United Nations

Reinforcement Training Package

for United Nations

Military Peacekeeping-Intelligence Officers

For United Nations Peace Operations

United Nations Department of Peace Operations

The Specialized Training Materials (STM) and Reinforcement Training Packages (RTP) for United Nations Peacekeeping Operations has been developed by the Integrated Training Service (ITS) of the UN Department of Peace Operations and Department of Operational Support.

This version has been released for use by Member States in their pre-deployment training for United Nations Peacekeeping Operations. The suite of STM / RTP products will be regularly updated so that it is fully responsive to the needs on the ground. Therefore, we strongly suggest that you check for updated versions before a training program 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.

All photographs have been sourced from the UN and the public domain unless otherwise indicated.

Integrated Training Service

Department of Peace Operations

United Nations

New York, NY, 10017, USA

Preface

Background

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

In the peacekeeping environment, United Nations personnel may operate in remote areas with fragile security conditions. Peace Operations are evolving and adapting in this complex operational environment. United Nations Staff Officers (UNSO), specifically Military Peacekeeping-Intelligence Officers (MPKIO) are required to undergo a robust pre-deployment training program in accordance with DPO's Operational Readiness Assurance and Performance Standards.

This Reinforcement Training Material (RTP) packet will provide member states with the UN pre-deployment requirements, lessons, and materials specifically designed for MPKIO. The intent and content of this RTP are not to duplicate guidelines and training materials that are already outlined in United Nations Military Staff Officers training materials or the Core Pre-Deployment Training Materials (CPTM); instead, these training materials focus on the intelligence frameworks and will supplement and expand on the UNSO lessons to better prepare the MPKIO for UN peacekeeping missions.

Aim

The 2017 General dos Santos Cruz report identifies a Peacekeeping environment that features armed groups, terrorists, organised crime, street gangs, criminal and political exploitation, and other threats against UN forces and civilian populations. The report noted, “The era of “Chapter VI-style” peacekeeping is over, but the United Nations and Troop/Police, Contributing Countries are, by and large, still gripped by a “Chapter VI Syndrome. If the United Nations and T/PCCs do not change their mindset, take risks and show a willingness to face these new challenges, they will be consciously sending troops into harm’s way. To prevent casualties, peacekeeping missions need tactical intelligence”.

UN forces must translate intelligence into tasks and actions that support security. We lack the basic intelligence system, management, networks of human intelligence, and situational awareness. The aim of this RTP for the MPKIO is to support the pre-deployment training efforts of Troop Contributing Countries by providing UN DPO training standards for a MPKIO to ensure a common approach to work at the Force and Sector levels in UN peace operations.

These training materials are a comprehensive training package that combines the Conceptual, Legal, and Operational Frameworks. The RTP mainstreams relevant aspects of the DPO Policy on Peacekeeping Intelligence, the Protection of Civilians, Gender, Security and Risk Management (SRM) into the intelligence frameworks and materials. The RTP includes learning activities/exercises, as well as a more comprehensive scenario-based exercise to be run at the end of a course to strengthen participants' understanding of how to better operate in a UN Peacekeeping environment. The training packages are designed for application in both pre-deployment and in-mission training.

Target audience

The priority target audience for this RTP package are military intelligence staff officers; however, this RTP is also relevant for military decision-makers and other staff officer deploying to UN Peace Operations. Leadership at all levels that supervise, support and coordinate the training for military intelligence staff officers may benefit from this material.

Structure of the training materials

The package is constructed in three modules:

Module 1: Conceptual Framework

Module 2: Legal Framework

Module 3: Operational Framework

Annexes:

- **Annex A:** PowerPoint Slide Lesson Presentations
- **Annex B:** Lesson Learning Activities and Tabletop Exercise (TTX)
- **Annex C:** References and background materials

For all practical purpose, throughout the Reinforcement Training Material documents, lessons, and slides, we will use the following abbreviations/acronyms for both in singular and the plural forms:

- **MPKI- United Nations Military Peacekeeping Intelligence**
- **UN PKI- United Nations Peacekeeping or Peace Operations Intelligence**
- **MPKIO- Military Peacekeeping-Intelligence Officer**
- **UNSO- United Nations Staff Officer**

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 input and feedback during the drafting process, and the numerous training personnel from national peacekeeping training institutions and field missions who participated in the development workshops. The following organisations, Member States and their Permanent Missions to the UN for their contribution in the RTP development;

Federative Republic of Brazil
Islamic Republic of Pakistan
Kingdom of Denmark
Kingdom of Morocco
Kingdom of the Netherlands
Kingdom of Norway
New Zealand
People's Republic of China
Republic of Ireland
Republic of Senegal
United Kingdom
United States of America
Office of Military Affairs, Assessment Team

Special recognition goes out to our United Nations comrade, Major Thomas Van Meijden from the Kingdom of Netherlands (deceased 21 June 2019 during the preparation of this material).

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) or write to 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

General Considerations for Instructors

This package is a compendium of critical training content for MPKIO operating in UN peace operations. No training material can cover the entire spectrum of complexity in a peace operation's environment, with all its challenges, complexity, and activities. The RTP package should, therefore, be viewed as the supplement and baseline to underpin related training efforts for MPKIO. When designing a course, trainers should adapt these materials to the needs of their audience. As a result, the duration of training courses delivered based on the materials may vary significantly.

Training Objectives of the RTP for MPKIO are to prepare the participants for duties in a peacekeeping operation so they can: contribute efficiently to implement military intelligence aspects of UN peace operation mandates in accordance with DPO principles and guidelines including adopting the spirit of the Force Headquarters (FHQ) handbook and UN Military Intelligence Handbook; perform their military intelligence staff functions in an effective, professional and integrated manner; and, demonstrate the core values and competencies of the United Nations.

Concerning necessary competencies for participants to benefit from this training package, it is recommended that personnel receiving this training be proficient in basic military tasks (individually and collectively) at the tactical and technical level. Also, it is expected that the officer is capable of performing proficiency in the following skills: staff officer skills/tasks, intelligence analysis, language, map reading, writing, reporting, briefing, and developing an intelligence staff assessment. It is critical for all participants to have received the Core Pre-Deployment Training Materials (CPTM) and UN Staff Officers STM, and MPKIO RTP as a pre-requisite to this training. The CPTM and the UNSO STM contain the fundamental principles, and concepts and ideas to UN Peace Operations (UNPO), which should be grasped by trainees before participating in the more detailed specific RTP course. Instructors should develop and implement an initial written test and final test (post-instruction) to reinforce learning objectives and evaluate the training level/knowledge of participants.

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

Instructor Profile

This training package is best presented by instructors who master the UNSO STM and this MPKIO RTP, have a basic knowledge of the military intelligence systems and frameworks, analysis, risk assessments, UN reporting, and identification of military vehicles, weapons and aircraft. Instructors should have previous experience working in a UN peace operation or as a MPKIO at the tactical/operational levels. The knowledge on the mission where participants are to be deployed is advisable, to be able to deliver a targeted course based on real experience. Finally, instructors should be familiar and comfortable with facilitator-based instruction and facilitating scenario-based Tabletop Exercises (TTX).

Tabletop Exercise (TTX) Considerations

Contained in the RTP is a TTX. This exercise is a scenario and situational driven learning activity to help consolidate learning outcomes and help reinforce the lesson "Take Away". TTXs provide a learning environment tailored to facilitate discussions. They are set in an informal learning environment where the target audience can discuss the principles and concepts when operating in a United Nations Peacekeeping operation using a hypothetical scenario and specific situations. The exercise will help participants to understand how to integrate intelligence in a peacekeeping environment.

Methodology: Using their national problem-solving doctrine, methodology, military decision-making processes, troop leading procedure, participants will analyse situations, missions and present intelligence analysis. The effectiveness of a TTX is derived from building blocks from lesson learning activities and energetic involvement by facilitators and participants. Facilitators / Instructors should highlight the adequacy of the core elements and principles when operating in support of peacekeeping operations. Also, they should assist participants in bridging gaps in the transition from standard military operations to peacekeeping operations. Instructors must emphasize that C2, the support structure, and the coordination with the various actors in a UNPO can be chaotic and challenging.

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 and encourage the participation of trainees
- Trainers should bring examples and antidotes from actual UN peace 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 handouts, relevant UN DPO / DOS Handbook and Policies
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 is to inform participants with the:

- An overview of the UN Peacekeeping Intelligence (UN PKI) Policy and Military Peacekeeping-Intelligence Course(MPKI)
- Nature and characteristics, roles, responsibilities and structure of the MPKI framework
- UN PKI and UN MPKI principles
- MPKI Cycles, management and tools
- Information Security

Overview

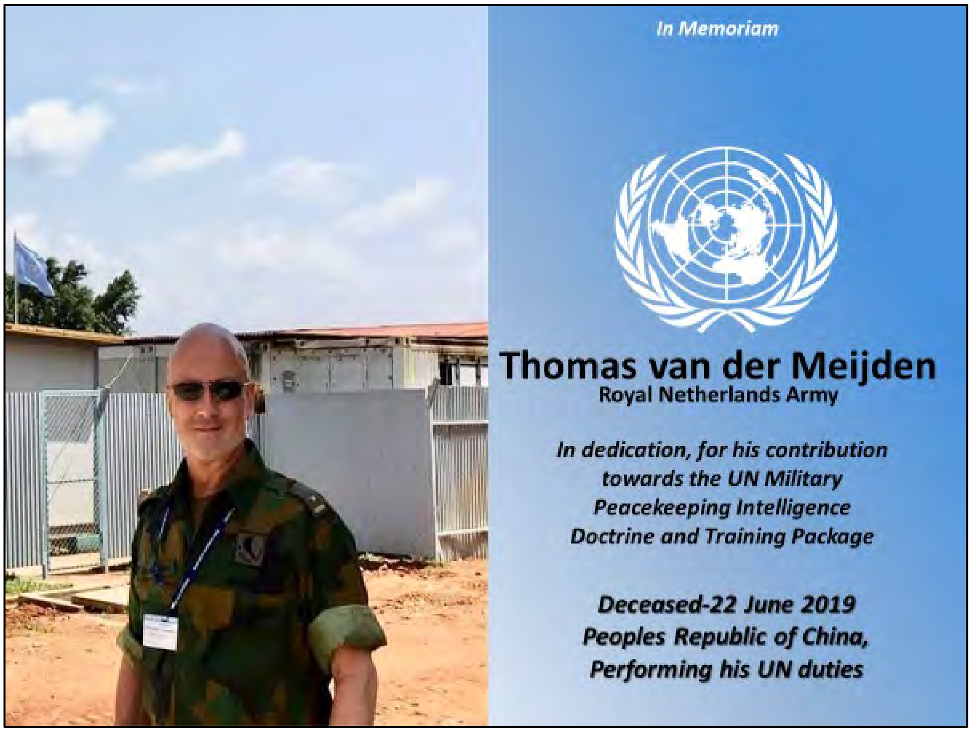
Module 1 provides an overview of the conceptual framework of the UN PKI and the MPKI for the MPKIO operating in a UN peace operation to support and help contribute towards a successful achievement of the mandate. It also examines the nature and characteristics of UN MPKI and how it supports the UN mission

Note to Instructor: *Recommend that the instructor read, DPKO Peacekeeping-Intelligence Policy and United Nations Military Peacekeeping-Intelligence Handbook (MPKI HB), before giving the lesson.*

For an interactive start to this module, ask the participants if they have had experience working in an intelligence position in their home countries or in a UNPKO. Ask them to tell the group about how peacekeeping-intelligence is different from their own national intelligence and their specific challenges working as peacekeeping-intelligence staff.

Introduction

Special Recognition -Slide 1



In Memoriam

Thomas van der Meijden
Royal Netherlands Army

In dedication, for his contribution towards the UN Military Peacekeeping Intelligence Doctrine and Training Package

Deceased-22 June 2019
Peoples Republic of China,
Performing his UN duties

Thomas was a true professional who was involved in the early stages of development of the Military Peacekeeping Intelligence handbook and training materials. His broad experience enabled him to actively support other Peace Operation projects. Our heartfelt thoughts go to his family and friends; Thomas is truly missed.

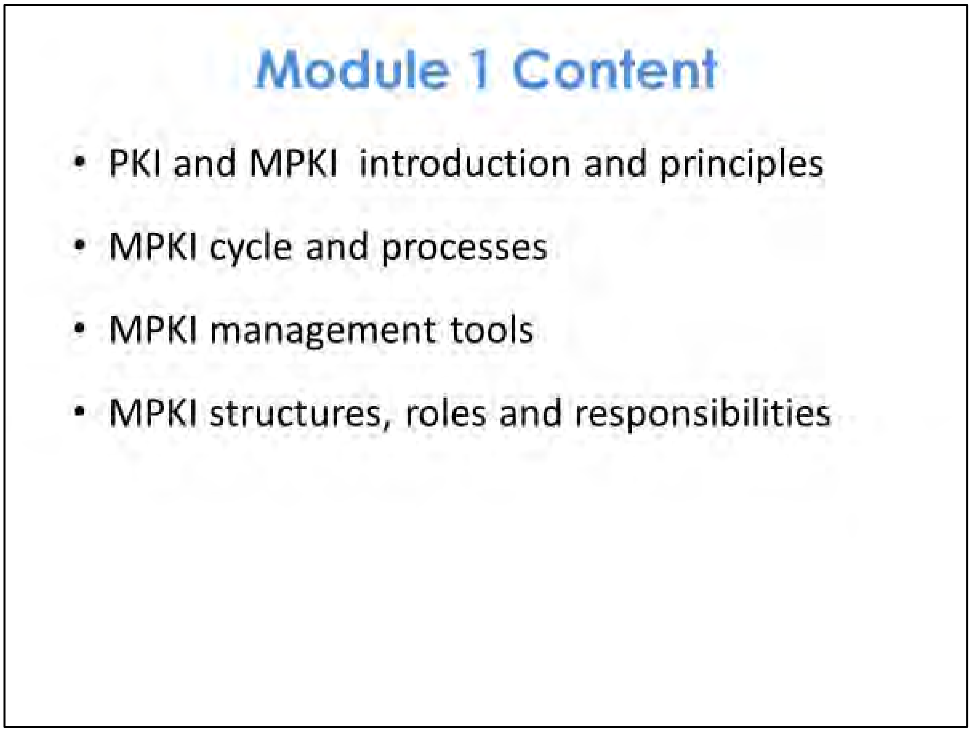
Slide 2

Module 1
Military Peacekeeping-
Intelligence
Conceptual Framework

Key Message: As the mandates and operating environments of United Nations peacekeeping operations have evolved, there is a need for peacekeeping missions to understand their operating environments better and to produce intelligence products to support the mandate implementation.

Of note, for all practical purpose, throughout these Reinforced Training Material documents, lessons, and slides, we will use the abbreviation/ acronym "MPKI" to refer to military peacekeeping-intelligence and "MPKIO' to refer to the Military Peacekeeping-Intelligence Officers.

Slide 3



Module 1 Content

- PKI and MPKI introduction and principles
- MPKI cycle and processes
- MPKI management tools
- MPKI structures, roles and responsibilities

UN peacekeeping-intelligence policy and guidance sets out why and how UN peacekeeping operations acquire, collate, analyse, disseminate, use, protect and manage peacekeeping-intelligence in support of UN peacekeeping operations in the field. In Module 1, we will cover these topics shown on this slide.

Lesson 1.1

UN PKI and MPKI Overview

The Lesson

Starting the Lesson

For an interactive start to this Lesson, ask the participants if they have had experience in a UNPKO as a staff officer. Ask them to tell the group about their specific challenges with staff coordination, command and control, logistics, security, and how intelligence products where developed, disseminated and used.

Note to Instructor:

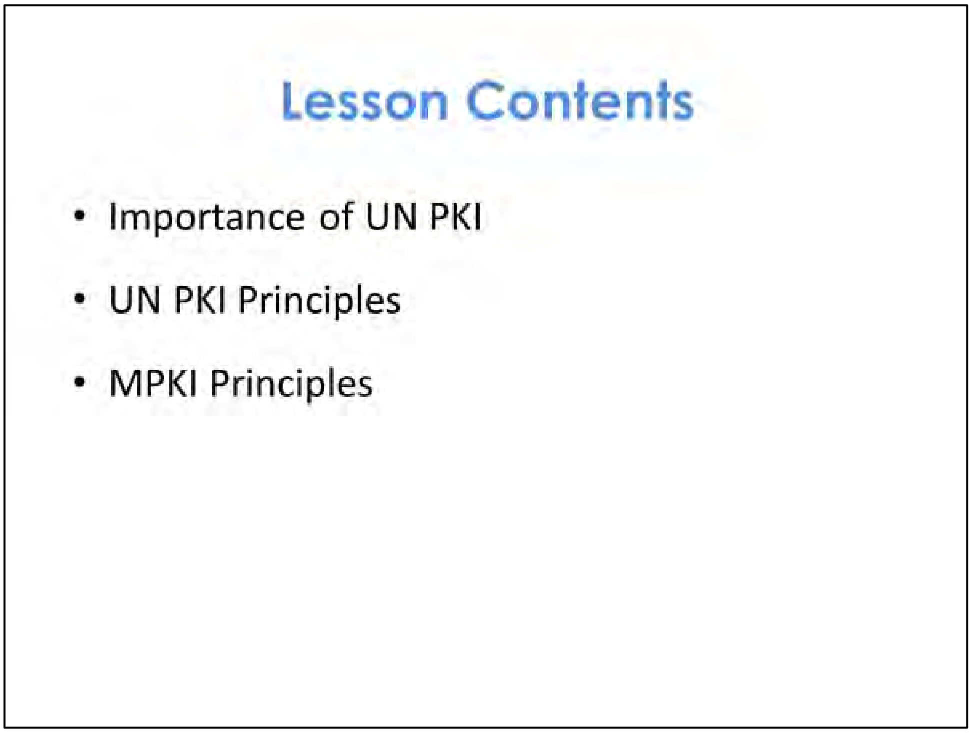
Suggest that you emphasize that for intelligence to be effective; all UN organisations must work collaboratively. Intelligence is considered a 'Team Sport'. The Force, Sector and Battalion intelligence organisations, UN police, and mission components etc. should all support and learn from each other. Recommend that the instructor review the *2019 Peacekeeping Intelligence Policy and the UN policy of the protection of civilians before giving this class.*

Slide 4

Lesson 1.1
UN PKI and MPKI Overview

The fundamental purpose of peacekeeping-intelligence is to enable missions to produce timely, accurate, relevant intelligence products to support planning and operations; to provide early warning of imminent threats, including threats to life, property and movement restrictions; and to provide mission leadership with information and understanding about shifts in the operational landscape, and emerging trends. This lesson will provide a general overview of the intelligence framework in the UN.

Slide 5

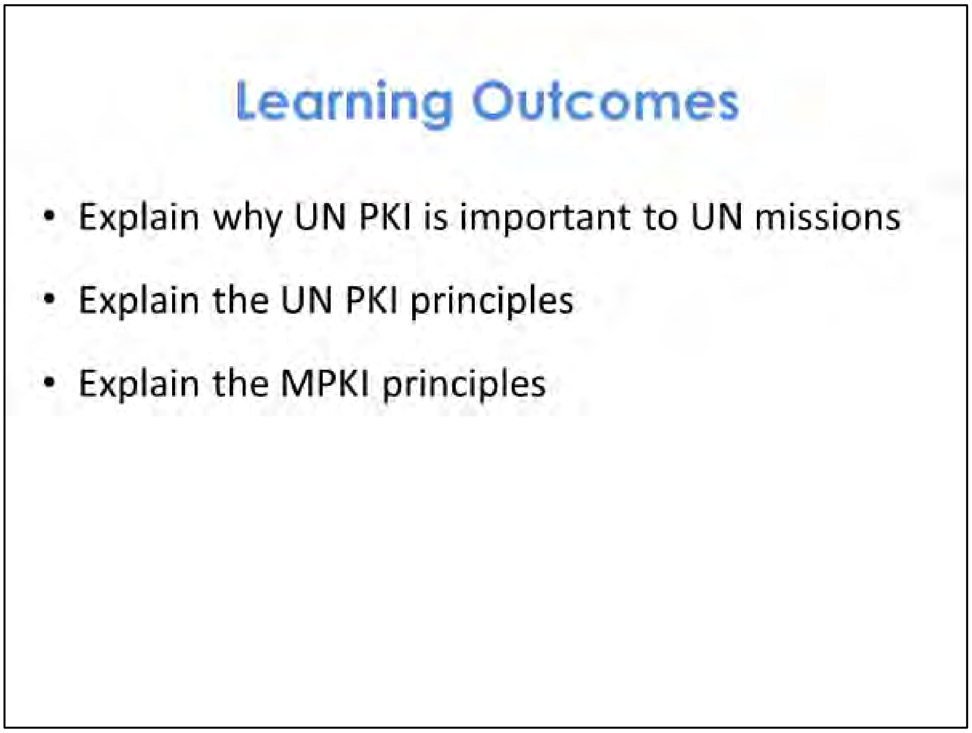


Lesson Contents

- Importance of UN PKI
- UN PKI Principles
- MPKI Principles

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

Slide 6

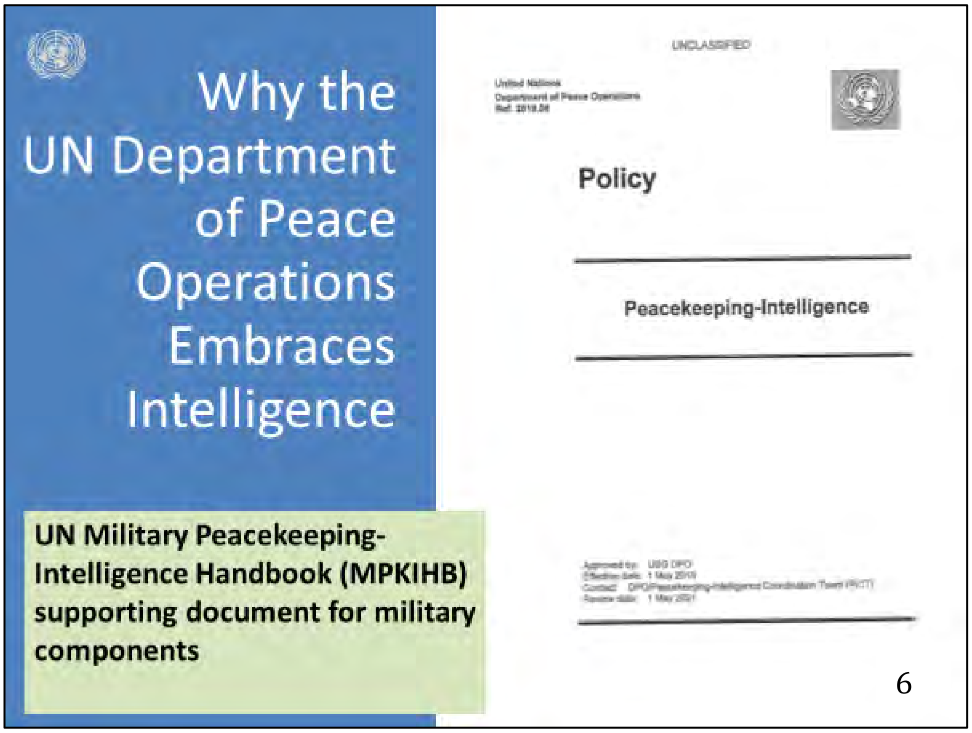


Learning Outcomes

- Explain why UN PKI is important to UN missions
- Explain the UN PKI principles
- Explain the MPKI principles

In all good training practices, let's review the learning outcomes. 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:

Slide 7



Why the UN Department of Peace Operations Embraces Intelligence

UN Military Peacekeeping-Intelligence Handbook (MPKIHB) supporting document for military components

UNCLASSIFIED

United Nations
Department of Peace Operations
Ref. 2019.08

Policy

Peacekeeping-Intelligence

Approved by: USG DPO
Effective date: 1 May 2019
Contact: DPO/Peacekeeping-Intelligence Coordination Team (PICT)
Review date: 1 May 2021

6

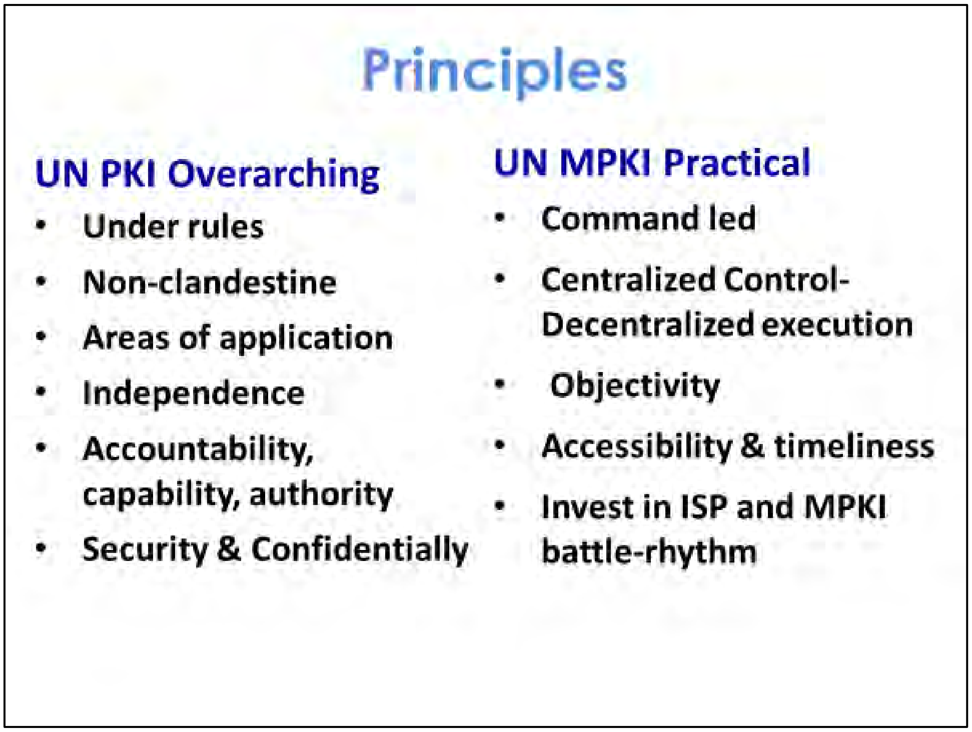
Here is the United Nations Department of Peace Operations policy on Peacekeeping Intelligence.

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

In high-tempo, complex and dangerous environments, where asymmetric, hybrid and transnational threats pose serious dangers to peacekeepers and the population and impact the mandate implementation. In these environments, there is a need for peacekeeping missions to understand their operating environments better. This also includes, maintaining a strategic overview of developments, and anticipated strengths, weaknesses of threats/spoilers that may impact on the ability of peacekeepers to execute their mandate effectively.

The Department of Peace Operations, OMA has developed the UN Peacekeeping Military Intelligence Handbook, which supports the military component who interact with the MPKI systems. The UN conducts peacekeeping intelligence may differ from your own national methodology; it is crucial to understand these differences.

Slide 8



Principles

UN PKI Overarching

- Under rules
- Non-clandestine
- Areas of application
- Independence
- Accountability, capability, authority
- Security & Confidentially

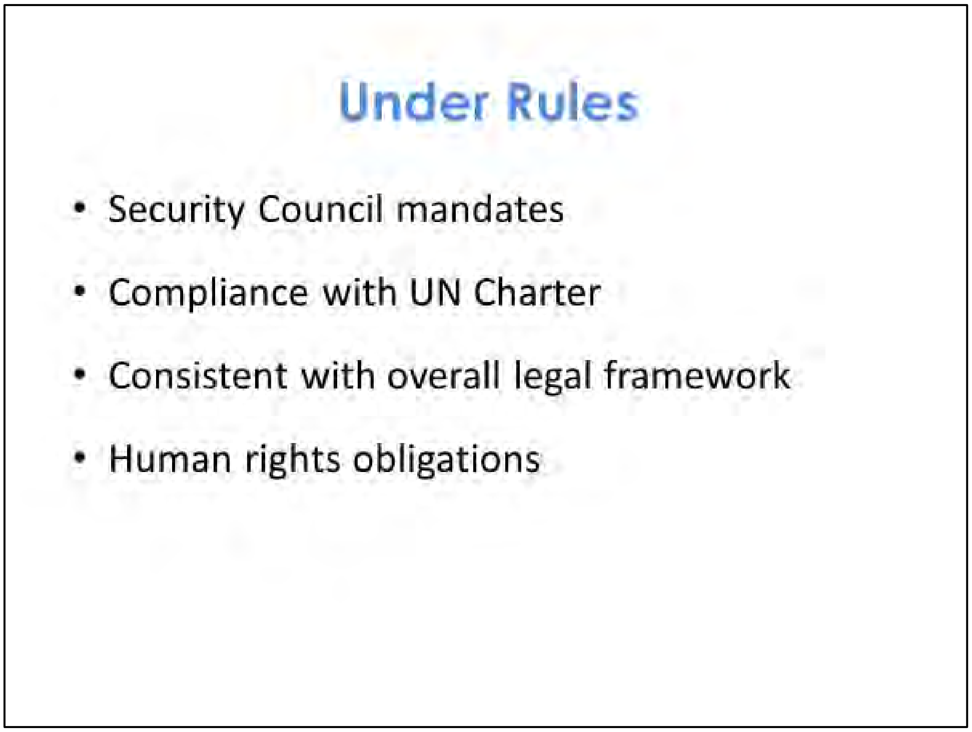
UN MPKI Practical

- Command led
- Centralized Control-Decentralized execution
- Objectivity
- Accessibility & timeliness
- Invest in ISP and MPKI battle-rhythm

There are two primary sets of principles guiding the PKI framework. One is the overarching set of principles from the UN Peacekeeping-Intelligence Policy, and the other set, on the right side are the practical principles from the UN Military Peacekeeping-Intelligence (MPKI) Handbook. The Handbook provides us with operating principles to help guide us in our duties.

These principles inform all activities of United Nations peacekeeping operations at all stages of the management of peacekeeping-intelligence. All subordinate guidance, directives, plans and operations shall comply with and apply these principles.

Slide 9

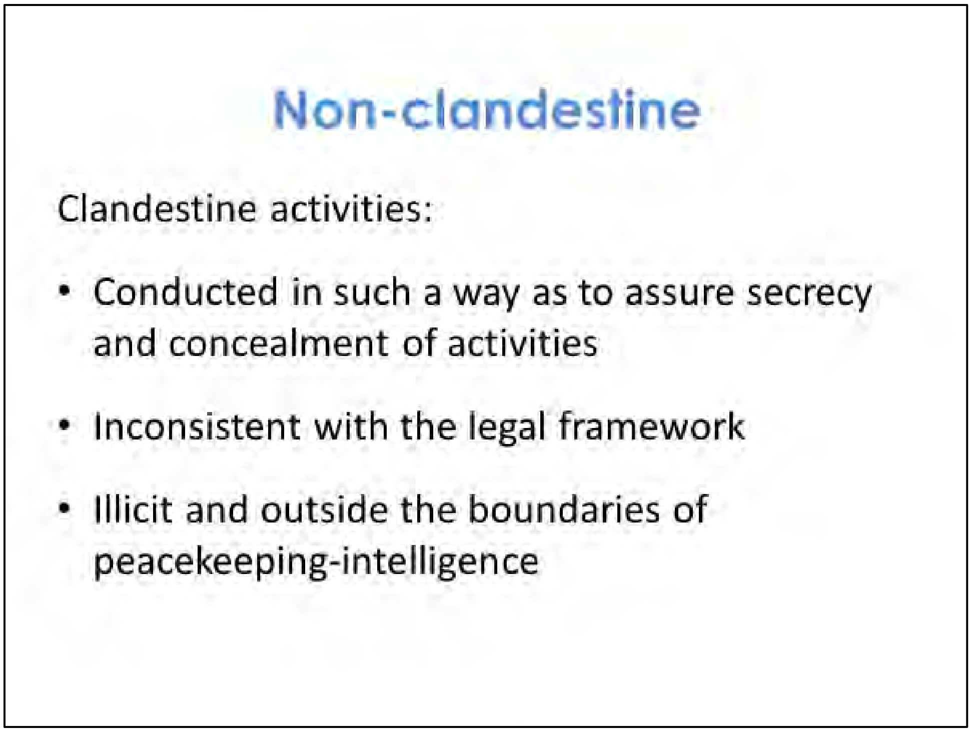


Under Rules

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

All Peacekeeping missions start with a Security Council Resolution that establishes a Mandate. The Mission members must follow the intent, goals, tasks, rules and regulations covered in the mandate. Every activity conducted in the peacekeeping-intelligence complies with the UN legal framework, international humanitarian and human rights law and host nation laws.

Slide 10



Non-clandestine

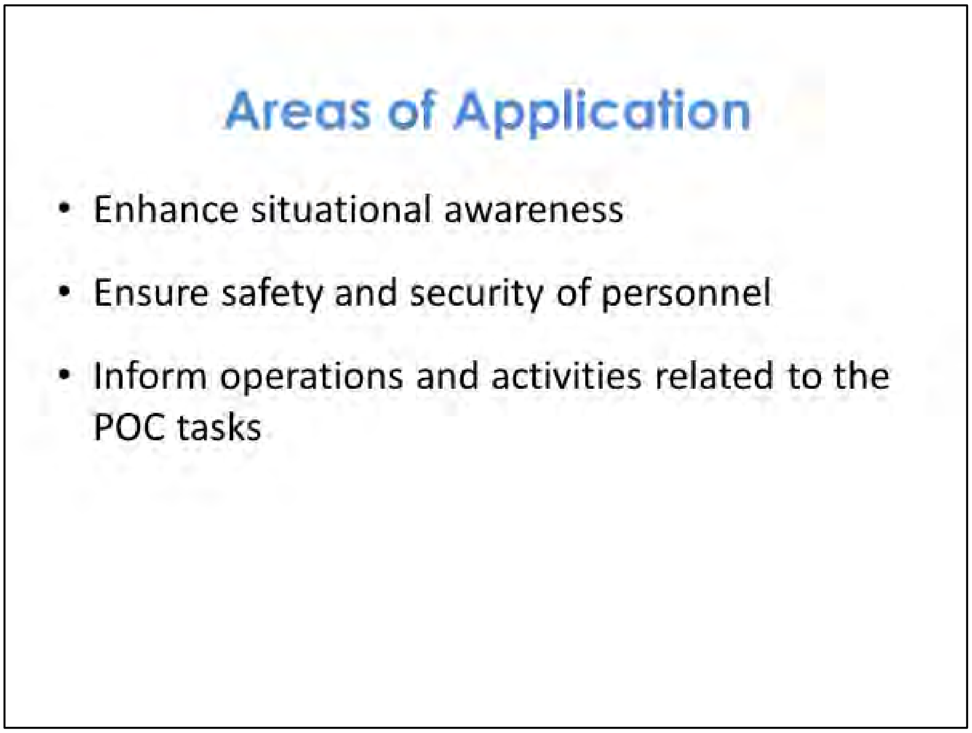
Clandestine activities:

- Conducted in such a way as to assure secrecy and concealment of activities
- Inconsistent with the legal framework
- Illicit and outside the boundaries of peacekeeping-intelligence

The UNPK principle of non-clandestine is best described as what we cannot do as shown on this slide. Clandestine activities are defined as the acquisition of information or intelligence conducted in such a way as to assure secrecy and concealment of activities. Because such activities are illicit and/or inconsistent with the legal framework, principles, policies and mandates of UN peacekeeping operations, they are outside the boundaries of peacekeeping-intelligence and shall not be undertaken by participating mission entities.

Interactive. *Ask the participants to give examples of possible clandestine activities in peacekeeping operations or conduct a short learning activity to discuss the meaning and specific examples of clandestine activities. Consider commencing a discussion by asking the students if it is appropriate to represent themselves to others as something other than what they are, for example, as individuals working for an NGO. It may also provoke debate by asking can the UN pay sources. The response in both cases is no.*

Slide 11



Areas of Application

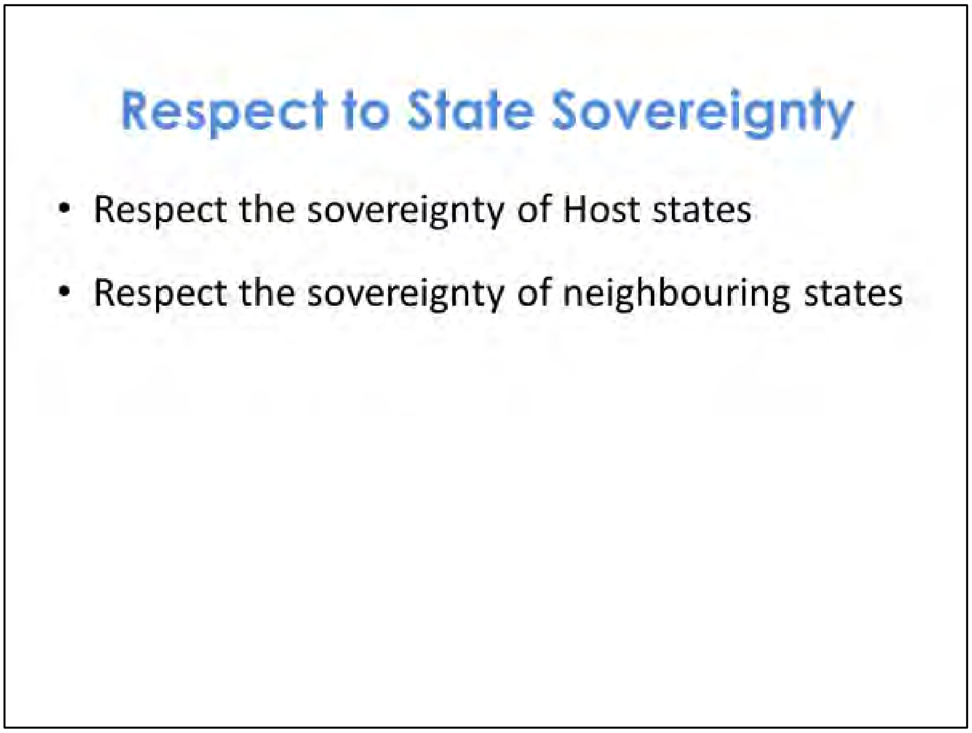
- Enhance situational awareness
- Ensure safety and security of personnel
- Inform operations and activities related to the POC tasks

The production of UN peacekeeping intelligence shall be limited to the following: to enhance situational awareness; to assure 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 the MPKI cell can operate.

Interactive. *Ask the students if it is ever permissible to acquire information on host nation security forces. The response here is yes if it relates to tasks UNMPKI is designed to support. For example, if host nation security forces act or are about to act to undermine the security of civilians. However, it is a very sensitive topic.*
Ask the participants to list what they think is not permissible in terms of information acquisition. This is designed to promote debate. Moreover, while it may appear that there are many limitations, the permissible areas of application support ***most*** *acquisition activity.*

Slide 12



Respect to State Sovereignty

- Respect the sovereignty of Host states
- Respect the sovereignty of neighbouring states

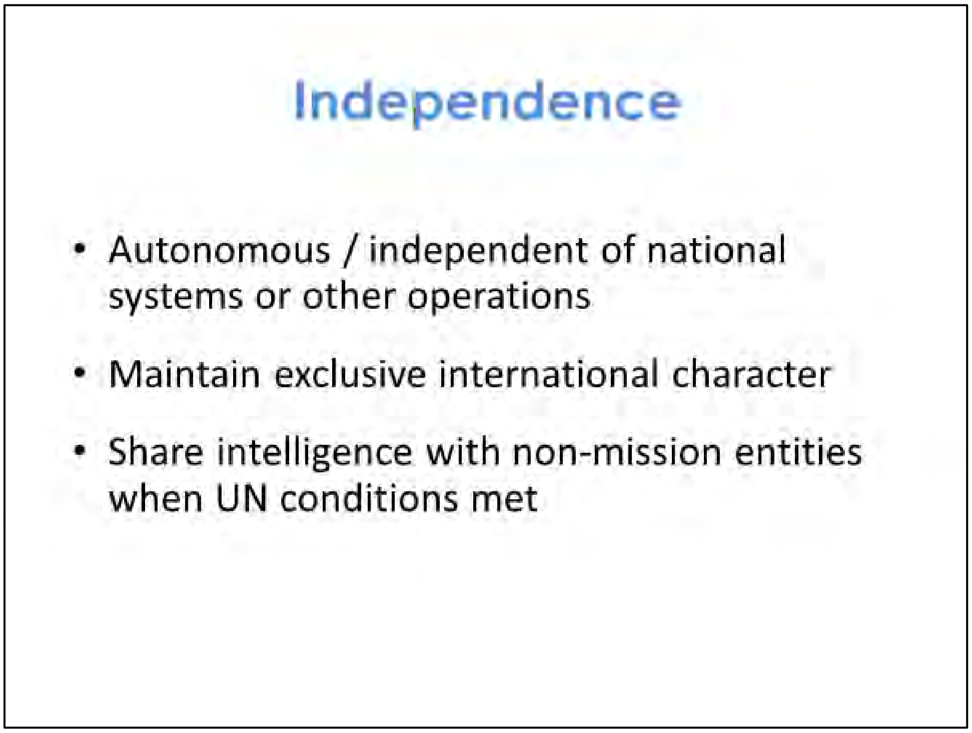
A UN peacekeeping operation is deployed with the consent of the Host government. Therefore, the sovereignty of states, including Host and neighbouring states, must always be respected.

Ask students if it is permissible to acquire information using mission assets in a neighbouring country. For example, armed groups often do not respect state borders and may use neighbouring states to consolidate and prepare for attacks. Can a mission monitor these areas using Unmanned Aerial Systems (UAS) as part of its information Acquisition Plan (IAP)?

The answer here is no, and this is not permissible unless done with the express permission of that state. However, the UN MPKI section may acquire some information passively by engaging with refugees, for example, or by engaging in open-source research. The key point is that it cannot task organic acquisition assets to operate in other states as part of its IAP.

Ask the participants how the attitude of a Host State can impact peacekeeping- intelligence activities and give examples, if possible. For example, Host Nations have been known to restrict freedom of movement and to deny access to areas where missions need to acquire information.

Slide 13



Independence

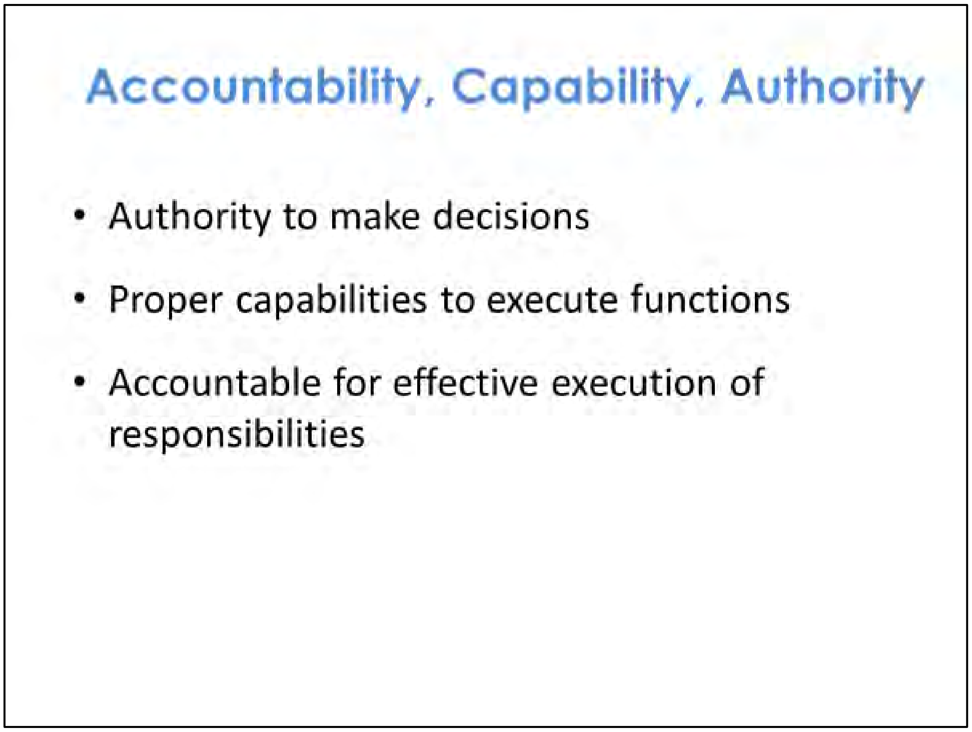
- Autonomous / independent of national systems or other operations
- Maintain exclusive international character
- Share intelligence with non-mission entities when UN conditions met

UN Peacekeeping-intelligence 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 to receive intelligence and may share specific peacekeeping-intelligence with non-mission entities, including Host States, provided they do so under conditions and within the parameters to be explained later in the section about information sharing.

Generally, it is the Head of Mission’s responsibility to determine the entities that the mission can share intelligence with. Still, he/she must be cognizant of source protection and ensure that he/she is satisfied that UN MPKI products will be used in such a way that aligns with the UN charter and principles of consent, impartiality, and non-use of force except in self-defence and defence of the mandate.

Slide 14



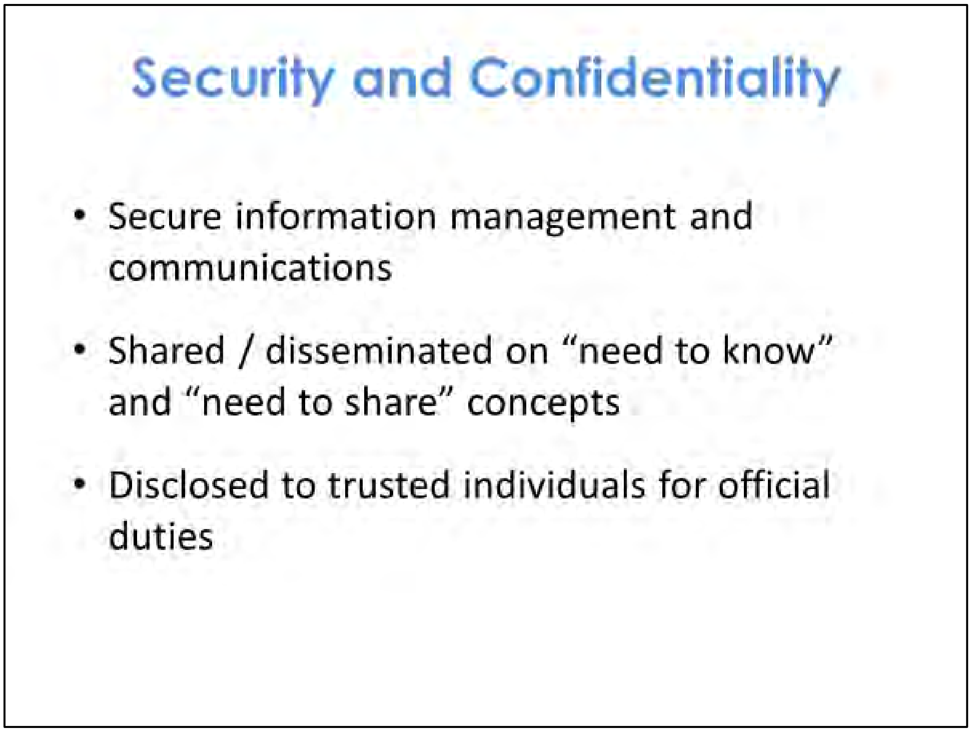
Accountability, Capability, Authority

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

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

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

Slide 15



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

MPKIO Peacekeeping-intelligence shall be stored and shared securely while ensuring access for those who require it for decision-making and operational planning.

Missions should assess risk involving information security and put in place procedural, technological and physical security measures to ensure secure information management within the peacekeeping-intelligence system.

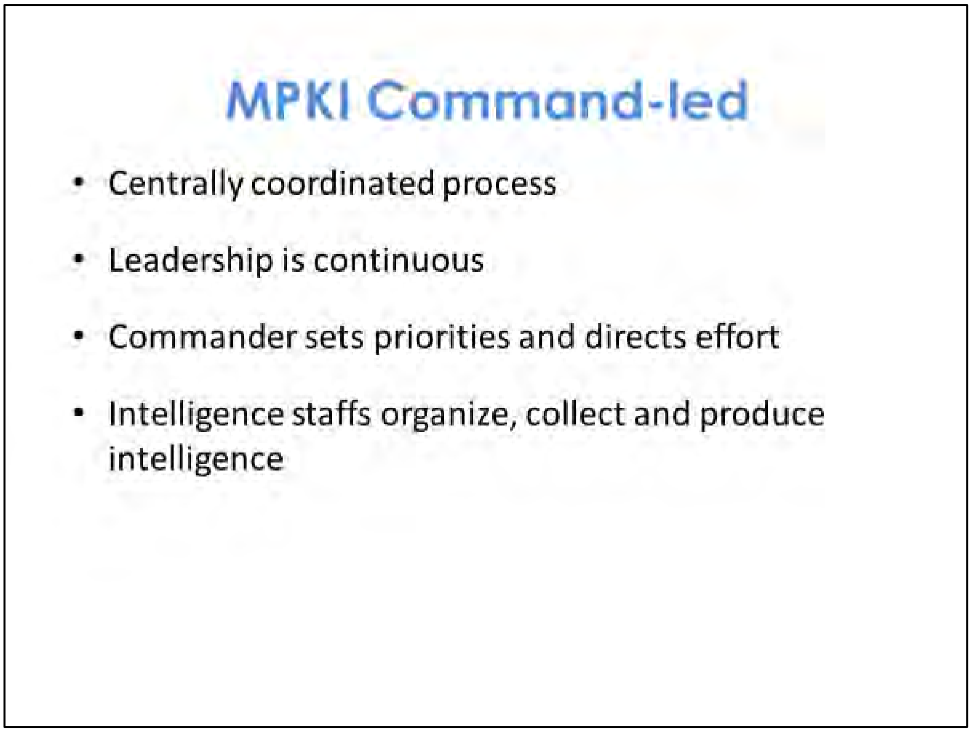
Peacekeeping-intelligence should be disclosed to mission personnel only if access to said information is required for them to carry out official duties. It also requires a written delegation of authority from the originator or staff member who originally applied the classification level.

It implies that peacekeeping-intelligence is only disclosed to trusted personnel, where disclosure is likely to endanger the safety or security of any individual or group, violate rights or invade privacy.

Interactive. *Ask the participants to debate the difference between ‘need to know’ and ‘need to share’. What we are looking for here is that there is no point in producing excellent intelligence product if it does not get to the right people.*

There may be problems with the over-classification of information and intelligence in the UN system.

