Reconnaissance Patrol
LTIOV	Latest Time Information is of Value
MASIC	Military All-Source Information Cell
MAOC	Mission Air Operations Centre
MICM	Mission Peacekeeping-Intelligence Coordination Mechanism
MIO	Military peacekeeping-intelligence Officer
MOU	Memorandum of Understanding
MPKI	Military Peacekeeping-Intelligence
MSI	Multispectral Imaging
NAI	Named Area of Interest
NLT	No Later Than
OHCHR	Office of the UN High Commissioner for Human Rights
OMA	Office of Military Affairs
OS	Open Source
OPKI	Open-Source Peacekeeping-Intelligence
PAI	Publicly Available Information
PICINTSUM	Picture peacekeeping-intelligence Summary
PIR	Priority Peacekeeping-Intelligence Requirement

PKI	Peacekeeping-Intelligence
PKIMB	Peacekeeping-Intelligence, Surveillance and Reconnaissance Management Board
PKISR	Peacekeeping-Intelligence, Surveillance and Reconnaissance
POC	Protection of Civilians
POC	Police Operations Centre
RFI	Request for Information
RLOS	Radio Line of Sight
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
S2	Battalion Level peacekeeping-intelligence Staff
SAR	Synthetic Aperture Radar
SOFA	Status of Forces Agreement
SOMA	Status of Mission Agreement
SOPs	Standard Operating Procedures
SPKI	Signals Peacekeeping-Intelligence
SIR	Specific Peacekeeping-Intelligence Requirement
TCC	Troop Contributing Country
U2	Force level peacekeeping-intelligence
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UN	United Nations
UNCT	United Nations Country Team
UNDSS	United Nations Department of Safety and Security
UNHCR	United Nations High Commissioner for Refugees
UNPOL	UN Police
UNSO	UN Staff Officer
VLOS	Visual Line of Sight

**[End of document]**