Slide 16



MPKI Command-led

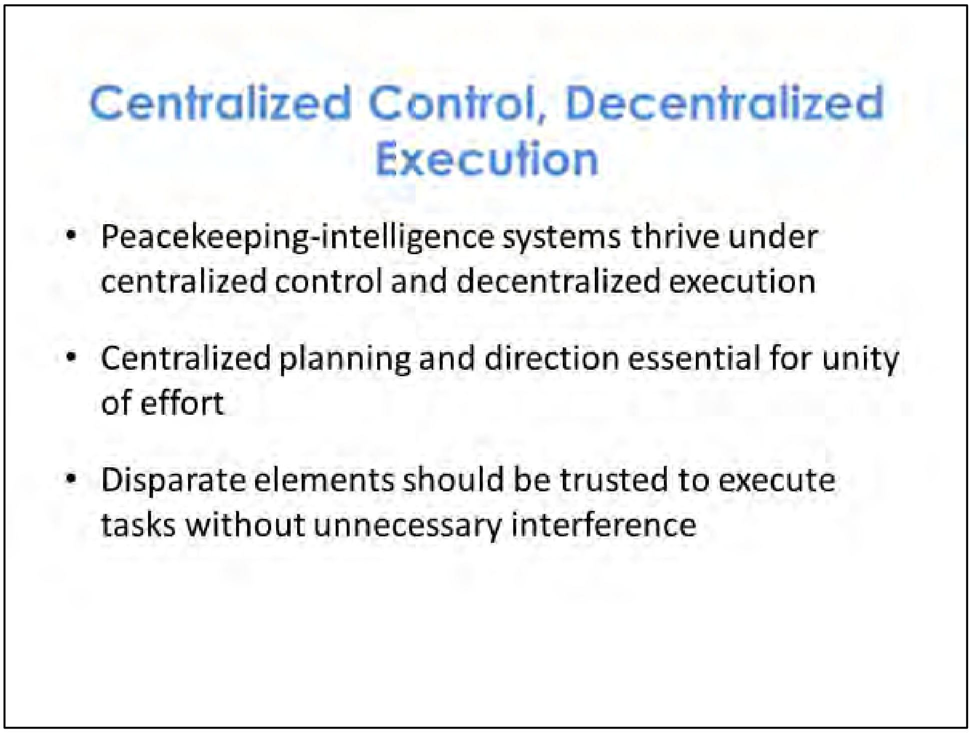
- Centrally coordinated process
- Leadership is continuous
- Commander sets priorities and directs effort
- Intelligence staffs organize, collect and produce intelligence

Practical principles are available in the Military Peacekeeping-Intelligence Handbook.

Peacekeeping-intelligence is a centrally coordinated process through which information inputs from decentralised entities, often deployed over a wide geographic area, are combined with different functions and expertise.

Ask the participants what tool is best used to ensure that the process is command-led and centralised. The response should lead to a discussion about a central Information Acquisition Plan (IAP), which guides both the information acquisition process and the tasking of acquisition assets. The students should also discuss the importance of direction and the requirement for the sum of acquired information responding to the commander’s Priority Intelligence Requirements.

Slide 17



Centralized Control, Decentralized Execution

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

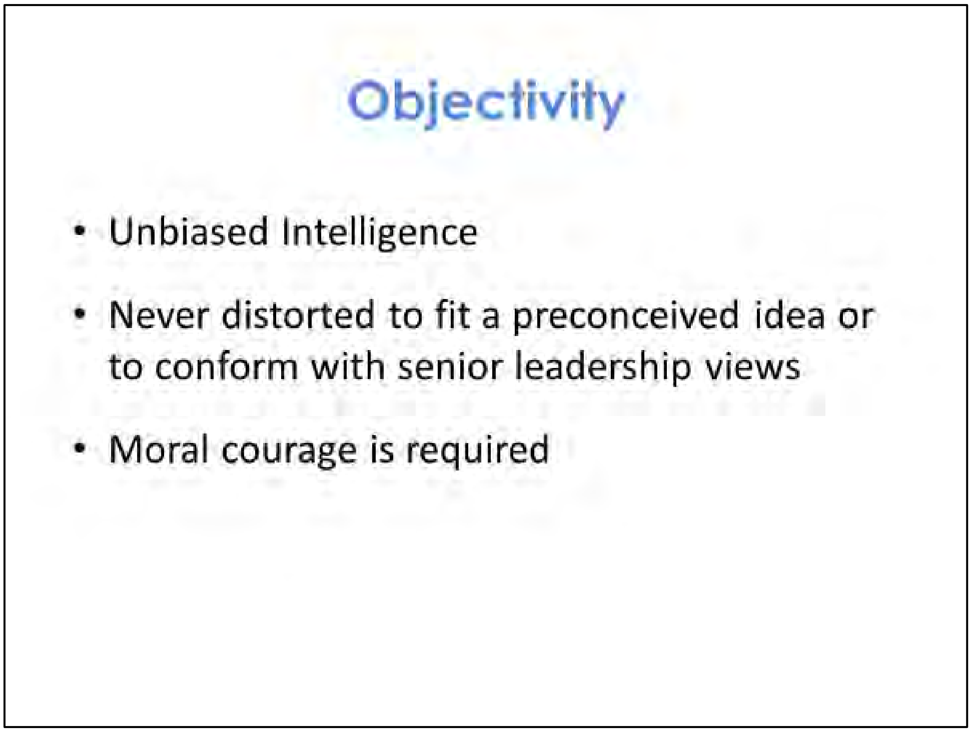
It is an accepted principle that peacekeeping-intelligence systems thrive under centralised control but with decentralised execution.

This principle means both the peacekeeping-intelligence effort is explicitly linked to the commander's requirement and that the MPKI organisation is operating as a homogenous system. Decentralised execution means that the disparate 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 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* *information requirement. This helps ensure that you have information from multiple different sources.*

Slide 18



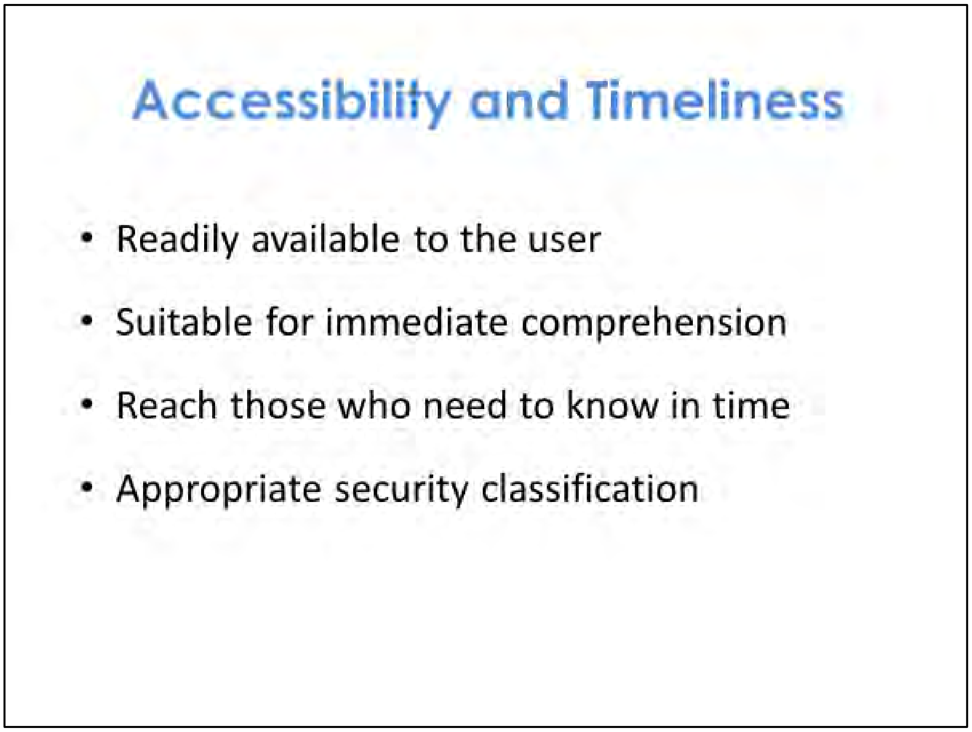
Objectivity

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

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

Equally, analysts must not become too emotionally invested in their assessments as it may skew their judgements.

Slide 19

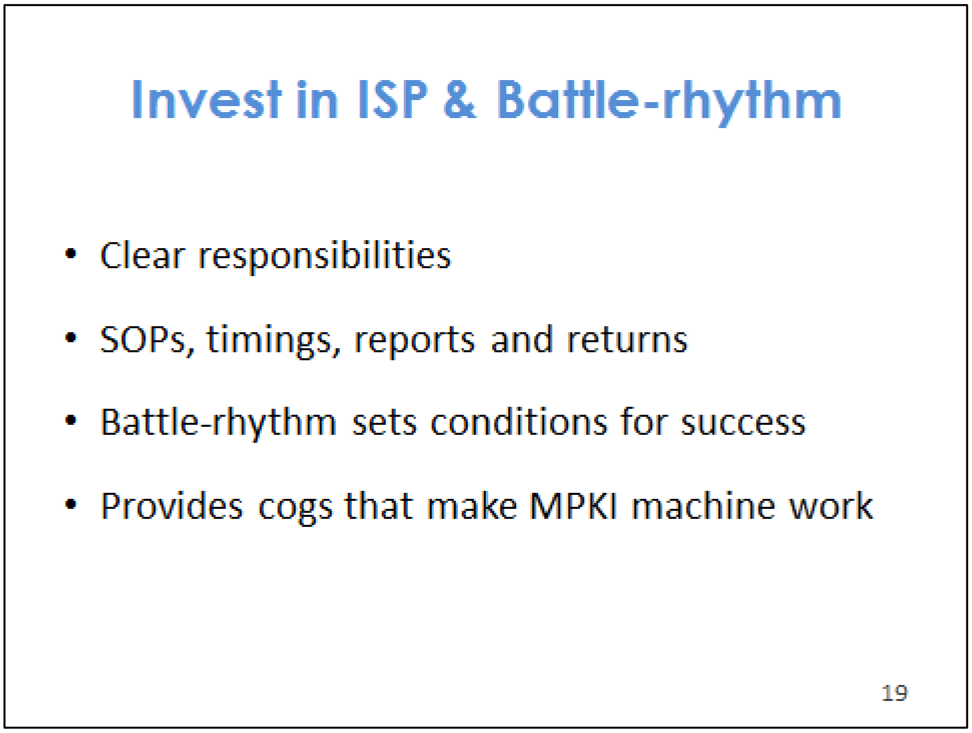


Accessibility and Timeliness

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

Ask the class if they think that there is a tendency for MPKI officers to over classify their intelligence products. Discuss the 'need to know' concept and the 'need to share' concept.

Slide 20



Invest in ISP & Battle-rhythm

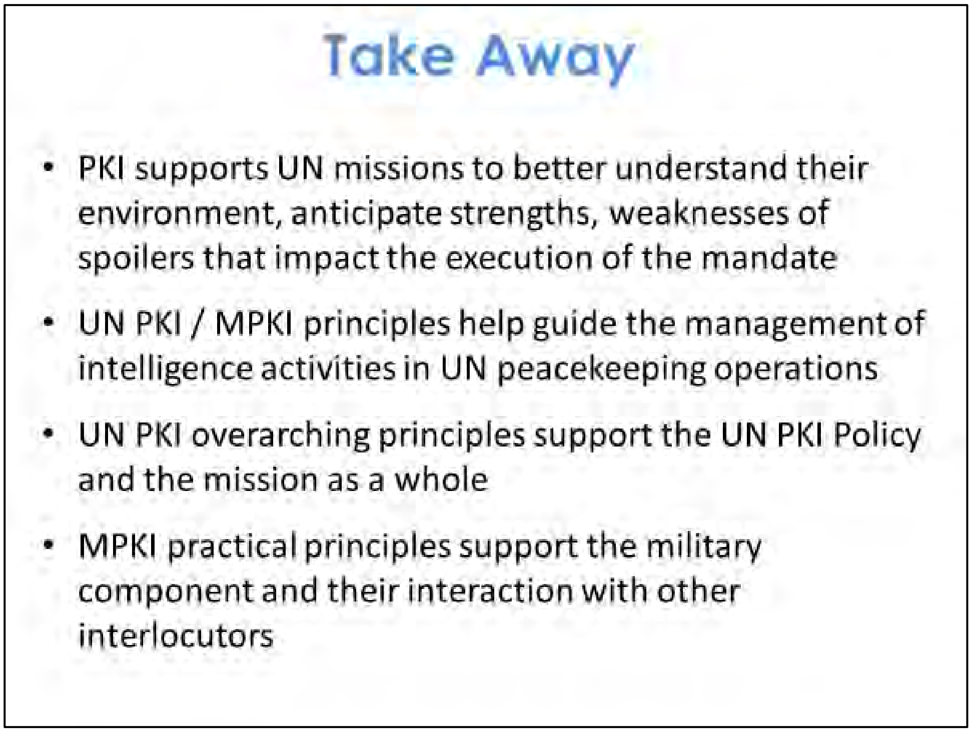
- Clear responsibilities
- SOPs, timings, reports and returns
- Battle-rhythm sets conditions for success
- Provides cogs that make MPKI machine work

19

The mission must invest time to ensure that the ISP is clear, up to date, well understood, and disseminated to those that need it. It needs to be made clear what an ISP is. This should not be an acronym at this point. This is not within the remit of the MPKI section. This will be drawn up by the Chief MICS/CJMAC.

Note to Instructor. *Here the students need to be reminded that most UN missions will have several other intelligence-producing and/or information* *acquiring entities such as the JMAC, UNDSS, the JOC, Political and Civil Affairs units, and UNPOL. The activities of these units must be centrally regulated.*

Slide 21



Take Away

- PKI supports UN missions to better understand their environment, anticipate strengths, weaknesses of spoilers that impact the execution of the mandate
- UN PKI / MPKI principles help guide the management of intelligence activities in UN peacekeeping operations
- UN PKI overarching principles support the UN PKI Policy and the mission as a whole
- MPKI practical principles support the military component and their interaction with other interlocutors

Summary

In conclusion, I would like to stress those peacekeeping-intelligence principles, processes and parameters, which have been set out to manage the peacekeeping-intelligence cycle, are key to the success of peacekeeping-intelligence. MPKI principles inform all activities of UN peacekeeping operations at all stages of the management of peacekeeping intelligence. In the next lesson we will further develop these concepts.

Lesson 1.2

MPKI Cycle and Management

The Lesson

Starting the Lesson

☞ ***Note to Instructor:***

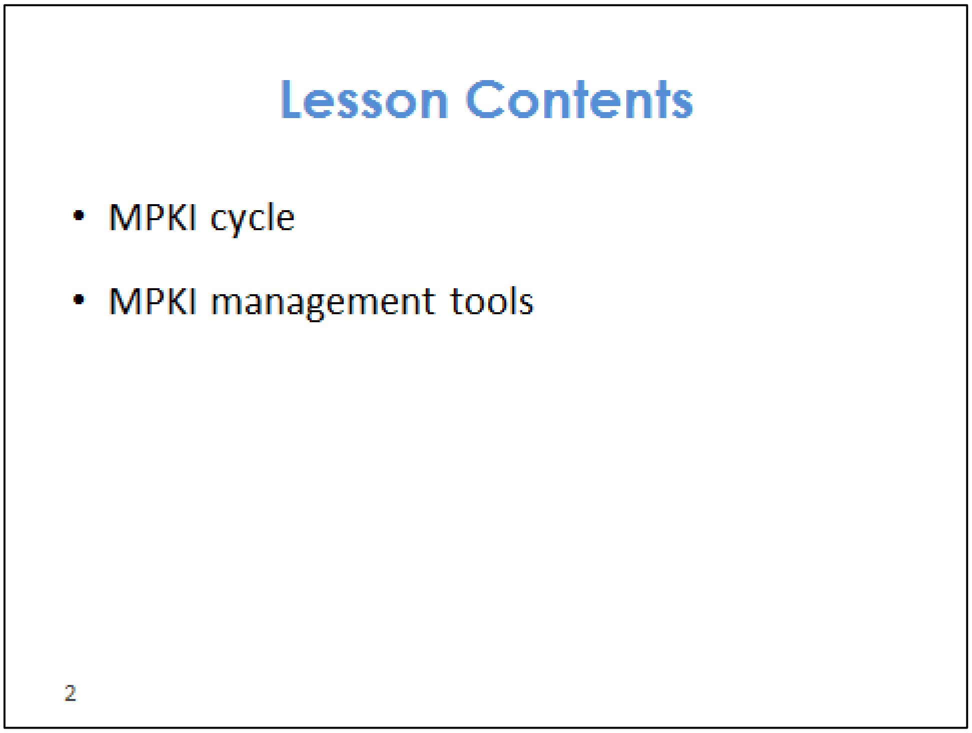
The UN Intelligence Policy includes a five step Intelligence Cycle; however, the MPKI / RTP agreed that a 4-step cycle was more common and best practice. A simpler 4-step PKI cycle aids in understanding. The difference being that the separate UN Policy step of Examination and Collation is included within Analysis in this RTP. The processes are the same; and the UN Intel handbook echoes this by also merging the two steps into one - Analysis.

Slide 1

Lesson 1.2 MPKI Cycle and Management

1

Slide 2



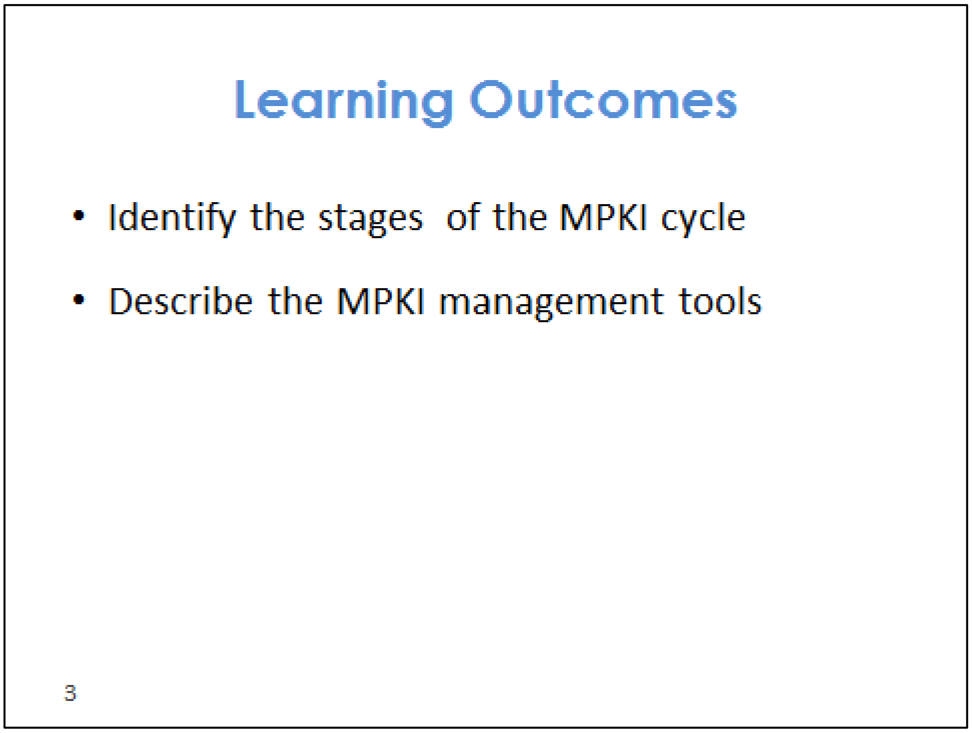
Lesson Contents

- MPKI cycle
- MPKI management tools

2

The MPKI management tools shown in this lesson are designed to show that the MPKI cell does not operate in a vacuum and that there are structures designed to manage mission-wide information and intelligence flows, incorporating all intelligence producing bodies such as the JMAC, UNDSS, UNPOL, JOC and the Military component, particularly on POC actions and force protection.

Slide 3



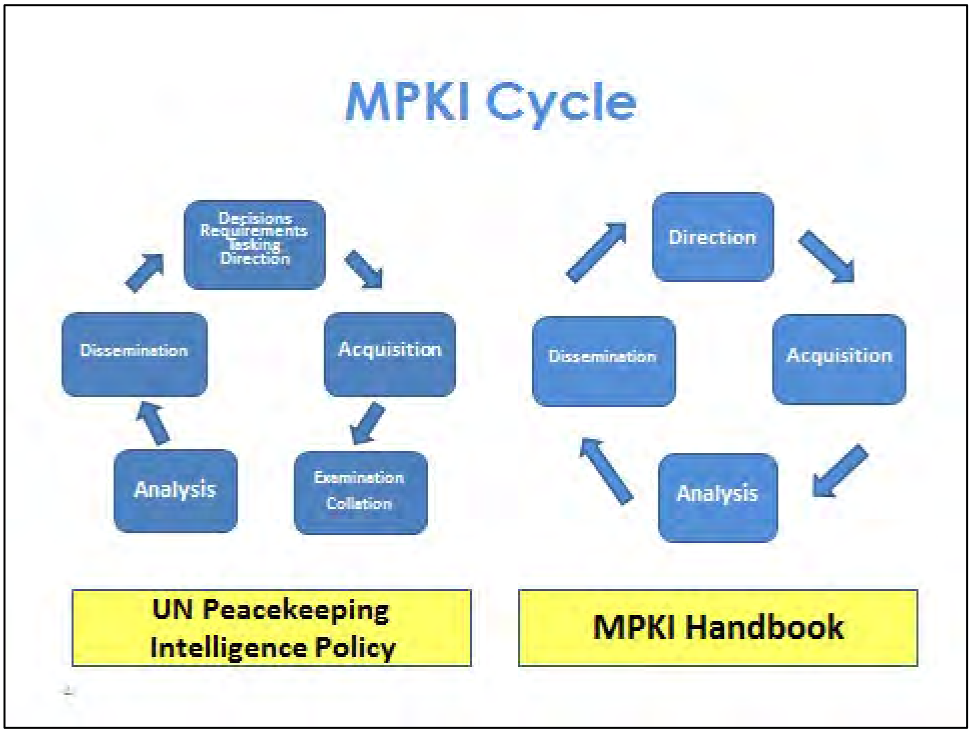
Learning Outcomes

- Identify the stages of the MPKI cycle
- Describe the MPKI management tools

3

At the end of this lesson, you should be able to perform the actions described on this slide. Take a moment to read and understand the requirements. This will help to focus on the most relevant aspects of the lesson.

Slide 4



MPKI Cycle

Decisions
Requirements
Tasking
Direction

Acquisition

Examination
Collation

Analysis

Dissemination

Direction

Acquisition

Analysis

Dissemination

UN Peacekeeping Intelligence Policy

MPKI Handbook

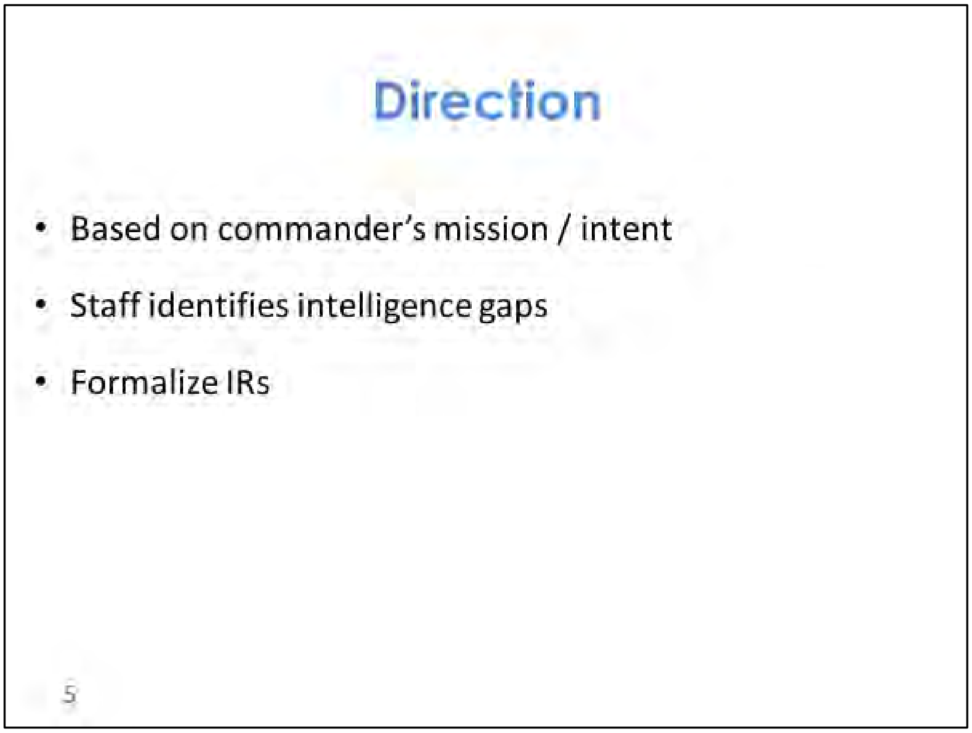
The MPKI cycle is the process by which data and/or information is converted into intelligence and made available to users. It is the mechanism used to produce MPKI. It is typically represented as a closed cyclical path of activities that takes you through direction, acquisition, analysis and dissemination.

It is important to note that if any part of this cycle fails, then the process does not work. If the direction is poor, then the wrong type of information is acquired. If the acquisition is poor, then the information may not be acquired at all. In both those cases, even if the MPKI section has the world's best analysts, the adage 'garbage in, garbage out' applies, whereby poor information is analysed, thereby giving a poor final intelligence product. If the information is good, yet the analysis is poor, it is an issue.

Once again, this will ensure the delivery of a poor final intelligence product. Finally, if dissemination practices are poor, the intelligence product – however brilliant it maybe – will not reach the right customer at the right time. There is no point in predicting that an armed group will attack at dawn if the commander does not receive it until 1000.

☞**Note to instructor:** *while the 4-step cycle in the Military Peacekeeping-Intelligence Handbook slightly differs in appearance from the 5-step cycle in the Peacekeeping-Intelligence Policy, the former incorporates examination and collation into a single step within the analysis, which is more common among military intelligence professionals.*

Slide 5



Direction

- Based on commander's mission / intent
- Staff identifies intelligence gaps
- Formalize IRs

5

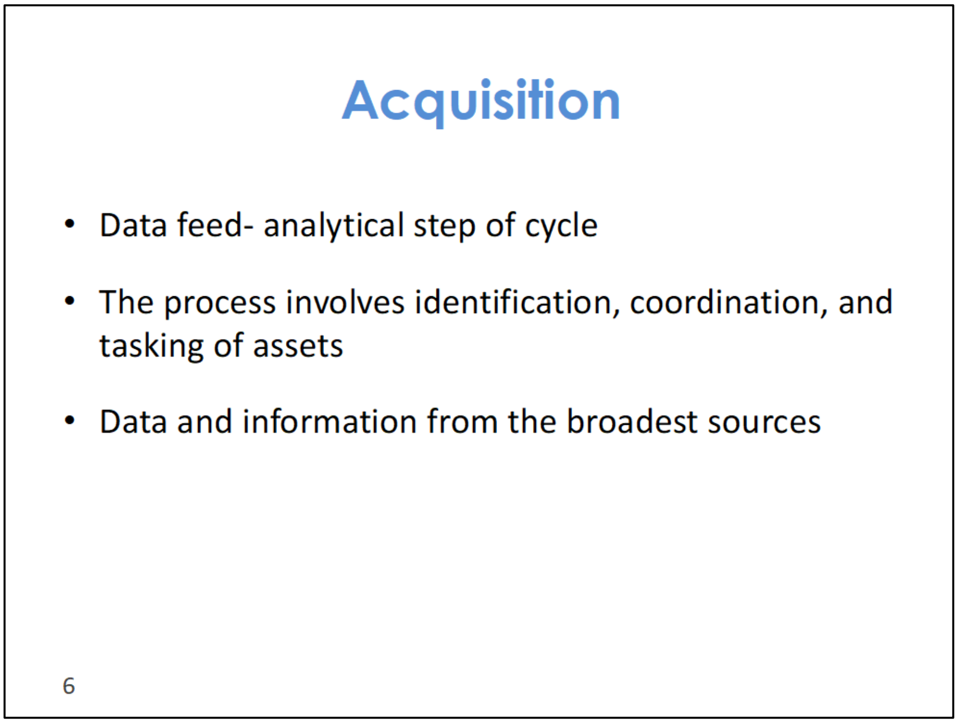
Clear direction from the commander, is the start point for the MPKI cycle. The direction outlines to the MPKI staff what the commander wants to know and ensures that the peacekeeping-intelligence staff has a clear focus for their acquisition efforts.

The direction is often taken from the following: commander's intent, the mission, the mandate, the MPKI cell's knowledge of the Operating Environment, and Commander's Critical Information Requirements (CCIRs).

Often the MPKI cell will have to present an IAP to the commander and his/her staff for approval, rather than being given PIRs. However, it is vital that this IAP is endorsed by the commander to give it the weight of an operation order.

☞ ***Note to instructor:*** *Since each step of the MPKI cycle will be explained in detail in Module 3 from an operational framework perspective, recommend providing the students with a conceptual overview and familiarisation of the materials.*

Slide 6



Acquisition

- Data feed- analytical step of cycle
- The process involves identification, coordination, and tasking of assets
- Data and information from the broadest sources

6

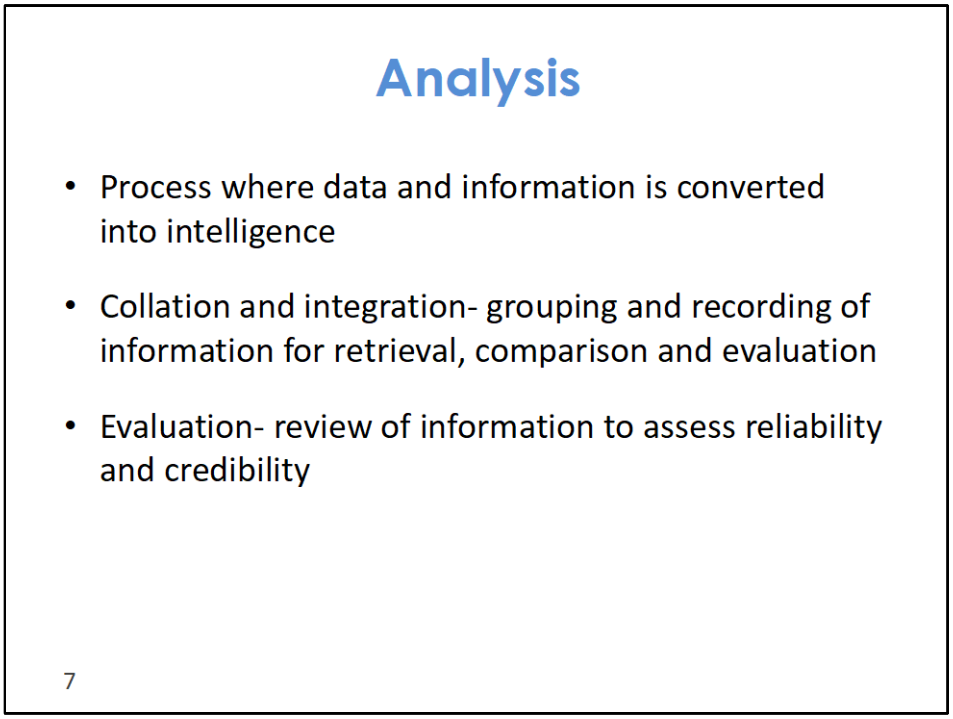
The acquisition of the data or information is the next step, which is required to feed the analytical step of the cycle.

It is important to note that the MPKI section will rarely have tasking authority over acquisition assets, as the operations section will normally be the tasking authority. Therefore, the MPKI cell must work to build relationships with other units, particularly the operations section, thereby fostering mutual understanding and encouraging mutual support.

It is also important that the MPKI cell gives feedback, whether positive or negative, to acquisition assets. This will serve to improve the acquisition process and to build and maintain a positive relationship.

It is important to note that Missions do not rely only on organic acquisition assets. Missions may also receive intelligence provided by Member States as well as other non-mission entities and shall establish mechanisms to facilitate the secure receipt and handling of such products. Modalities for sharing and the legal acquisition of information will be contained in the mission ISP.

Slide 7

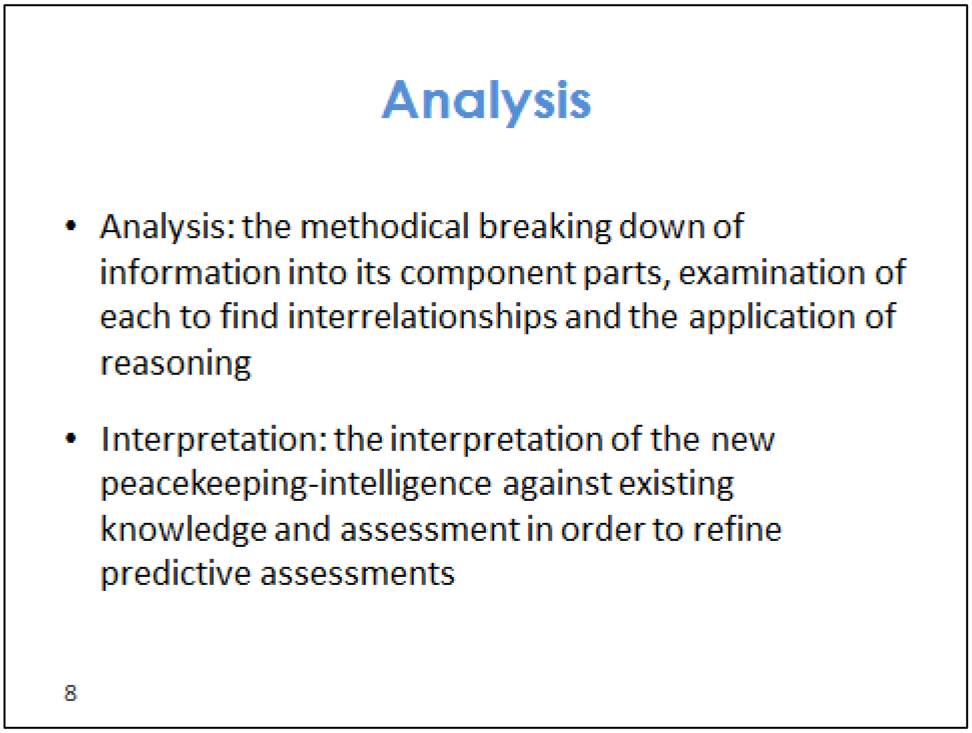


Analysis

- Process where data and information is converted into intelligence
- Collation and integration- grouping and recording of information for retrieval, comparison and evaluation
- Evaluation- review of information to assess reliability and credibility

7

Slide 8



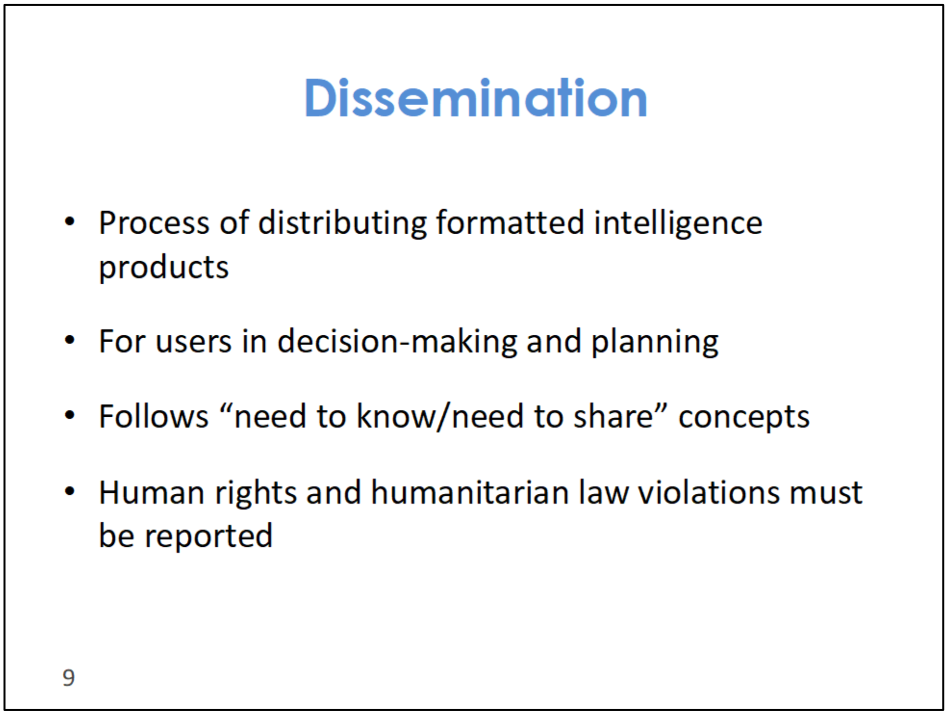
Analysis

- Analysis: the methodical breaking down of information into its component parts, examination of each to find interrelationships and the application of reasoning
- Interpretation: the interpretation of the new peacekeeping-intelligence against existing knowledge and assessment in order to refine predictive assessments

8

Strong analysis gives advance warning of events or courses of action that could threaten effective mandate implementation relating to the protection of UN personnel and civilians.

Slide 9



Dissemination

- Process of distributing formatted intelligence products
- For users in decision-making and planning
- Follows “need to know/need to share” concepts
- Human rights and humanitarian law violations must be reported

9

Some information must be communicated directly to leadership 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/or to force protection. However, this information must be adequately caveated if it has not been processed. For example, the commander must be informed that it has not yet been corroborated or validated if this is the case, or that it is a single source.

Strong dissemination protocols must be in place to ensure that intelligence products reach leadership in a timely and secure manner.

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

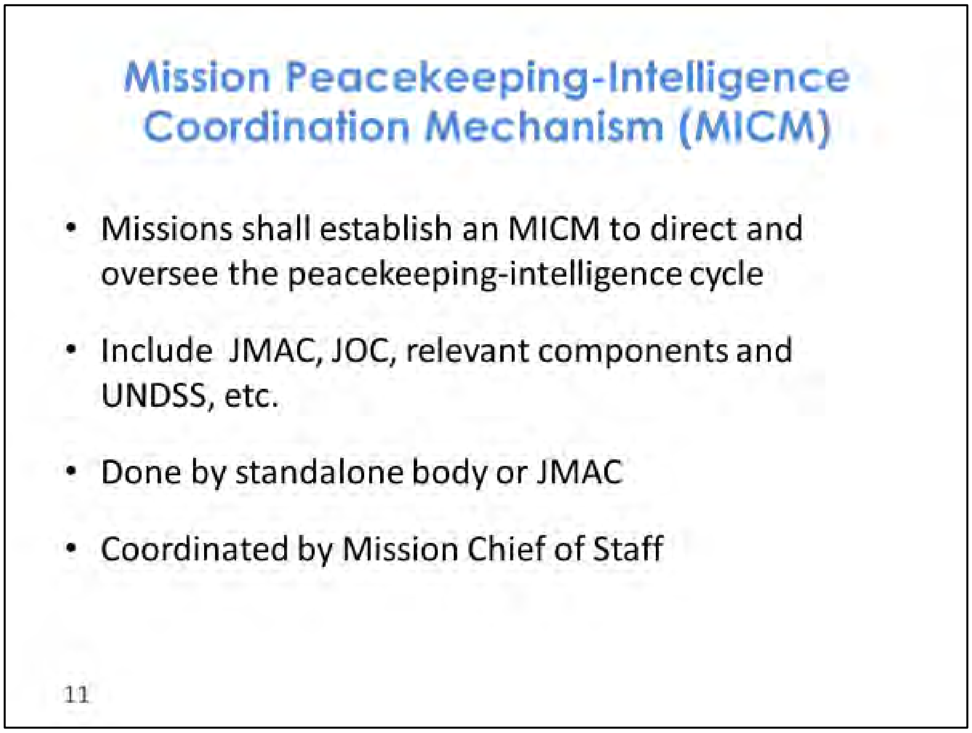
Slide 10

MPKI Management Systems and Tools

10

Now we will shift from principles to the management tools and systems that help support and drive the intelligence cycle.

Slide 11



Mission Peacekeeping-Intelligence Coordination Mechanism (MICM)

- Missions shall establish an MICM to direct and oversee the peacekeeping-intelligence cycle
- Include JMAC, JOC, relevant components and UNDSS, etc.
- Done by standalone body or JMAC
- Coordinated by Mission Chief of Staff

11

The purpose of the Mechanism is to provide centralised control, direction and coordination of the mission's peacekeeping-intelligence system. It may be a standalone body, while in other cases, the functions may be played by the JMAC.

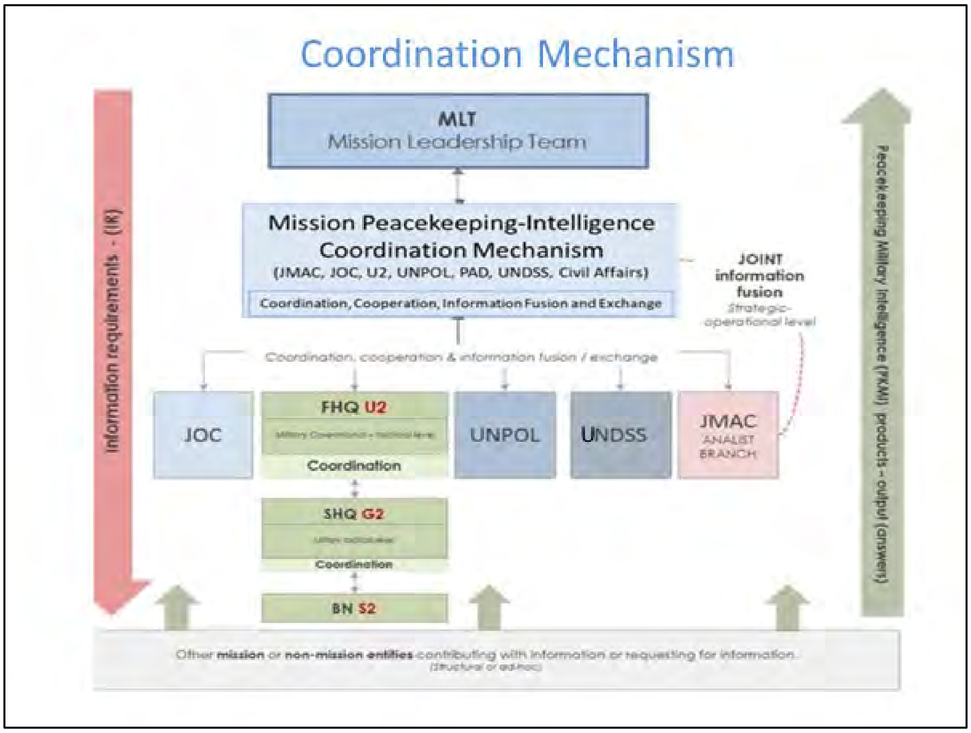
The functions of the MICM shall preferably be coordinated by the Mission Chief of Staff in his/her role as the Chair of the Mechanism. The primary responsibilities of the MICM include drawing strategic guidance from the senior mission leadership and translating this guidance into PIRs and IRs, developing and maintaining ISP and management of the IAP and the acquisition effort, satisfying all leadership IRs.

Ideally, the MICM would allocate specific PIRs and IRs to the various mission components, within their areas of competence. For example, PIRs relating to political issues would likely be allocated to the JMAC, while PIRs relating to security might be given to UNDSS, to the Military component, and to UNPOL. This mission-level IAP is a tool for de-conflicting acquisition activities.

The MICM should meet regularly, thereby ensuring that all mission intelligence producing bodies share information. This process also ensures that no information is 'lost', ensuring that the 'dots can be connected'.

Most important to remember is that you do not do your job in isolation.

Slide 12



Coordination Mechanism

MLT
Mission Leadership Team

Mission Peacekeeping-Intelligence Coordination Mechanism
(JMAC, JOC, U2, UNPOL, PAD, UNDSS, Civil Affairs)
Coordination, Cooperation, Information Fusion and Exchange

JOINT information fusion
Strategic-operational level

Coordination, cooperation & information fusion / exchange

JOC

FHQ U2
Military Operational – tactical level
Coordination

UNPOL

UNDSS

JMAC
ANALIST BRANCH

SHQ G2
Coordination

BN S2

Other mission or non-mission entities contributing with information or requesting for information
(Structural or ad-hoc)

Information requirements - (IR)

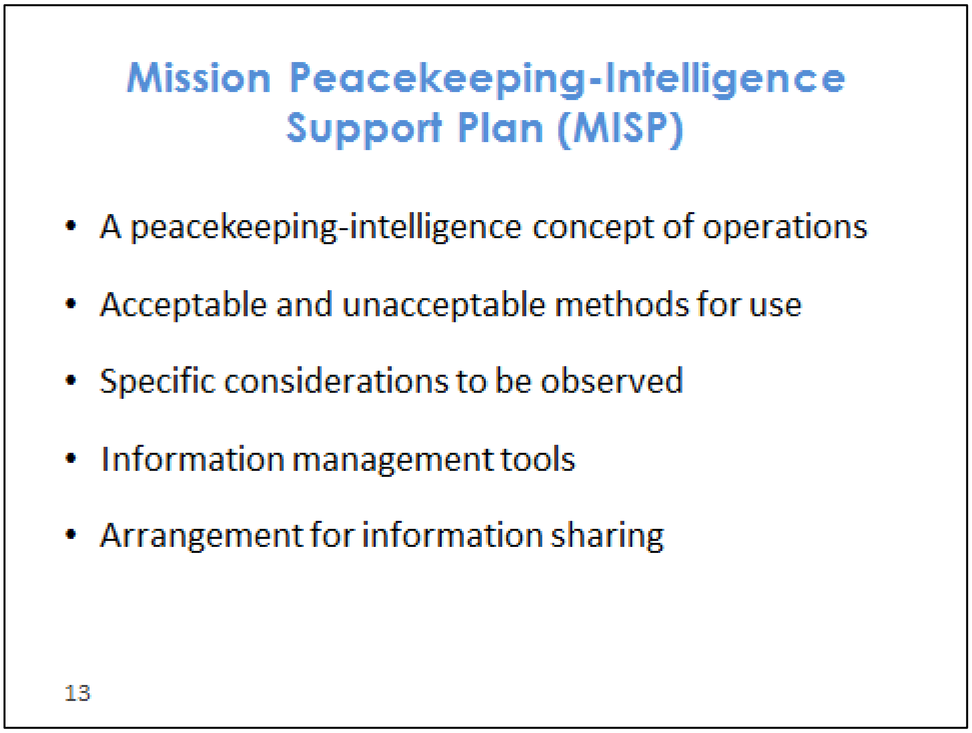
Peacekeeping Military Intelligence (PKMI) products – output (answer)

As you can see, there are various peacekeeping-intelligence entities in a UN peacekeeping mission, each with its own roles and responsibilities.

It is imperative that a Mission Peacekeeping-intelligence Coordination Mechanism is established to exercise centralised control of peacekeeping-intelligence activities to ensure unity of peacekeeping-intelligence effort throughout the mission.

For Interaction. *Ask the students how the MICM coordinates mission PKI entities. Among the responses required here are, the imposition of a mission-level Information Acquisition Plan (IAP), which gives each entity the duty for acquiring information for one or several HoM PIRs; ensuring that regular meetings are held between all entities, which ensure that information is shared. For example, often political information acquired by the JMAC can enhance the U2's situational awareness and understanding.*

Slide 13

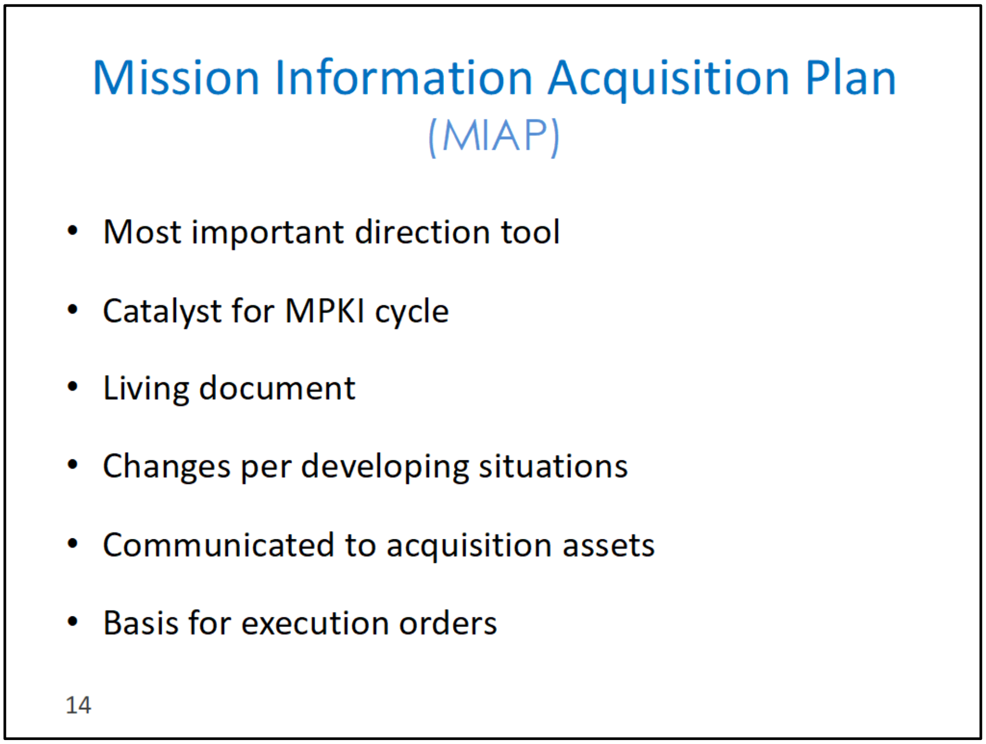


Mission Peacekeeping-Intelligence Support Plan (MISP)

- A peacekeeping-intelligence concept of operations
- Acceptable and unacceptable methods for use
- Specific considerations to be observed
- Information management tools
- Arrangement for information sharing

13

Slide 14



Mission Information Acquisition Plan (MIAP)

- Most important direction tool
- Catalyst for MPKI cycle
- Living document
- Changes per developing situations
- Communicated to acquisition assets
- Basis for execution orders

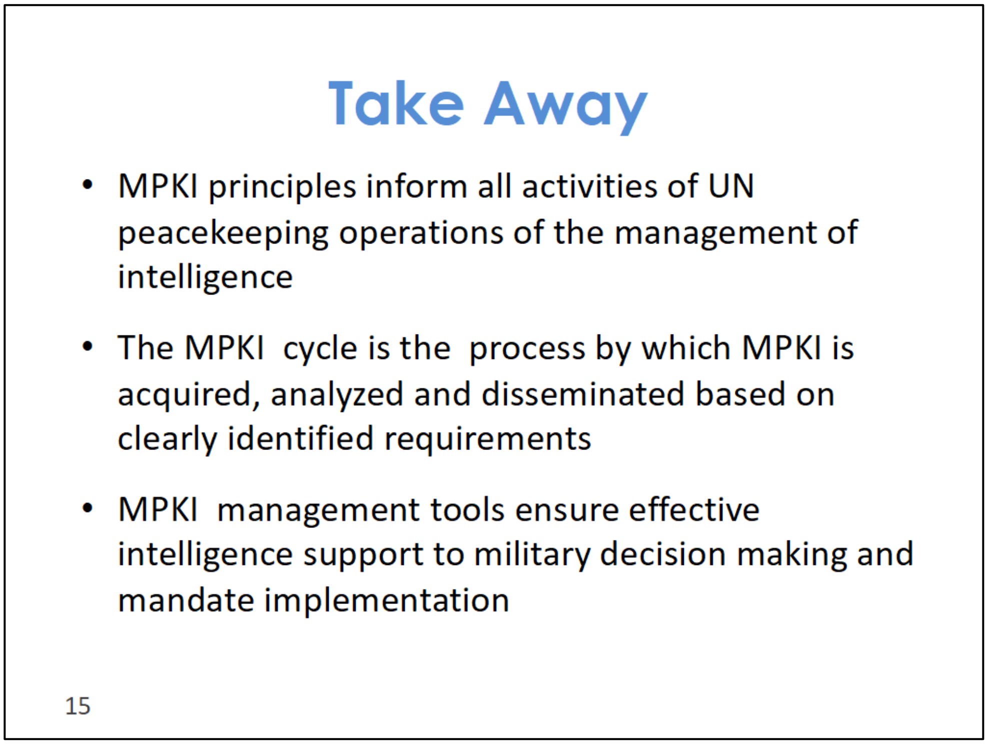
14

Mission components should produce their own Component Peacekeeping-Intelligence Acquisition Plan bringing all Mission-imposed and deducted tasks and including Component leadership new CCIRs and tasking Components assets, according to the commander's priorities and assets capabilities.

IAP is the basis for an executive order. It may be written and published in the operation order format following the mission's SOP. The staffs use the IAP to task, direct, and manage acquisition assets (both assigned and attached assets) to acquire against the requirements. It is worth noting that the Operations Officer tasks information acquisition assets that are not OPCON to the MPKI cell. Generally, the MPKI cell will only have tasking authority over ISR assets.

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 word ‘collect’.*

Slide 15



Take Away

- MPKI principles inform all activities of UN peacekeeping operations of the management of intelligence
- The MPKI cycle is the process by which MPKI is acquired, analyzed and disseminated based on clearly identified requirements
- MPKI management tools ensure effective intelligence support to military decision making and mandate implementation

15

Summary

In conclusion, we would like to stress those peacekeeping-intelligence principles, processes and parameters addressed in lesson 1 that are key to setting the framework for the management of the peacekeeping-intelligence cycle and UN PKI / MPKI management systems and tools. This framework is the key to the success of peacekeeping-intelligence. Here are a few areas to take away from this lesson:

- MPKI principles inform all activities of UN peacekeeping operations at all stages of the management of peacekeeping intelligence
- The MPKI cycle is the process by which MPKI is acquired, analysed and disseminated based on clearly identified requirements
- MPKI management tools ensure effective intelligence support to military decision making and mandate implementation

Learning Activity

RESOURCES
N/A

APPROX. TIME
10 minutes

PREPARATION
Ask the participants to answer the following questions.

NOTE TO INSTRUCTORS:
Reinforce the learning outcomes and access the knowledge of the group and individuals by asking these questions. Discuss the answers as a group.

Question:

Ask the participants why peacekeeping intelligence is important and how the MPKIO and other Force HQ staffs support the Intel cycle.

Lesson 1.3

MPKI Structure & Roles

The Lesson

Starting the Lesson

For an interactive start to the Lesson engage participants to seek their understanding of the MPKI structure and roles in a UNPKO. Who do they work for?

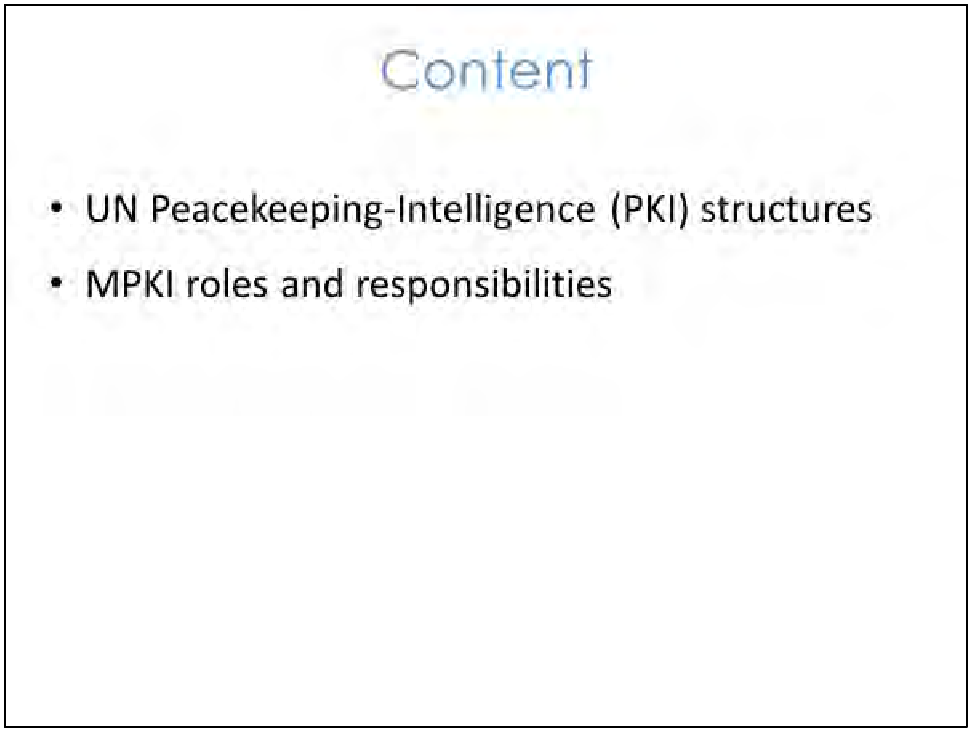
Note to instructor *– Review Chapter 2 and 3 of United Nations Military Peacekeeping-Intelligence Handbook.*

Slide 1

Lesson 1.3
MPKI Structure & Roles

We will give an overview of the roles and responsibilities of the PKI structure. As an MPKIO, you should be in the mindset of wearing the Blue Beret and being fully integrated into the mission concept, operational and information, and intelligence frameworks. The MPKIO has its own unique skills, characteristics that add a dimension in the accomplishment of MPKI tasks and therefore, the Mission's mandate. Because you are a trained and experienced intelligence officer, you can provide a predictive perspective of what is happening on the ground and help populate the common operating picture (COP). You are key to feeding information into the MDMP framework.

Slide 2

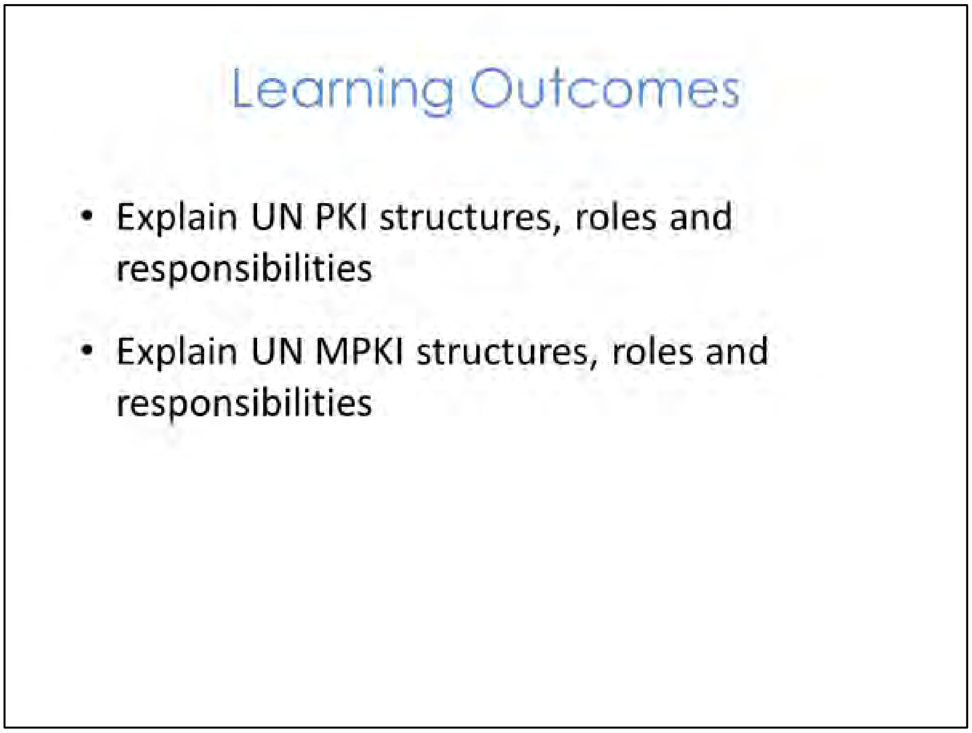


Content

- UN Peacekeeping-Intelligence (PKI) structures
- MPKI roles and responsibilities

The topics that will be covered in this lesson.

Slide 3

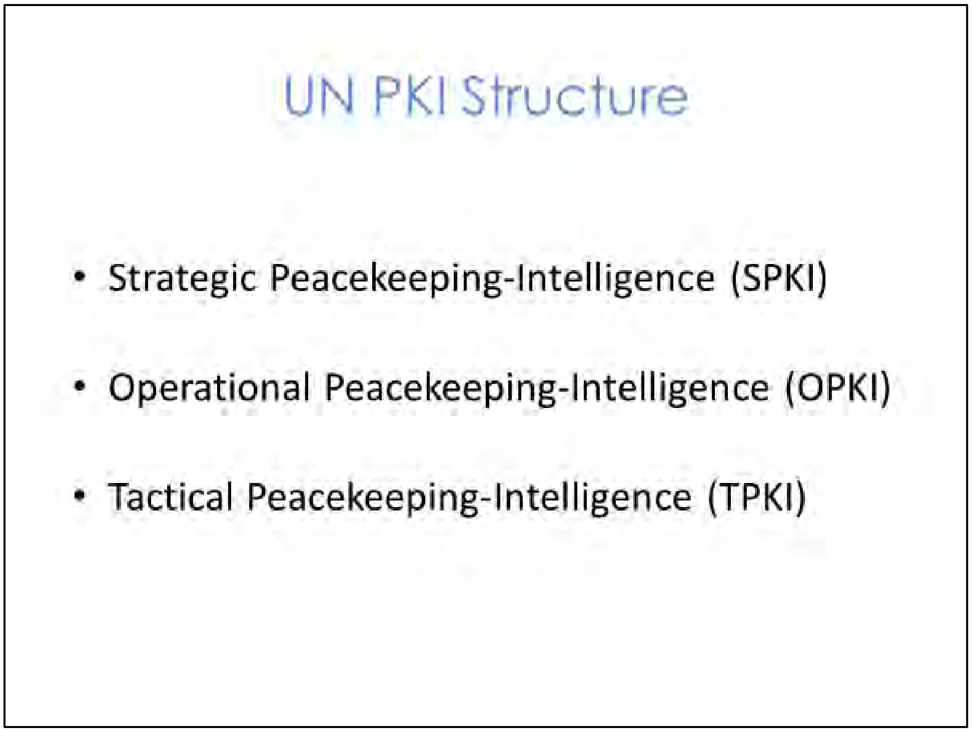


Learning Outcomes

- Explain UN PKI structures, roles and responsibilities
- Explain UN MPKI structures, roles and responsibilities

At the end of this lesson, you should be able to perform the actions described on the slide. Please take a moment to read and understand the requirements. This may help you to focus on the most relevant aspects of the lesson.

Slide 4

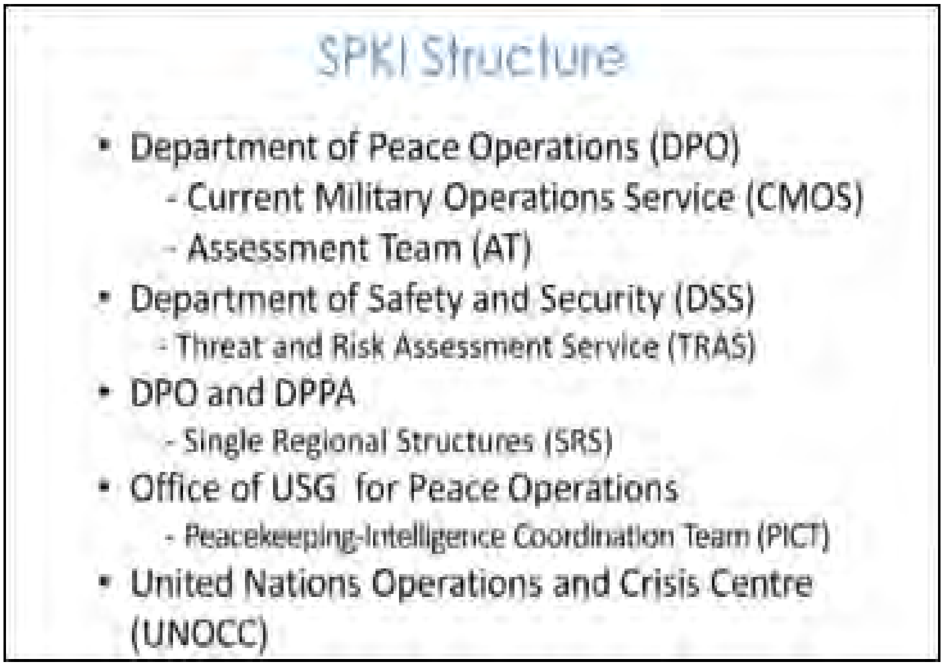


UN PKI Structure

- Strategic Peacekeeping-Intelligence (SPKI)
- Operational Peacekeeping-Intelligence (OPKI)
- Tactical Peacekeeping-Intelligence (TPKI)

The UN Peacekeeping-Intelligence Cycle is designed to direct, acquire, collate, analyse, and disseminate peacekeeping intelligence at the strategic, operational, and tactical levels. This is necessary to inform decision making at all levels of the UN structure.

Slide 5



SPKI Structure

- Department of Peace Operations (DPO)
  - Current Military Operations Service (CMOS)
  - Assessment Team (AT)
- Department of Safety and Security (DSS)
  - Threat and Risk Assessment Service (TRAS)
- DPO and DPPA
  - Single Regional Structures (SRS)
- Office of USG for Peace Operations
  - Peacekeeping-Intelligence Coordination Team (PICT)
- United Nations Operations and Crisis Centre (UNOCC)

Within the Department of Peace Operations (DPO), the Office of Military Affairs (OMA) has the **Current Military Operations Service (CMOS)** dealing with current information from the military channel in UN peacekeeping missions, as well as an **Assessment Team (AT),** composed of trained and experienced intelligence officers, focusing on the production of regional peacekeeping-intelligence assessments, and information or intelligence sharing with Member States.

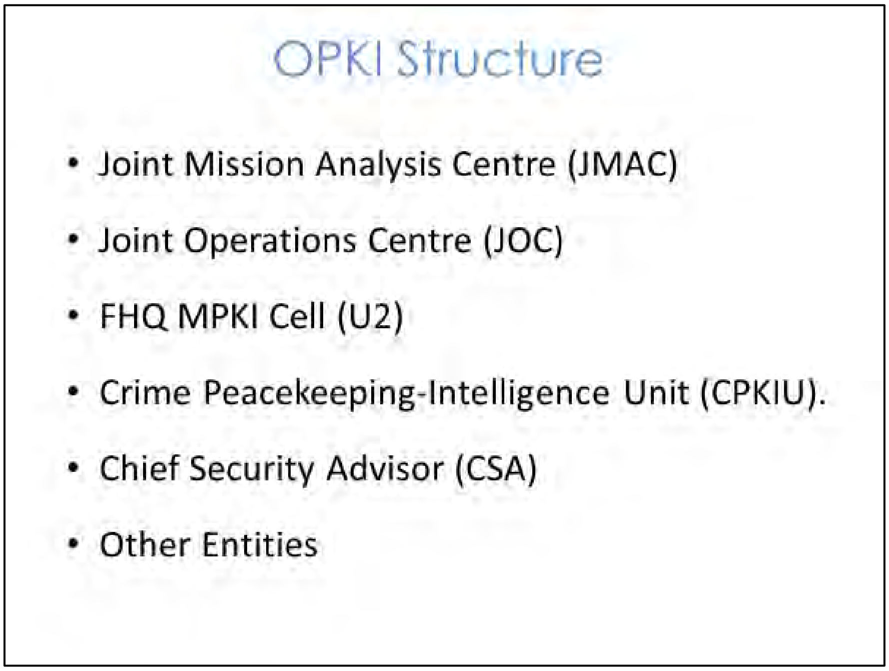
The Department of Safety and Security (DSS) has a **Threat and Risk Assessment Service** in charge of providing intelligence through regional- and country-specific threat assessments to support field duty stations, and to ensure the safety and security of all civilian personnel.

In addition, the **Single Regional Structures** reporting to both DPO and the Department of Political and Peacebuilding Affairs (DPPA) serve as a mechanism to deliver strategic and operational guidance to field missions.

Furthermore, the **Peacekeeping-Intelligence Coordination Team (PICT)** in the Office of the Under-Secretary-General for Peace Operations oversees the coordination of peacekeeping-intelligence activities by all participating actors at UNHQ and in the field ensuring compliance with the Peacekeeping-Intelligence Policy Framework.

The **UN Operations and Crisis Centre (UNOCC)** monitors and updates the situation development in the field, issues "alerts" in case of major incidents and events, produces daily integrated situation reports and briefings, provides information or intelligence support to field missions and UN headquarters.

Slide 6



OPKI 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

Joint Mission Analysis Centre (JMAC).

It is an integrated entity comprising civilian, military, and police personnel, established to support mission-level planning and decision-making through the provision of integrated analysis and predictive assessments. It manages the Peacekeeping-Intelligence Requirements (IRs) of the HoM and the Mission Leadership Team (MLT) through the development of a mission-level Information Acquisition Plan (IAP), through collating and analysing all-source information, and by identifying threats and other challenges to the mandate.

The JMAC acquires and analyses multi-source information to prepare mid- to long-term integrated analysis and assessments for strategic, operational and contingency planning, decision-making and crisis management. In some missions, the JMAC fulfils an important leading role in the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM) that directs and oversees the peacekeeping-intelligence cycle within the mission.

The Chief JMAC is a civilian, who reports directly to the HoM. The Peacekeeping-Intelligence Policy indicates that the Chief JMAC may, in some instances, lead the MICM. All MPKI and other relevant information should be shared with the JMAC and the MICM, particularly where it relates to the 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. JOCs are also responsible for coordinating the operational activities of the components to ensure they are complementary and coherent. 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 UNCT/HCT entities.

The JOC focuses on current operations and can also support short-term planning. JOC reporting to its clients must reflect the composition (multidimensional or more traditional PKO) of the mission. In the context of MPKI, the JOC and the JMAC will align their activities in the MICM to avoid any gaps in the provision of situational awareness and analytical support to mission leadership. The JOC should be co-located in the same operational space as the Military Operations Centre (MOC), Police Operations Centre (POC) and the Security Operations Centre (SOC), or their equivalents where they exist.

The military component ensures that daily situation reports, and relevant information is sent to the JOC daily or more frequently, as required. It is important to recognize that the sharing relationship must be '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).

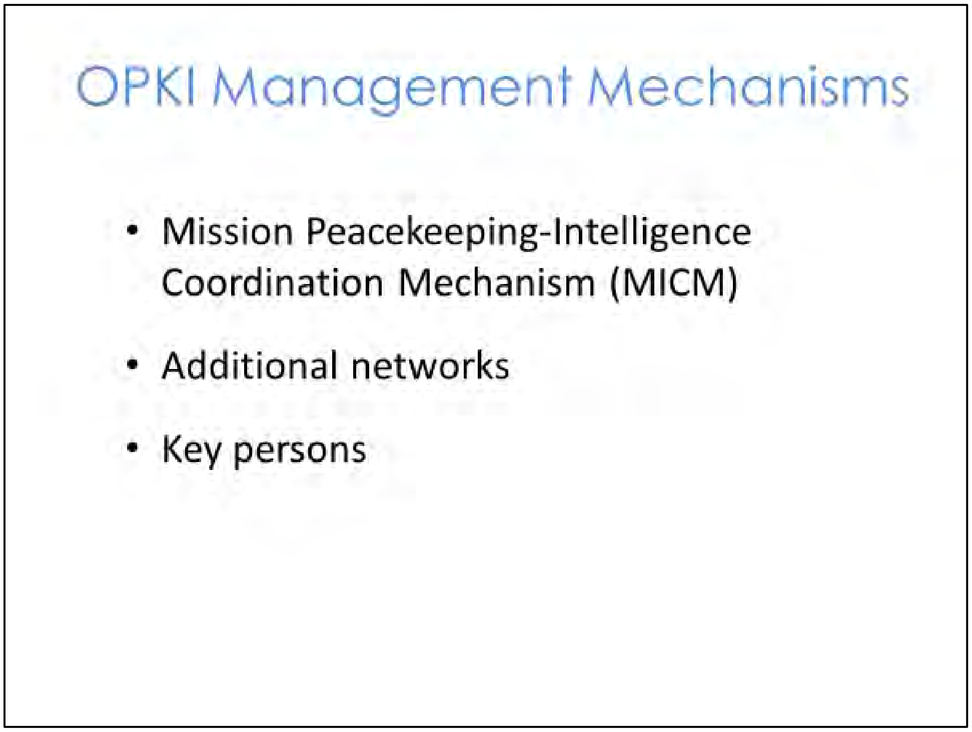
Force Headquarters (FHQ) MPKI Cell (U2). While the U2 cell is obviously part of the MPKI structure, it is important to recognize that it is also part of the Mission's OPKI structure. Military units beneath the FHQ level often have unique access and a valuable perspective on the tactical situation. As 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 protection and security advice for UN civilian personnel, the CSA and other UNDSS personnel have access to security-related information. As such, they have much to offer to the MPKI organisation.

Other Entities. Political Affairs, Civil Affairs, Liaison, Civil-Military Affairs personnel, as well as those working under Disarmament, Demobilisation, and Reintegration (DDR) mandates 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 7



OPKI Management Mechanisms

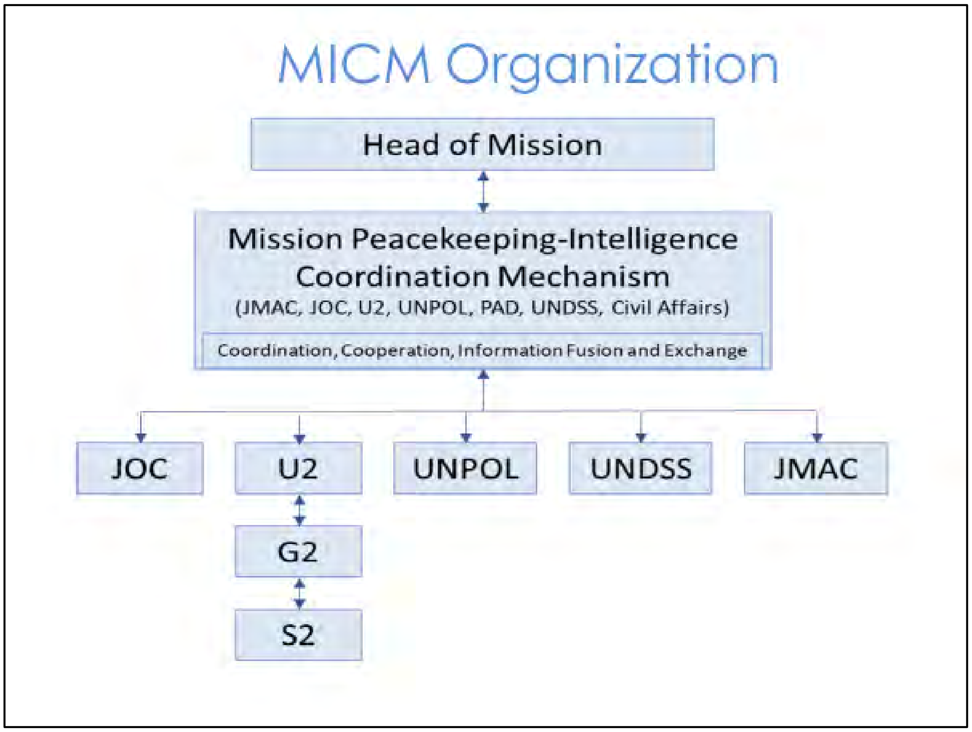
- Mission Peacekeeping-Intelligence Coordination Mechanism (MICM)
- Additional networks
- Key persons

UN Peacekeeping-Intelligence Management Mechanisms is established for better cooperation and coordination among the OPKI providers throughout a UN mission.

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 operational peacekeeping-intelligence. This cooperation is achieved through UN Peacekeeping-Intelligence Management Mechanisms at the operational level.

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

Slide 8



MICM Organization

Head of Mission

Mission Peacekeeping-Intelligence Coordination Mechanism

(JMAC, JOC, U2, UNPOL, PAD, UNDSS, Civil Affairs)

Coordination, Cooperation, Information Fusion and Exchange

JOC

U2

G2

S2

UNPOL

UNDSS

JMAC

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

This slide shows the generic structure of MICM organisation. The exact nature of the MICM will vary from mission to mission, but the fundamentals are as follows:

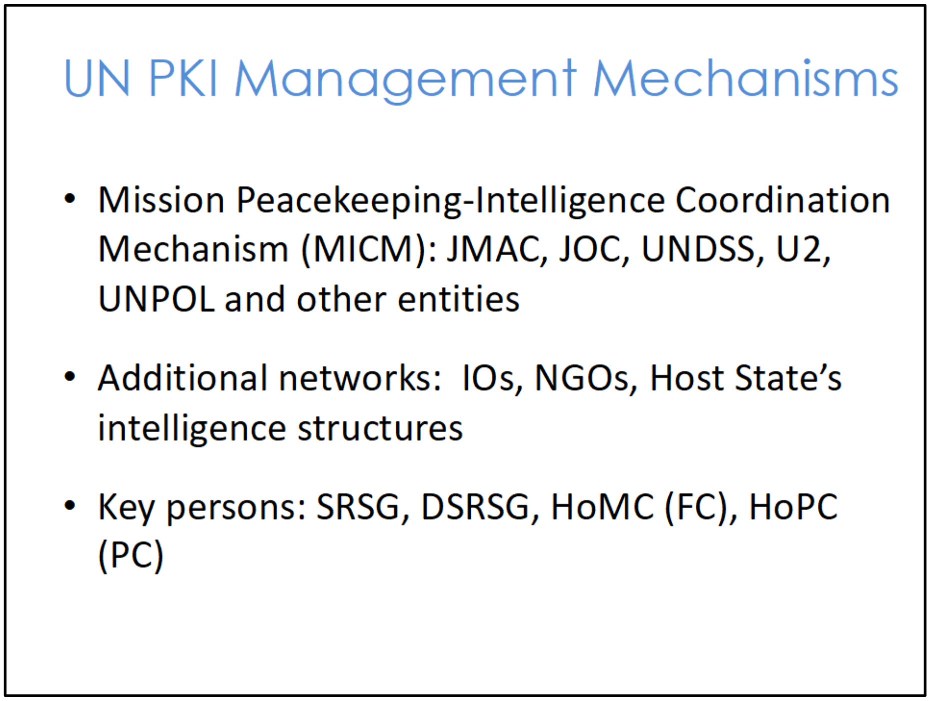
- The structure is comprised of mission entities responsible for peacekeeping intelligence acquisition, analysis, and dissemination. This will typically include the JMAC, JOC, UNDSS, and the relevant military and police components (such as the U2). Other mission entities may be invited to participate, as required
- The purpose of the MICM is to provide centralised control (allowing de-centralised execution), direction and coordination of the mission's peacekeeping-intelligence system
- The functions of the MICM shall preferably be coordinated by the Mission Chief of Staff in his/her role as the Chair of the Mechanism, or maybe played by the JMAC, while in other cases, a stand-alone body may be necessary

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

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

It is important to note that some of the MPKI IRs will originate from the 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.

Slide 9



UN PKI Management Mechanisms

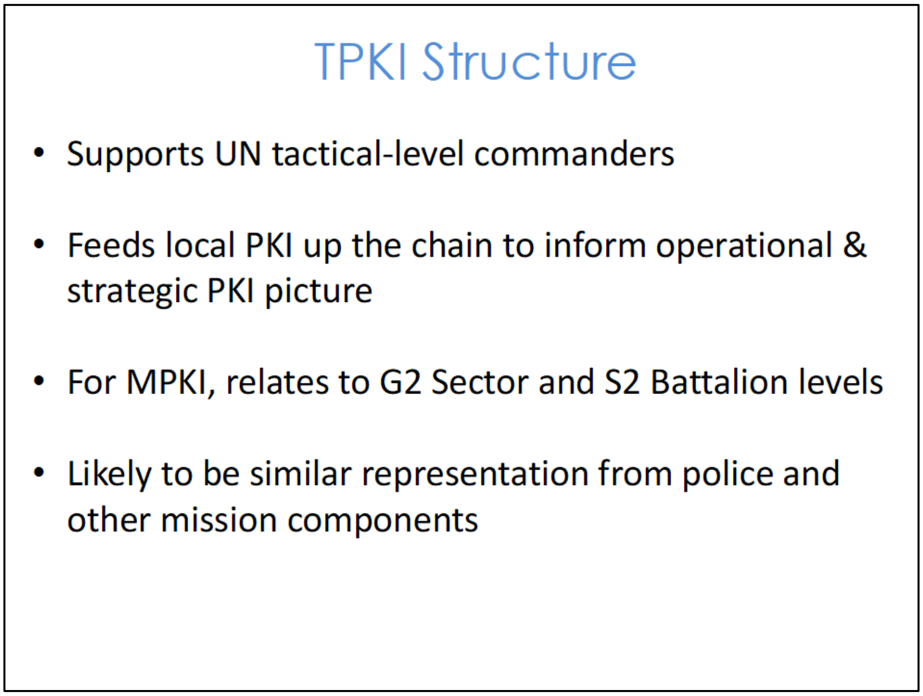
- Mission Peacekeeping-Intelligence Coordination Mechanism (MICM): JMAC, JOC, UNDSS, U2, UNPOL and other entities
- Additional networks: IOs, NGOs, Host State's intelligence structures
- Key persons: SRSG, DSRSG, HoMC (FC), HoPC (PC)

Besides the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM), there are other elements worth mentioning here, which may play a very important role in the PKI management mechanism. They are additional networks linked to IOs, NGOs, and Host State's intelligence structures. SRSG is one of the most important key persons contributing to the mechanism.

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

Key persons. There are several key persons, such as SRSG, DSRSG, HoMC(FC), HoPC(PC), who are, necessarily, involved in the peacekeeping-intelligence process. The SRSG, for example, must give guidance on their peacekeeping-intelligence priorities to the MICM. Always remember, due to their unique position, access and attendance at meetings, they can be a significant source of information.

Slide 10



TPKI Structure

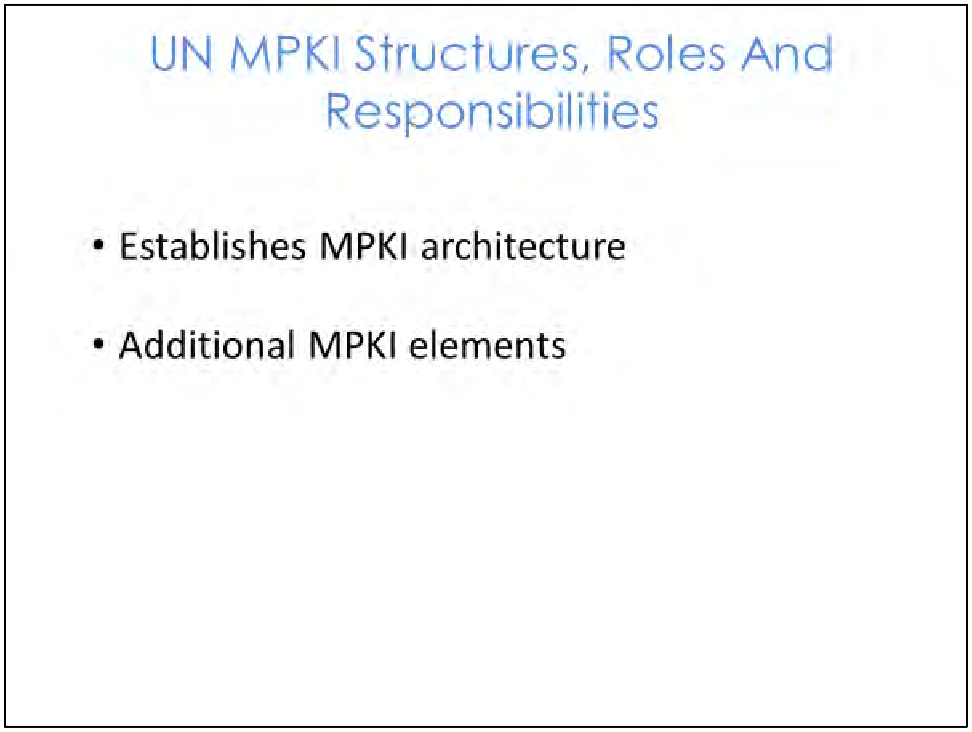
- Supports UN tactical-level commanders
- Feeds local PKI up the chain to inform operational & strategic PKI picture
- For MPKI, relates to G2 Sector and S2 Battalion levels
- Likely to be similar representation from police and other mission components

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

In many large UN peacekeeping mission areas, the G2 must also be able to provide a short- and medium-term analysis by acquiring and analyzing information from multiple sources and preparing integrated analysis and predictive assessments to support the decision-making, planning, and crisis management of the Sector Commander.

Just because it is conducted at the lowest level does not mean that TPKI is not important. TPKI or even unprocessed information acquired at the tactical level may have strategic importance.

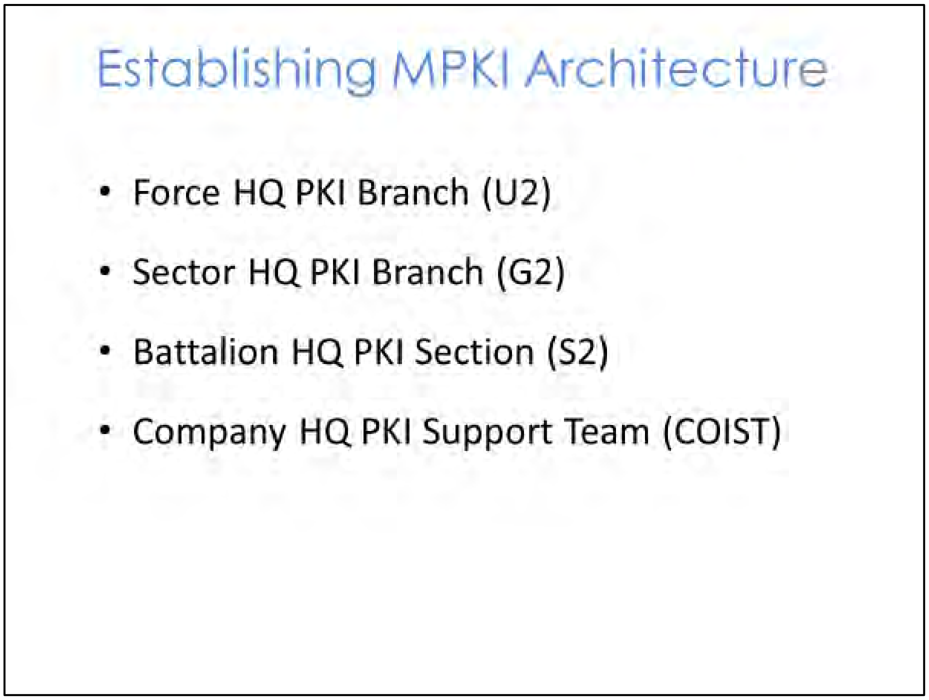
Slide 11



UN MPKI Structures, Roles And Responsibilities

- Establishes MPKI architecture
- Additional MPKI elements

Slide 12



Establishing MPKI Architecture

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

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

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

The outline of functions and tasks at each level are as follows:

FHQ U2 Branch. Within the FHQ, the U2 Branch is responsible for providing MPKI support to the Force Commander and the other functions in the FHQ such as planning and operations. All peacekeeping-intelligence support should aim at enhancing situational awareness and the safety and security of UN personnel, as well as informing activities and operations related to the protection of civilians. At this level, there are likely to be separate functions within the MPKI structure supporting the Direction, Acquisition, Analysis and Dissemination requirements of the MPKI cycle.

The peacekeeping-intelligence assessments are generally mid- to long-term and designed to support the Force Commander's planning process; although there may also be a need to respond to crises. Key functions are to provide peacekeeping-intelligence assessments to support decision making and force protection measures. In addition to the requirement to provide peacekeeping-intelligence support to the FHQ, the U2 also has the responsibility to lead and direct the mission-wide MPKI structure.

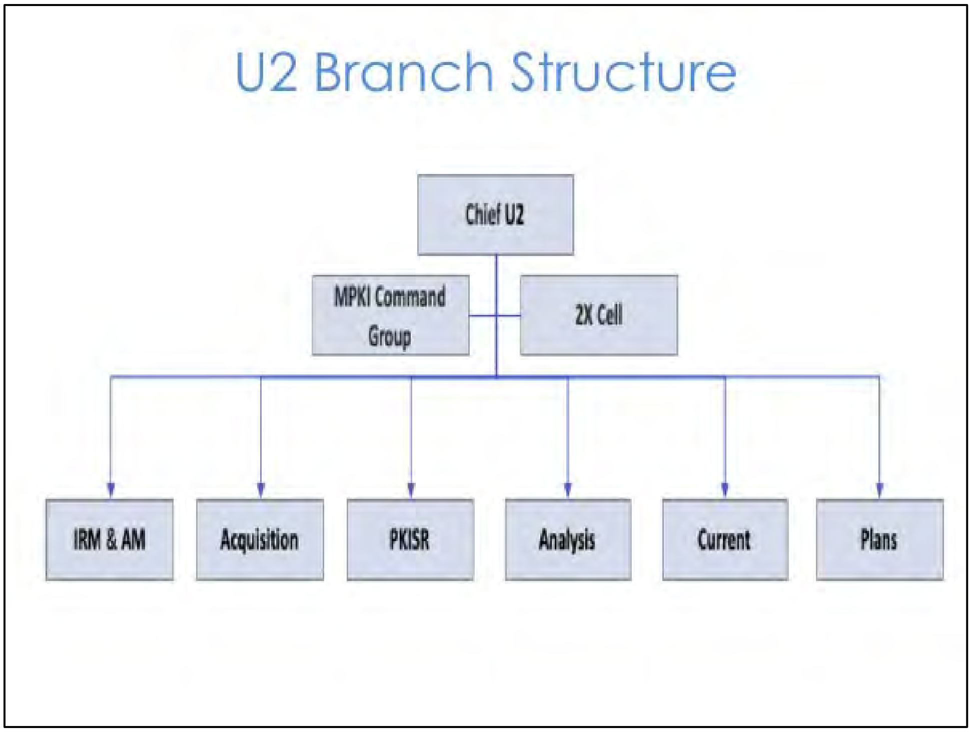
This responsibility can involve decisions such as determining how limited analytical or acquisition capabilities are best placed, the MPKI battle-rhythm, and the development of MPKI Standard Operating Procedures (SOPs). The MPKI battle rhythm is supported and directed by the Peacekeeping-Intelligence Support Plan (ISP), which the U2 is charged with producing. The U2 should attend all MICM meetings and ensure liaison is taking place across the military peacekeeping-intelligence entities at the operational level. The use of dedicated peacekeeping-intelligence liaison officers should be considered.

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

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

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

Slide 13



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 according to the mission's mandate, the Status of Forces Agreement (SOFA) in place between the Host State and the UN, the information acquisition parameters as outlined in the MISP, and according to the information acquisition capabilities within the Military Component.

The U2 acts as a focal point to coordinate with other components and entities in the mission and may request support from UN headquarters when necessary. It is important to note that all personnel should have the rank and training commensurate with their roles and responsibilities. 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. Depending on the number of personnel assigned, all sections should be represented, and an individual or group should be assigned the responsibility for the respective role/tasks. Let us go over each cell/section's responsibilities from left to right.

- Information Requirements Management and Acquisition Management (IRM&AM) cell manage and organise the collection of intelligence from various sources. The collection department of an intelligence organisation may attempt basic validation of what it collects. Usually, the cell does not analyse its significance

- Acquisition – is responsible for matching resources, tasking resources to the information requirements.

- PKISR - Peacekeeping Intelligence surveillance and reconnaissance section is the section that interfaces between intelligence discipline with the military surveillance and reconnaissance assets in order to assist in employing its sensors and managing the information they gather.

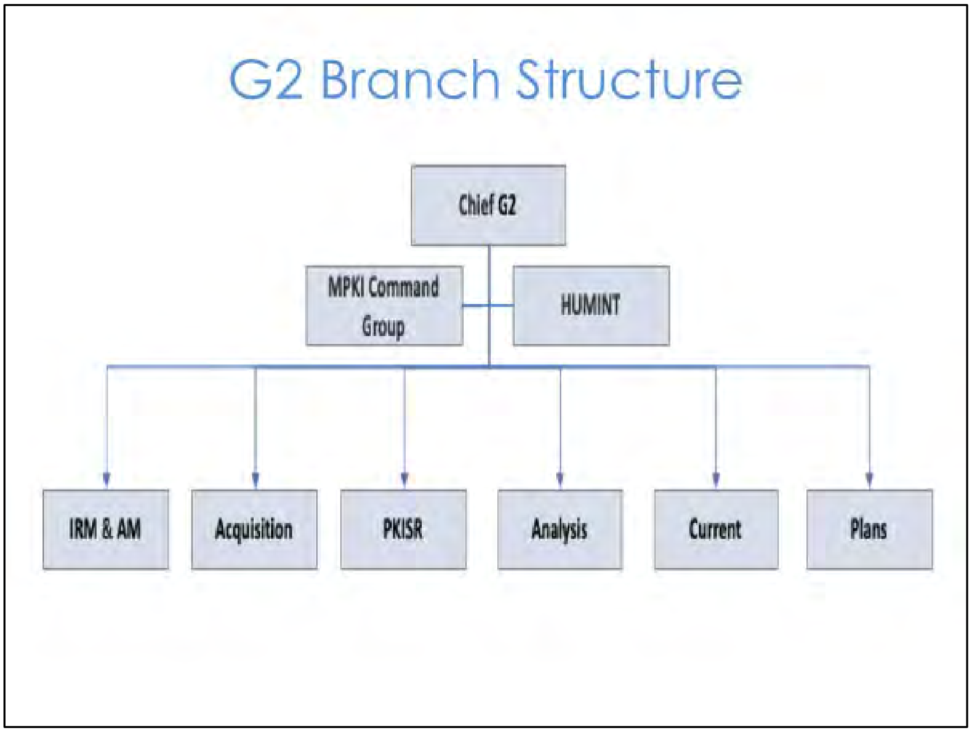
- Analysis section - gather information from multiple echelons and sources to produce intelligence products to meet the commander's requirements and to assist the commander in the UN MDMP.

- The current peacekeeping-intelligence section tracks and disseminates information and intelligence upon collection based upon operational necessity and potential impact on current operations and supports the common operating picture.

- Plans section- develops intelligence products to support future operations. Assist and supports the military planning process of future operations and contingency planning.

- Also, other sections/cells can be stood up if required, and personnel are available. I.e., Open Source Peacekeeping-Intelligence (OSINT) cell, and production (analysis) cell; depending on the available sensors and units in the mission, the Geospatial/Imagery Peacekeeping-Intelligence (GEOINT/IMINT) cell, Signals Peacekeeping-Intelligence (SIGINT) cell, and Human Peacekeeping-Intelligence (HUMINT) cell.

Slide 14



G2 Branch Structure

Chief G2

MPKI Command Group

HUMINT

IRM & AM

Acquisition

PKISR

Analysis

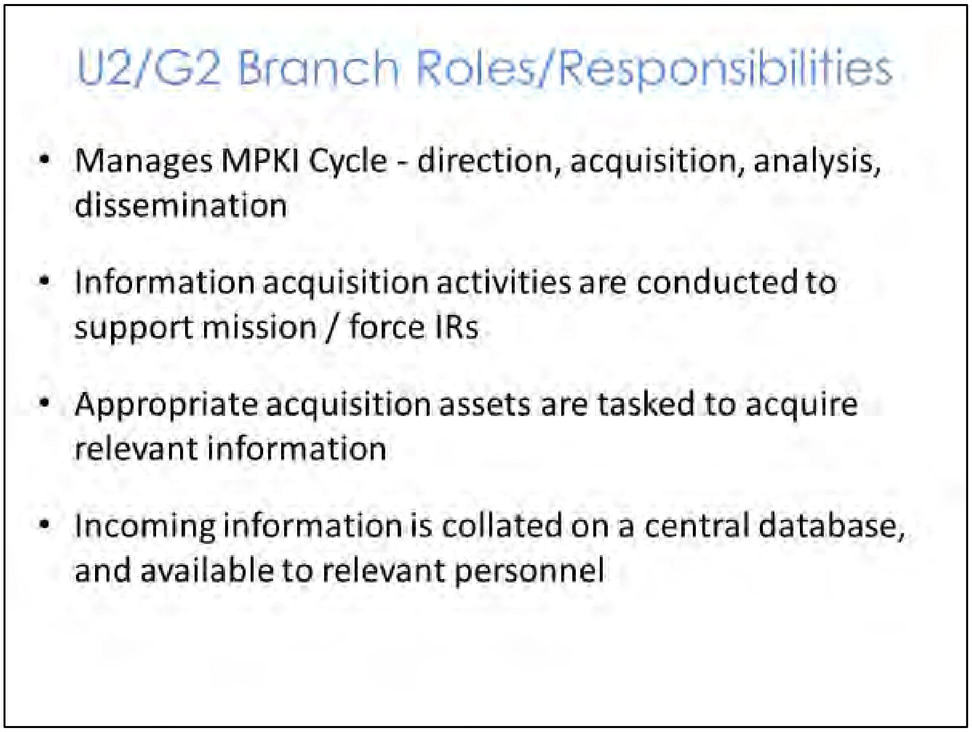
Current

Plans

The G2 peacekeeping-intelligence branch in a Sector deals with all matters concerning peacekeeping-intelligence and military security operations at tactical/ operational level within the battalion AOR. Its recommended structure is depicted above, and roles and functions for the cells/sections are like the U2 sections/cells.

Ask students what the structural differences between U2 branch and G2 branch and why such differences exist are?

Slide 15



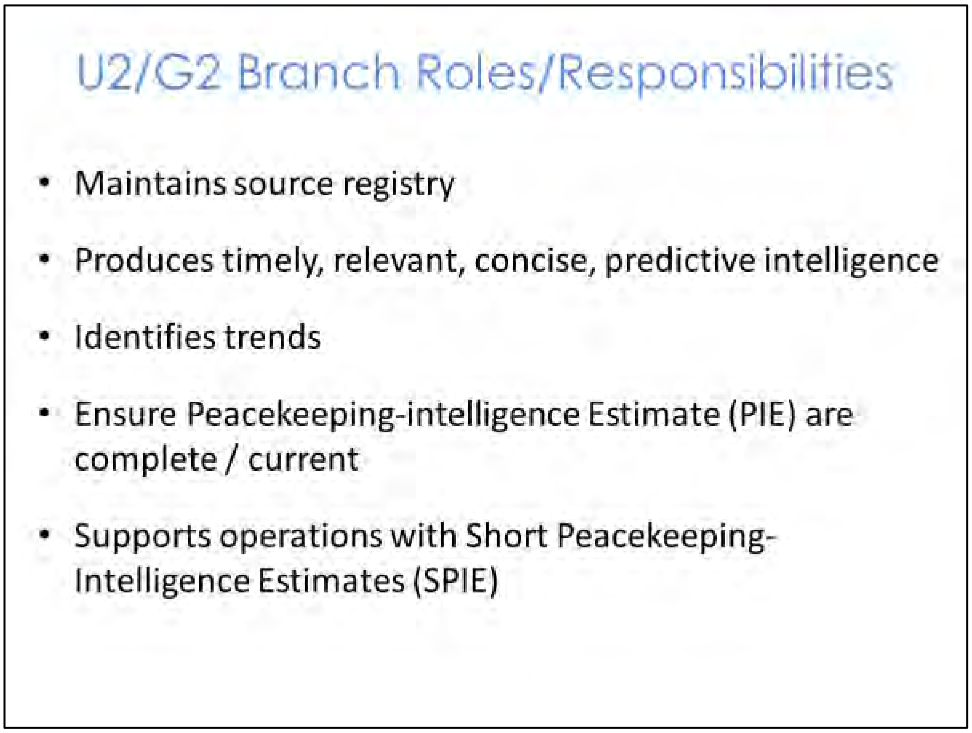
U2/G2 Branch Roles/Responsibilities

- 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

Roles and Responsibilities of the U2/G2 Branch:

- Ensures that its information acquisition activities are conducted in support of mission and force Priority and other IRs. To this end, the U2 cell will maintain an IAP that fully aligns with HoM and FHQ IRs. This will be regularly updated
- Ensures that appropriate acquisition assets are tasked to acquire relevant information
- Ensures that all incoming information is collated on a central database, and available to the relevant personnel

Slide 16



U2/G2 Branch Roles/Responsibilities

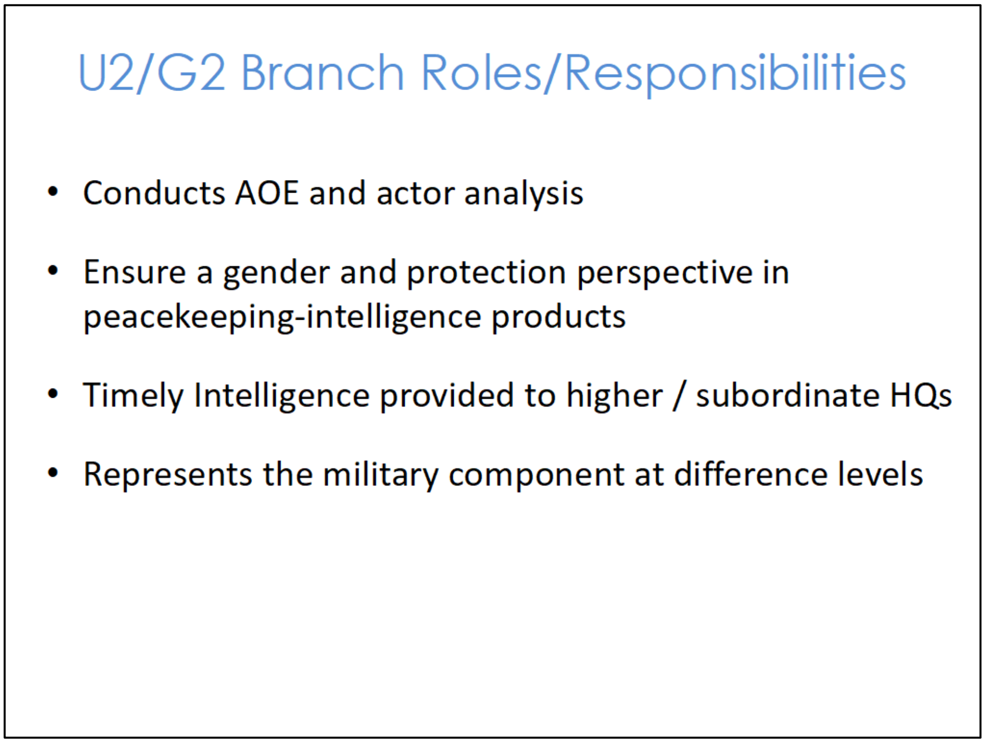
- Maintains source registry
- Produces timely, relevant, concise, predictive intelligence
- Identifies trends
- Ensure Peacekeeping-intelligence Estimate (PIE) are complete / current
- Supports operations with Short Peacekeeping-Intelligence Estimates (SPIE)

This is a continuation of the last slide.

- Maintains a source registry

- Identifies relevant trends
- Ensure that the Peacekeeping-intelligence Estimate (PIE) is complete and up to date
- Supports all operations with a Short Peacekeeping-Intelligence Estimate (SPIE)

Slide 17



U2/G2 Branch Roles/Responsibilities

- Conducts AOE and actor analysis
- Ensure a gender and protection perspective in peacekeeping-intelligence products
- Timely Intelligence provided to higher / subordinate HQs
- Represents the military component at difference levels

Roles and Responsibilities of the U2 Branch

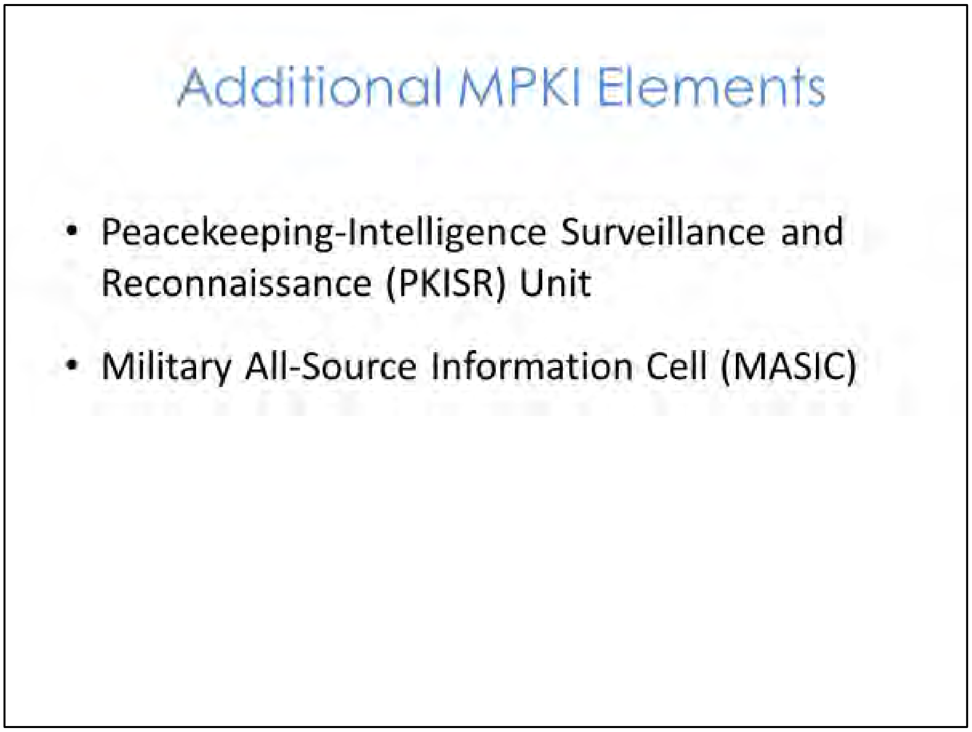
- Conducts a full Assessment of the Operating Environment (AOE) and Actor Analysis for the entire Area of Operational Responsibility (AOR)
- Works with the Military Gender and Protection Advisor to ensure that a gender and protection perspective is mainstreamed into all peacekeeping-intelligence products
- Ensures that all relevant information and peacekeeping-intelligence is provided to higher and subordinate HQs in a timely fashion
- Represents the Force at different levels

Note to instructor –

G2 branches have similar roles and responsibilities as U2 Branches, which are shown for the instructor's reference:

- Manages the Sector MPKI Cycle, in line with the Peacekeeping-Intelligence Policy and this Handbook, through the direction, acquisition, analysis and dissemination phases. This is to ensure that the Sector Commander's decision-making process is fully supported with timely, succinct, and relevant peacekeeping-intelligence products
- Ensures that its information acquisition activities are conducted in support of Force Priority and other IRs. To this end, the G2 branch will maintain an IAP that fully aligns with FHQ IRs. This will be regularly updated
- Ensures that appropriate acquisition assets are tasked to acquire relevant information
- Ensures that all incoming information is collated on a central database, and available to the relevant personnel
- Maintains its source register and registers its sources with the U2
- Produces timely, relevant, concise, and predictive peacekeeping-intelligence products to support effective mandate implementation relating to the protection of UN personnel and civilians, and to enhance situational awareness, as required
- Identifies relevant trends
- Supports all operations with an SPIE
- Conducts a full AOE and Actor Analysis for the entire AOR
- Ensures that a full AOE, and Actor Analysis is carried out by all subordinate units down to Company level, or whenever a new FOB is established. A detailed AOE must be carried out for all areas of interest for the military component, to include: Protection of Civilian sites, all FOBs, and other areas related to mandate implementation, and as directed by the FC
- Works with the Military Gender and Protection Advisor, if resources permit at Sector-level, to ensure that a gender and protection perspective is mainstreamed into all peacekeeping-intelligence products
- Ensures that all relevant information and peacekeeping-intelligence is provided to higher and subordinate HQs in a timely fashion

Slide 18



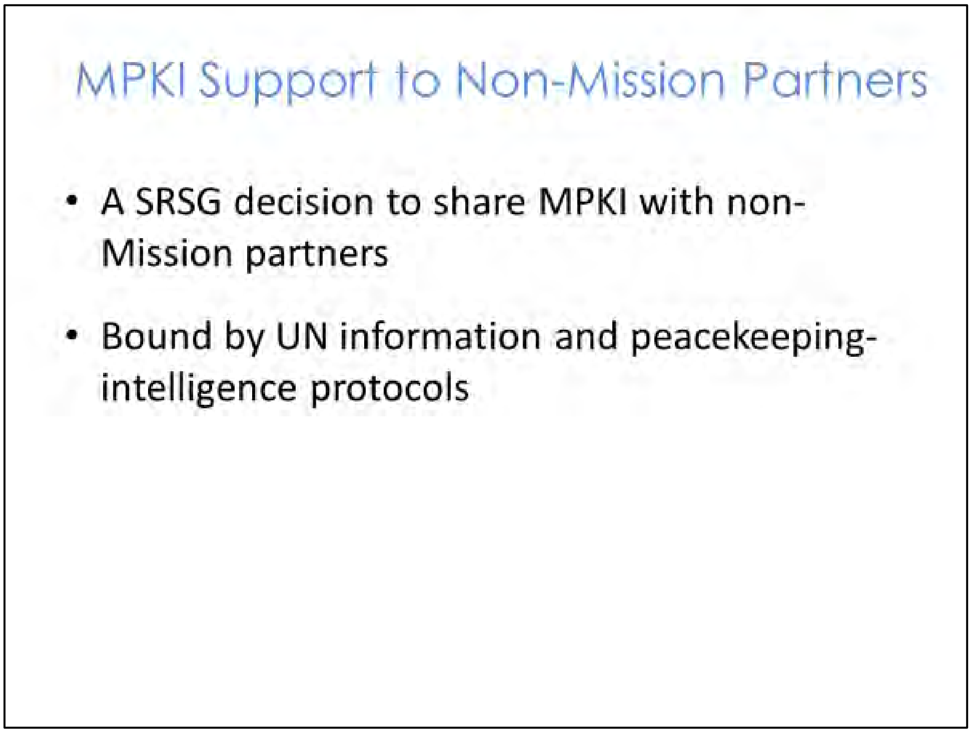
Additional MPKI Elements

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

Key Message: Depending on the mission, there may be additional peacekeeping-intelligence elements in the MPKI structure, such as Peacekeeping-Intelligence Surveillance and Reconnaissance (PKISR) Unit or Military All-Source Information Cell (MASIC).

A MASIC is an all-source analytical team designed to increase the thinking and analytical elements of an MPKI entity. This may be required because of scarce specialist resources or because MPKI would benefit from having a range of analysts with different specialities working together to holistically look at a peacekeeping-intelligence problem: aspects and developments in the OE should not only be viewed from a military perspective. This broad approach ensures that all relevant factors, actors, relations and interactions are considered and analyse to achieve a complete understanding.

Slide 19

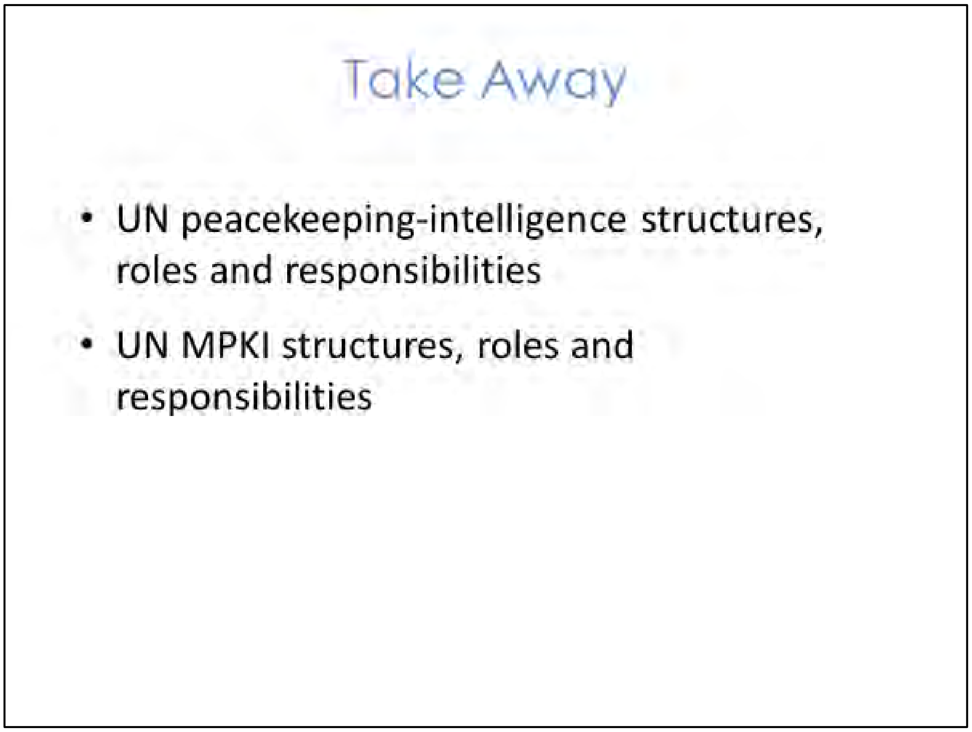


MPKI Support to Non-Mission Partners

- A SRSG decision to share MPKI with non-Mission partners
- Bound by UN information and peacekeeping-intelligence protocols

The UN mission can assist and support non-mission partners and interlocutors; however, there are set parameters, requirements and policies that frame this support. Approval from the SRSG is required in all cases.

Slide 20



Take Away

- UN peacekeeping-intelligence structures, roles and responsibilities
- UN MPKI structures, roles and responsibilities

Summary

Students should retain the following topics from this lesson. The takeaways from this brief Introduction to UN MPKI structure and roles include the following:

- UN peacekeeping intelligence structures, roles and responsibilities
- UN MPKI structures, roles and responsibilities

Learning Activity

Structure and roles of S2 branch

RESOURCES
3-4 flip chart, 3-4 large pieces of paper, sticky tape

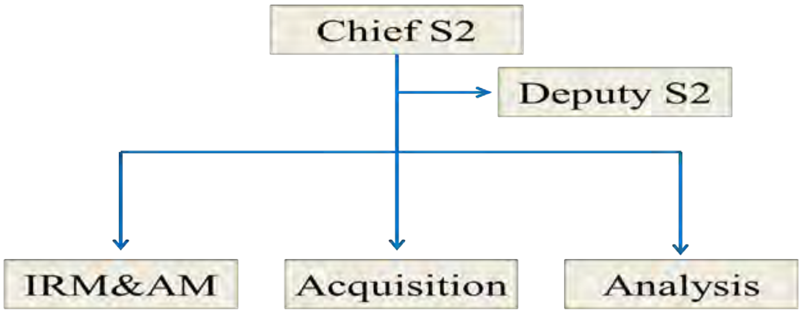
TIME
Total: 15 minutes

PREPARATION
Divide the participants into 3-4 teams.

EXERCISE
Ask participants to discuss the possible structure of the S2 section at battalion level and then list and explain their roles and responsibilities.

☞ NOTE TO INSTRUCTOR

The following answers should be considered:
The S2 section at battalion level supports the battalion commander and staff with peacekeeping-intelligence products. The S2 also deals with security tasks within the battalion. Outside the battalion staff, the S2 is responsible for directing and coordinating the MPKI needs and information acquisition at the company level.



Chief S2: Head of S2 MPKI command group
Deputy S2: Counterintelligence and information security
IRM & AM: Information requirement and acquisition management

Analysis: military peacekeeping-intelligence support to current and future operations

Suggested roles and responsibilities of the MPKI S2 Section

- Manages the Battalion MPKI Cycle, in line with Peacekeeping-Intelligence Policy and this Handbook, through the direction, acquisition, analysis and dissemination phases. This is to ensure that the Battalion Commander's decision-making process is fully supported with timely, succinct, and relevant peacekeeping-intelligence products

- Ensures that its information acquisition activities are conducted in support of Sector Priority and other IRs. To this end, the S2 section will maintain an IAP that fully aligns with Sector Headquarters IRs. This will be regularly updated

- Ensures that appropriate acquisition assets are tasked to acquire relevant information

- Ensures that all incoming information is collated on a central database, and available to the relevant personnel

- Maintains its own source registry and registers its sources with the G2

- Produces timely, relevant, concise, and predictive peacekeeping-intelligence products to support effective mandate implementation relating to the protection of UN personnel and civilians, as required

- Identifies relevant trends

- Supports all operations with an SPIE

- Conducts a full AOE and Actor Analysis for the entire AOR

- Ensures that a full AOE, and Actor Analysis is carried out by all subordinate units down to Company level, or whenever a new FOB is established. A detailed AOE must be carried out for all areas of interest for the military component, to include: Protection of Civilian sites, all FOBs, and other areas related to mandate implementation, and as directed by the FC

- Works with the Military Gender and Protection Advisor, if resources permit at Sector-level, to ensure that a gender and protection perspective is mainstreamed into all peacekeeping-intelligence products

- Ensures that all relevant information and peacekeeping-intelligence is provided to higher and subordinate HQs in a timely fashion

Lesson 1.4

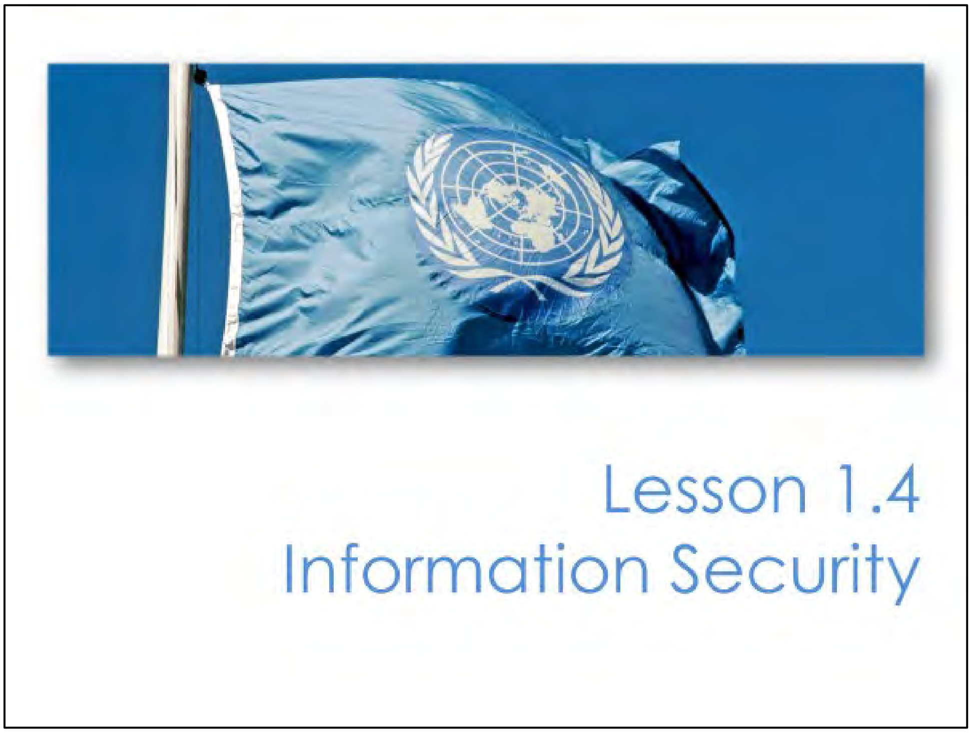
Information Security

The Lesson

Starting the Lesson

Interaction*. Ask the students to tell the group how important information security is for UN operations. Also, ask them to expand on their experiences and knowledge of information security measures and UN information security policy.*

Slide 1



Lesson 1.4
Information Security

Key Message: As a MPKIO you must keep in mind that information security is a task that must be observed throughout the intelligence cycle

We will give an introduction and overview of Information Security, and remark how important this task is for the intelligence cycle.

Interaction: *Ask the students to tell the group how important the information security on UN operations is and ask them about their knowledge of information security measures and their knowledge of UN information security policy.*
The answers here could be regarding how aware they are about the UN information security policy and the importance of information security.

Slide 2

Content

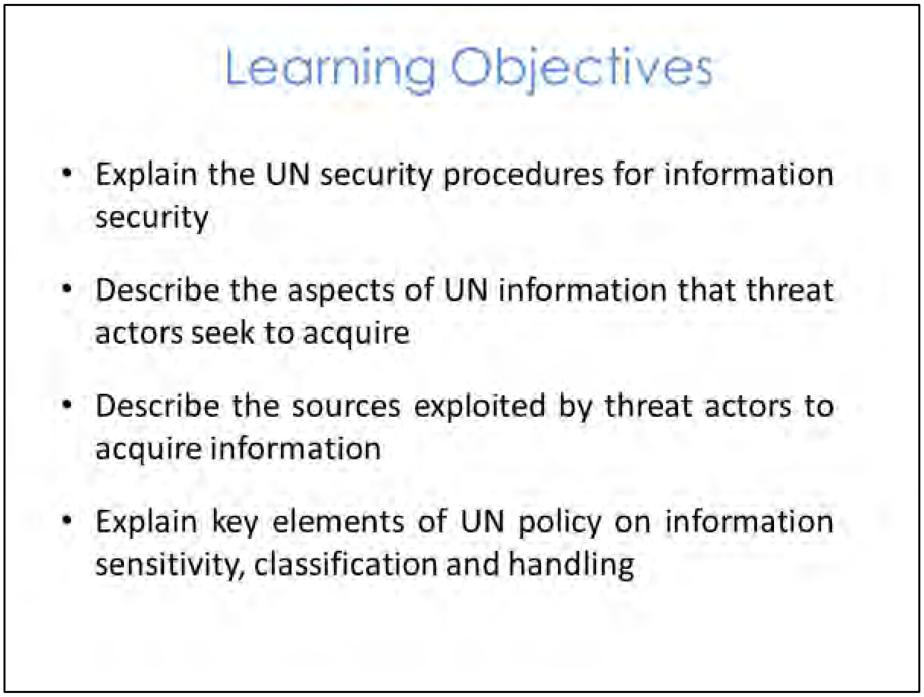
- Security Foundation for UN Operations
- UN Security Policy
- Information Security

2

The lesson will cover these three topics. The knowledge of these topics is important for the MPKIO to contribute to information security during the intelligence cycle.

Initially, we will address the Security Foundation for UN Operations. Information security is part of the United Nations' security objectives. We will then address the UN Security Policy and the responsibilities of the MPKIO into the Security Policy. Finally, the issues related to Information Security, its objectives, and what sources the threat uses to acquire information, classifications and handling of information.

Slide 3



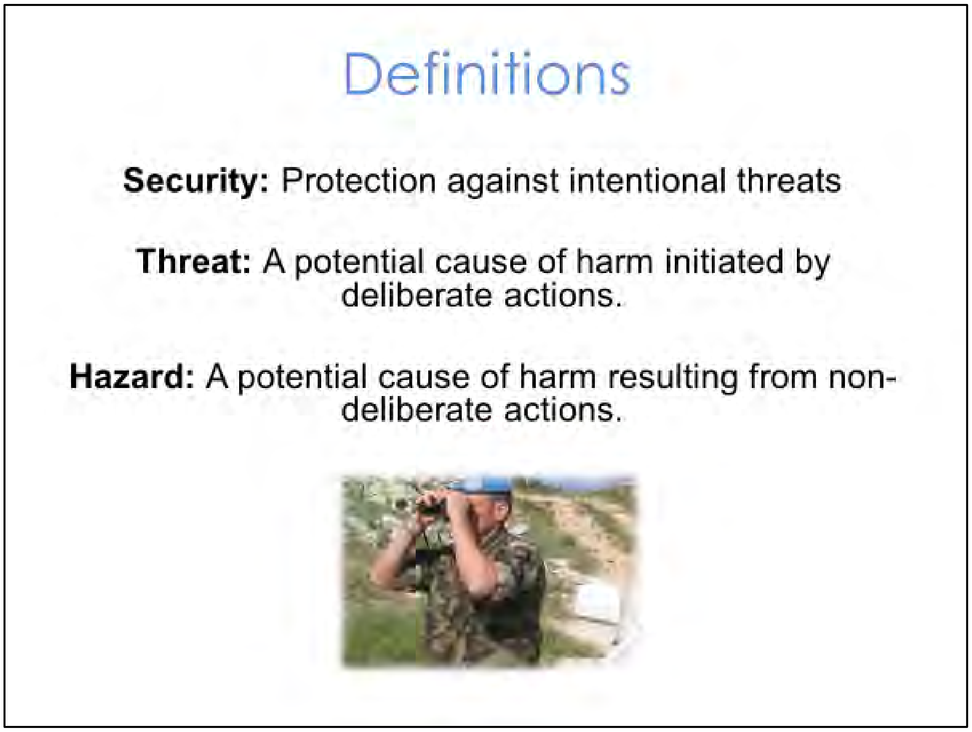
Learning Objectives

- Explain the UN security procedures for information security
- Describe the aspects of UN information that threat actors seek to acquire
- Describe the sources exploited by threat actors to acquire information
- Explain key elements of UN policy on information sensitivity, classification and handling

Key Message: All procedures relating to the intelligence cycle will be compromised if the UN personnel do not observe the importance of information security.

As usual, for all good training practices, let's review the learning outcomes. At the end of the lesson, our aim is for you to be able to understand the documents relating to the information security, how to keep the information secure and how to prevent the handled information to be acquired by the threat.

Slide 4



Definitions

Security: Protection against intentional threats

Threat: A potential cause of harm initiated by deliberate actions.

Hazard: A potential cause of harm resulting from non-deliberate actions.

First, we will cover some key definitions related to security. A "Threat" is a potential cause of harm initiated by deliberate actions. A "Hazard" is a potential cause of harm resulting from non-deliberate actions.

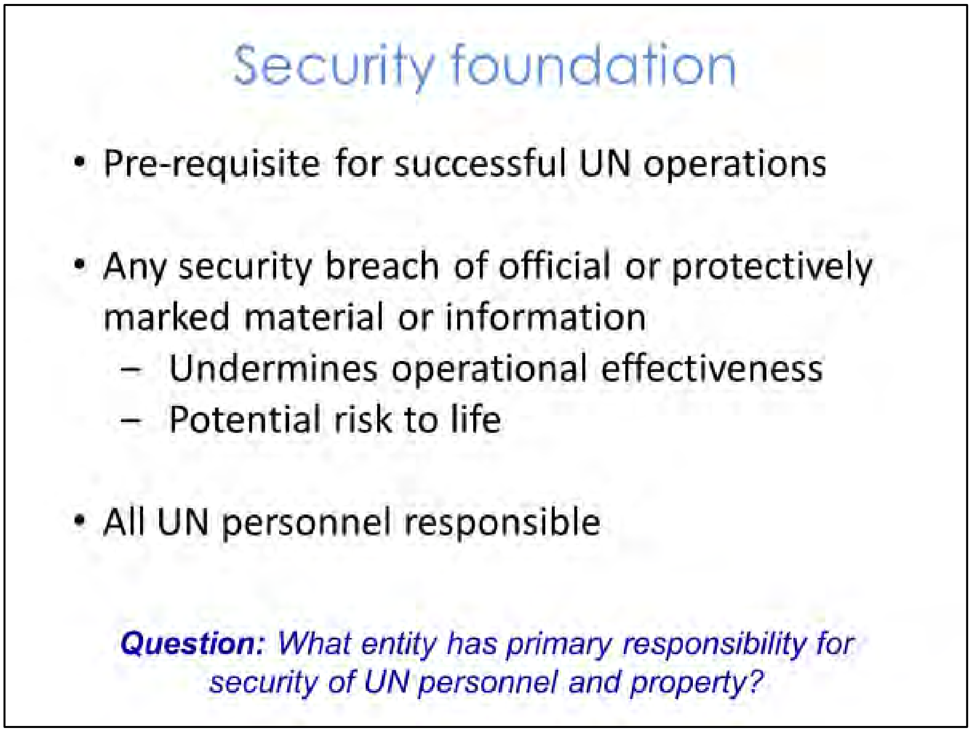
The MPKI Cell must always understand and assume that information security is threatened and operate under the assumption that external actors will seek to penetrate its systems.

Interaction: *Ask the participants if they can give the components of safety in the UN. Students should respond that safety in the UN is addressed in three distinct areas:*

- Staff

- Information

Slide 5



Security foundation

- Pre-requisite for successful UN operations
- Any security breach of official or protectively marked material or information
  - Undermines operational effectiveness
  - Potential risk to life
- All UN personnel responsible

Question: *What entity has primary responsibility for security of UN personnel and property?*

Knowledge of the Security Foundation is essential in all peacekeeping activities. Any threat to security, whether material or information, can cause a risk to the lives of UN personnel. The diversity and multitude of threat environments in which the United Nations Operations operates require mechanisms to help identify threats to allow senior managers to assess and mitigate them.

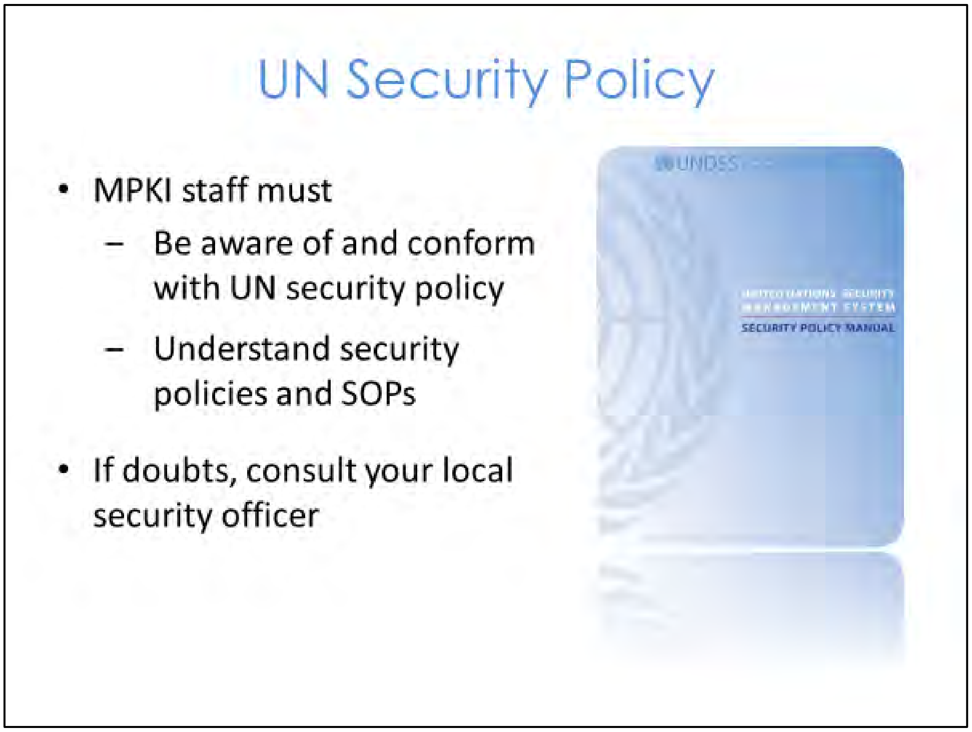
All UN Personnel should be aware of the policies, procedures, standards and other arrangements of the United Nations Security Management System.

***Interaction**: The Instructor should ask students who have primary responsibility for security. Answer: According to the UN Security Manual, the primary responsibility for the security of UN personnel and property rests with the Host Government. The Instructor should further ask whether the Host Government may itself present a threat to information security. The instructor should discuss that the Host Government may also be seeking access to sensitive UN information.*

of international organisations and their officials, the Government is considered to have a special responsibility under the Charter of the United Nations or the Government's agreements with individual organisations.

Without prejudice to the above and while not abrogating the responsibility of the host Government for its obligations, the United Nations has a duty as an employer to reinforce and, where necessary, supplement the capacities of host Governments to fulfil their obligations in circumstances where United Nations personnel are working in areas that are subject to conditions of insecurity which require mitigation measures beyond those which the host Government can reasonably be expected to provide. In this regard, the United Nations Security Management System (UNSMS), in seeking to establish and maintain operations in insecure and unstable environments, adopts the principle of “how to stay” as opposed to “when to leave” as a tenet of its security management approach.

Slide 6



UN Security Policy

- MPKI staff must
  - Be aware of and conform with UN security policy
  - Understand security policies and SOPs
- If doubts, consult your local security officer

UNDSS
UNITED NATIONS SECURITY MANAGEMENT SYSTEM
SECURITY POLICY MANUAL

Key message: The MPKI students must understand and be able to find the relevant documents for security operations.

MPKI Staff should understand the Mission’s security SOPs and UN documents/publications concerning security operations. Depending on your position on the staff, you may need to have a detailed knowledge of some of these selected documents.

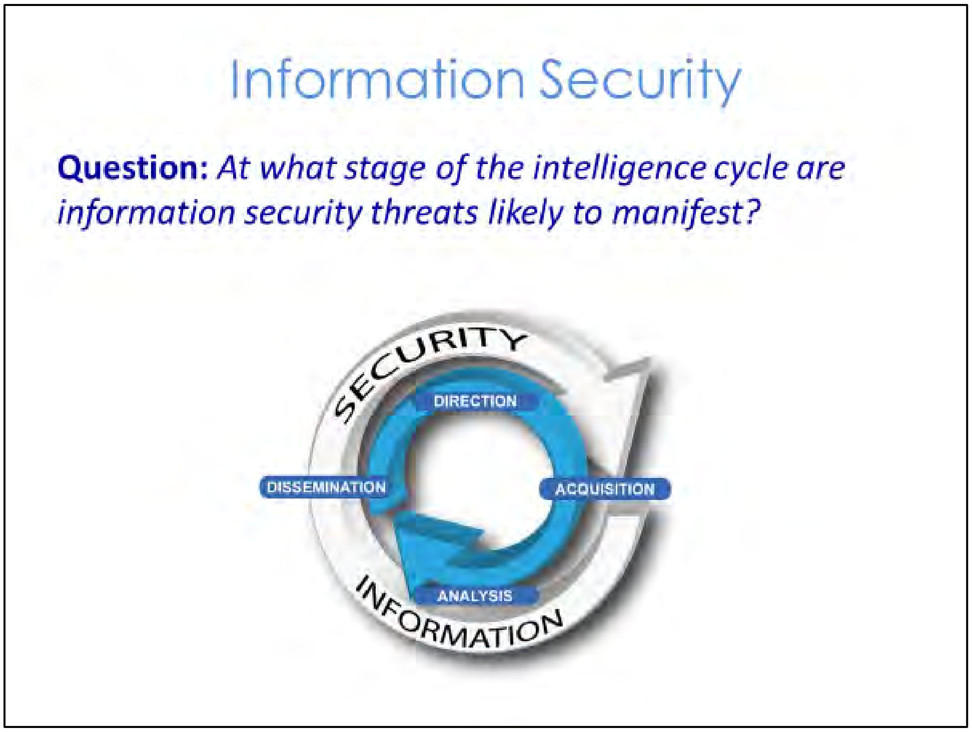
Instructor Note: *Prepare a handout for the students with the following documents:*
-ST/SGB/2007/6;
-Un Field Security Handbook;
-UN Security Management System protocols;
-MPKI Handbook;

-Peacekeeping Intelligence Policy

***Interaction**: The instructor should ask students if they are aware of the UN Security Policy and its content. The instructor should encourage students to access and read the reference material. Those students who respond that they know should be encouraged to discuss with the group their understanding of Security Foundation.*

***Instructor Note**. All MPKI students should be told to complete the basic UN Information Security E-course. This is accessible via the INSPIRA home page. In-theatre, UNDSS will provide further details on this course, which only takes two hours to complete online.*

Slide 7



Information Security

Question: *At what stage of the intelligence cycle are information security threats likely to manifest?*

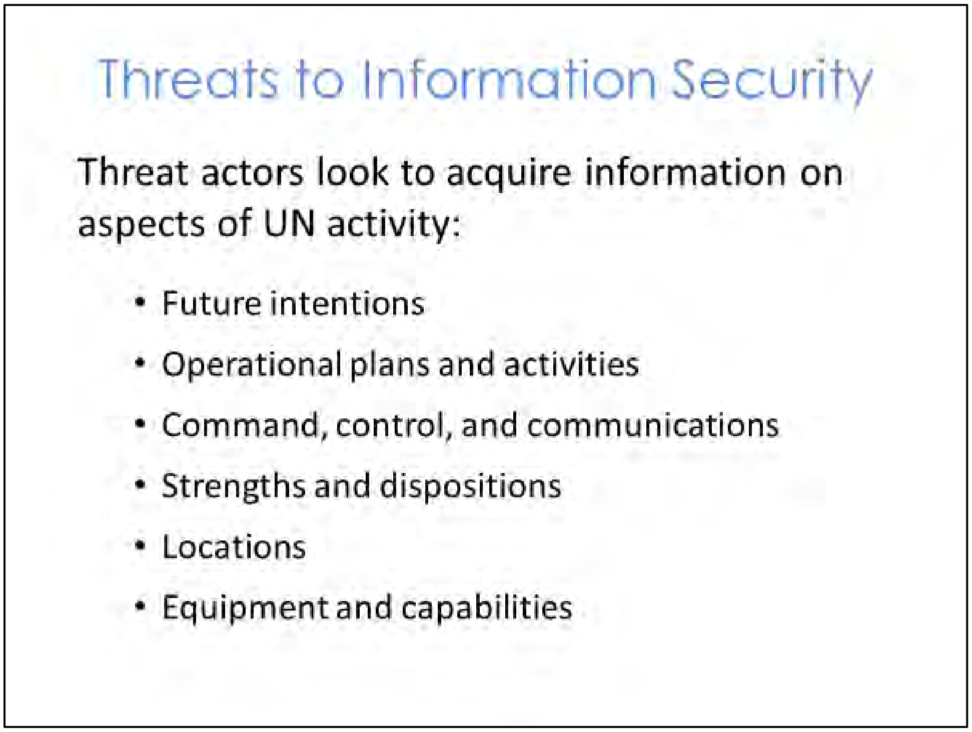
Information security must be achieved during the whole knowledge production process (intelligence cycle). In order to keep the information secure, the MPKIO must be aware of the possible threats, who should be handling the information, how to disseminate it, and who should be aware of the information.

Interaction: *Ask students at what stage of the MPKI cycle are information security threats likely to manifest.* ***Expected answers include****:*

- *During the Direction phase, a threat actor may seek to understand the Mission's PIRs to deny information that we require*
- *During the Acquisition phase, if the threat actor understands acquisition capabilities, they may take measures to reduce or prevent our sensors from conducting acquisition*

  During the Dissemination phase, we should ensure that sensitive information is disseminated via appropriate systems to those who need to know the information

Slide 8



Threats to Information Security

Threat actors look to acquire information on aspects of UN activity:

- Future intentions
- Operational plans and activities
- Command, control, and communications
- Strengths and dispositions
- Locations
- Equipment and capabilities

The information produced or manipulated by the United Nations will always be the target of threat actors. It is important to identify the threats, their "modus operandi", their sources to acquire information, and how to maintain information security throughout the intelligence cycle. The level of threat should be factored into information security policy and procedures.

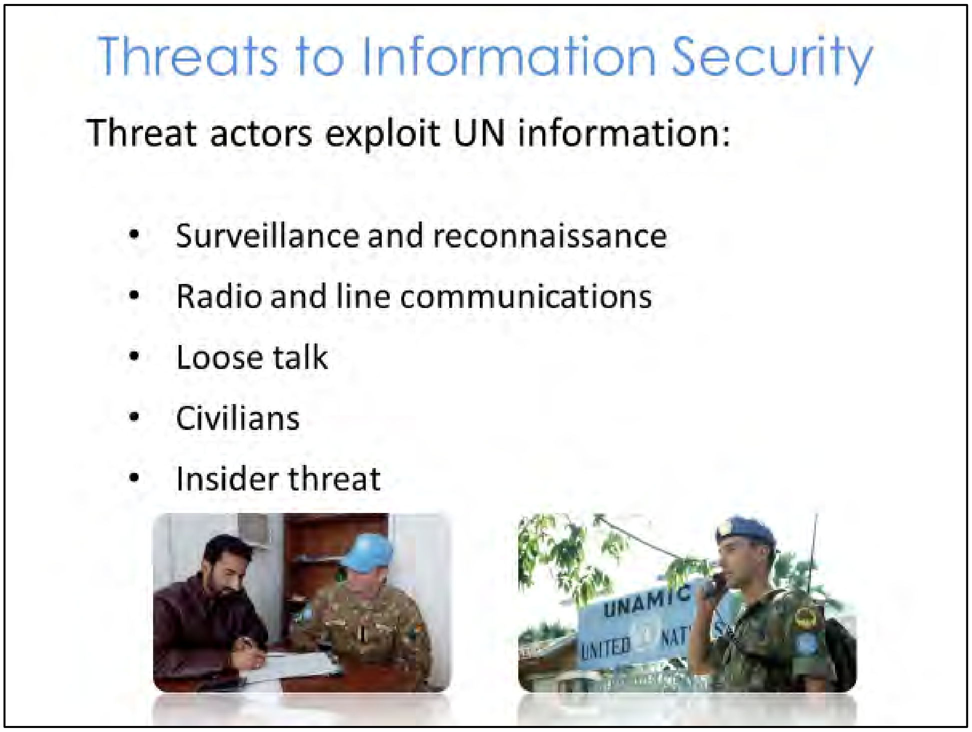
***Interaction**. Ask the students these questions:*

1. *What is the intention to obtain information from the UN?*

Answer: To commit a hostile act against UN personnel or material; to gain an advantage against the UN; to deny information to the UN; to commit a hostile act against UN personnel or UN property; to embarrass the UN or to undermine the UN's ability to act.

Answer: - current and future of the UN forces; strengths and weaknesses of the UN forces and current and future locations.

Slide 9



Threats to Information Security

Threat actors exploit UN information:

- Surveillance and reconnaissance
- Radio and line communications
- Loose talk
- Civilians
- Insider threat

UNAMIC
UNITED NAT

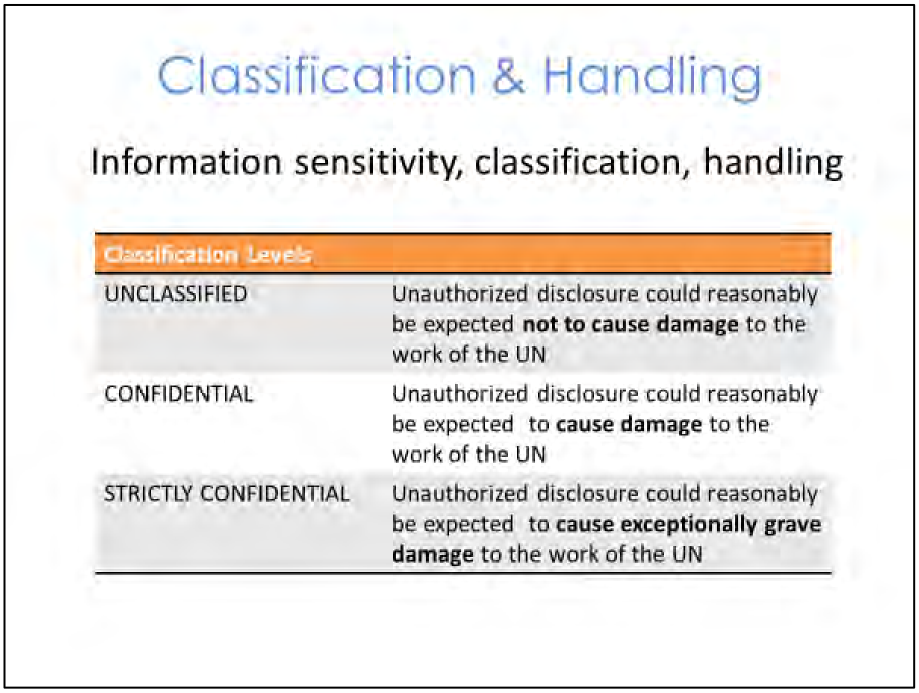
The MPKI cell should be aware of how the threat attempts to acquire UN information.

The main sources used to acquire information are Surveillance and Reconnaissance, and the MPKIO should appropriately brief units on surveillance methods and indicators.

Every unit must recognise that the threat actor will seek to gather information through direct observation from the ground and air assets (such as UAS); this may include peacekeeping intelligence gained from locally employed civilians.

Loose Talk: MPKI staff should be careful to talk only about the essential aspects of peacekeeping-intelligence with UN Staff who hold the appropriate clearance. You should generally avoid sharing UN information with external civilians. Be aware of the information that UN or other interpreters have access to. Staff working directly or indirectly for the UN may pass information to threat actors.

Slide 10



Classification & Handling

Information sensitivity, classification, handling

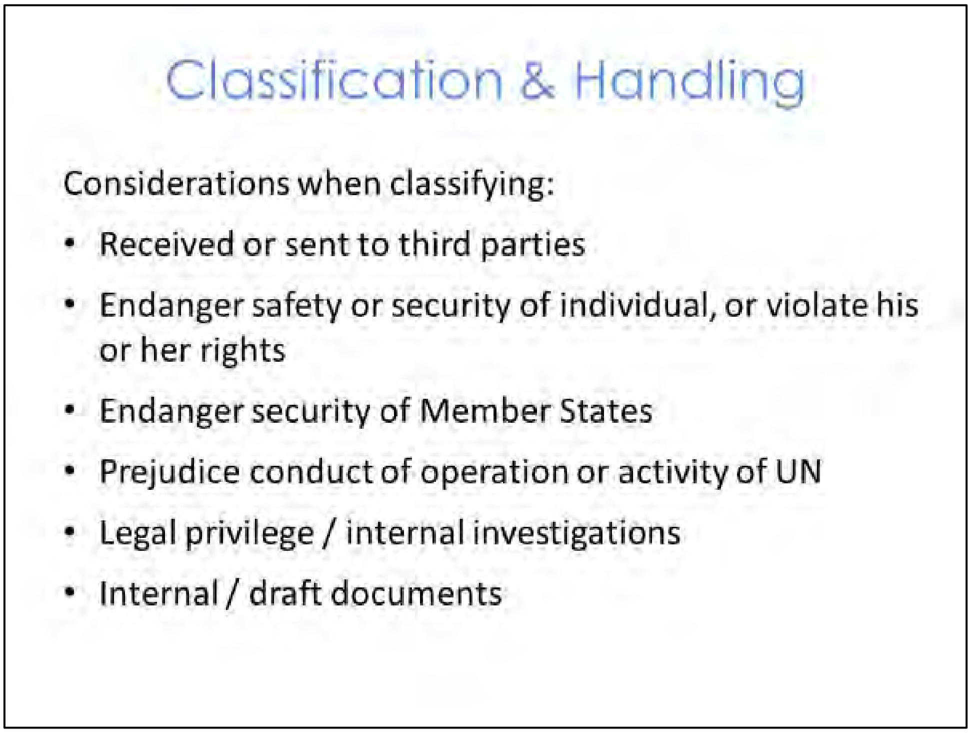
Classification Levels	
UNCLASSIFIED	Unauthorized disclosure could reasonably be expected **not to cause damage** to the work of the UN
CONFIDENTIAL	Unauthorized disclosure could reasonably be expected to **cause damage** to the work of the UN
STRICTLY CONFIDENTIAL	Unauthorized disclosure could reasonably be expected to **cause exceptionally grave damage** to the work of the UN

Key Message: Know the type of information being handled, its classification, and what security procedures should be adopted in each case according to UN policy.

This slide shows the UN classification levels as per the UN Security Policy. MPKI staff should understand how to apply these definitions and be wary of overclassifying or automatically applying classifications.

If a MPKI report includes information from another entity, the report must be classified at the highest level of the external information. For example, if an MPKI report includes information from a STRICTLY CONFIDENTIAL code cable, the report must be classified as STRICTLY CONFIDENTIAL.

Slide 11



Classification & Handling

Considerations when classifying:

- Received or sent to third parties
- Endanger safety or security of individual, or violate his or her rights
- Endanger security of Member States
- Prejudice conduct of operation or activity of UN
- Legal privilege / internal investigations
- Internal / draft documents

When considering classification, information deemed sensitive shall include the following:

(a) Documents created by the United Nations received from or sent to third parties, under an expectation of confidentiality;

(b) Documents whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights or invade his or her privacy;

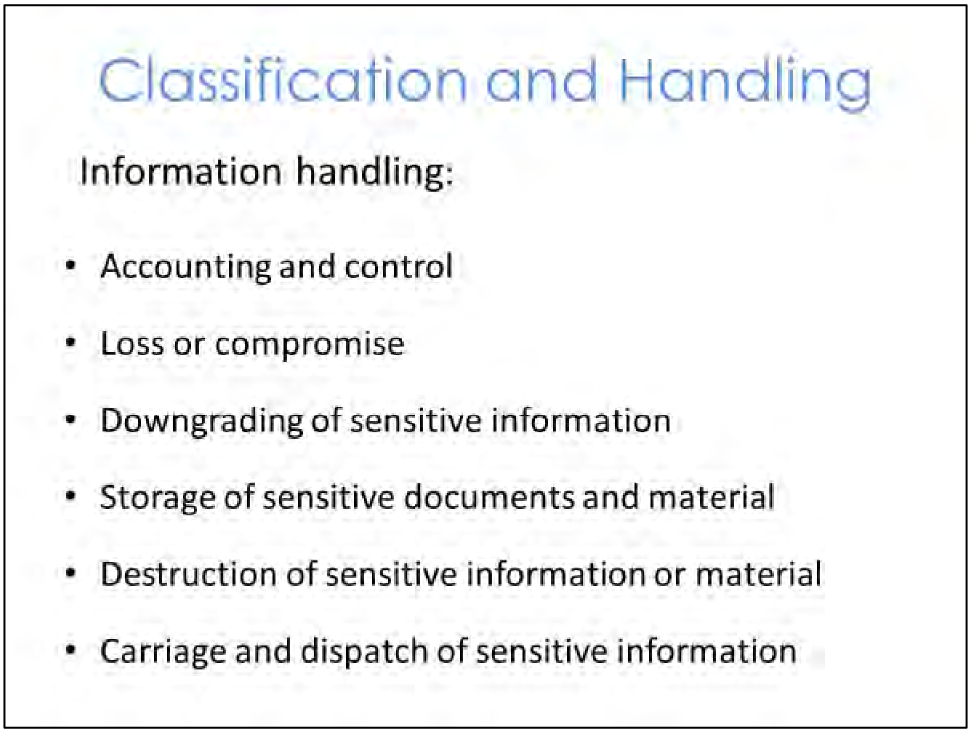
(c) Documents whose disclosure is likely to endanger the security of Member States or prejudice the security or proper conduct of any operation or activity of the United Nations, including any of its peacekeeping operations;

(e) Internal inter-office or intra-office documents, including draft documents, if disclosure would undermine the Organisation's free and independent decision-making process;

(f) Documents containing commercial information, if disclosure would harm either the financial interests of the United Nations or those of other parties involved;

(g) Other kinds of information, which, because of their content or the circumstances of their creation or communication, must be deemed confidential.

Slide 12



Classification and Handling

Information handling:

- Accounting and control
- Loss or compromise
- Downgrading of sensitive information
- Storage of sensitive documents and material
- Destruction of sensitive information or material
- Carriage and dispatch of sensitive information

Information handling includes all those measures put in place to protect information:

- **Accounting and control** of classified information received/produced. This is paramount to effective security. Originators and recipients should maintain a record of the movement of classified information and material within and external to their respective organisation. This includes the continued storage or destruction of this classified information or material

- **Loss or compromise.** The following actions should be taken within the respective unit location:

  - Thorough search to be made to ensure a simple handling error has not been made
  - The suspected loss or compromise should be reported to UN security staff immediately
  - The unit should initiate a security investigation directed by UN security staff

- **The downgrading of sensitive information** is to be conducted periodically. Documents may only be downgraded by the person/post/appointment from whom the document originated

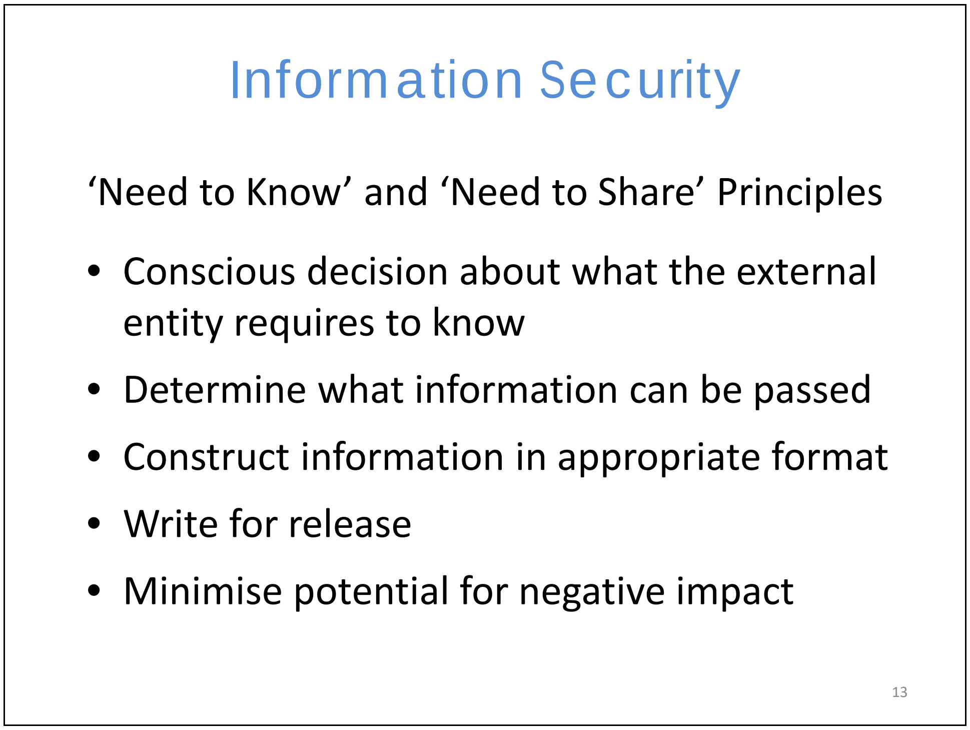
- **Storage of sensitive documents and material** should meet the standards stated by the UN security staff as outlined in the MOSS within the location

Security Plan. Advice is to be sought from UN security staff should location-specific security advice be required

- **Destruction of sensitive information or material.** All strictly confidential information and material should be shredded or placed in burn bags and stored in a security container or locked room where it cannot be accessed by unauthorised personnel. Destruction is to be recorded in the documents log and is to be certified by two authorised personnel

- **Carriage and dispatch of sensitive information.** Strictly confidential information and material may only be carried by authorised personnel as endorsed by UN security personnel. Every effort should be made to pass information electronically over secure means. When required, items should be delivered by hand with the envelope clearly stating the security classification of the information or material contained and signed by an authorised person; also, both receiving and sending parties should receive a receipt of delivery

Slide 13



Information Security

‘Need to Know’ and ‘Need to Share’ Principles

- Conscious decision about what the external entity requires to know
- Determine what information can be passed
- Construct information in appropriate format
- Write for release
- Minimise potential for negative impact

13

Key Message: There is always a requirement to protect peacekeeping-intelligence sources and conform to UN information handling protocols; however, there is also a requirement to ensure that assessments are ‘written for release’ and therefore are as widely available as deemed possible.

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

- Make a conscious decision about what the external entity requires to know
- Determine what information can be passed on
- Construct that information in the most appropriate format
- Minimise the potential for the negative impact

Slide 14

Take Away

- Understand the threat
- Understand your role
- Security policies and manuals provide additional information

Summary

The key takeaways from this lesson are to understand the potential threat to Mission information; understand the MPKI cell's role in protecting, handling and classifying sensitive information, and recognise that additional guidance is available in UN policies, manuals and online courses.

Learning Activity

Interaction*: You should encourage the discussion by asking questions about what each participant has understood about the topic covered.*

- *The student must respond that information security must be sought throughout the entire intelligence cycle.*
- *The MPKIO should be aware that ignorance of the Security Foundation may result in damage to personnel, material and the peacekeeping operation.*

Module 1

Conceptual Framework

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

- Policies, manuals, guidelines, philosophy and principles have been developed to create an understanding of MPKI operations in UN peacekeeping missions

- Nevertheless, the implementation and execution of MPKIO in a mission is never straightforward; you need a general understanding and an open, flexible attitude within the United Nations' PKI / MPKI conceptual framework. This understanding should be common to the leadership, staff, forces and other components in the mission

- The MPKIO's skill set can help leverage the MPKI that will help decision-makers be better equipped to execute the mandate. MPKIO personnel must establish working coordination, liaison and support networks based on this conceptual framework that will facilitate planning and execution of MPKIO tasks in a UN PKO

- MPKIO must have a good working understanding of the UNPKI and MPKI frameworks

- For intelligence to be effective, all UN organisations must work collaboratively. Intelligence is considered a 'Team Sport'. The Force, Sector and Battalion intelligence organisations, UN police, and mission components etc. should all support and learn from each other

- The UNPI supports COP, threat early warning, IDs risks and opportunities

- UNPI supports the mandate, is centralised (command/mission) leader driven and a total mission process

- The Intel cycle includes direction, acquisition, analysis and dissemination

- The intel coordination structure directs and oversees the intel-cycle; the JMAC, JOC, MIC team, components HQs, U2 all support the MPKI framework

- Predicting potential threats to civilians is a mission-wide priority for information requirements and should be a priority in driving the Intel cycle

Module 2

Legal Framework

Module 2 at a Glance

Aim

This module conveys to United Nations personnel working on peacekeeping intelligence (PKI) key aspects of the legal framework governing their work.

Relevance

Module 2 empowers PKI personnel to approach their task with confidence by providing them a clear understanding of the legal authority and guarantees underpinning their work, while also setting out legal limits and expectations they must respect.

Learning Objectives

Learners will be able to:

- Apply key rules of international law relevant for peacekeeping intelligence
- Cooperate with host state authorities within the limits established by international human rights, humanitarian, criminal and refugee law
- Assert the privileges and immunities enjoyed by UN personnel working on peacekeeping intelligence

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, 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.

Symbols Legend Reminder

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

Lesson 2.1

International Legal Framework

The Lesson

Starting the Lesson

Overview

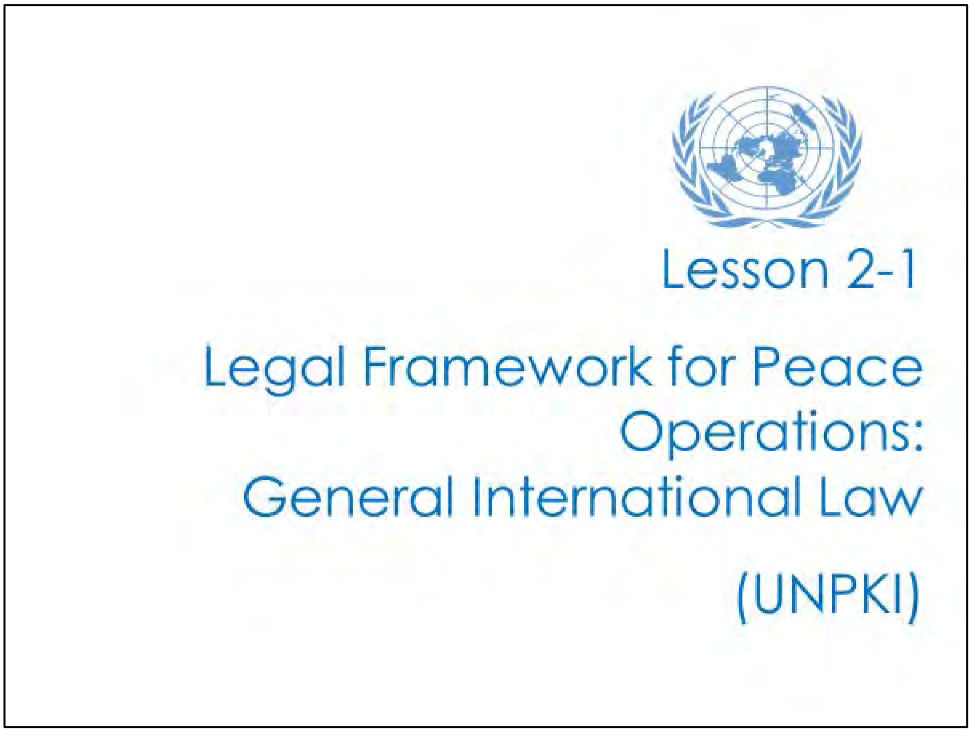
This module begins with an overview of how international law impacts PKI work.

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.

The lesson commences with the introduction of the United Nations Charter, which is the equivalent of the UN's constitution. Thereafter, it covers fields of international law that are particularly relevant for the work of PKI, namely International Human Rights Law, International Humanitarian Law, International Criminal Law and International Refugee Law.

International Law

Slide 1

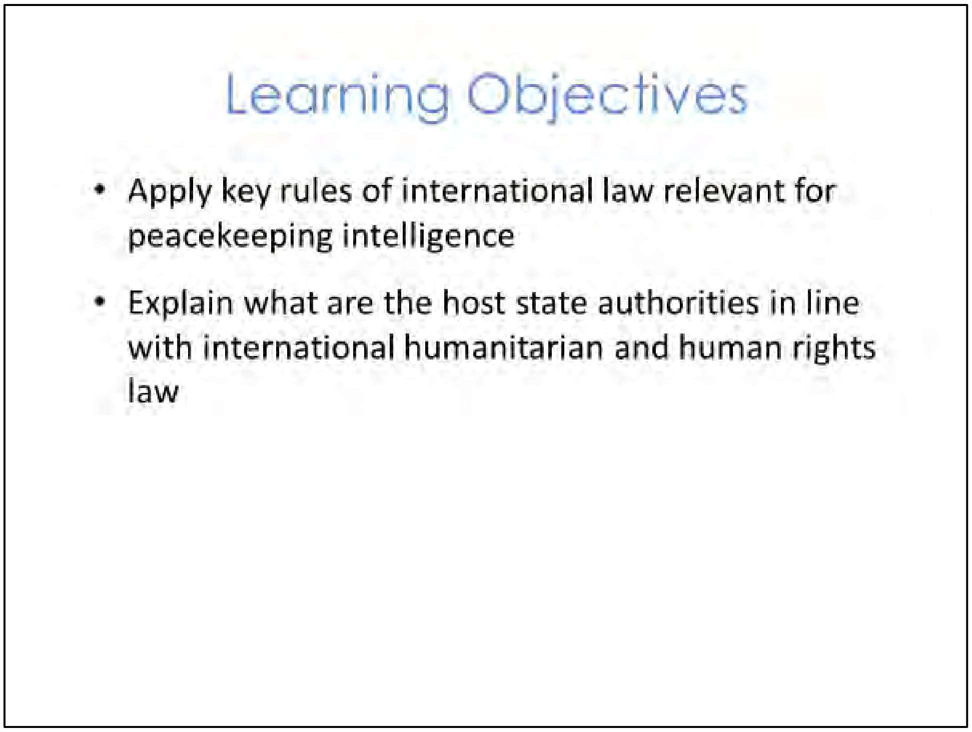


Lesson 2-1

Legal Framework for Peace Operations:
General International Law

(UNPKI)

Slide 2

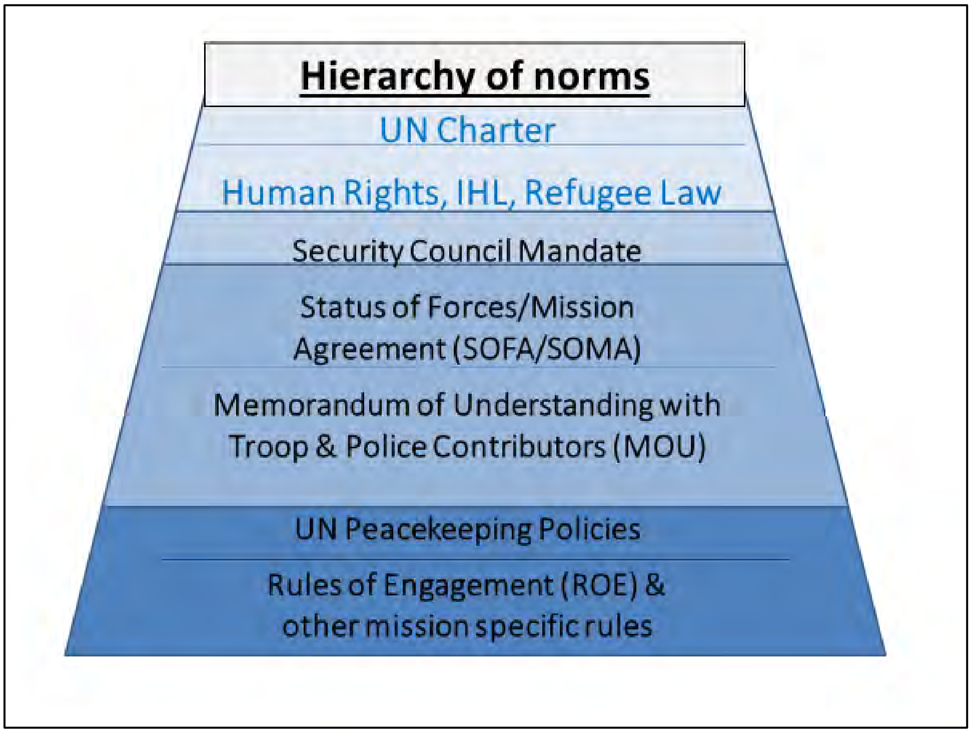


Learning Objectives

- 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 objectives for this lesson.

Slide 3



Hierarchy of norms

UN Charter

Human Rights, IHL, Refugee Law

Security Council Mandate

Status of Forces/Mission Agreement (SOFA/SOMA)

Memorandum of Understanding with Troop & Police Contributors (MOU)

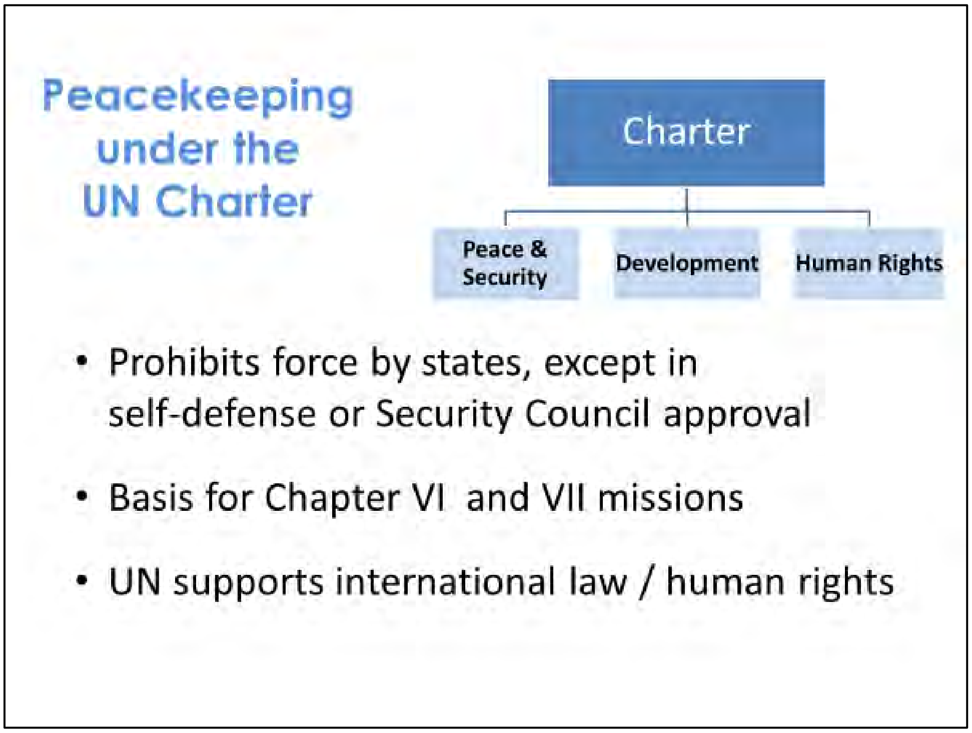
UN Peacekeeping Policies

Rules of Engagement (ROE) & other mission specific rules

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 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 4



Peacekeeping under the UN Charter

Charter

Peace & Security

Development

Human Rights

- Prohibits force by states, except in self-defense or Security Council approval
- Basis for Chapter VI and VII missions
- UN supports international law / human rights

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.

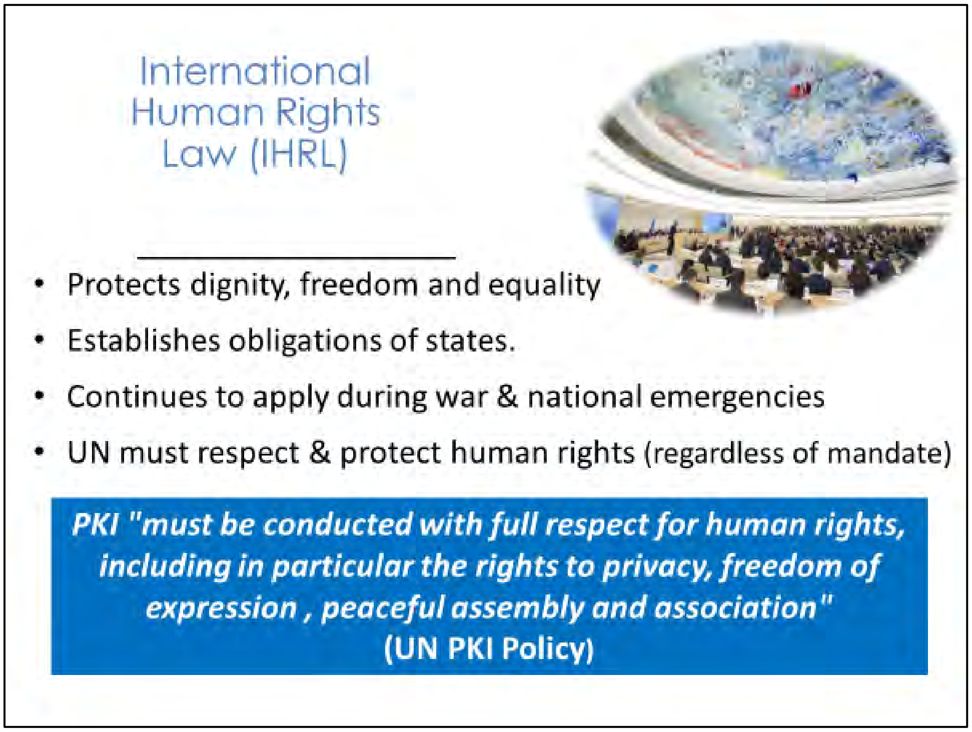
While the UN Charter does not make explicit reference to peace operations, it is undisputed that the UN Security Council may establish peacekeeping and special political missions. All UN peace operations are deployed based on:

- Chapter VI (deals with pacific settlement of disputes), and/or
- 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 intelligence agencies conduct themselves in conformity with international human rights law and are made subject to appropriate civilian democratic oversight mechanisms.

Slide 5



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)

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.

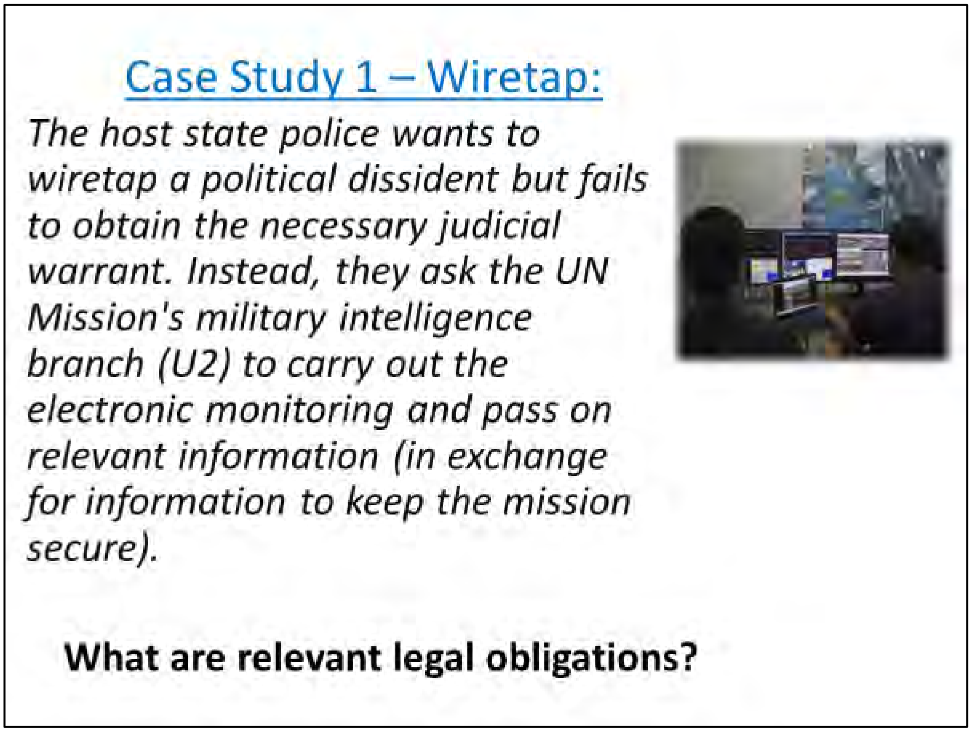
Human rights are universal. Everyone is entitled to the same fundamental rights. There are some groups, who may have specific needs or are particularly at risk of discrimination and rights violations. These have been given specific rights protections (e.g. children, women, indigenous people, persons with disabilities).

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, right not to be tortured, 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 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.*

Slide 6



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?

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 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 require legal basis & legitimate objective*
- *The mission must respect national law as per SOFA/SOMA*
- *United Nations must not aid or assist human rights violations*
- *Risk assessment under United Nations Human Rights Due Diligence Policy*

The case suggests that the host state police is using surveillance for an illegitimate objective, namely, to suppress 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.

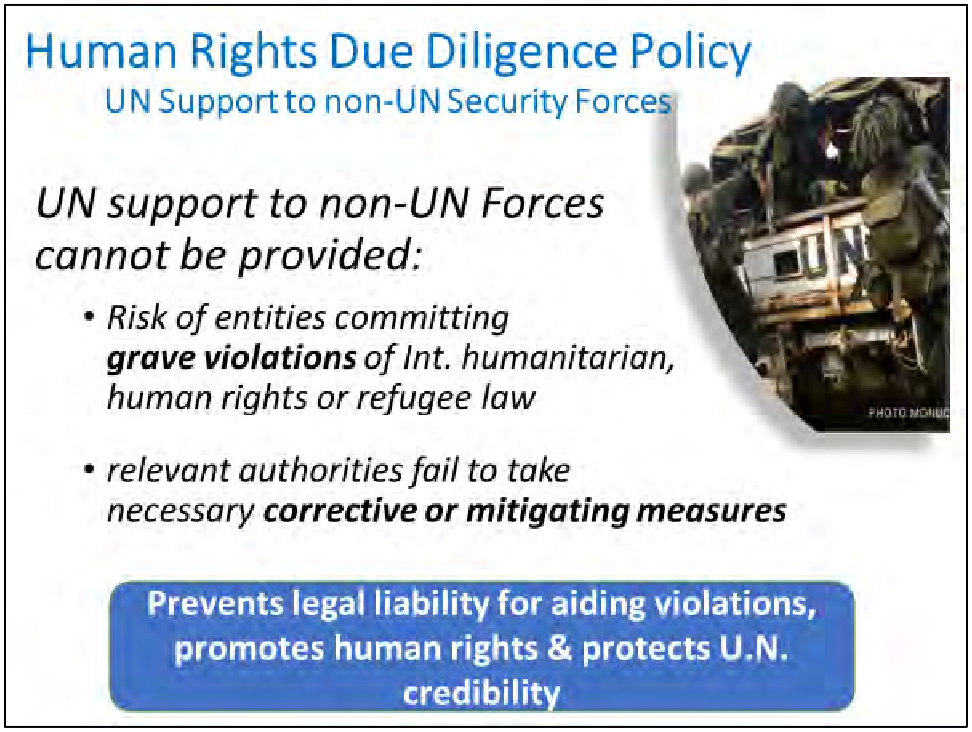
Law enforcement authorities may not evade privacy safeguards by "outsourcing" their surveillance to intelligence actors, whether to national intelligence agencies or, as in this case, the UN's military intelligence resources.

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 to 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 intelligence.*

Slide 7



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

The Human Rights Due Diligence Policy (HRDDP) is binding for the entire United Nations (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.

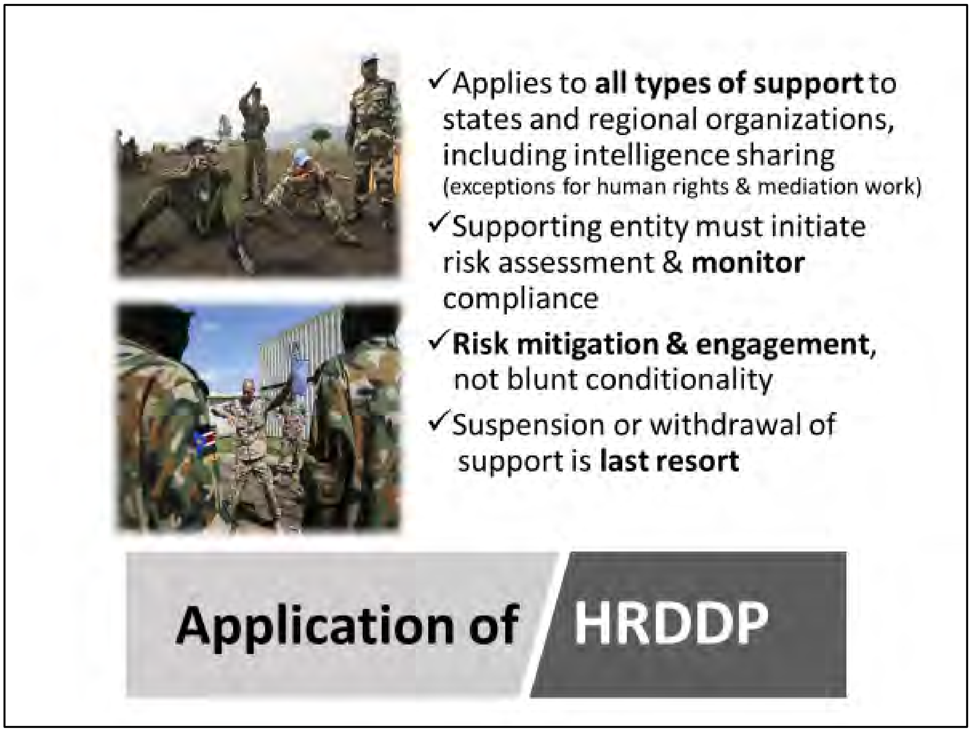
All UN entities that plan to or are already providing support to non-UN security forces must, therefore, assess the risks involved in providing or not providing such support. This assessment needs to consider the risk of the recipient entity committing grave violations of international humanitarian law, 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 intelligence shared or excluding problematic areas from intelligence sharing agreement).

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 U.N. from state forces involved in grave violations also protects the UN’s reputation and perceived impartiality.

In peacekeeping settings, some 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. 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 MONUC 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 8



✓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

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 intelligence, training, capacity building, mentoring, technical cooperation, and financial support. As noted, sharing intelligence amounts to provide technical advice, capacity building or equipment to national 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]

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

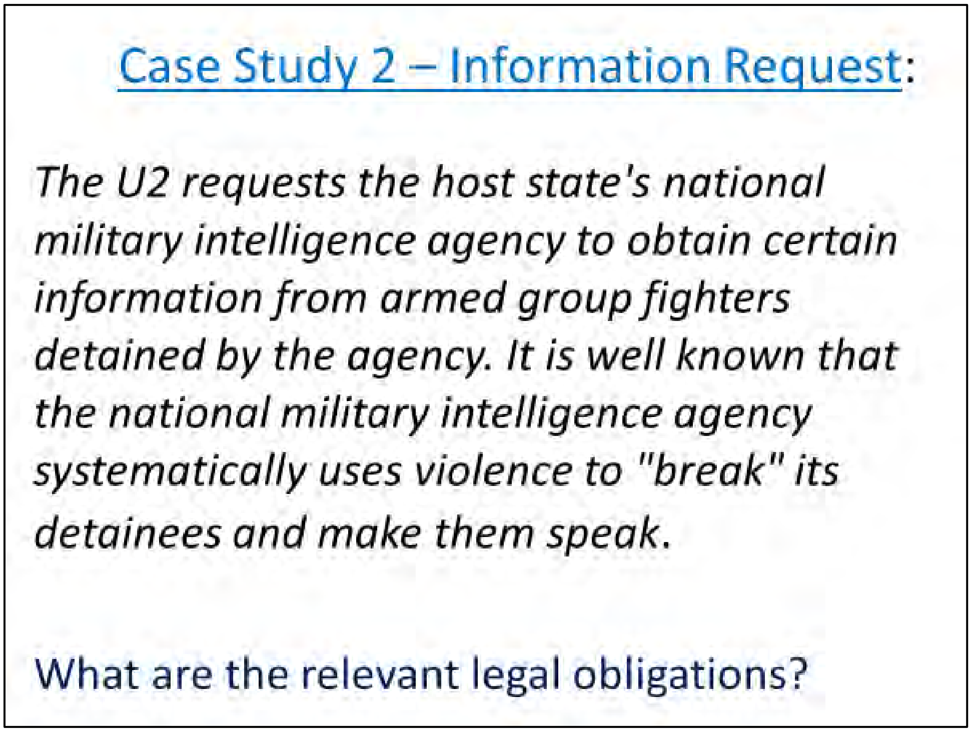
Applying the HRDDP, notably when sharing intelligence, requires several steps: Before sharing any intelligence, the entity within the mission that wants to share (e.g. the UN Force) must initiate a risk assessment and determine if there is a real risk that the recipient is or will be committing grave 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 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 intelligence sharing (e.g. any intelligence on unarmed civilians). Or it may insist on joint after-action reviews on how shared 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 intelligence sector.

Before sharing 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 violations, e.g. through advocacy between military counterparts or, where appropriate, the mission leadership. If grave violations persist despite such interventions, the mission must temporarily suspend intelligence sharing or, if no improvement can be expected, terminate intelligence sharing altogether.

☞*UN Photos shows UN training national armies, which must comply with HRDDP.*

Slide 9



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?

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*

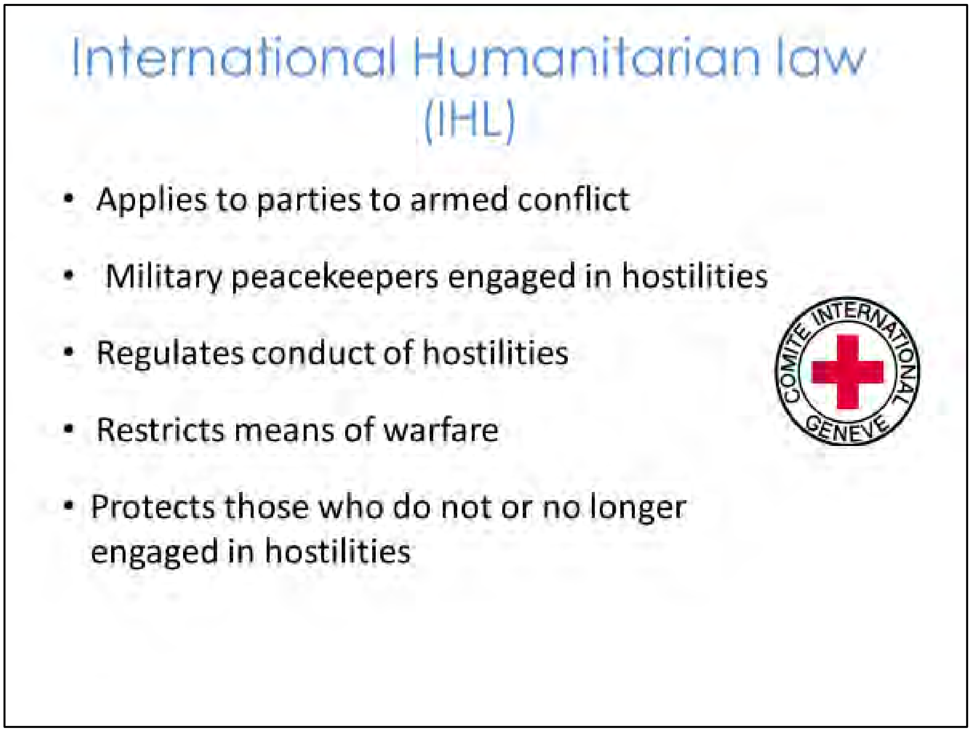
Mission components like security (UNDSS), UNPOL or the Force will regularly set up channels of communication to share sensitive information, including intelligence products, notably to keep the mission safe and protect civilians. Details on the process and relevant safeguards to avoid misuse are set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

While the HRDDP applies to share information with national 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.

Slide 10



COMITE INTERNATIONAL
GENEVE

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

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.

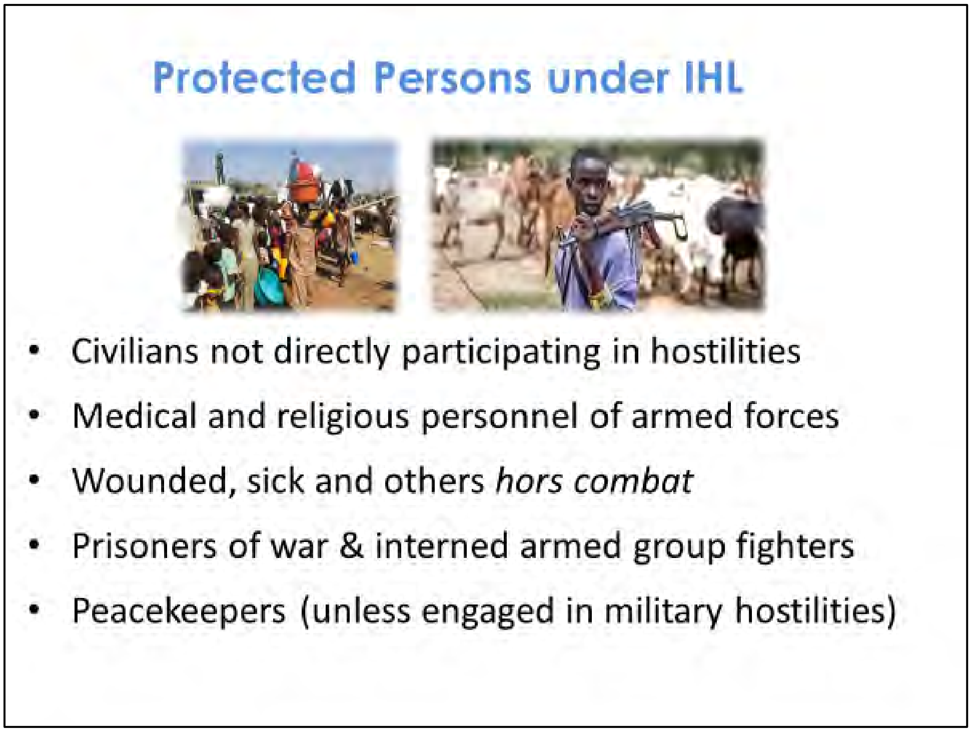
Parties must respect International Humanitarian Law (IHL) to armed conflicts, such as States forces fighting each other in an international armed conflict. In a non-international armed conflict involving non-state armed groups, the state military forces, and the non-state armed groups involved must all 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 19th century. The ICRC remains the neutral guardian of IHL in conflict areas worldwide.*

Slide 11



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)

Ask participants who are a 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.

Under IHL, any person who is not or is no longer directly participating in hostilities shall be considered a civilian, unless he or she is 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.

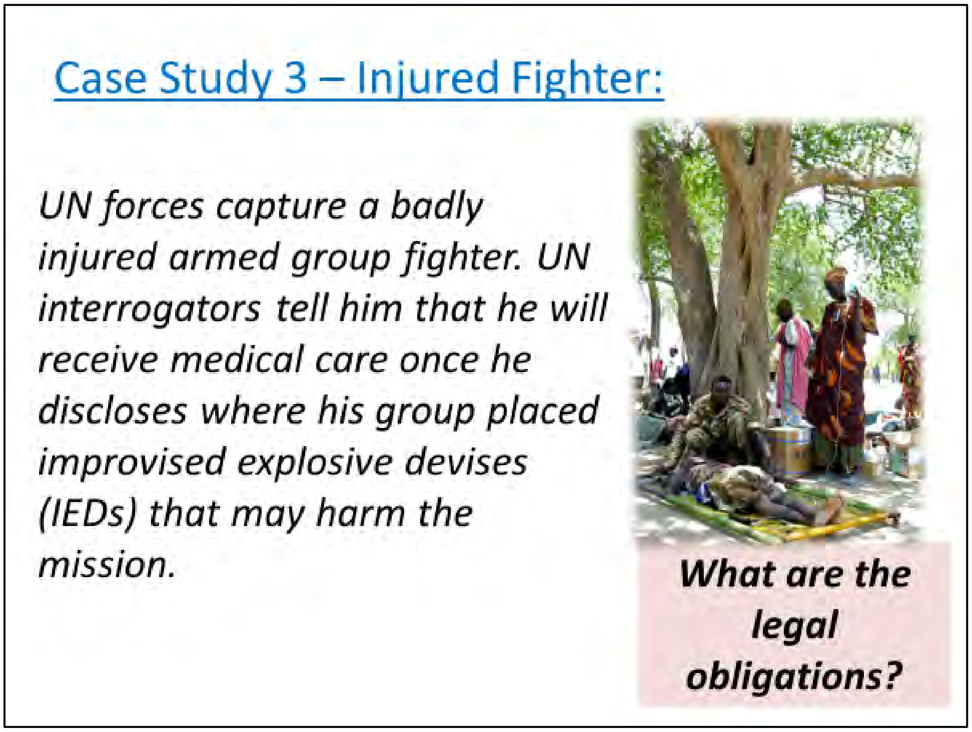
Members of armed forces or armed groups that are hors de combat (“out of battle”) also enjoy protection under international humanitarian law. Notably, those who can no longer fight because they are wounded and sick must not be attacked but collected and medically cared for.

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.

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

Slide 12



Case Study 3 – Injured Fighter:

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

What are the legal obligations?

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*

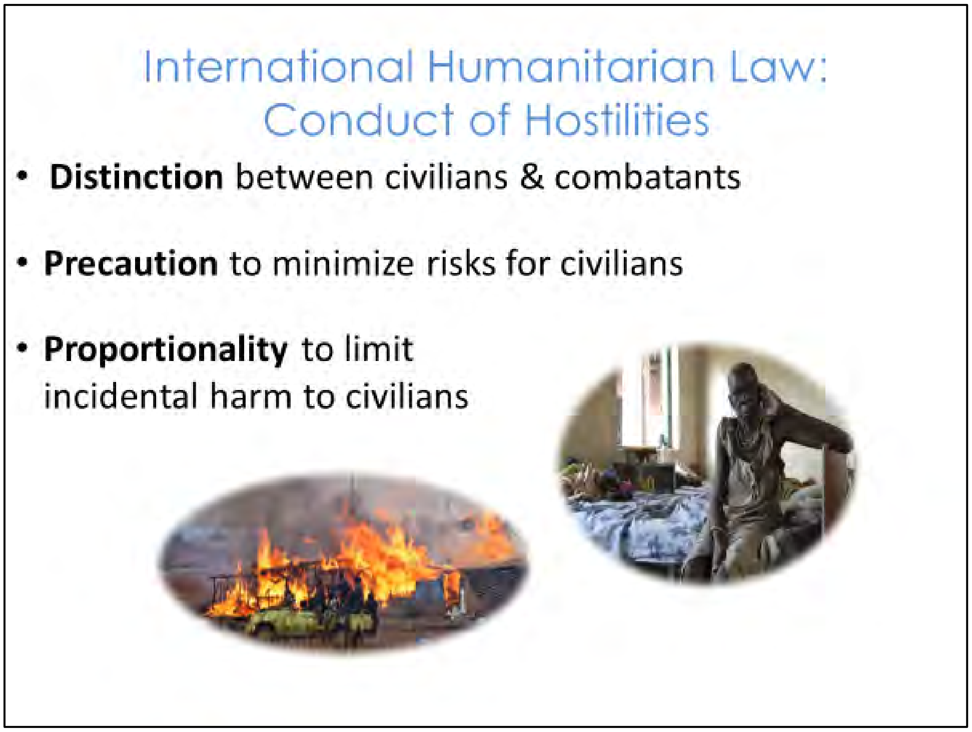
IHL also protects combatants who can no longer take part in hostilities, notably because they are incapacitated (hors de combat), injured, have surrendered or are detained.

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 intelligence.

☞ *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 & apply it.*

Slide 13



International Humanitarian Law: Conduct of Hostilities

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

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: In order 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

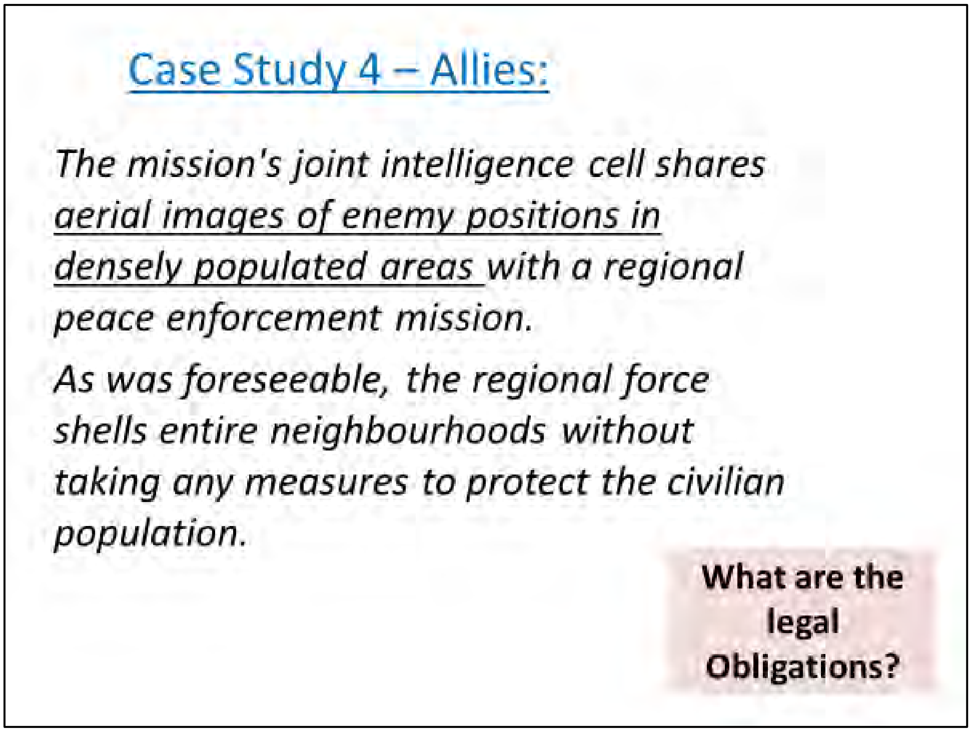
- Precaution: In the conduct of military operations, constant care must be taken to spare civilians and civilian objects. All feasible precautions must be taken to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects. Examples of violations:

    - 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.*

Slide 14:



Case Study 4 – Allies:

The mission's joint intelligence 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?

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.

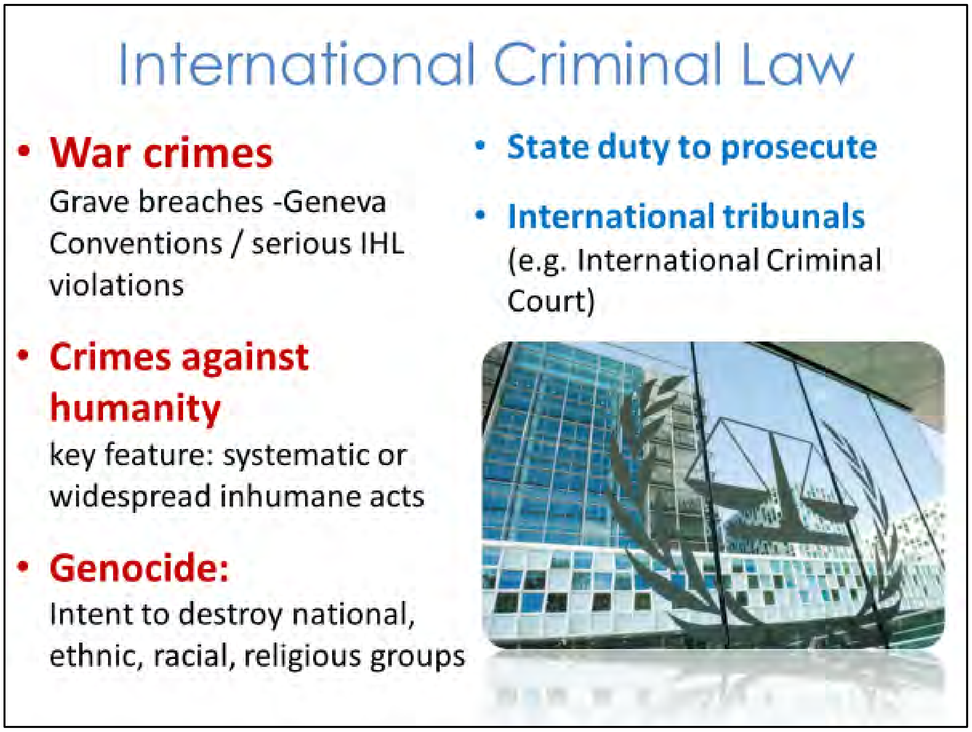
- *War crime: Indiscriminate attack*
- *IHL Duty of Precaution*
- *Avoid complicity in war crime*
- *Human Rights Due Diligence Policy*

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 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 PoC adviser to monitor the conduct of the regional force. If violations persist despite mitigatory measures, intelligence can no longer be shared.

Slide 15



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)

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 UNMO 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.

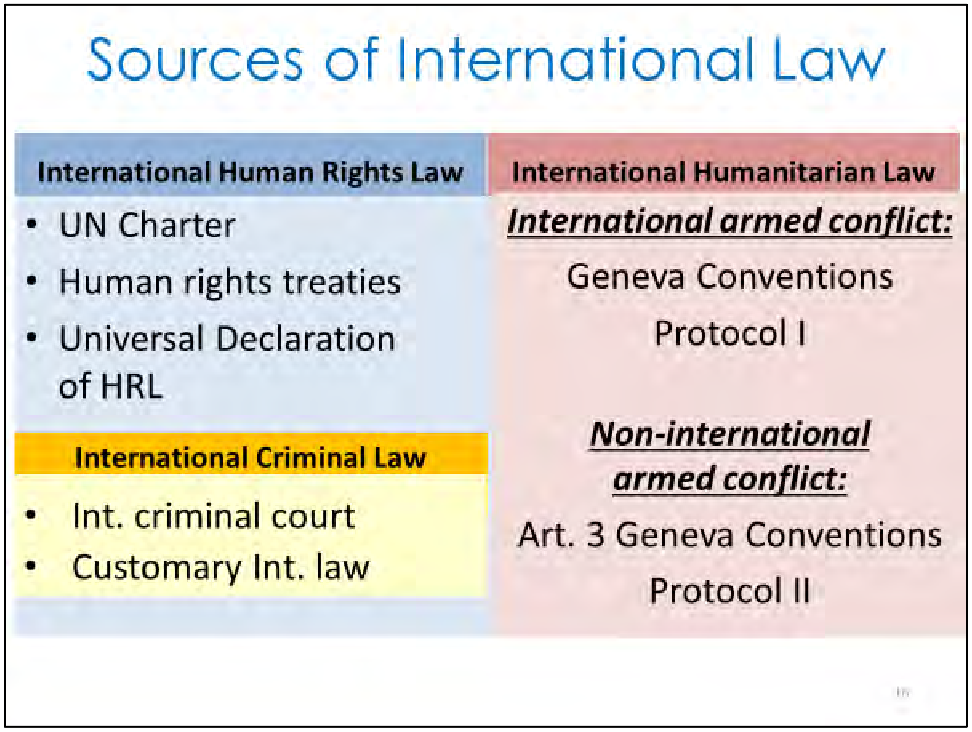
Crimes against humanity: Where state authorities or armed groups commit inhumane acts such as murder, rape, torture in a systematic or widespread manner attack, with knowledge of this broader attack, this may entail crimes against humanity. Such crimes typically involve an underlying policy to commit crimes and/or 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 intelligence with security forces engaged in international crimes can lead to legal complicity (soliciting or assisting crimes) if risks are not properly assessed before 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.*

Slide 16



Sources of International Law

International Human Rights Law

- UN Charter
- Human rights treaties
- Universal Declaration of HRL

International Criminal Law

- Int. criminal court
- Customary Int. law

International Humanitarian Law

International armed conflict:

Geneva Conventions

Protocol I

Non-international armed conflict:

Art. 3 Geneva Conventions

Protocol II

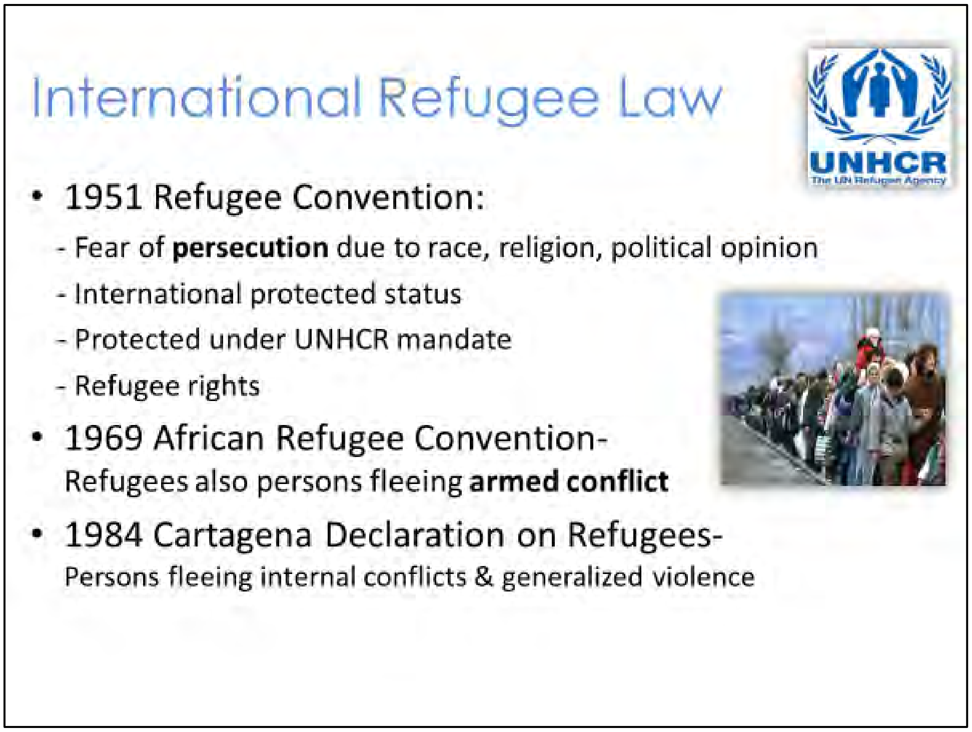
The content of international humanitarian, human rights and criminal law is defined by international treaties that states have voluntarily signed and ratified. Many of the norms have also been practised and accepted by states to such a degree that they have become customary law that binds all states.

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.

Slide 17



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

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.

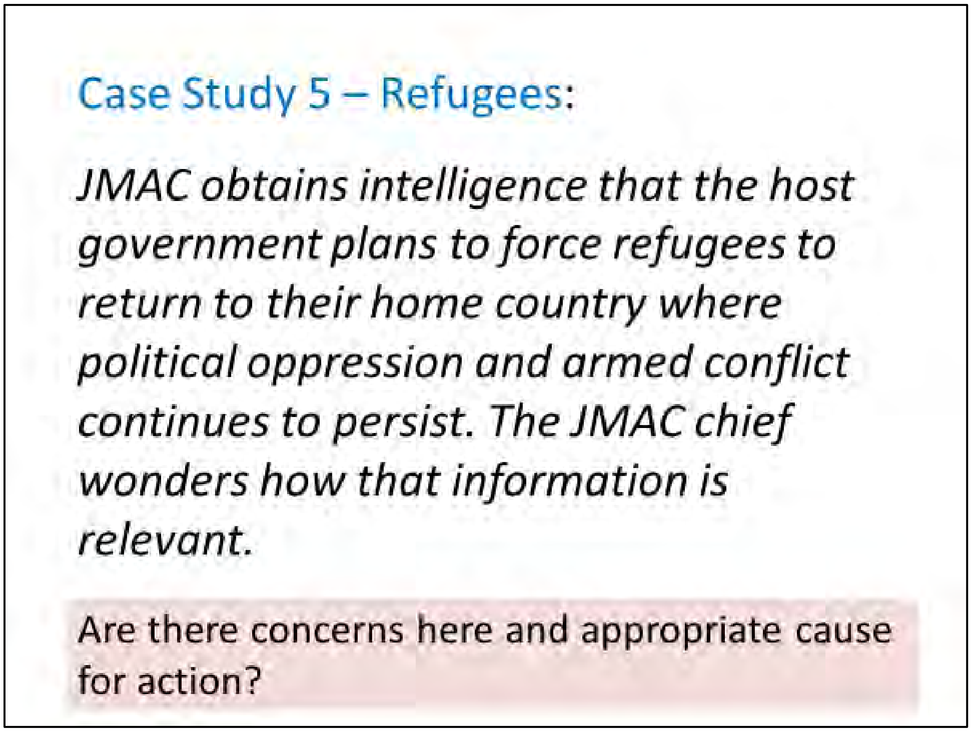
Fleeing a country where an armed conflict is taking place qualifies a person only as a refugee if specific requirements are met (notably evidence of individual "well-founded fear of being persecuted"). However, regional instruments have expanded the scope of the refugee definition. Under the 1969 African 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.

☞ *Refugees exist around the world. The UN Photo shows refugees in the Balkans.*

Slide 18



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?

Case Study to be discussed in group work or in plenary.

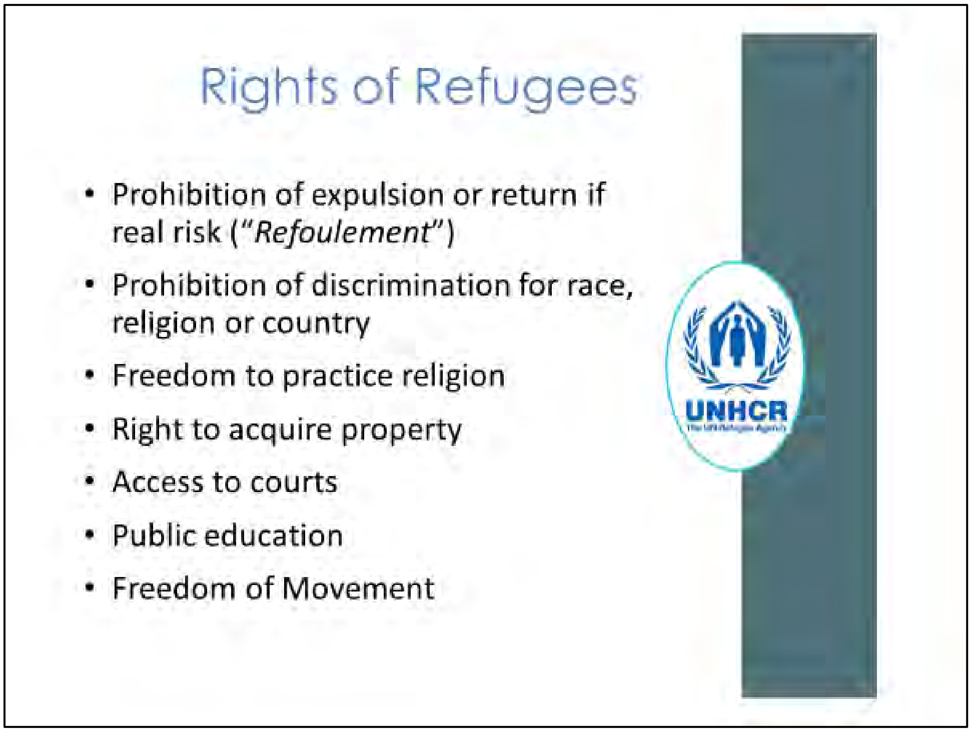
Ask the students if there are concerns and if there is an appropriate cause for action. Here are points to consider for facilitating the discussions:

- *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 coordination structures*
- *Responsibility to alert human rights component & UNHCR*

The 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 his life or freedom would be threatened on account of his 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 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 19



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

UNHCR
The UN Refugee Agency

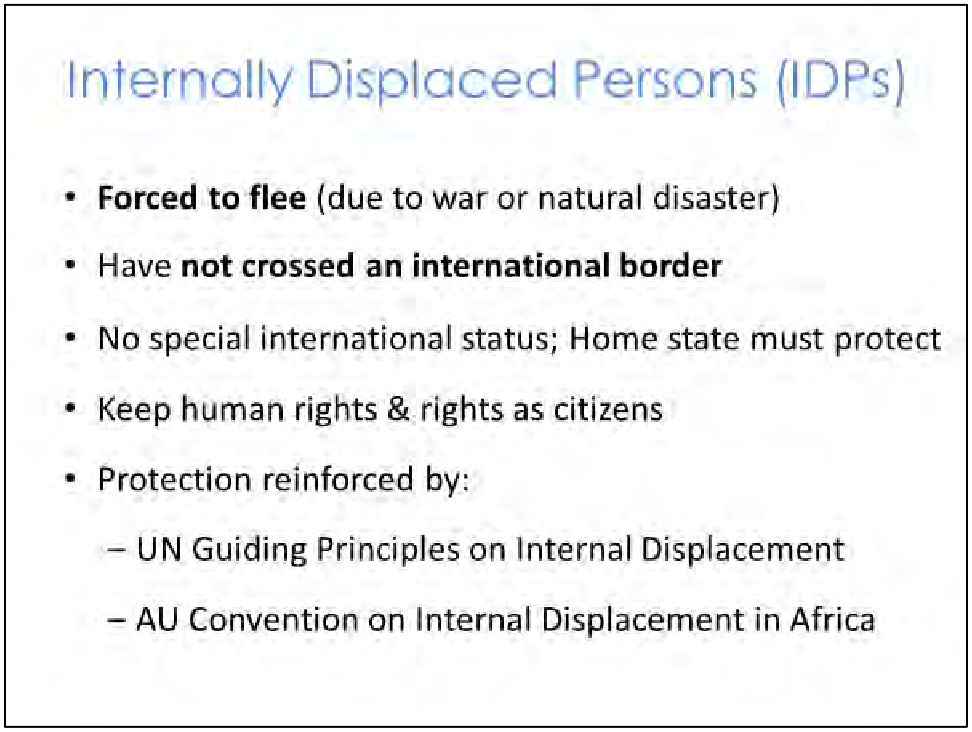
Refugees enjoy special status and related rights under international law. Since they have lost the protection of their home country, which has persecuted them, they are under the protection of the United Nations High Commissioner for Refugees.

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).

Slide 20



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

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

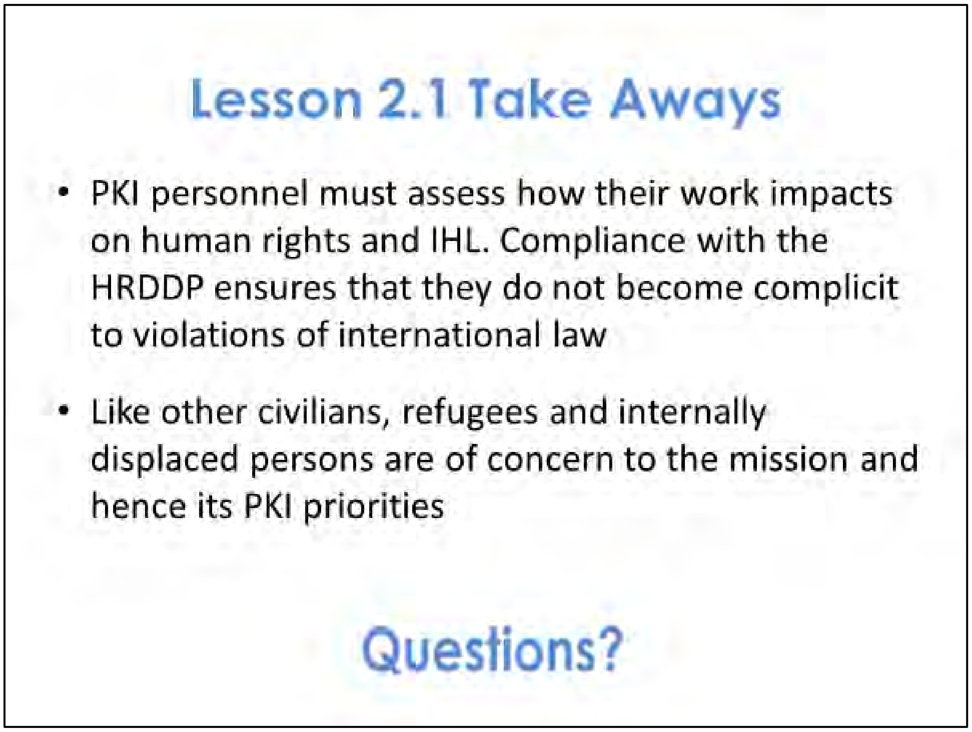
The protection of IDPs and other affected populations within their own country is primarily the responsibility of national authorities. Unlike refugees, IDPs do not enjoy a special legal status under international law. However, the international community has a role to play in promoting and reinforcing 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 make an arrangement 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.

Slide 21



Lesson 2.1 Take Aways

- 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

Questions?

Summary

Key takeaways 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

United Nations Peace Operations-Specific Legal Framework

The Lesson

Starting 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 collection, use and sharing of PKI.

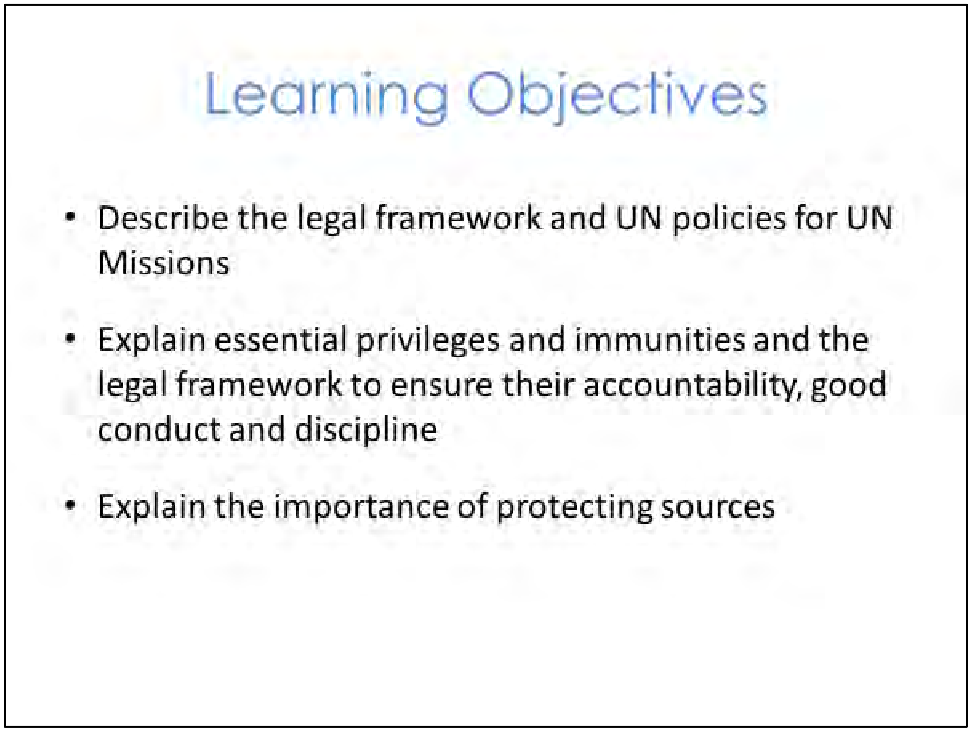
UN Peace Operation-Specific Legal Framework

Slide 1

Lesson 2-2
Legal Framework for Peace Operations- Mission Specific (UNPKI)

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

Slide 2

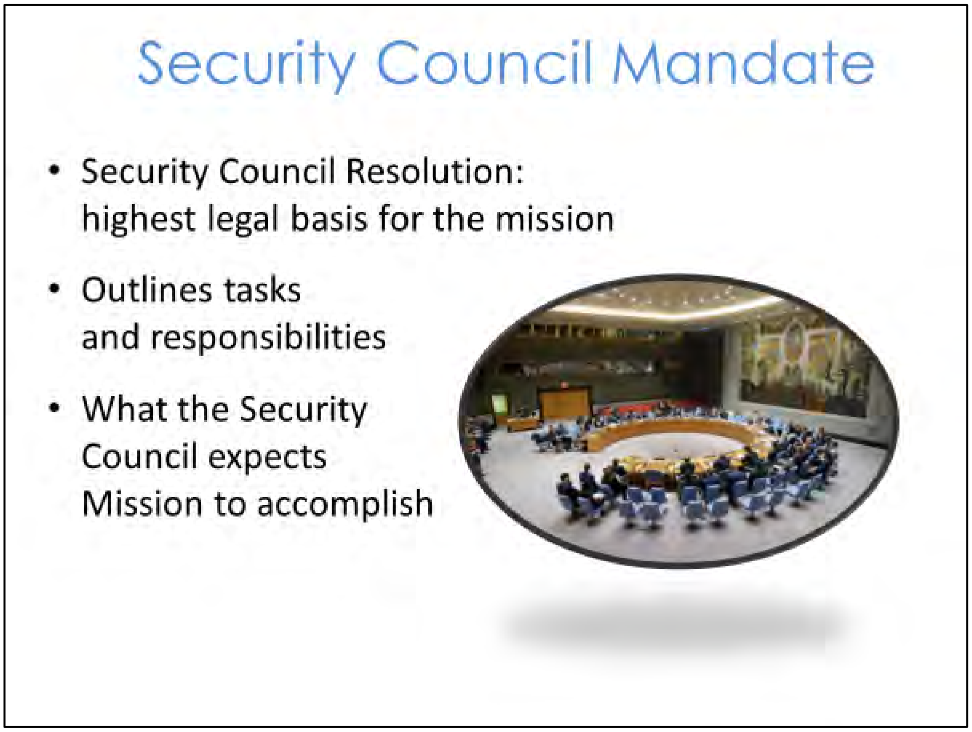


Learning Objectives

- 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 objectives for this lesson. Take a minute to read over the objectives.

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

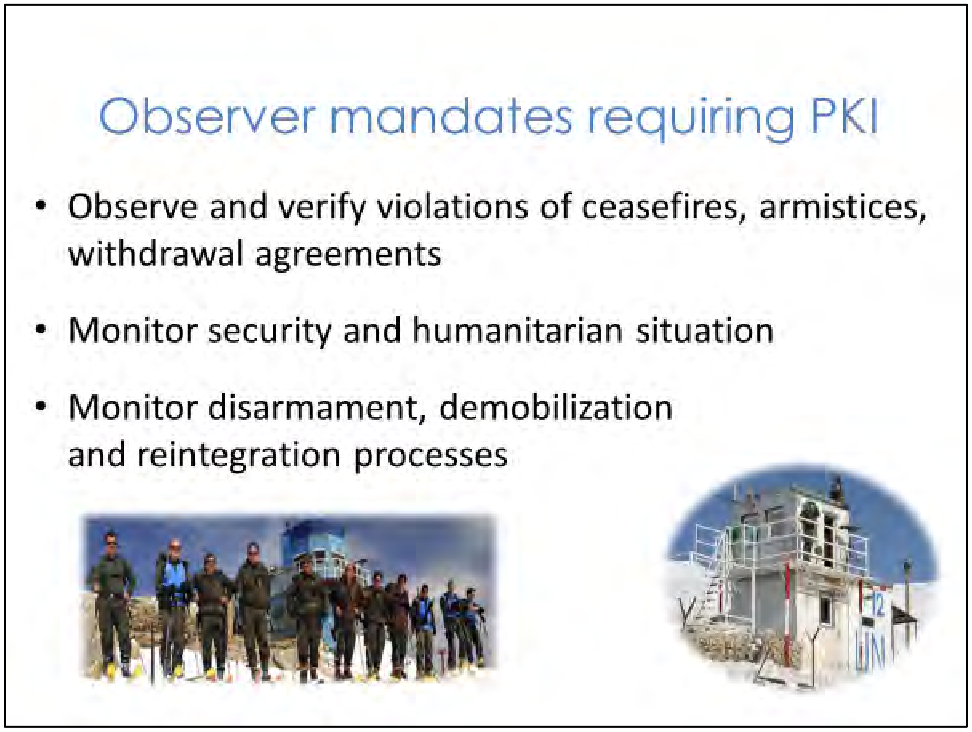
Every peacekeeping operation begins with the Security Council adopting a resolution that establishes the mission. The Council will seek to establish a mission with the consent of the Host State to its deployment. Depending on the mission's mandate and role, it will also want the consent of the other 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 intelligence by United Nations peacekeeping operations will be conducted to enhance situational awareness and the safety and security of UN personnel and to inform operations and activities related to the protection of civilians tasks of the Security Council mandates.

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

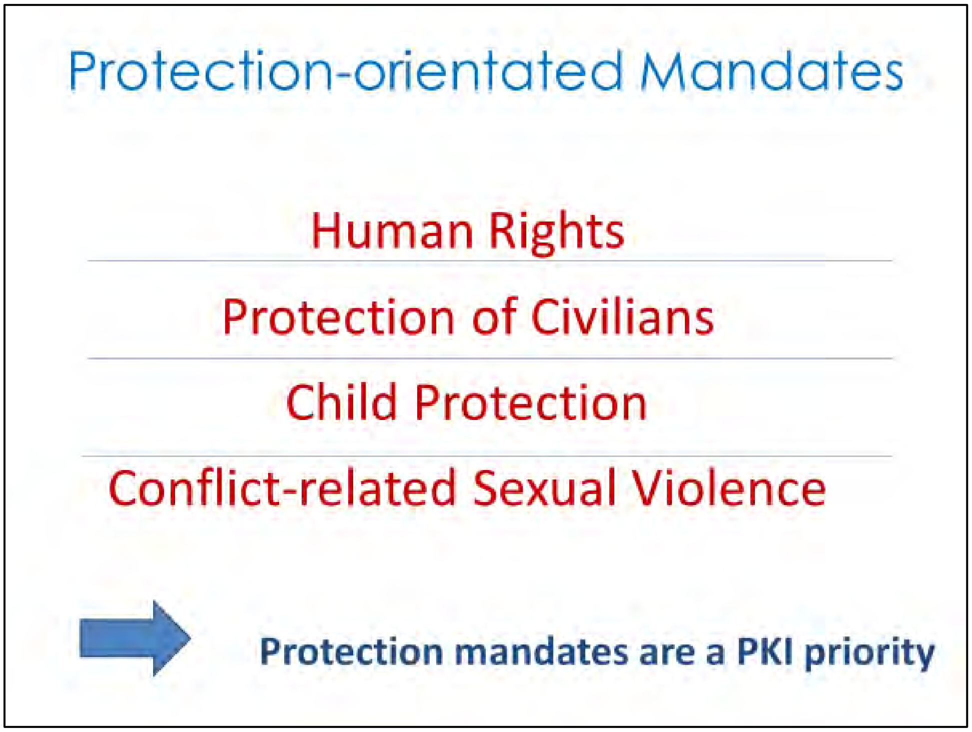
The scope of PKI activities follows the scope of the mission's mandate. As the mandates and operating environments of United Nations peacekeeping missions have evolved, so too have the capabilities, processes and procedures required to gather and analyse information. In the high-tempo complex and dangerous 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 better understand their operating environments and contexts, maintain a strategic overview of developments, and predict specific threats and opportunities to enable peacekeepers to effectively execute their mandates.

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

- 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



Protection-orientated Mandates

Human Rights

Protection of Civilians

Child Protection

Conflict-related Sexual Violence

Protection mandates are a PKI priority

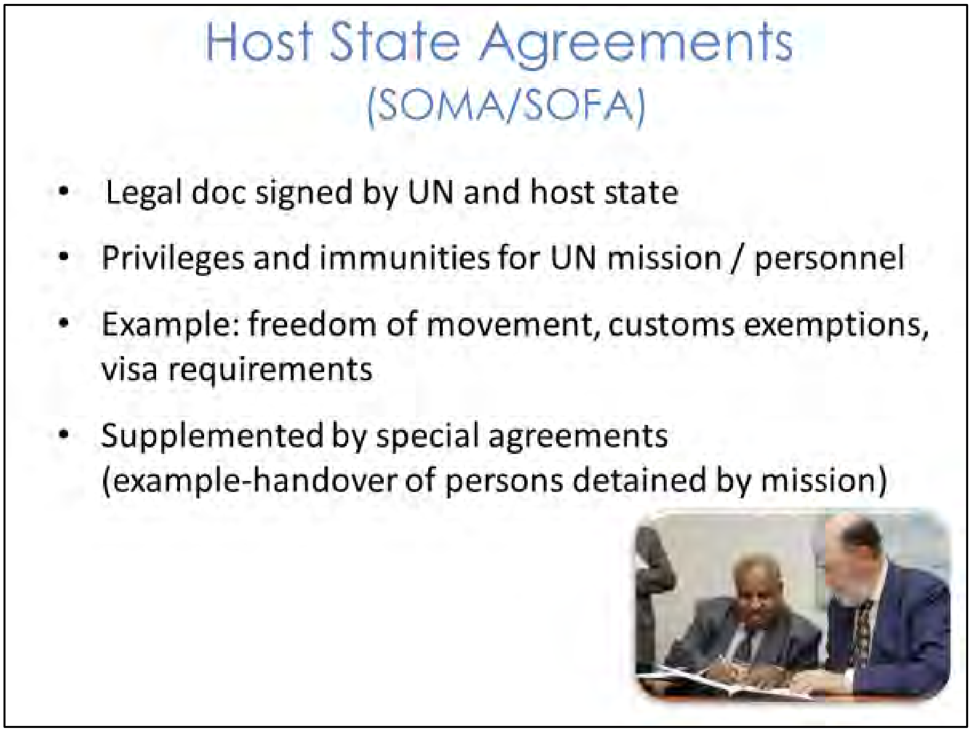
Multidimensional peacekeeping missions are regularly assigned protection mandates. Specialized civilian staff work on these mandates, including human rights officers, protection of civilians advisers, child protection advisers and women protection advisers. However, these mandates remain whole of mission 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 so as 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 civilians 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 authorizes 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 requires a nexus between the sexual violence and the conflict (e.g. domestic violence would typically not be covered)

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 discussions.

- *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 physically assault the journalists, 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 children protection and CRSV mandate.*

Slide 6



Host State Agreements (SOMA/SOFA)

- Legal doc 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)

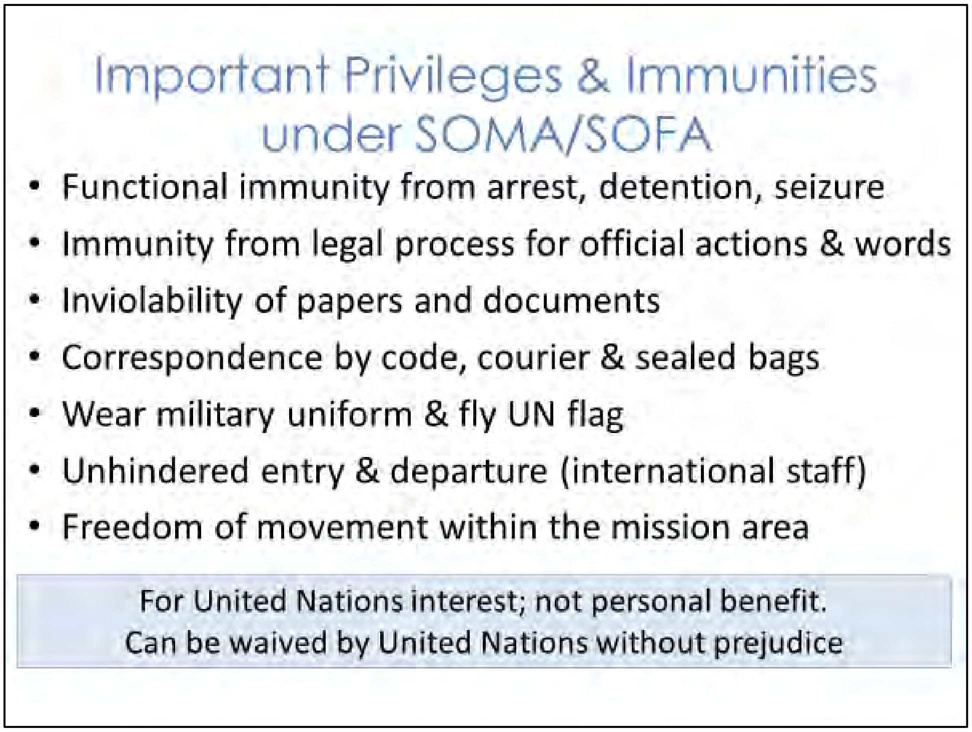
Before the deployment of a peace operation, the UN and the host Government sign a Status of Forces Agreement (for peacekeeping missions) or Status of Mission Agreement (for special political missions). The SOFA/SOMA establishes the legal framework that regulates the status of the mission and its members 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 intelligence sharing to mitigate any risks of its 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

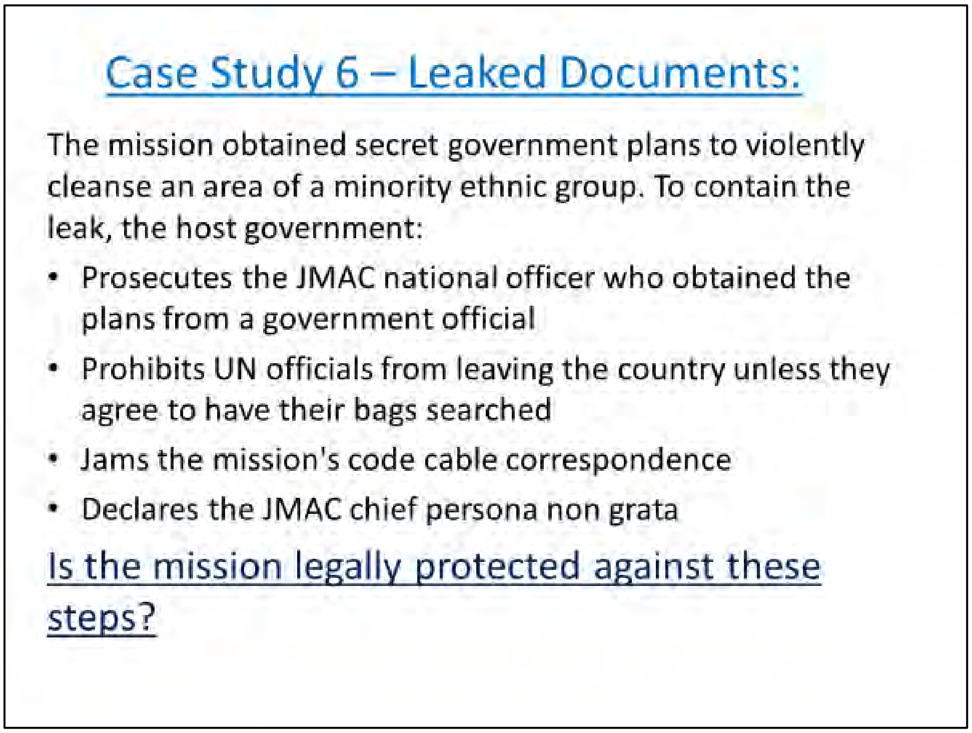
Beyond technical/financial issues like exemption from customs duties, the SOFA/SOMA provides privileges and immunities that are very relevant for personnel working on PKI:

- The host state cannot arrest and detain mission staff or seize any of their belongings concerning any functions they carry out in their official functions. 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 United Nations 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 United Nations to work without obstacles. They are not for the personal benefit of individual staff. In particular, the United Nations may waive any of these immunities if it is in their interest of the organisation and the course of justice.

Slide 8



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?

Case Study to be discussed in group work or in plenary.

Some SOFA/SOMA Immunities for discussion points:

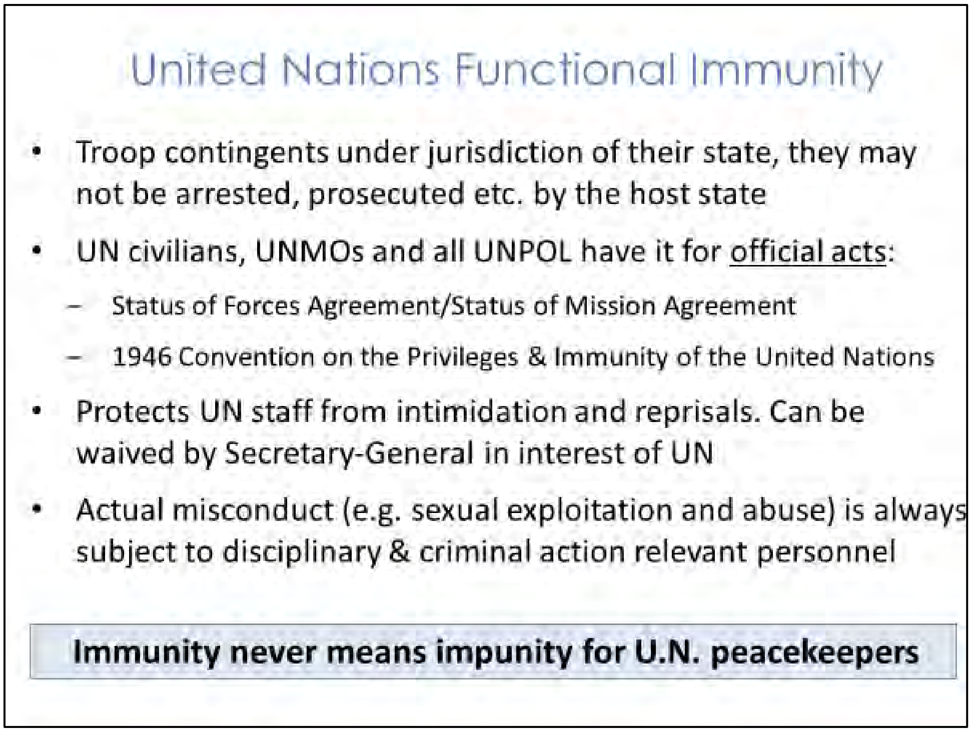
- *Freedom of movement*
- *Inviolability of papers*
- *Use of Codes*
- *Functional immunity from legal process*

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 intelligence conducted in such a way as to assure secrecy or concealment of the activities, because they are illicit and/or are inconsistent with the legal framework, principles, policies and mandates of United Nations peacekeeping operations).

In any case, the privileges and immunities of the United Nations, 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 document 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, requiring 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, United Nations 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 relevant personnel

Immunity never means impunity for U.N. peacekeepers

Even though following the mission's Security Council mandate, PKI activities may occasionally render United Nations 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.

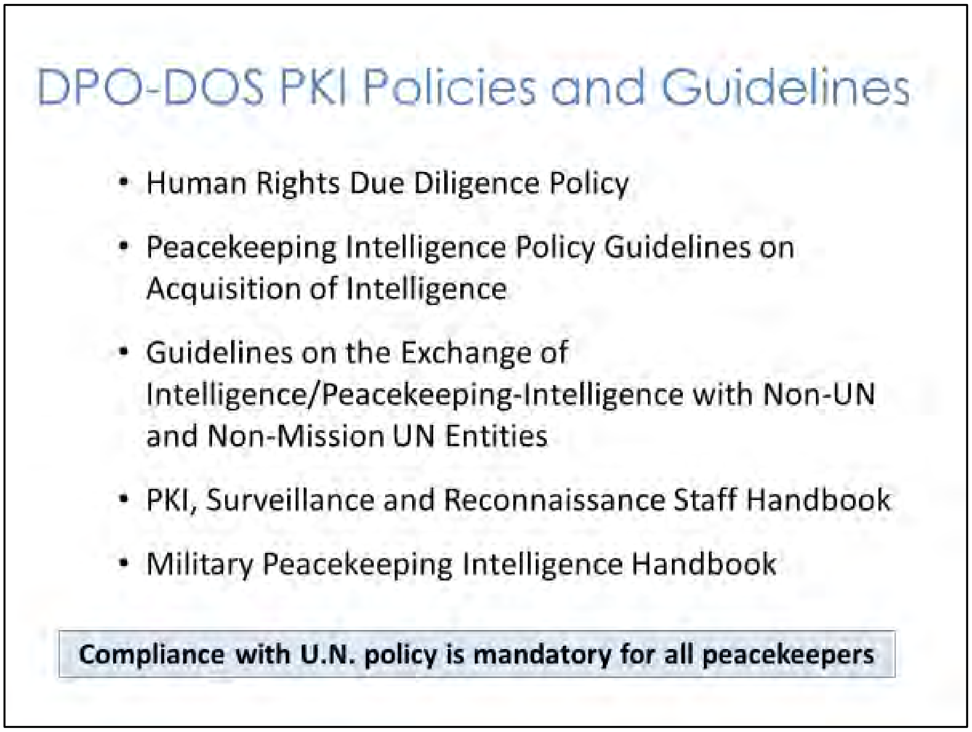
As per the SOFA, troop contingents, including staff officers (e.g. in the U2/Military Intelligence), remain under the exclusive jurisdiction of the sending state. The host state has no jurisdiction to prosecute them or otherwise subject them to legal process.

UN Military Observers and UNPOL officers may also be involved in PKI. They are considered United Nations 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 United Nations 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 United Nations 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.

Slide 10



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

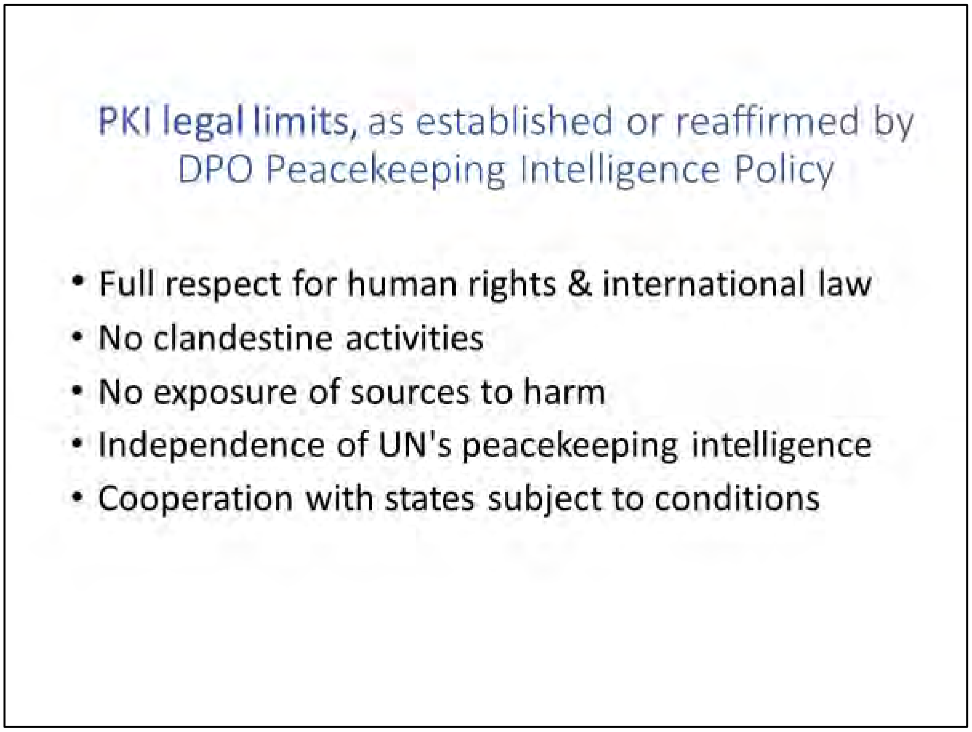
Compliance with U.N. policy is mandatory for all peacekeepers

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 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 these policy and guidance documents is mandatory for all peacekeepers.

Slides 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

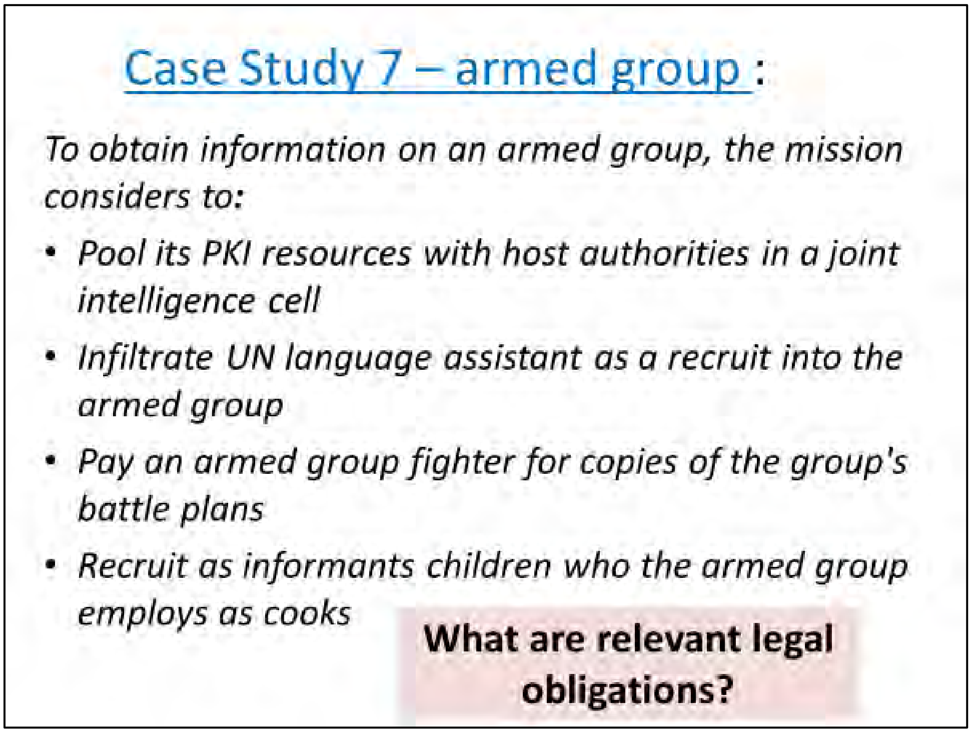
Gathering and sharing United Nations Peacekeeping Intelligence is subject to legal limits. Some limits follow directly from international human rights law and have been set out in lesson 2.2. Others are established by the Peacekeeping Intelligence Policy to protect the independence and impartiality of 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 peacekeeping-intelligence 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 intelligence conducted in such a way as to assure secrecy or concealment of the activities because they are illicit and/or are inconsistent with the legal framework, principles, policies and mandates of United Nations peacekeeping operations”. For example, United Nations 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. To 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.

United Nations peacekeeping intelligence 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.

Slide 12



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 as a recruit 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?

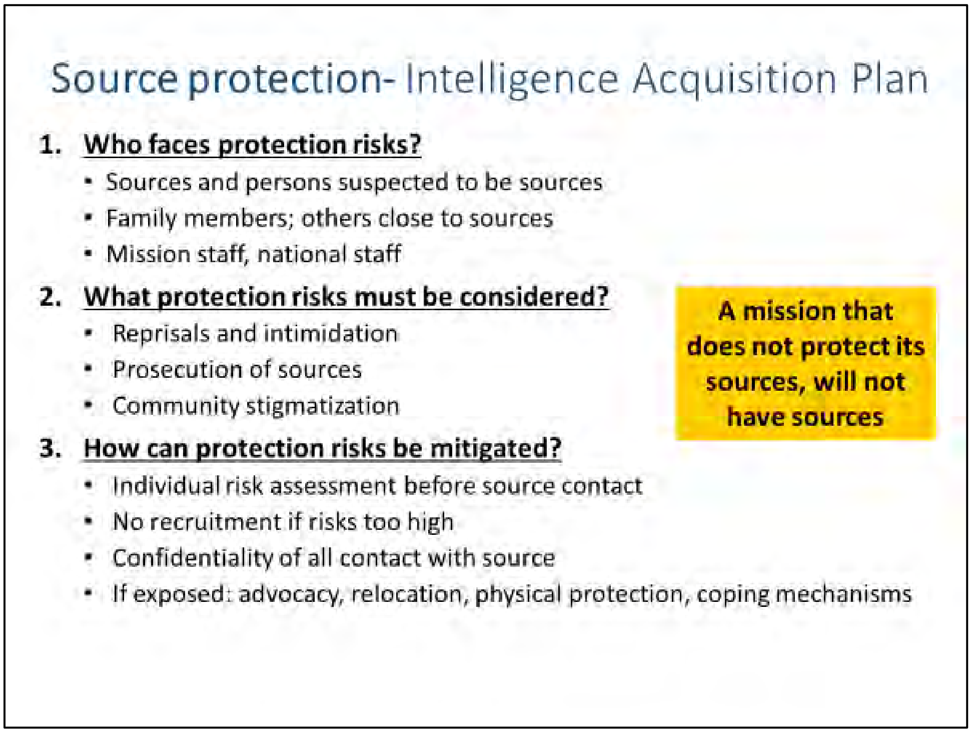
Case Study to be discussed in group work or in plenary. Ask the students to bring out some relevant legal obligations. Here are the points for you to use in facilitating the discussions.

- *Independence of PKI processes*
- *Protect sources from harm*
- *No covert action*
- *No children as sources*
- *The mission may share intelligence with national 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 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 an impartial risk 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 Peacekeeping Intelligence Policy does not rule out paying informants in clearly defined circumstances, although such arrangements always bear the risk of resulting in unreliable information. However, this should be done discretely, and it should be made clear that this is a specific course of action reserved for PKI, as many civilian mission components (e.g. human rights components) have a policy never to offer payment to receive information.*
- *Following the UN's PKI principles, the mission must never recruit or otherwise develop children as sources of intelligence, because they cannot give*
- *The mission may share intelligence with national 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 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 an impartial risk 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 Peacekeeping Intelligence Policy does not rule out paying informants in clearly defined circumstances, although such arrangements always bear the risk of resulting in unreliable information. However, this should be done discretely, and it should be made clear that this is a specific course of action reserved for PKI, as many civilian mission components (e.g. human rights components) have a policy never to offer payment to receive information.*
- *Following the UN's PKI principles, the mission must never recruit or otherwise develop children as sources of 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.*

Slide 13



Source protection- Intelligence 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

UN Policy requires the mission to take particular care not to expose any 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 intelligence officers apply in their national context.

Source protection cannot be ensured in an ad hoc manner but requires careful assessment, planning and integration in the mission's Intelligence Acquisition Plan (IAP). 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:

1. Who faces protection risks?

Not only actual 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. Mission staff may also face risks, national staff and their families. It is also important that, in its outside communication, the mission strictly distinguishes its PKI processes from the information gathering of 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.

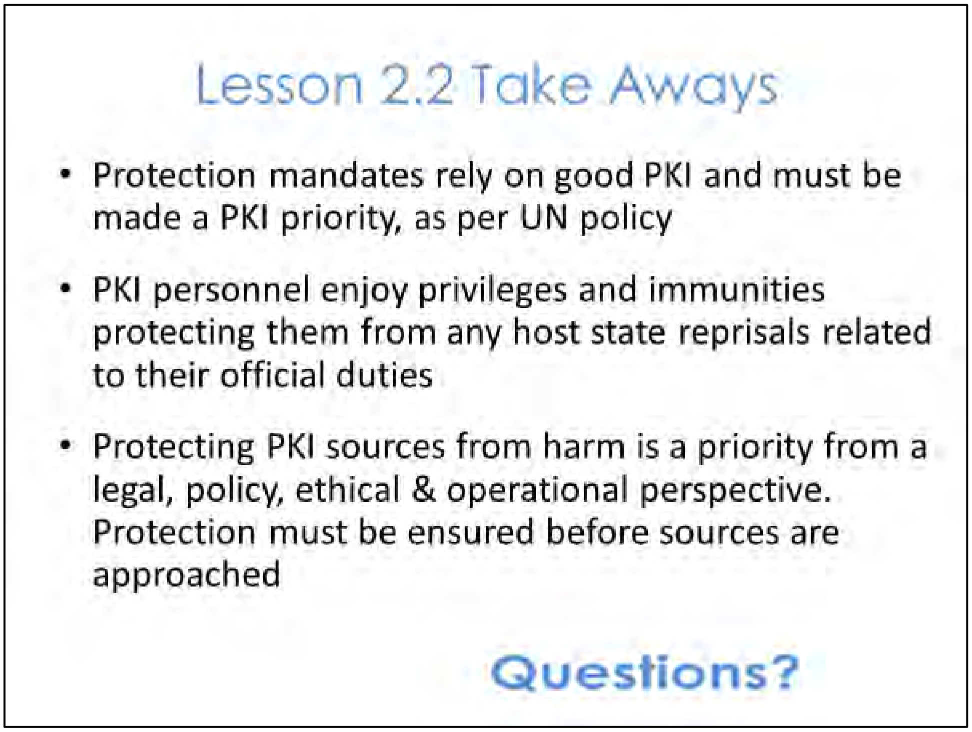
2. What must protection risks be considered?

If exposed, 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 no 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 on charges of espionage or similar offences. Depending on the reputation the mission enjoys communities, a person may be subject to social stigma and ostracised by his/her own community if s/he is seen as a "traitor" who shares intelligence with the UN.

3. <u>How can protection risks be mitigated?</u>

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 cause of action since most sources will already have coping mechanisms to deal with protection risks. These can be further reinforced by appropriate mission action.

Slide 14



Lesson 2.2 Take Aways

- 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

Questions?

Summary

Key takeaways 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 & operational perspective. Protection must be ensured before sources are approached

Module 2

Legal Framework

Take away from Module 2 include:

- International and national humanitarian legal frameworks impact and guide peacekeeping in the field
- Bodies of international law provide special protection for those members of 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 MPKIO 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
- 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 United Nations Staff Officers / MPKIO to better understand the key operational framework to include staff techniques for operating in UN peacekeeping operations.

Learning Objectives

The learning objectives for Module 3 are based on being able to understand and apply the fundamentals of the first two modules into the operational framework:

- To better understand the fundamental skill sets and techniques required for MPKIO to successfully operate in a UN mission

- Apply basic techniques and procedures when performing the duties of a MPKIO on a staff

- Be able to develop and use basic analysis tools

- Be able to conduct an Analysis of the Operating Environment (AOE)

- Understand and explain how package intelligence products for decision makers and why MPKI is important to MDMP

Overview

Module 3 provides an overview of the operational framework and skills related to MPKIO tasks, as well as, a general understanding of how MPKIO can effective operate in a UNPKO using these general techniques in the following lessons.

While this module focuses on the tactical level skills for employment; the lessons in total, provides a general overview how MPKIO assist the Mission leadership in the accomplishment of the mandated tasks

Introduction

Slide 1

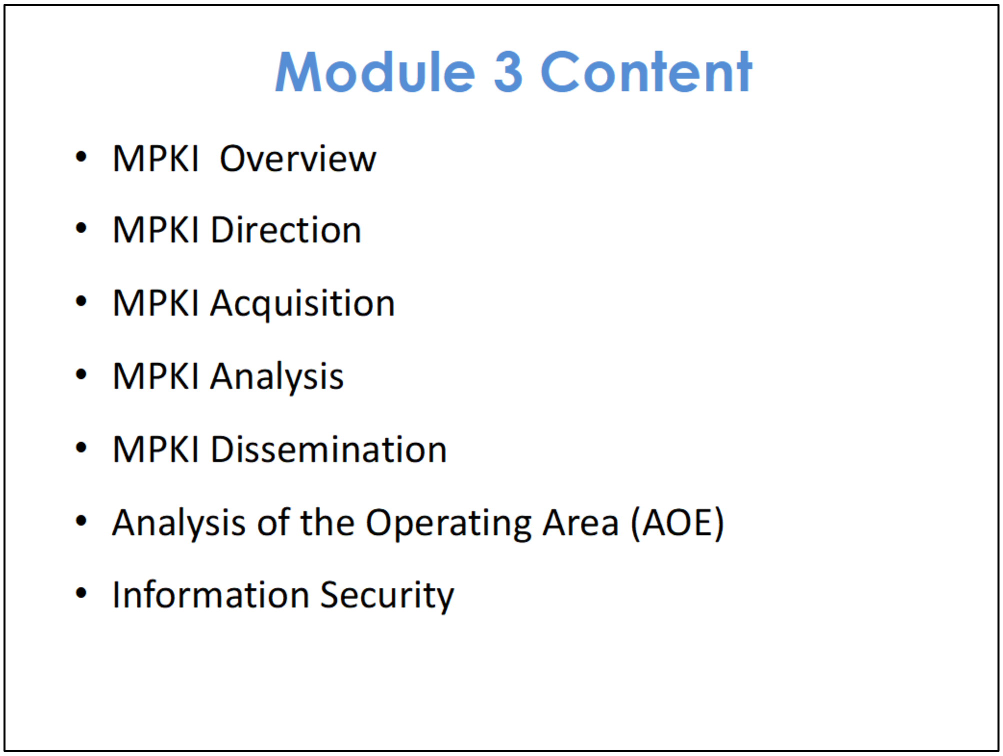
Module3
Military Peacekeeping-
Intelligence
Operational Framework

The Module 3 lessons will help us understand the operational framework for MPKI that include lessons on how to employ the techniques, and skillsets required of an MPKIO.

☞ ***Note to instructor*** *– Review the United Nations MPKI and the Force Headquarters Handbooks before module 3 lessons*

Introduction

Slide 2



Module 3 Content

- MPKI Overview
- MPKI Direction
- MPKI Acquisition
- MPKI Analysis
- MPKI Dissemination
- Analysis of the Operating Area (AOE)
- Information Security

Module 3 contains lessons on these subjects.

Lesson 3.0

MPKI Cycle and Intelligence Functions

The Lesson

Starting the Lesson

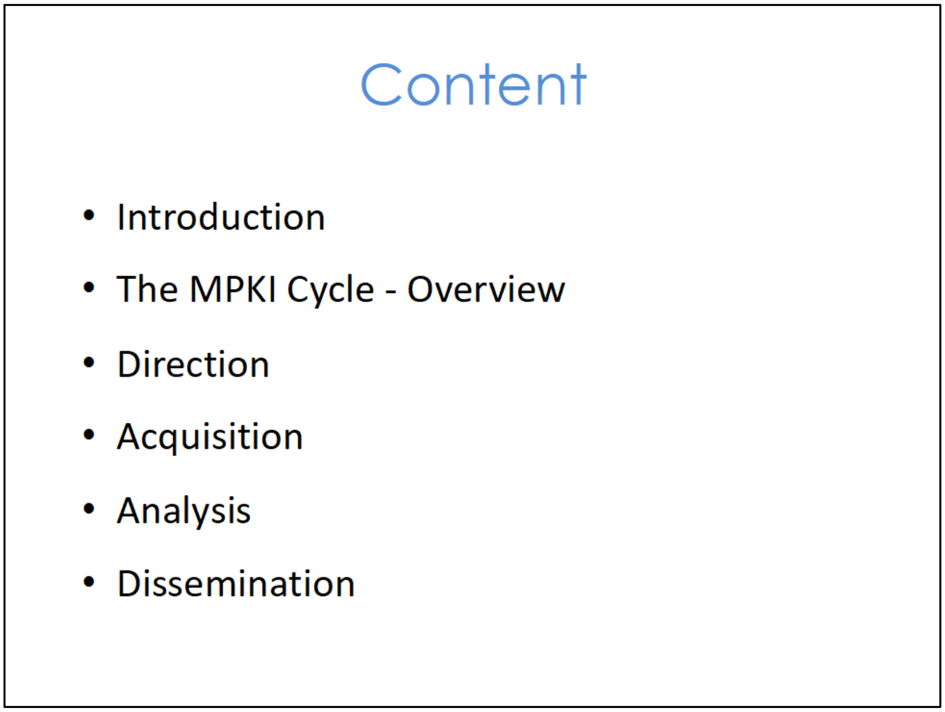
Slide 3

Lesson 3.0
MPKI Cycle &
Intelligence Functions

In this lesson, we will give you an overview of the MKPI Cycle and Intelligence functions.

☞**Note to Instructor-** It is important for the instructor NOT to go too deeply into detail on each Intelligence Function in this lecture, and to clearly convey to the students that this lecture provides an introduction and overview only to the MPKI Cycle and Intelligence Functions

Slide 4

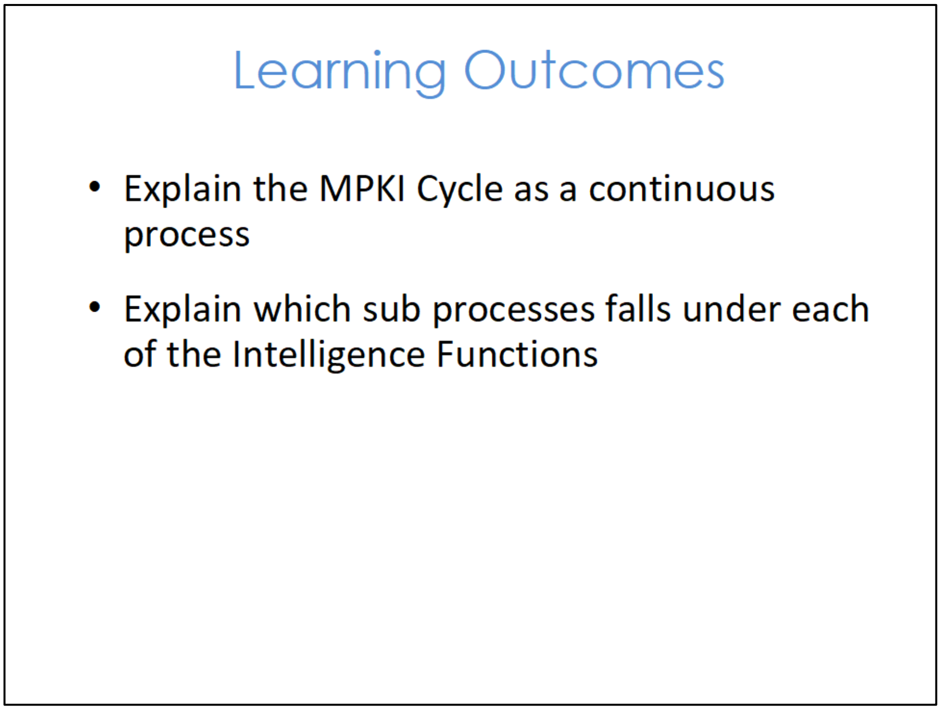


Content

- Introduction
- The MPKI Cycle - Overview
- Direction
- Acquisition
- Analysis
- Dissemination

Here is the lesson content.

Slide 5

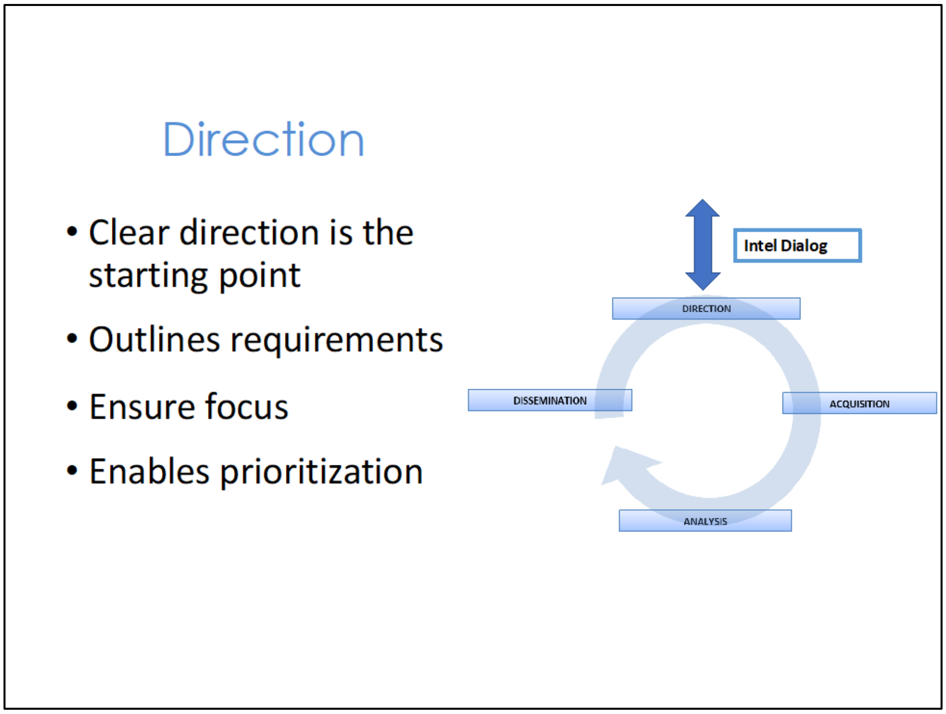


Learning Outcomes

- Explain the MPKI Cycle as a continuous process
- Explain which sub processes falls under each of the Intelligence Functions

The learning objectives for this lecture is to give a high-level overview of the MPKI Cycle, in order to gain an understanding of the overarching process that ties the Intelligence Functions together.

Slide 6



Direction

- Clear direction is the starting point
- Outlines requirements
- Ensure focus
- Enables prioritization

Key Message: The MPKI Cycle is the process that will – if used correctly – perpetually increase our understanding of the operational environment, in a structured manner, in order to support the MDMP. It contains four Intelligence Functions:

- Direction
- Acquisition
- Analysis
- Dissemination

The PKMI Cycle is the UN-recognized mechanism used to produce PKMI. It is typically represented as a cyclical flow-chart containing the four Intelligence Functions. It is called a 'cycle', as it is an ongoing, perpetual process because:

- The production of peacekeeping intelligence is constant throughout a PK mission
- Disseminated peacekeeping intelligence may feed and drive further Direction, and so the cycle starts again

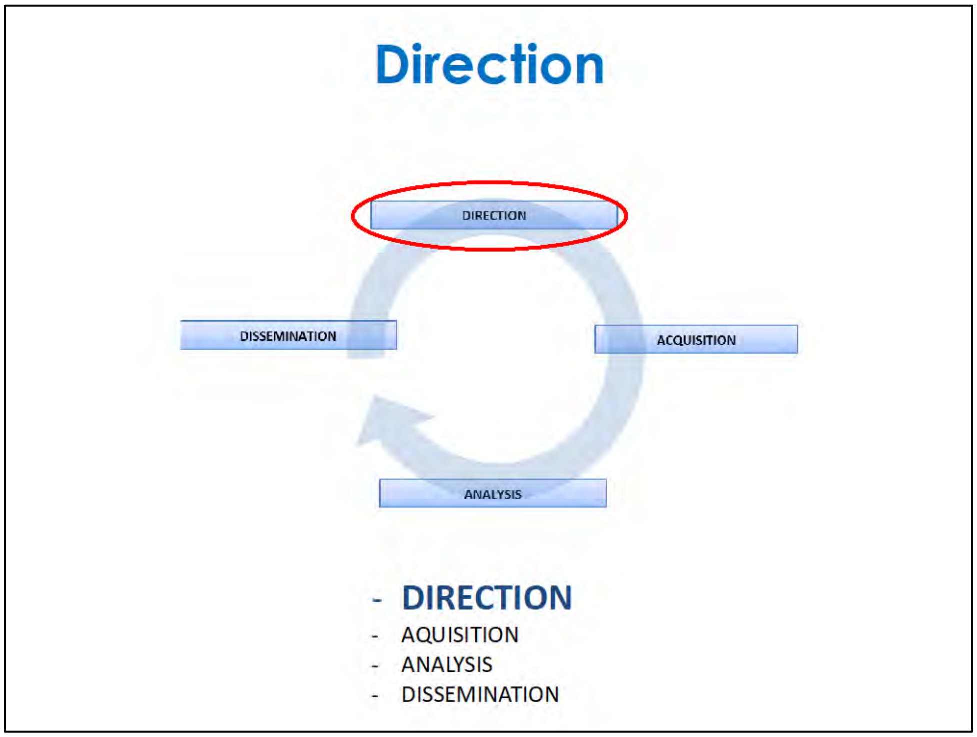
The PKMI cycle is a fundamental tool for PKMI practitioners. It outlines how the PKMI practitioner receives direction from their commander, acquires the relevant information, analyses the information to produce peacekeeping intelligence, which is then disseminated to the commander and others that have the necessary permissions and the need to know.

This cycle shown in the slide) with each step – or Intelligence Function – put in the correct chronological order. In the subsequent slides, we will provide a brief overview of each of the Intelligence Functions shown in the figure.

It is important that peacekeeping intelligence staff ‘own’ the peacekeeping intelligence cycle and are recognised as the «Intelligence Subject Matter Experts» of the Mission.

To effectively support command and the MDMP, the intelligence actors must understand all the elements of it. The importance of running the MPKI Cycle as a continuous process - in the correct order - is very high, as the order and links between each respective stage are vitally important.

Slide 7



Direction

DIRECTION

DISSEMINATION

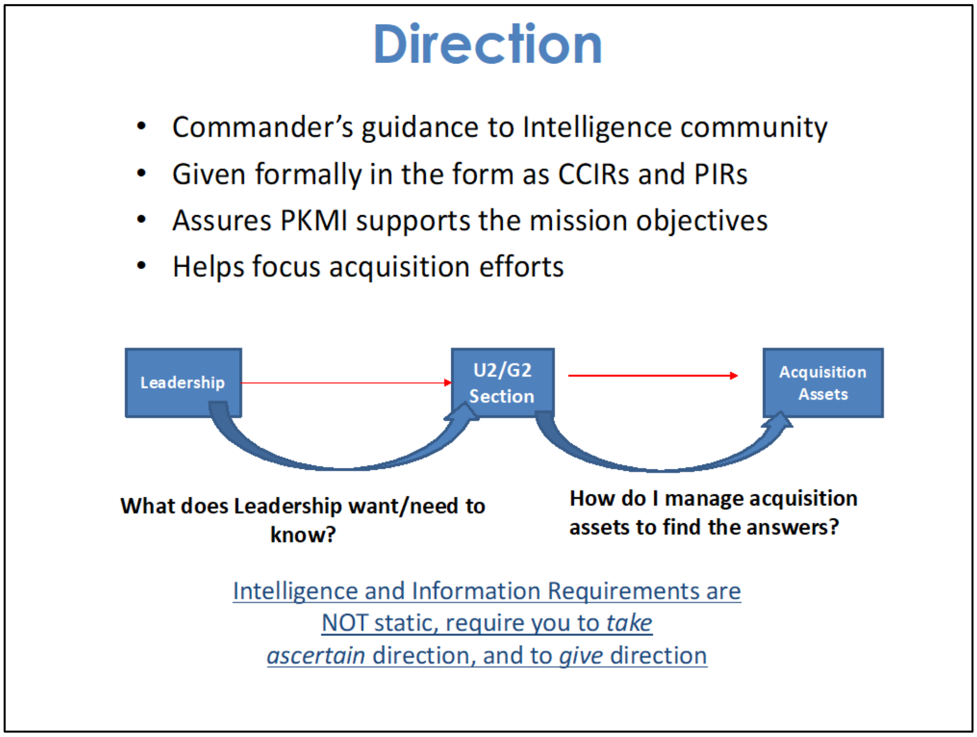
ACQUISITION

ANALYSIS

- **DIRECTION**
- AQUISITION
- ANALYSIS
- DISSEMINATION

The direction is the starting point of intelligence dialogue. The direction is the Intelligence Function that shall assure that the Peacekeeping Intelligence Community always conducts its activities in support of the mission. Without direction, there exists a risk of irrelevant activities and poor resource management. The direction keeps the intelligence community “on target”.

Slide 8



Direction

- Commander’s guidance to Intelligence community
- Given formally in the form as CCIRs and PIRs
- Assures PKMI supports the mission objectives
- Helps focus acquisition efforts

Leadership

U2/G2 Section

Acquisition Assets

What does Leadership want/need to know?

How do I manage acquisition assets to find the answers?

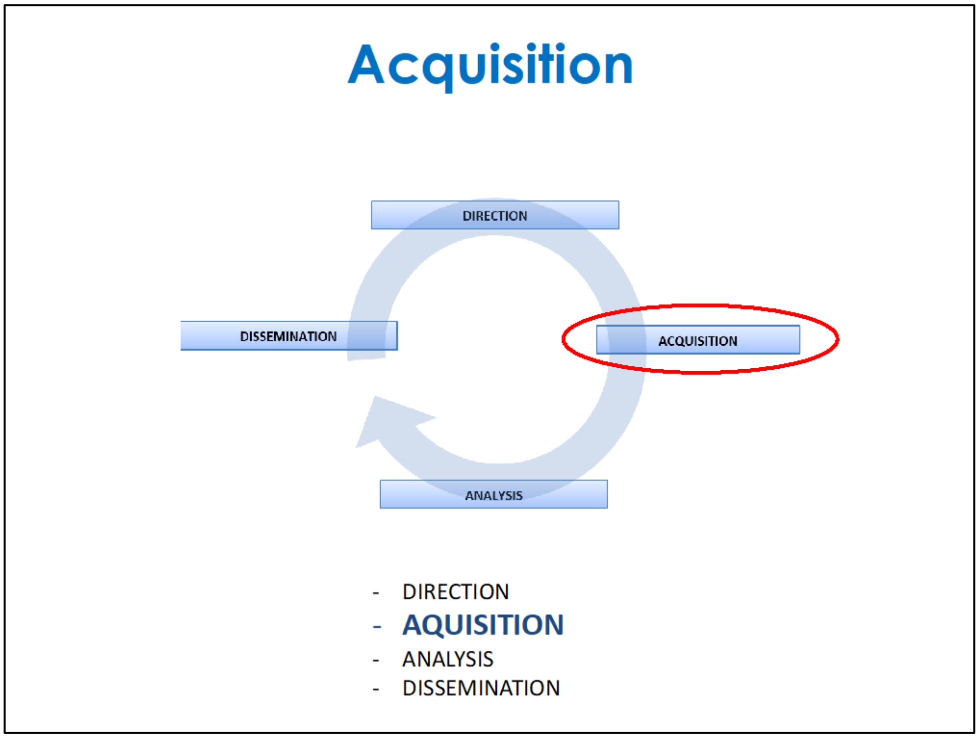
Intelligence and Information Requirements are NOT static, require you to *take* *ascertain* direction, and to *give* direction

The commander may often require assistance in formulating his/her direction so that the intelligence community can produce a feasible and *relevant* product.

This Clear direction from the Commander, at all levels, is the starting point for the PKMI Cycle. The direction outlines to the PKMI staff what the commander wants to know and ensures that the intelligence staff have a clear focus for their acquisition efforts.

It is also important to understand that intelligence acquisition and analytical capabilities are usually limited. Therefore direction should ideally include prioritisation (whether an IR is Mission Critical, Mission Essential, or Mission Desirable) so limited capabilities can be focussed on the highest priorities.

Slide 9



Acquisition

- DIRECTION
- **AQUISITION**
- ANALYSIS
- DISSEMINATION

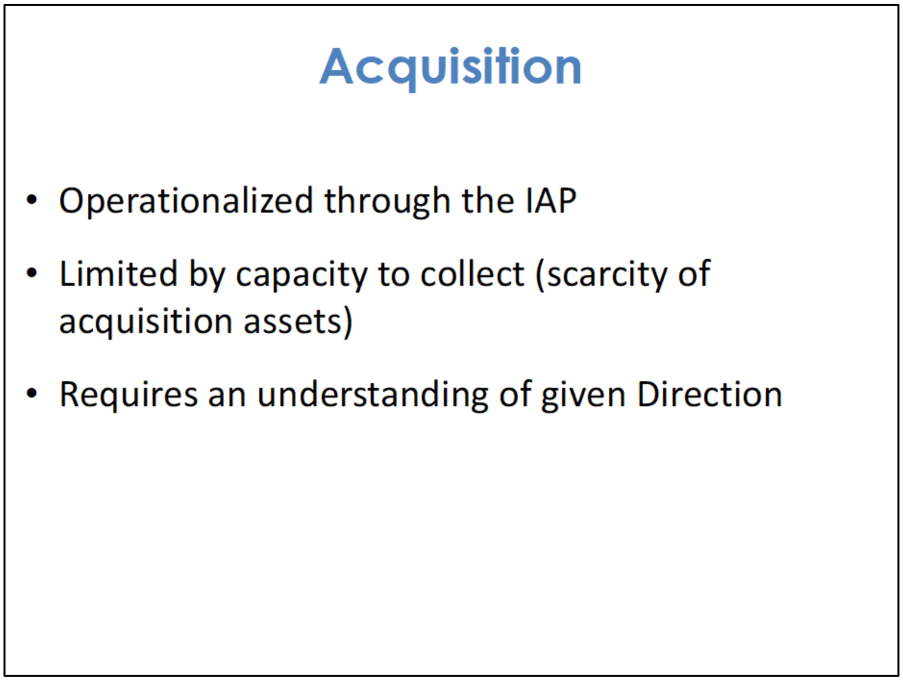
Key Message: This is the actual collection of data and information. The focus of acquisition comes from the previous stage in the cycle.

After ascertaining the requirements and sorting them according to priority, the next step is the acquisition of the data or information, which is required to feed the analytical step of the cycle.

While many PKMI acquisition resources will be the same across missions (e.g. UN Military patrols and observers), some specialised acquisition capabilities (e.g. HUMINT, IMINT, SIGINT, Recce) will only be available in certain missions.

PKMI personnel must develop the fullest awareness of all the sources and agencies they are able to task with the acquisition. It should be noted that data and information should be sought from the broadest sources available and be sourced from women as well as men.

Slide 10



Acquisition

- Operationalized through the IAP
- Limited by capacity to collect (scarcity of acquisition assets)
- Requires an understanding of given Direction

Key Message: Acquisition is the Intelligence Function that contains the planning, focusing, prioritisation and tasking of acquisition assets in order to support the Commander's CCIRs and PIRs.

When Prioritisation. The prioritisation of IRs is important to make the acquisition effort more efficient and focused. Prioritisation is the ordering of IRs according to whether they are Mission Critical, Essential, or Desirable. IRs can also be time. The effective acquisition greatly depends on the clarity of requirements to ensure that resources are used most effectively. Experience suggests that some requirements warrant one specific type of acquisition, whereas others may require several different types of acquisition.

PKMI acquisition can be broken down into two types, I(IR) and RFI:

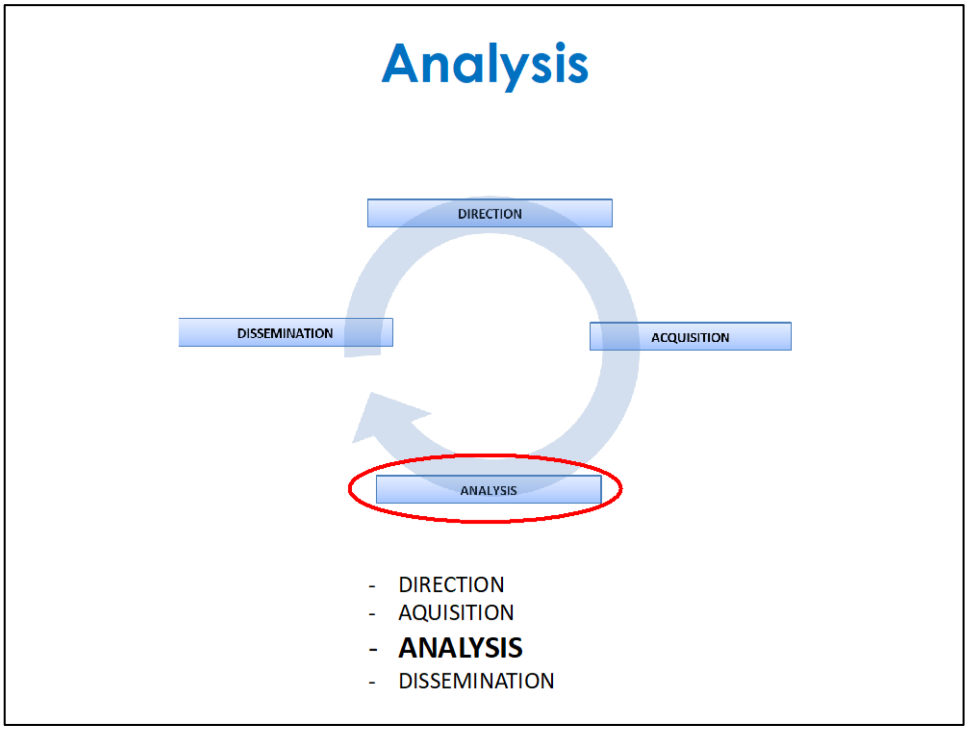
- An IR where the PKMI entity owns the capability required to acquire the information. The acquisition assets are considered organic to the organisation. e.g. a Battalion S2 tasking a Company patrol

- An RFI is made when the PKMI entity does not own the assets required to acquire the needed information, and thus must send an external request to another part of the PKMI architecture in the form of an RFI. All RFIs must receive a response, even if it is a nil response from those asked

It is important to note that more than one acquisition capability can be applied against a requirement. If deemed necessary, it is possible to task multiple Company patrols through IRs and also request support from a higher formation – perhaps one that owns a specific capability such as a UAS – through an RFI.

Sensitive, and often include a 'Not Later Than' (NLT) or 'Last Time Information is of Value' (LTIOV) label. This also helps the PKMI cell to focus its acquisition effort. Most RFIs adhere to the same system, and will always have an NLT or LTIOV label. There should also be a review process that assesses the degree of fulfilment of the requirement so that if fulfilled, it can be removed from the list.

Slide 11



Analysis

DIRECTION

DISSEMINATION

ACQUISITION

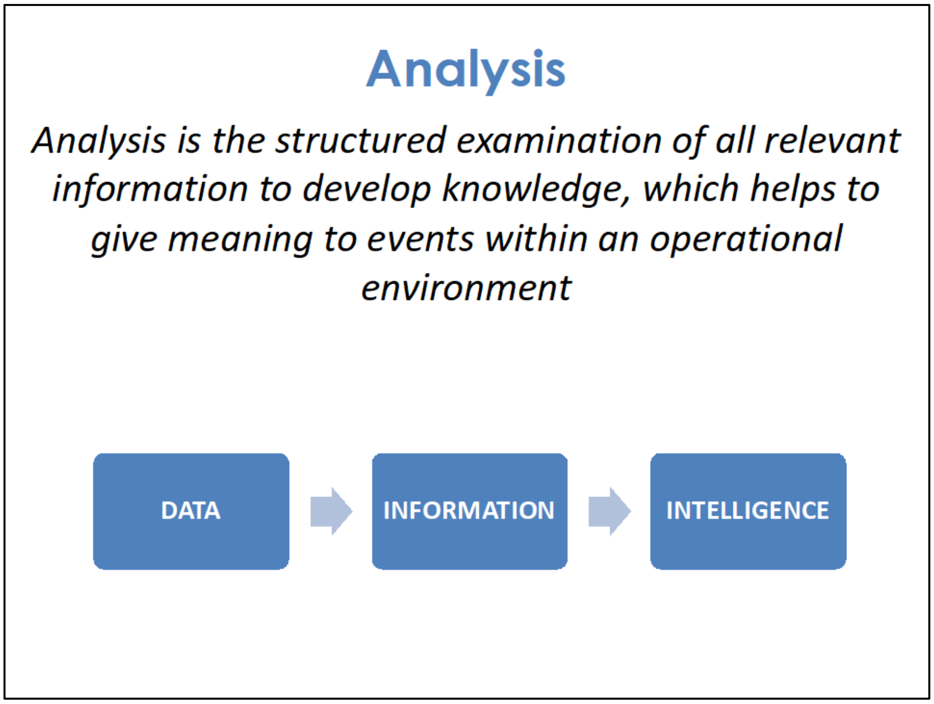
ANALYSIS

- DIRECTION
- AQUISITION
- **ANALYSIS**
- DISSEMINATION

This Intelligence function is the most complex part of the PKMI Cycle.

The analysis is the Intelligence function where the analysts add value to the mission. This is where information is sifted and processed to create the outcome that is needed for the leadership. The input to the analysis function is data, which is collated to create information, and finally processed to create intelligence

Slide 12



Analysis

Analysis is the structured examination of all relevant information to develop knowledge, which helps to give meaning to events within an operational environment

DATA → INFORMATION → INTELLIGENCE

Key Message: Without analysis, there will be a mass of raw data floating around randomly, leaving the leadership to make decisions based on whatever unprocessed data available to them at the time. This will reduce the leadership's capability to make unified and well-supported decisions.

The key part of the PKMI Cycle where raw, unprocessed data and/or information is converted into all-source, fused intelligence. This step is composed of the following stages:

- Review. Search the information system/database to identify already existing information/peacekeeping intelligence about the IR/RFI

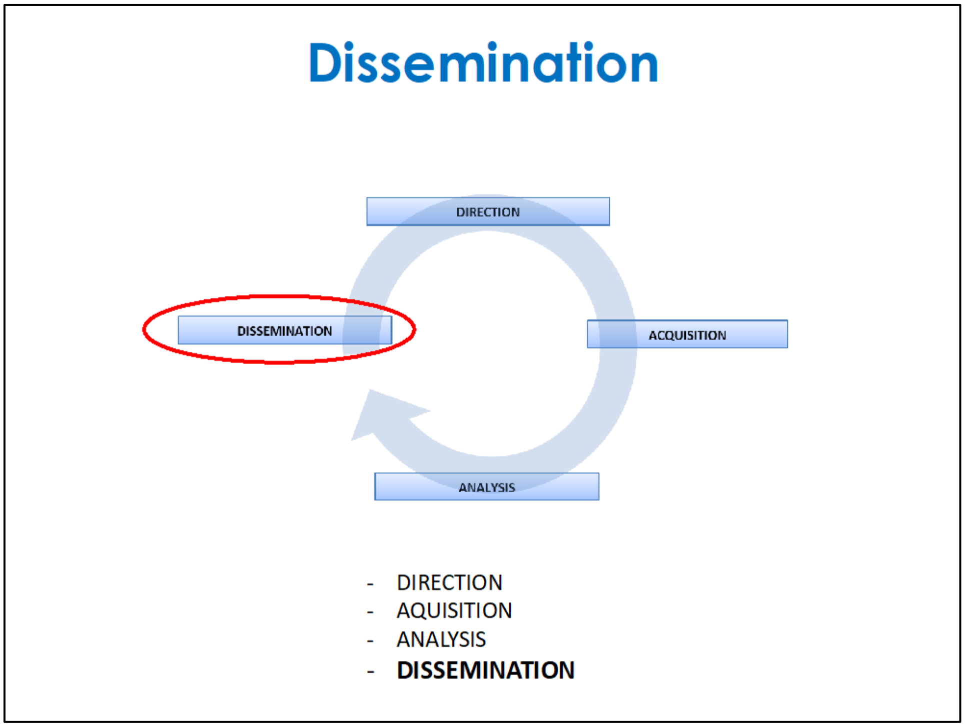
- Collation. The grouping and recording of information in a manner that allows it to be readily accessible and traceable when required; it also enables convenient comparison, evaluation, assessment and retrieval whenever required. However, experience suggests that for better collation, all available information should be logged and then evaluated for relevancy, degree of urgency and reliability and probability. This is a result of good IM practices (covered in Chapter 11)

- Evaluation. This requires the review of an item of information to assess its reliability and credibility. This evaluation enables analysts to prevent unreliable information from being given too much credibility thus leading to incorrect judgments

- Analysis & Integration. The methodical breaking down of information into its parts; examination of each to find interrelationships; and application of reasoning to determine the meaning of the parts and the whole. The result should be a predictive peacekeeping intelligence assessment that will enhance current understanding

- Interpretation. This is the interpretation of the new peacekeeping intelligence against existing knowledge and assessments. Essentially, interpreting the new peacekeeping intelligence in the context of what is already understood or assessed to refine predictive assessments

Slide 13



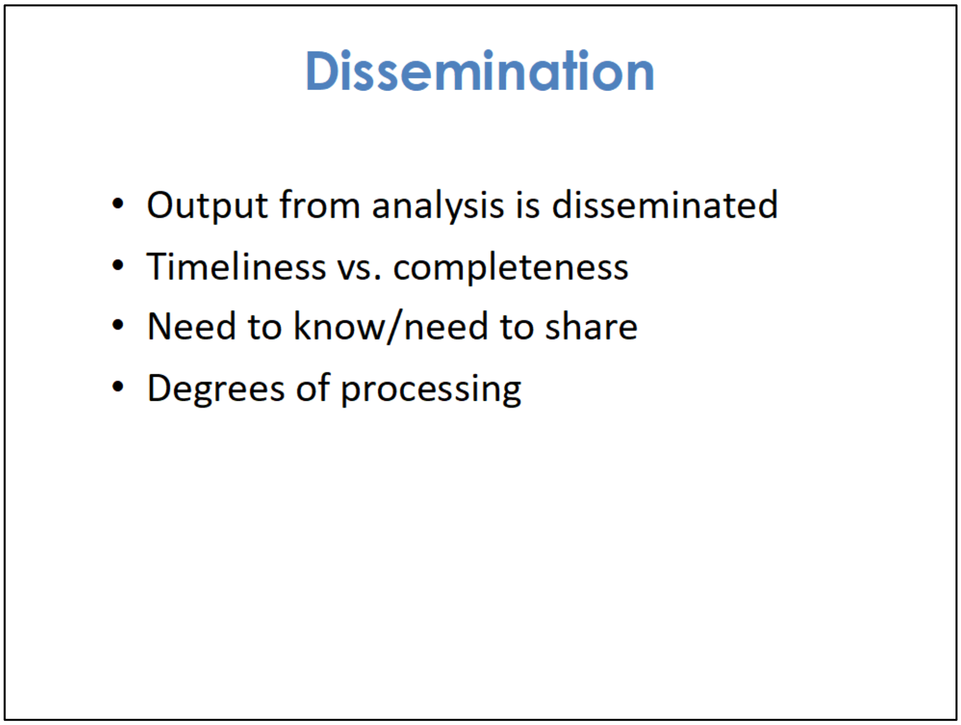
Dissemination

- DIRECTION
- AQUISITION
- ANALYSIS
- **DISSEMINATION**

The production of Intelligence has no purpose unless the output is disseminated to those who need for it. To stay relevant, it is important that proper dissemination-directives are given and followed.

When the Analysis Intelligence Function is working, it will provide useful output to be given to the planners and decision-makers. If the previous steps in the PKMI Cycle have been followed correctly, this output will be relevant, and hopefully timely.

Slide 14



Dissemination

- Output from analysis is disseminated
- Timeliness vs. completeness
- Need to know/need to share
- Degrees of processing

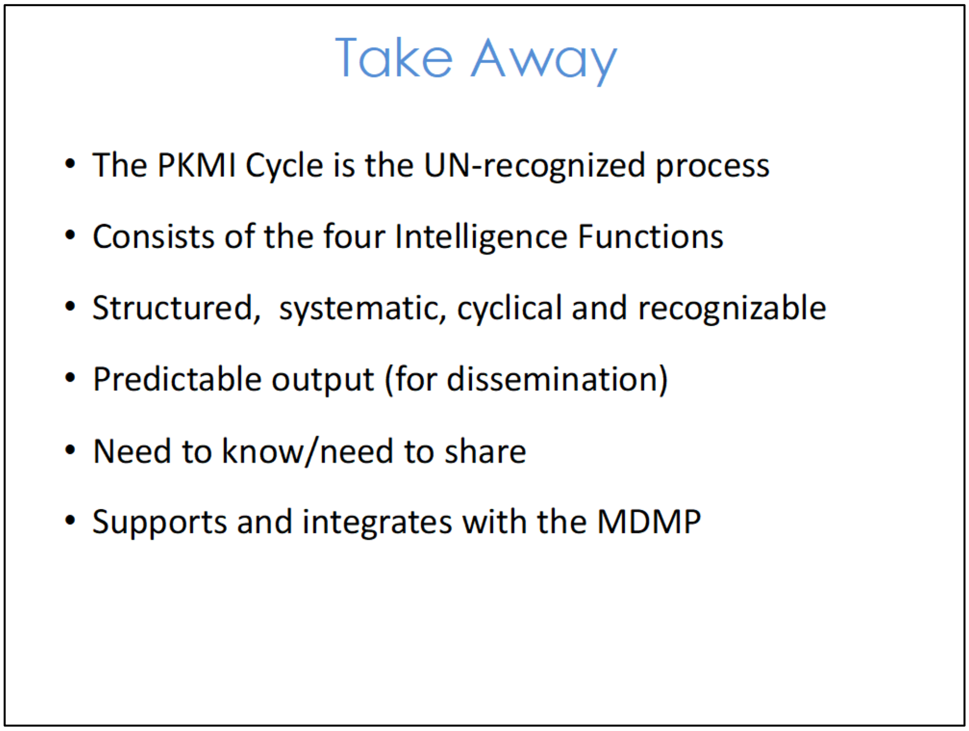
Key Message: There are many nuances to this intelligence function. There will always be judgement calls on when, how and to whom to disseminate.

The final stage of the PKMI Cycle is the process of conveying or distributing peacekeeping intelligence to decision-makers and other relevant mission personnel, which must be done without loss of timeliness.

The dissemination of peacekeeping intelligence products shall be done in compliance with the 'Need to Know / Need to Share' concepts as stipulated in either the Peacekeeping Intelligence Support Plan and / or relevant SOPs.

It should be noted that human rights and humanitarian law violations, including trafficking, combat-related sexual violence (CRSV) and crimes against children, have mandatory reporting requirements. Any information about these offences that are uncovered during the PKMI cycle must be reported through the appropriate channels.

Slide 15



Take Away

- The PKMI Cycle is the UN-recognized process
- Consists of the four Intelligence Functions
- Structured, systematic, cyclical and recognizable
- Predictable output (for dissemination)
- Need to know/need to share
- Supports and integrates with the MDMP

Summary

The PKMI Cycle is the chosen process to produce decision support in the form of PKMI but may in some cases be adjusted. Highly experienced MI Officers may not need to follow the PKMI Cycle rigidly. However, in order to create accountability, repeatability, records and consistency, the process should as a rule be followed. The experienced peacekeeping intelligence professional will be able to ascertain where risk can be taken within the peacekeeping intelligence cycle process - he/she doesn't always have to follow the cycle step by step.

For example, while trying to follow the direction, it is possible that the organisation already has all the data and information it needs to answer the question, so no acquisition is required. Accordingly, all that is required is analysis of the data followed by dissemination. In another unusual or extreme case, once direction has been received, it is possible that the desired or required peacekeeping intelligence already exists, and thus acquisition and analysis can be omitted while disseminating immediately, which would be the only required phase.

Lesson 3.1

Direction

The Lesson

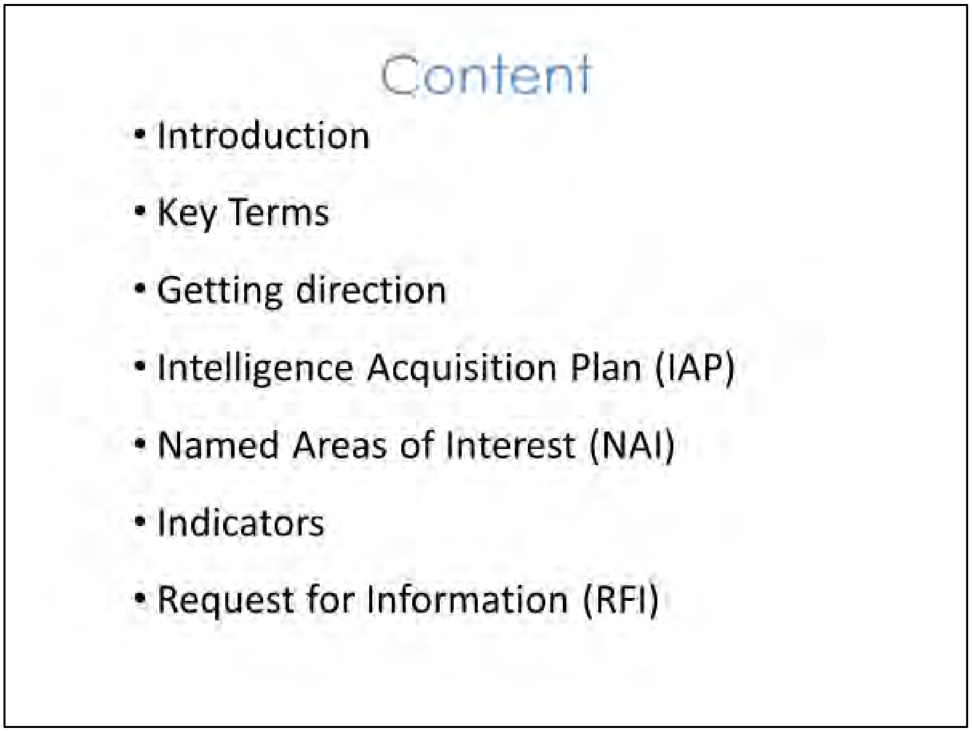
Starting the Lesson

Slide 1

Lesson 3.1
Direction

Welcome to the Direction portion of the RTB. The overall Direction lesson will take several sub lessons. This includes breaks and learning activities.

Slide 2

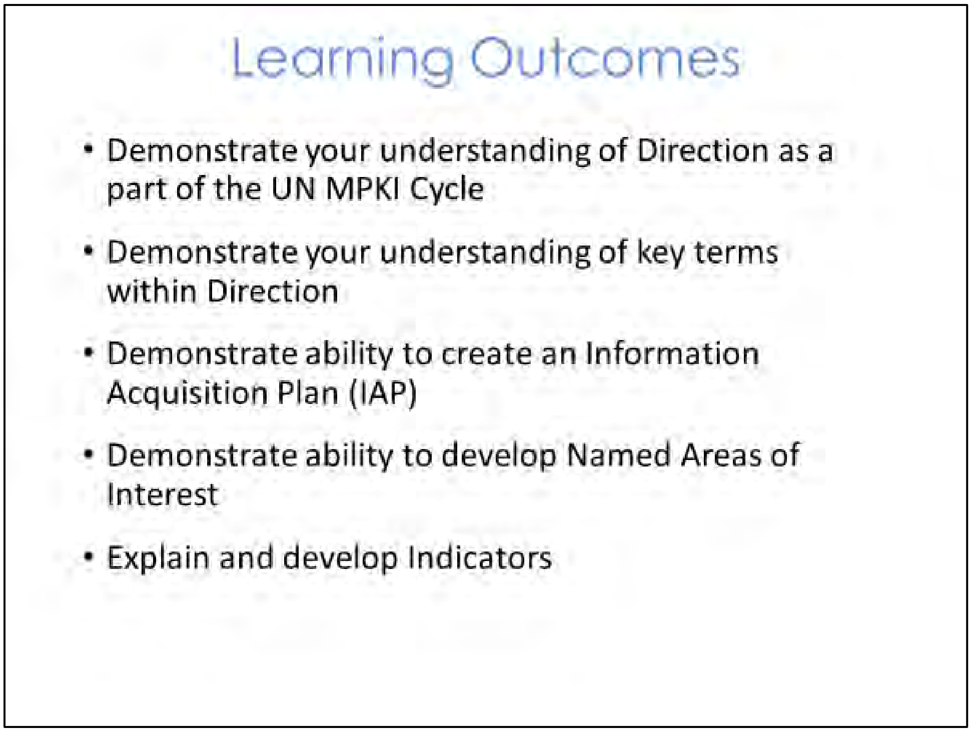


Content

- Introduction
- Key Terms
- Getting direction
- Intelligence Acquisition Plan (IAP)
- Named Areas of Interest (NAI)
- Indicators
- Request for Information (RFI)

Here is the lesson content. There will also be two learning activities where you will be working within the syndicates.

Slide 3

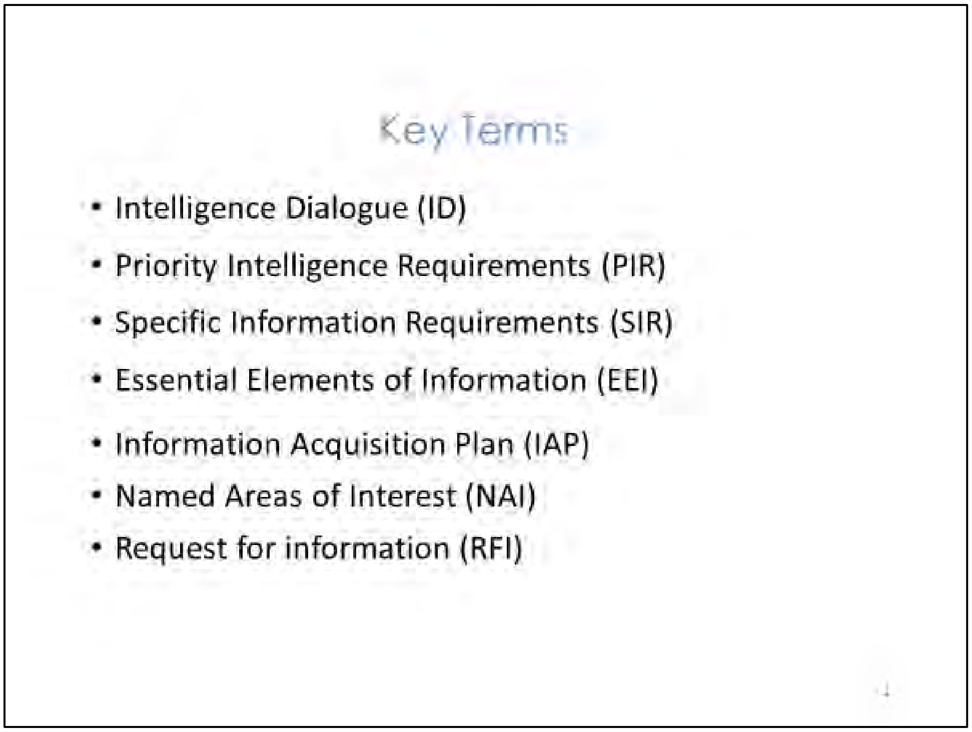


Learning Outcomes

- Demonstrate your understanding of Direction as a part of the UN MPKI Cycle
- Demonstrate your understanding of key terms within Direction
- Demonstrate ability to create an Information Acquisition Plan (IAP)
- Demonstrate ability to develop Named Areas of Interest
- Explain and develop Indicators

By the end of this lesson, you will be able to explain the fundamentals of direction, and how it is a key starting point of the UN MPKI Cycle. Furthermore, you will be expected to name and explain the primary terms related to direction. You will also be able to explain and demonstrate how to draw direction from the commander and his/her staff, how to create Priority Intelligence Requirements (PIRs), and how to break these PIRs down to sets of smaller questions, which can be used to acquire detailed information. You will be expected to create a basic Information Acquisition Plan (IAP), and to guide acquisition assets to locations (NAIs) where information is likely to be found.

Slide 4



Key Terms

- Intelligence Dialogue (ID)
- Priority Intelligence Requirements (PIR)
- Specific Information Requirements (SIR)
- Essential Elements of Information (EEI)
- Information Acquisition Plan (IAP)
- Named Areas of Interest (NAI)
- Request for information (RFI)

Key Message: This is an overview of the key terms that are prevalent in the Direction portion of the cycle.

The **Intelligence Dialogue** is a continuous dialogue with your leadership group (the commander and his/her staff), which seeks to determine what the commander's information and intelligence requirements are/what the commander and his/her staff need and want to know. The commander and his/her staff will rarely seek this dialogue. Therefore, it is up to the MPKI cell to ensure that the meeting with leadership is scheduled. This creates leadership support for the MPKI cell. It is important to understand that the commander will rarely frame these requirements as easy to understand Priority Intelligence Requirements (PIRs). This is often the role of the MPKI cell.

Priority Intelligence Requirements. PIRs are those requirements raised by a commander for intelligence to support his/her immediate mission. Once again, the commander will rarely frame these as coherent questions. Rather, the MPKI cell must take his/her general requirements and transform them into no more than 6-8 broad questions, which are known as PIRs.

Specific Information Requirements (SIR) come from breaking down PIR's into sub-questions, that when answered, can provide partial answers to the PIRs. They are known as information rather than intelligence requirements as the sum of the information drawn from SIRs should form the basis for responding to the PIR.

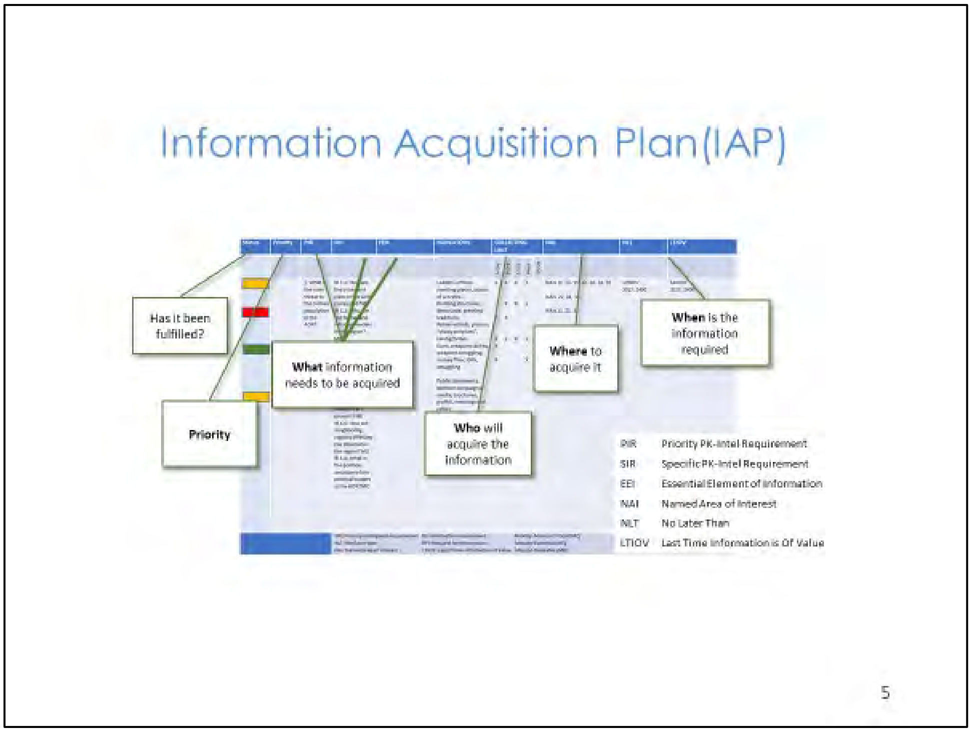
Essential Elements of Information (EEI): Often the SIR is too broad a question for acquisition assets and will need to be further broken down into several sub-questions (EEIs), which can be responded to.

Information Acquisition Plan (IAP) is the main direction tool, and the overall plan that breaks down the PIR into its smaller components (SIR/EEI) and also tasks the various acquisition assets to acquire information pertaining to the EEIs.

Named Area of Interest. These are locations where the MPKI cell identifies as locations where the information can be found. For example, if the commander is interested in locating smuggling locations, then border crossing points could be an NAI.

Request for Information (RFI) is used when a level is unable to acquire answers with its own resources and is sent to higher levels or neighbouring units. This is known as asking, rather than tasking.

Slide 5



Information Acquisition Plan(IAP)

Has it been fulfilled?
Priority
What information needs to be acquired
Who will acquire the information
Where to acquire it
When is the information required

PIR	Priority PK-Intel Requirement
SIR	Specific PK-Intel Requirement
EEI	Essential Element of Information
NAI	Named Area of Interest
NLT	No Later Than
LTIOV	Last Time Information is Of Value

5

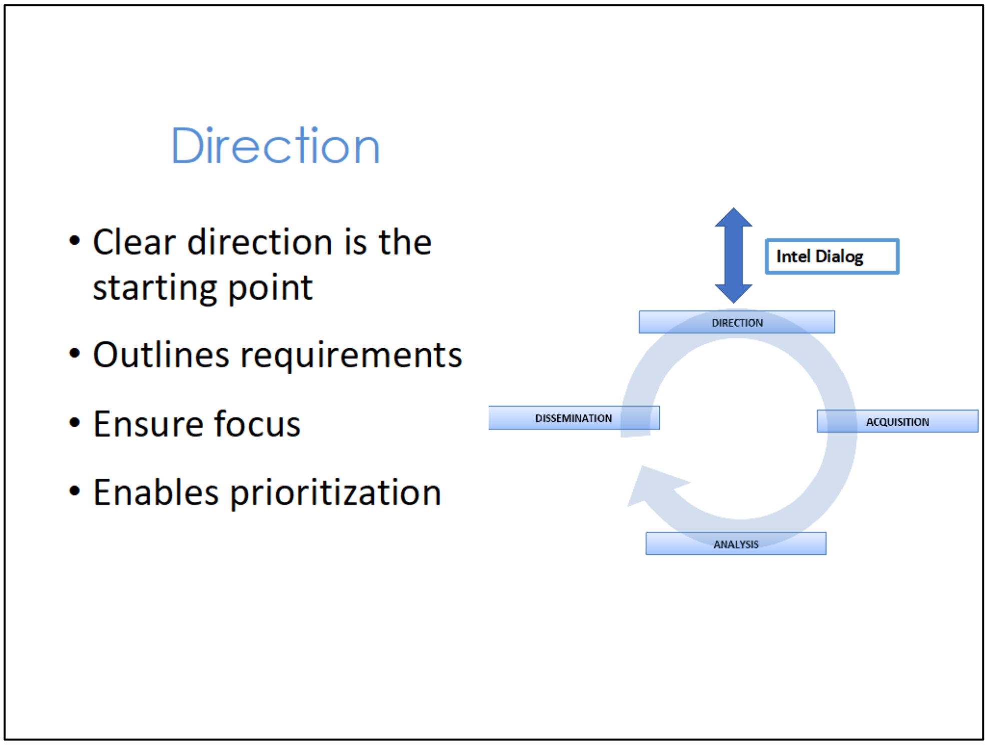
This is what we want you to construct at the end of this lecture series.

Narrative. Take note of the different headings moving from left to right. Pay attention to Priority, PIRs, SIRs, EEIs, the acquisition unit column, the NAIs, the NLT and LTIOV columns. This is what you will be expected to fill on your IAP. We have already gone through the meaning of PIRs, SIRs, and EEIs.

Status refers is a means to manage acquisition. This is a quick reckoner to see whether the acquisition is going well (green), partially met (orange), or not met (red). Priority means whether an information or intelligence requirement is mission-critical, mission essential, or mission desirable.

NLT is timing, and it means information is required Not Later Than. LTIOV is also timing, and it means the Last Time Information is Of Value. The acquiring unit is those assets, organic to the unit, which can be tasked.

Slide 6



Direction

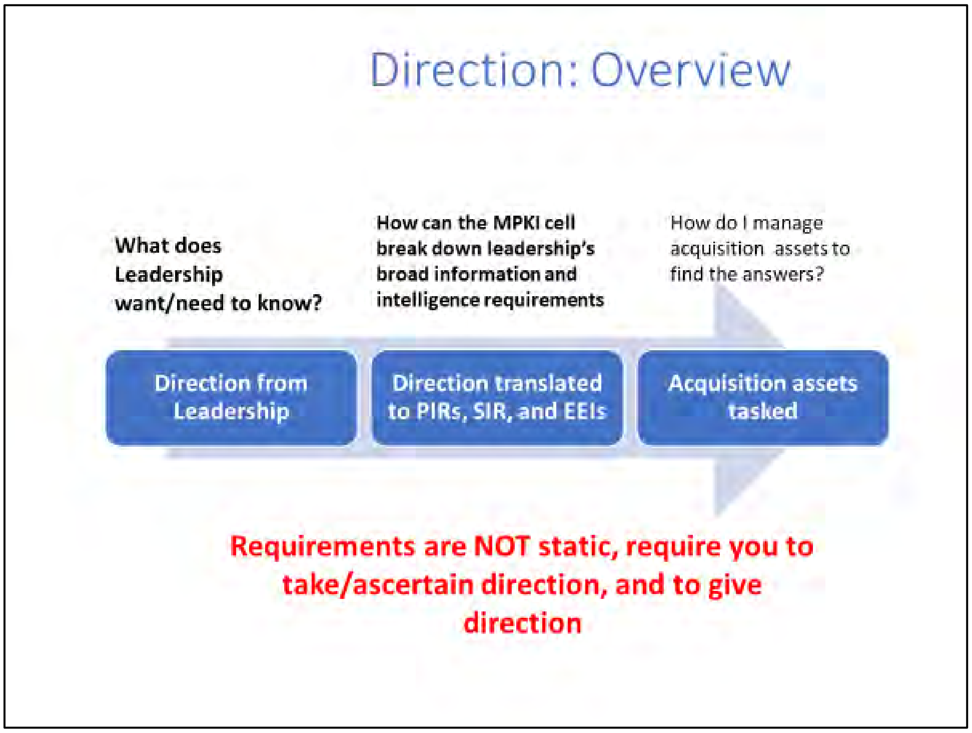
- Clear direction is the starting point
- Outlines requirements
- Ensure focus
- Enables prioritization

Key Message: Clear direction from the Commanders, at all levels, is the start point for the MPKI Cycle. The direction outlines to the MPKI staff what the commander wants/needs to know and ensures that the MPKI staff have 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. Prioritisation will be outlined later in this lecture.

The direction is both the starting- and ending point of the MPKI Cycle. It is heavily reliant on the input from the commander/decision-maker that is supported in order to ensure that the MPKI efforts are focused on underpinning the overall mission and the operational lines that are part of the operation. If a clear direction is not given, the MPKI must ask for it. In some instances, MPKI staff 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 utilising the oftenlimited resources in the best possible manner. The Direction and guidance will also be key in order to prioritise these resources, to the point that MPKI should be cognizant of where the commander is willing to take the risk in terms of lack of knowledge.

Slide 7



Direction: Overview

What does Leadership want/need to know?

How can the MPKI cell break down leadership's broad information and intelligence requirements

How do I manage acquisition assets to find the answers?

Direction from Leadership

Direction translated to PIRs, SIR, and EEIs

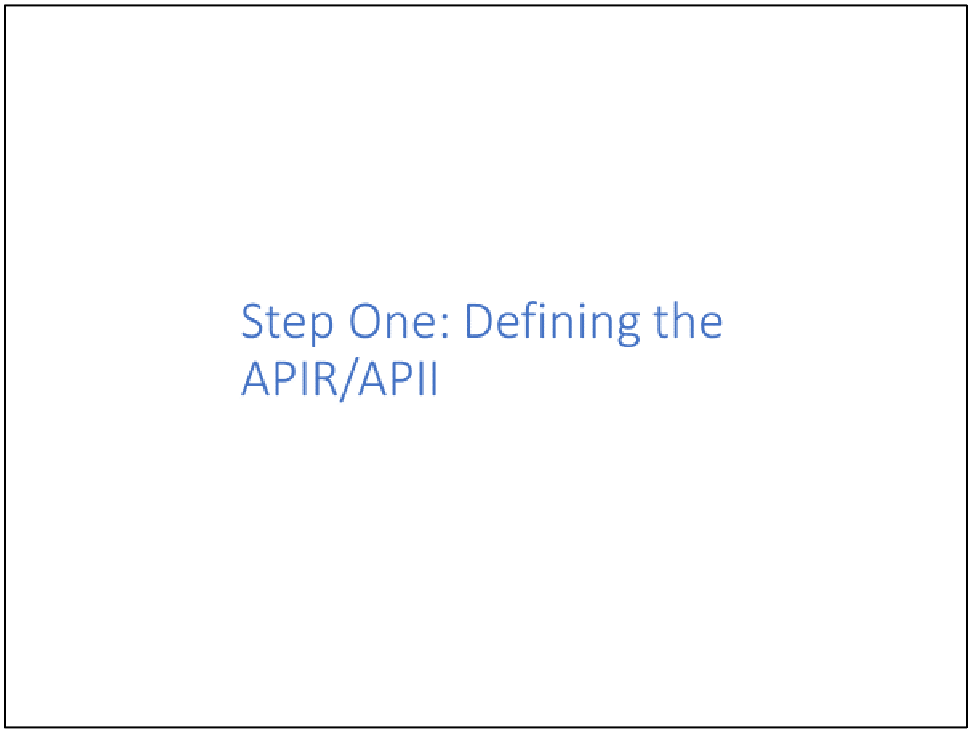
Acquisition assets tasked

Requirements are NOT static, require you to take/ascertain direction, and to give direction

This slide is a visual graphic to support student understanding of the direction and acquisition process. Leadership first outlines its information and intelligence requirements to the MPKI cell at force, sector or battalion level. The MPKI cell then takes these requirements and breaks them down into SIRs and EEIs. The MPKI cell will also decide where these EEIs can be found by location. These are known as 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 8

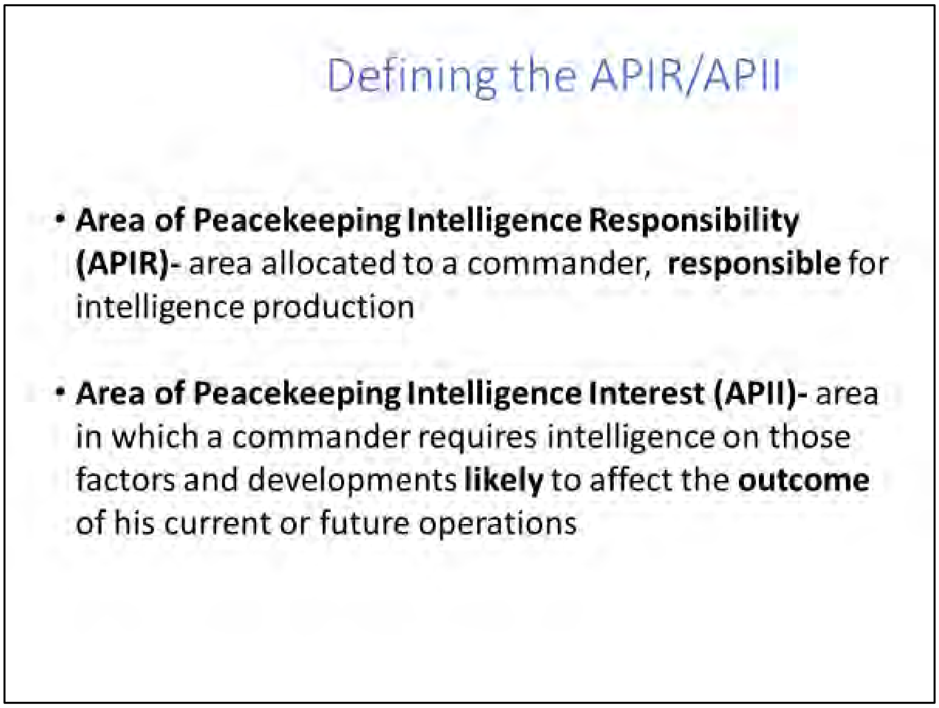


Step One: Defining the APIR/APII

Before we begin the direction process, we must first decide the MPKI Area of Intelligence Responsibility (AIR), and the Area of Intelligence Interest (AII). It is vital to define our AIR, the area that our unit has primary acquisition responsibility, and the AII, the area which is of interest to our unit because incidents and events in that area may have an impact in our Area of Operations.

It is important to know the difference as our unit will usually not have permission to engage in acquisition activities in the AII. This is because the AII will often be the AIR of a neighbouring unit. If we were to acquire information in the AIR of another unit, we would be wasting resources.

Slide 9



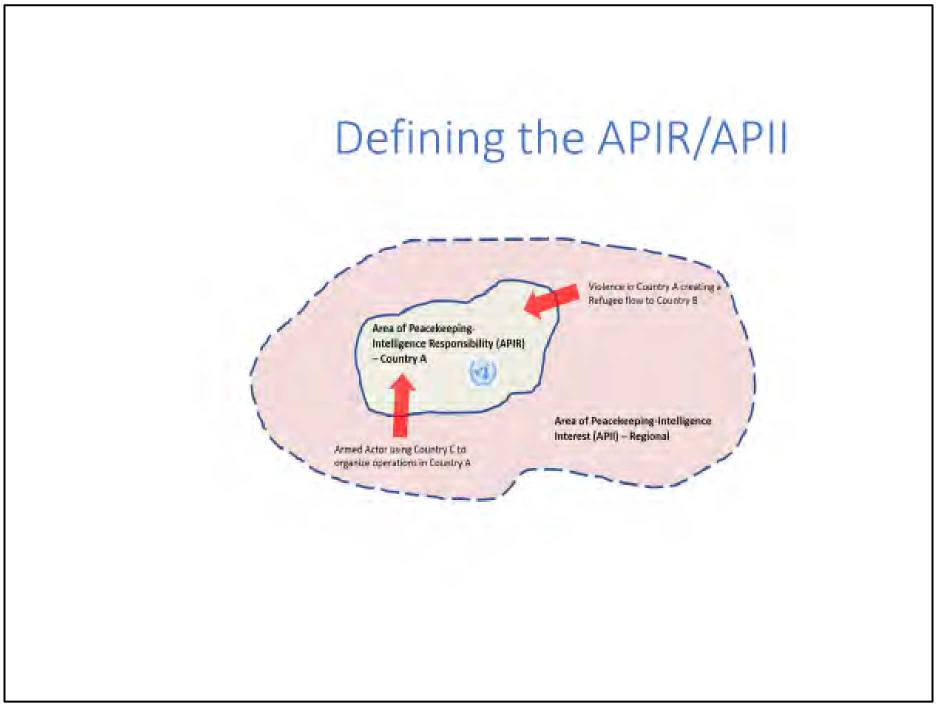
Defining the APIR/APII

- **Area of Peacekeeping Intelligence Responsibility (APIR)-** area allocated to a commander, **responsible** for intelligence production
- **Area of Peacekeeping Intelligence Interest (APII)-** area in which a commander requires intelligence on those factors and developments **likely** to affect the **outcome** of his current or future operations

Key Message: We have the responsibility to acquire information and intelligence in our AIR, but not in our AII, which is only of interest to our unit.

We acquire information in our AIR as we are responsible for it, but we ask for information about our AII, which we are not responsible for. If our AII is a UN Operating Area, then we should send a Request for Information (RFI) to higher HQ, or to the neighbouring unit to satisfy our IR. If the AII is in a neighbouring country, then we will often have to rely on open sources. We will explain an RFI later in this lesson.

Slide 10



Defining the APIR/APII

Violence in Country A creating a Refugee flow to Country B

Area of Peacekeeping-Intelligence Responsibility (APIR) – Country A

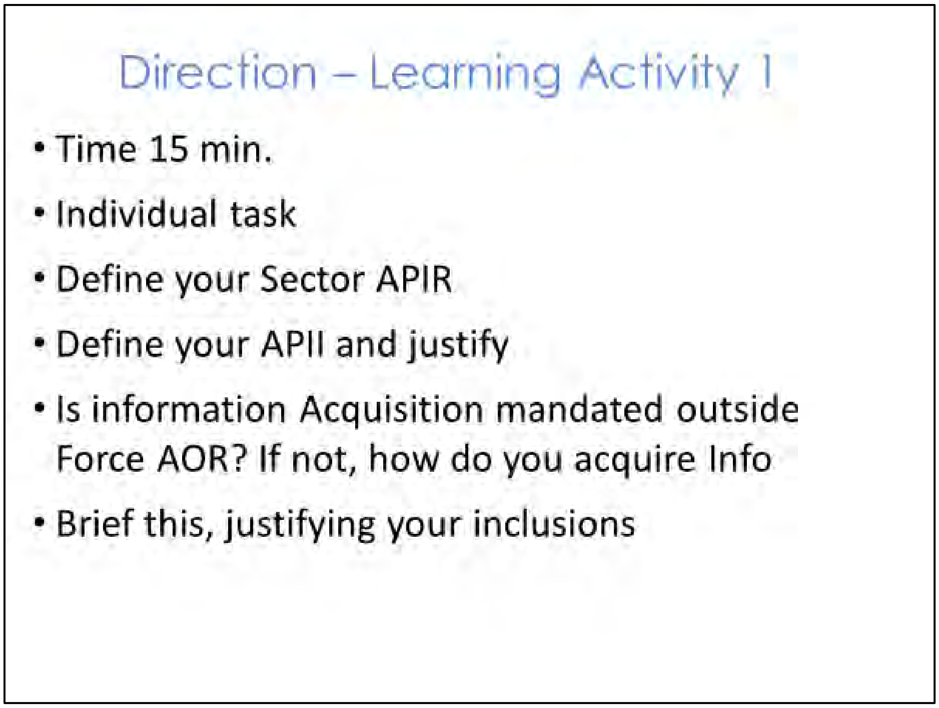
Area of Peacekeeping-Intelligence Interest (APII) – Regional

Armed Actor using Country C to organize operations in Country A

This graphic visually depicts a possible UN APIR and an APII. The key point here is that incidents and events in one country can have an impact on the situation in a UN AO.

Interaction. *Ask the students to describe a situation where this can happen in a UN context. Responses here would include a conflict in one country leading to a refugee flow into the UN AO; one country arming or otherwise supporting threat actors that act as spoilers in a UN AO.*

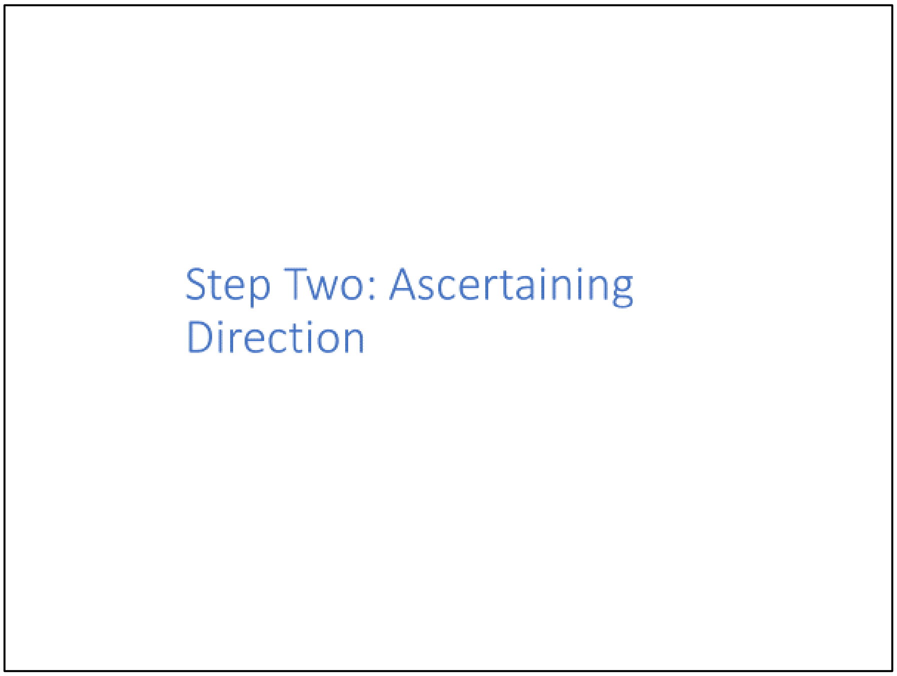
Slide 11



Direction – Learning Activity 1

- Time 15 min.
- Individual task
- Define your Sector APIR
- Define your APII and justify
- Is information Acquisition mandated outside Force AOR? If not, how do you acquire Info
- Brief this, justifying your inclusions

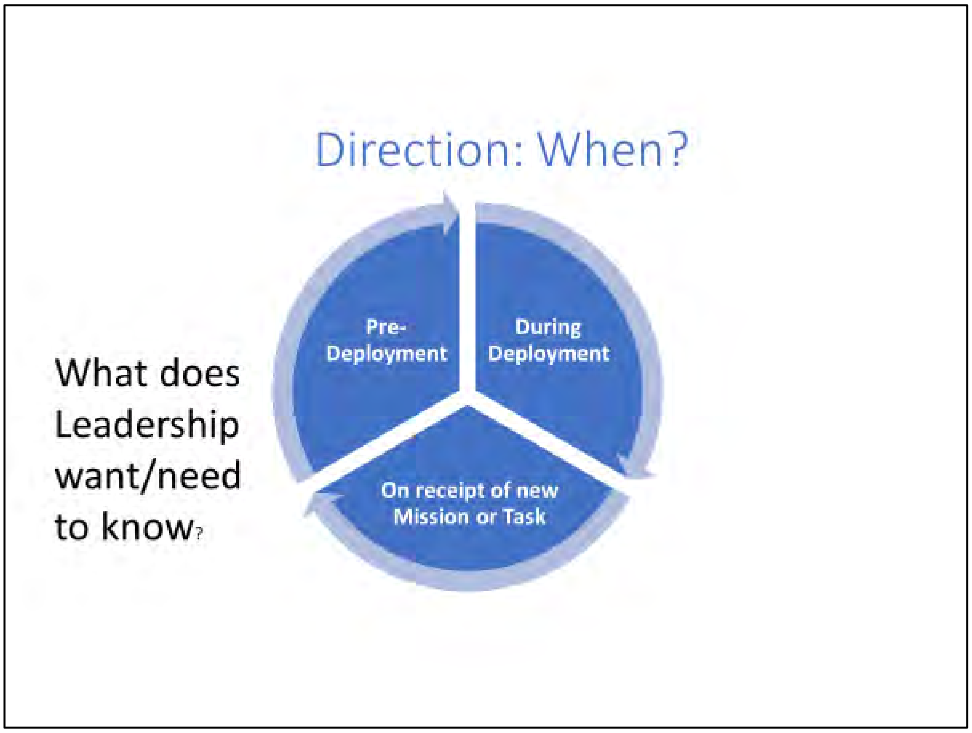
Interaction. *Have the students conduct this individual learning activity. Students should focus on the central scenario for this exercise. Students are expected to brief their results. Student responses should include reasons why the surrounding countries and UN Sectors are within their AII, during their sector in their AIR. Students should brief on where the UN can acquire information (the UN AIR), and where the UN cannot use acquisition assets to acquire information (neighbouring countries).*



Step Two: Ascertaining Direction

We can begin the direction process. This is the second step in the process or ascertaining direction.

Slide 13



Direction: When?

What does Leadership want/need to know?

Pre-Deployment

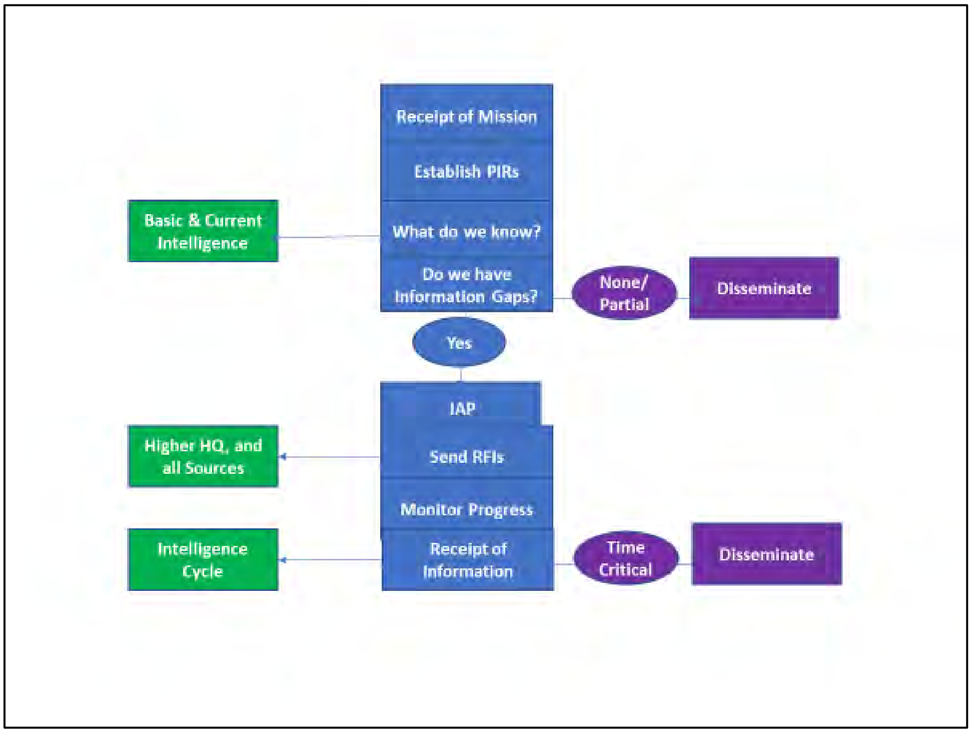
During Deployment

On receipt of new Mission or Task

The direction is a continuous process, and it happens at all stages of the operational cycle, including before deployment, on deployment, and on receipt of a new mission.

We have highlighted the receipt of a new mission or task as before each new mission the MPKI cell will often require information that it does not know or have access to assist planning. Therefore, in the time leading up to the new mission (for example, a convoy to an area to which the unit has not visited before or a convoy to an area where the situation has recently changed), the MPKI section will have to ensure that acquisition assets are tasked to acquire new information, or that they send RFIs to higher HQ or to neighbouring units to satisfy all possible unknowns. This will greatly assist the local commander's planning and decision-making process, the central role of the MPKI cell.

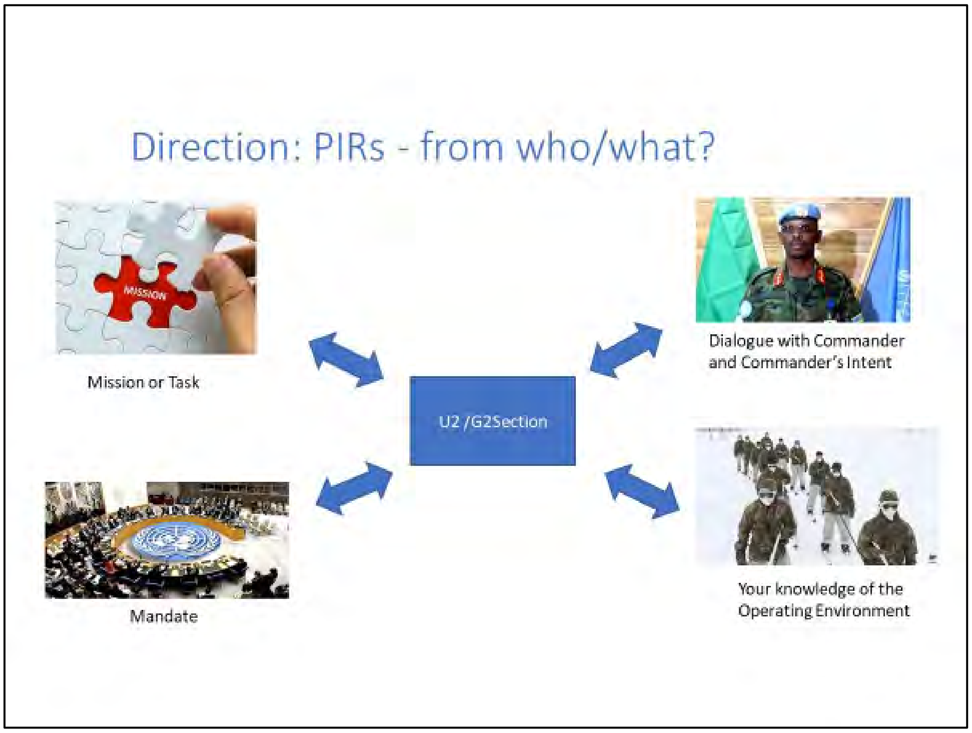
Slide 14



The key element is as follows. On receipt of the mission, PIRs are ascertained and broken down into IRs. The MPKI cell then searches its databases to find out what is already known and whether these PIRs/IRs can be immediately responded to. If we have no information gaps, then the intelligence product is immediately sent to the commander and his/her staff. If information gaps are identified, then the new IRs are moved to the IAP and assets will be tasked to acquire the information, or RFIs will be sent to neighbouring units and/or higher HQ. It is important to note that as information flows into the MPKI cell, it is continually processed, analysed and updated intelligence products are sent to the commander and his/her staff.

It is important to note that time-critical information (such as information pertaining to UN Force Protection, the threat to POC, of violations of international humanitarian law) are sent directly to the commander and his/her staff, together with a warning that the information is unprocessed as is often the case when raw data is passed directly to decision-makers.

Slide 15



Direction: PIRs - from who/what?

Mission or Task

Dialogue with Commander and Commander's Intent

U2 /G2Section

Mandate

Your knowledge of the Operating Environment

Key Message: The MPKI cell must not rely on the commander and his/her staff to give them a set of PIRs to work with. Rather, the MPKI cell must often work it out for themselves. However, the MPKI cell must suggest PIRs to the commander in order to gain his backing and support for its Information Acquisition Plan (IAP). Ideally, this support will be demonstrable, and the MPKI cell would have their commander sign the IAP, thereby making it an order.

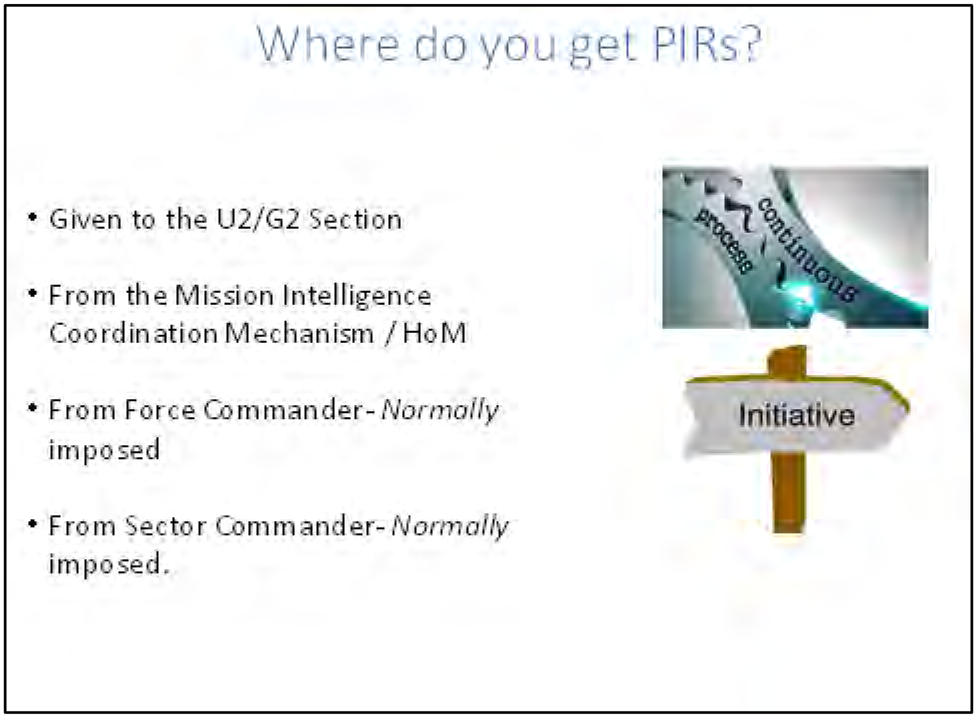
There are many sources of direction, which the MPKI cell must use in order to deepen its understanding of what the commander and his/her staff need to know.

Much of this work will take place during the Analysis of the Operating Environment (AOE), which students will be introduced to later in this course. Essentially, it means that the MPKI cell uses what it knows about the UN operating environment to identify the most pertinent information the commander needs. Therefore, the first step in gaining direction is the MPKI having a detailed knowledge of the AOE and understanding what it does not yet know or identifying unknowns.

The MPKI cell should also look at the mission and mandated tasks and decide what information the commander needs in order to achieve the mission and mandate. The MPKI cell should study the commander's intent so it is aware of the commander's operational priorities. In this case, the MPKI cell works to decide what information and intelligence the commander needs to ensure his/her intent is achieved.

Finally, the MPKI cell should engage the commander and his staff in an intelligence dialogue to discuss their and specific information and intelligence requirements. Normally, the MPKI cell will not get many opportunities to engage at this level and so needs to make it count. Therefore, this is the final stage in the direction process. An MPKI cell should never meet the commander and his/her staff without in-depth preparation of the subject matter, which is what an in-depth understanding of the AOE, mission, mandate, commander's intent, and tasks will achieve in the context of direction.

Slide 16



Where do you get PIRs?

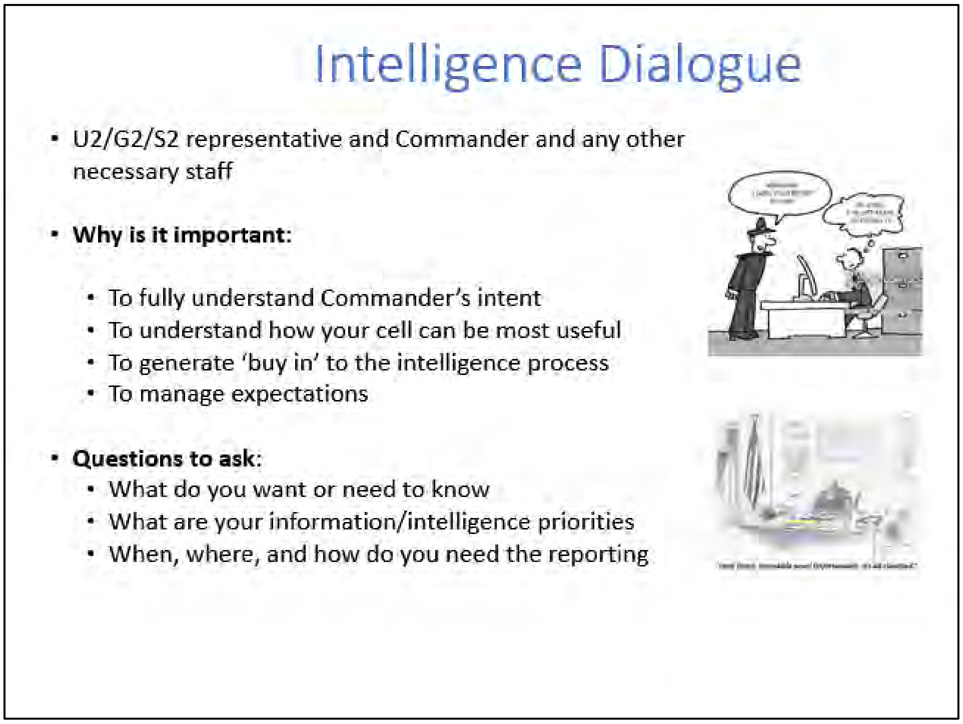
- Given to the U2/G2 Section
- From the Mission Intelligence Coordination Mechanism / HoM
- From Force Commander- *Normally* imposed
- From Sector Commander- *Normally* imposed.

continuous
process
Initiative

In addition to drawing PIRs from mission, mandate, commander's intent, specific tasks, and the intelligence-oriented dialogue, MPKI cells will often have PIRs imposed on them by higher HQ. The MICM will often give the MPKI cell PIRs. These PIRs will generally reflect the strategic priorities of the Head of Mission.

The MPKI cell will also get PIRs from higher force echelons. For example, a G2 MPKI cell will be given PIRs by the Force, and the Battalion level will be given PIRs by the Sector. This cascading of PIRs will occur right down to patrol level.

Slide 17



Intelligence Dialogue

- U2/G2/S2 representative and Commander and any other necessary staff
- **Why is it important:**
  - To fully understand Commander's intent
  - To understand how your cell can be most useful
  - To generate 'buy in' to the intelligence process
  - To manage expectations
- **Questions to ask:**
  - What do you want or need to know
  - What are your information/intelligence priorities
  - When, where, and how do you need the reporting

Intelligence Dialogue is vital for direction. MPKI cells are likely to get few chances to engage the commander and his/her staff in an intelligence dialogue. Therefore, it has to count.

The MPKI cell leader must meet his/her commander when he/she is fully prepared. Indeed, it is a good idea to have the intelligence dialogue after the MPKI cell has drawn up a coherent and complete set of PIRs and add to them or subtly change them based on the commander's guidance. This means that the MPKI cell uses all tools available to it to ascertain PIRs before the dialogue takes place.

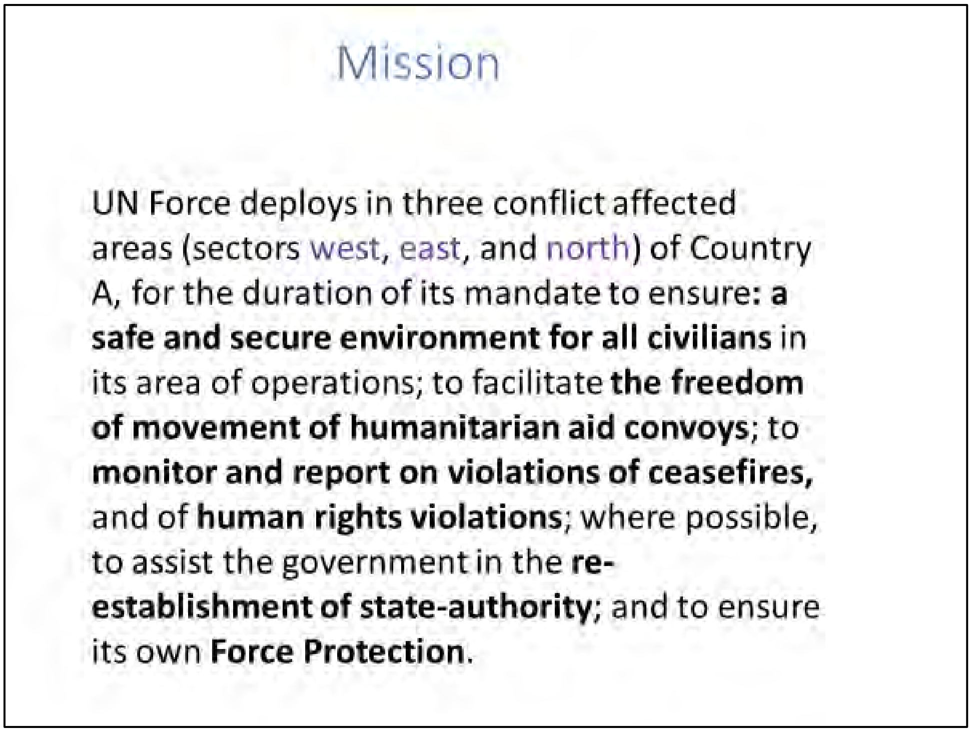
Interaction*. Ask students what they should study to ascertain direction? Responses should include Operating Environment; commander's intent; mission and mandate; and specified and implied tasks.*

It is important to gain the commander's support for your IAP during the Intelligence Dialogue. Therefore, you must arrive fully prepared as it will increase his/her confidence in your MPKI cell. Ideally, when the IAP is fully formed, it would be signed by the commander to give it the weight of an operation order. This will help the MPKI cell when they must ask the operations section to task acquisition assets.

It is also important during the dialogue to manage the commander's expectations of intelligence. Outline any limitations the MPKI cell has. For example, is it fully staffed with qualified personnel? The MPKI cell can also speak about the shortcomings of some ISR assets, such as drones. Often commanders believe that drones are the answer to everything. This is clearly not the case. A drone's capability is based on its ISR suite and its range. A drone cannot ascertain, for example, the location where an IED is buried.

The kinds of questions you should ask your commander and his/her staff during the dialogue are onscreen.

Slide 18



Mission

UN Force deploys in three conflict affected areas (sectors west, east, and north) of Country A, for the duration of its mandate to ensure: **a safe and secure environment for all civilians** in its area of operations; to facilitate **the freedom of movement of humanitarian aid convoys**; to **monitor and report on violations of ceasefires,** and of **human rights violations**; where possible, to assist the government in the **re-establishment of state-authority**; and to ensure its own **Force Protection**.

Let us now discuss the factors for consideration are drawn from the mission, mandate and commander's intent.

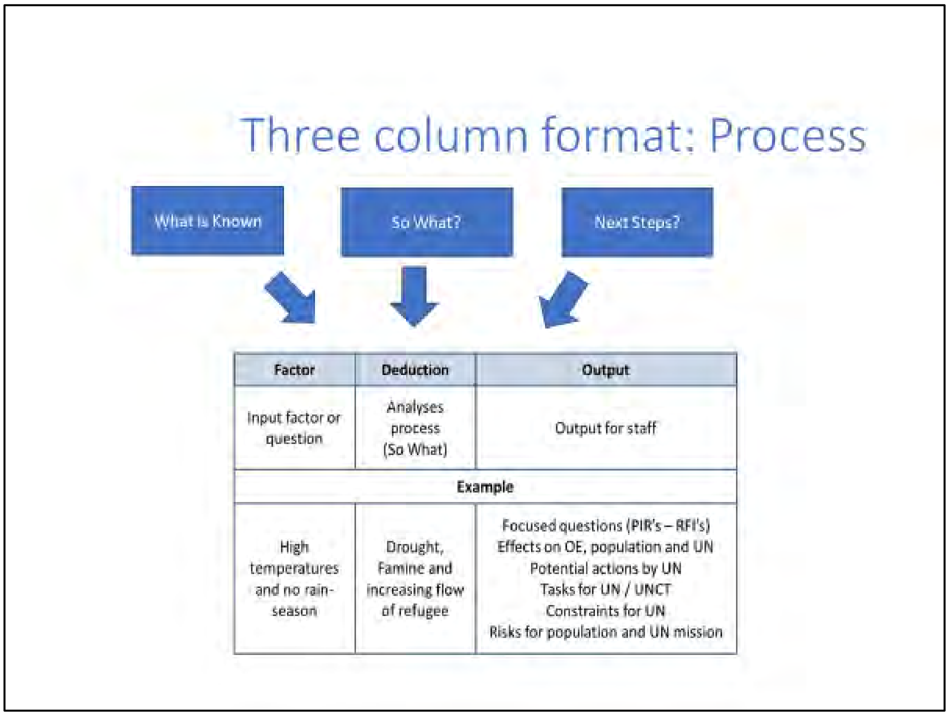
***Interaction**. Ask students to draw factors from the mission onscreen. Responses should include the factors outlined in bold. Ideally, the instructor would obscure the paragraph with the red highlights to ensure that the students do this without prompting.*

The key factors are outlined in bold. These are the overarching tasks that your commander will need to achieve or contribute to. Therefore, the commander will need the information to inform his/her decision making and planning in this regard.

The same process is carried out with the mandate, the commander's intent and tasks. The students must identify all pertinent factors.

These factors will then be transferred to the 3-column format, where a series of deductions will be made, which will uncover things that we need to know. These information gaps will then be grouped and distilled to become the initial set of PIRs.

Slide 19



Three column format: Process

What is Known

So What?

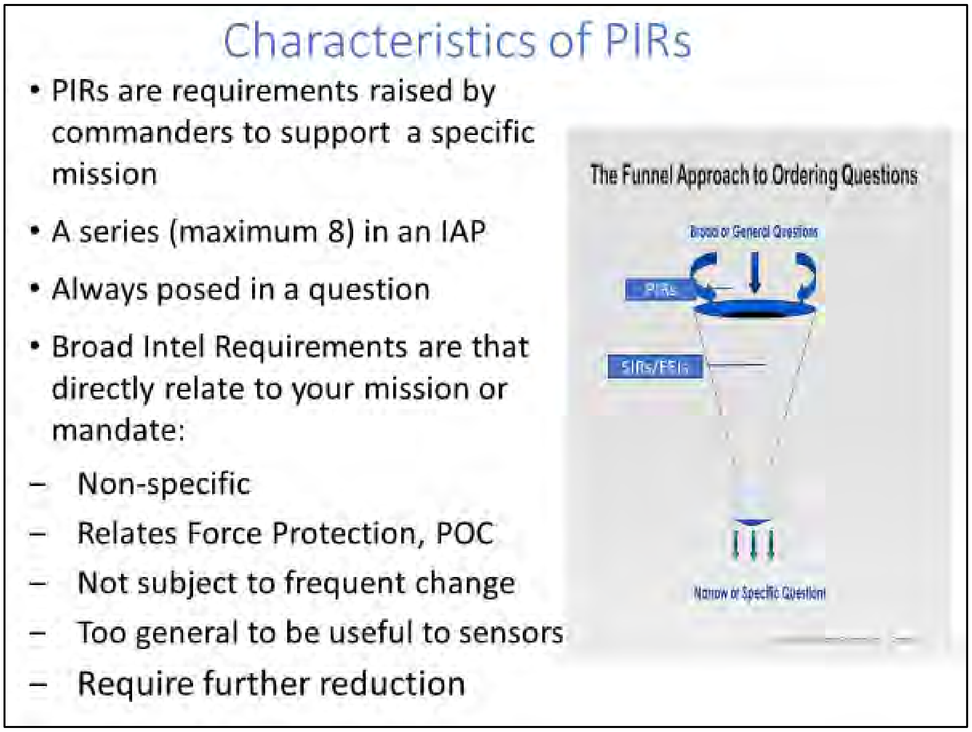
Next Steps?

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

These factors will then be worked through using the three-column format methodology, which will create several deductions from each factor. These deductions should uncover information requirements.

The final step in the process to identify PIRs is grouping these IRs thematically to create PIRs. For example, if there are several IRs relating to various threats to the civilian population, it would be logical to deduce that at least one PIR should be linked to POC. A suitable PIR, in that case, would be 'What are the threats to the civilian population?'.

Slide 20



Characteristics of PIRs

- PIRs are requirements raised by commanders to support a specific mission
- A series (maximum 8) in an IAP
- Always posed in a question
- Broad Intel Requirements are that directly relate to your mission or mandate:

– Non-specific

– Relates Force Protection, POC

– Not subject to frequent change

– Too general to be useful to sensors

– Require further reduction

The Funnel Approach to Ordering Questions
Broad or General Questions
PIRs
SIRs/EEIs
Narrow or Specific Questions

There are guidelines for what constitutes a well and a poorly phrased PIR. PIRs are always posed in question form. They should be limited in number to focus a limited number of acquisition assets. Ideally, there would be 6-8 PIRs. These PIRs will then be broken down to SIRs and EEIs.

PIRs will be general, broad questions rather than specific questions.

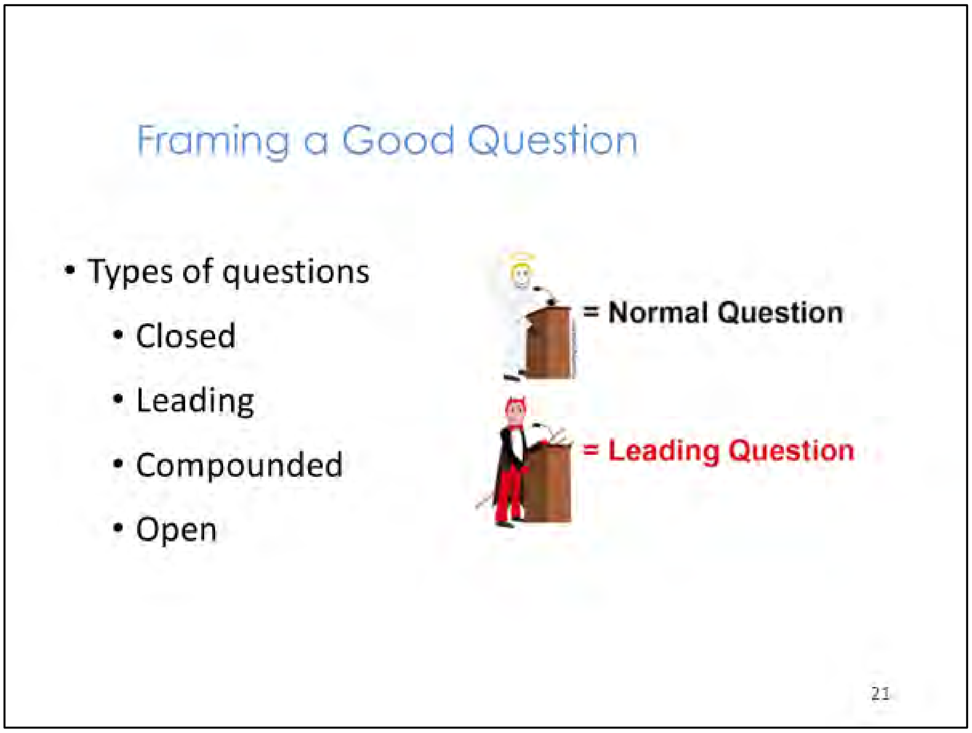
For example, a good PIR would be 'what is the threat posed by threat actor A?'. This PIR can then be broken down to SIRs and EEIs which can drill down for further detail. A poor PIR would be phrased as follows 'what threat does Threat Actor A pose in village X'. This is far too focused, it might work as an EEI, but not as a PIR.

Although the IAP is a living document and therefore can be changed, PIRs should be general enough to avoid very frequent change.

PIRs can generally not be acquired by sensors. For example, it is unrealistic to ask a soldier to acquire information on a question as general as 'what threat does threat actor A pose?'. The soldier needs a more focused question with a specific answer, as do other acquisition assets. For example, a soldier could ask 'is a threat actor A present in this village' or 'does threat actor A harm people in this area?'. The sum of the responses to SIRs and EEIs should give enough information to the MPKI cell to respond to the PIR with an intelligence product. PIRs always require further reduction.

Interaction. *Ask the students for a good and bad example of a PIR. Initiate debate with the students. Ask the students why it is that EEIs and SIRs are referred to as information requirements rather than intelligence requirements? The response, in this case, is that intelligence is comprised of lots of different elements of evaluated information. Therefore, the sum of information or data acquired based on responding to EEIs and SIRs as they relate to a specific PIR will when processed and analysed, will produce a response to a PIR. This will be presented as an intelligence product which will be disseminated to leadership.*

Slide 21



Framing a Good Question

- Types of questions
  - Closed
  - Leading
  - Compounded
  - Open

= Normal Question

= Leading Question

21

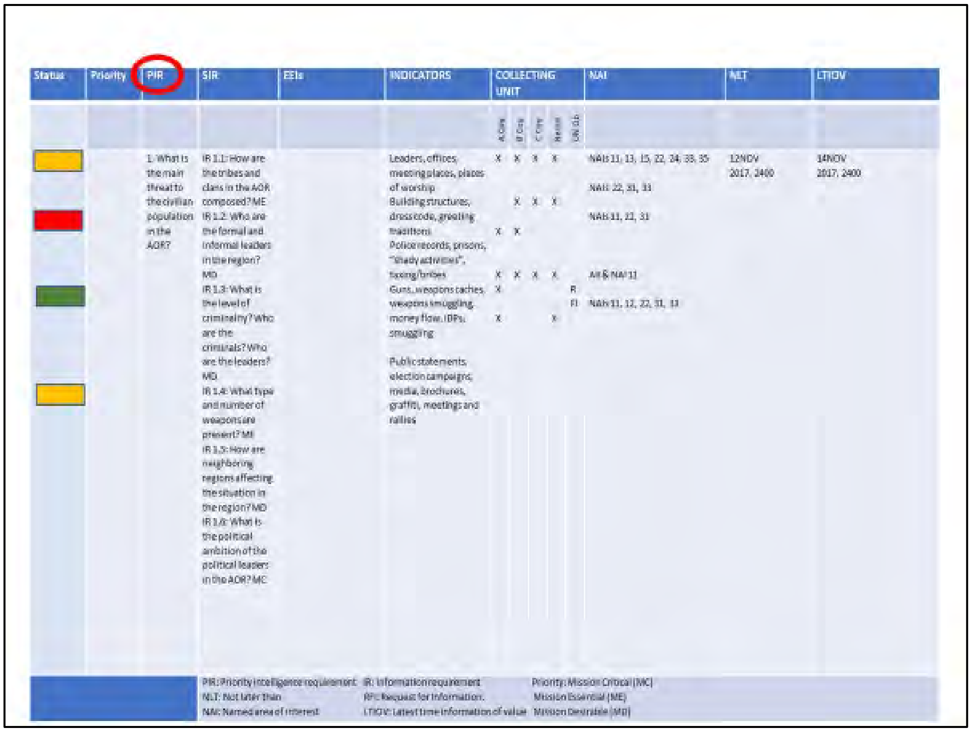
How we ask a given question is important. Listed on the slide are some types of questions. The closed questions are those that can be answered with a yes or no. (Is Actor A a threat?) This is not a good type of question and should be avoided. The leading questions are also unhelpful as they are limiting those that are providing answers to a specific point of view. (When Actor A attacks Village B, how will they use their Heavy Weapons?).

Compounded questions are when the question consists of several elements. This should also be avoided, as they are less helpful for those engaged in the acquisition and can cause confusion. (When and how will Actor A attack the local population in Village A and B). If your questions are built up like this, break them down into individual questions.

As far as possible pose open questions using 5W and H (Who / What / Where / Why / When / How). For example, how will Actor A pose a threat to the civilian population?

.

Slide 22



Status	Priority	PIR	SIR	EEIs	INDICATORS	COLLECTING UNIT					NAI	NLT	LTIOV
						A Coy	B Coy	C Coy	Recce	UN Ob			
🟨		1. What is the main threat to the civilian population in the AOR?	IR 1.1: How are the tribes and clans in the AOR composed? ME IR 1.2: Who are the formal and informal leaders in the region? MD IR 1.3: What is the level of criminalny? Who are the criminals? Who are the leaders? MD IR 1.4: What type and number of weapons are present? ME IR 1.5: How are neighboring regions affecting the situation in the region? MD IR 1.6: What is the political ambition of the political leaders in the AOR? MC		Leaders, offices, meeting places, places of worship	X	X	X	X		NAIs 11, 13, 15, 22, 24, 33, 35 NAI: 22, 31, 33	12NOV 2017, 2400	14NOV 2017, 2400
🟥					Building structures, dress code, greeting traditions	 X	X X	X	X		NAIs 11, 22, 31		
					Police records, prisons, "Shady activities", taxing/bribes	X	X	X	X		All & NAI 11		
🟩					Guns, weapons caches, weapons smuggling,	X				R FI	NAIs 11, 12, 22, 31, 33		
					money flow, IDPs, smuggling	X			X				
🟨					Public statements, election campaigns, media, brochures, graffiti, meetings and rallies								

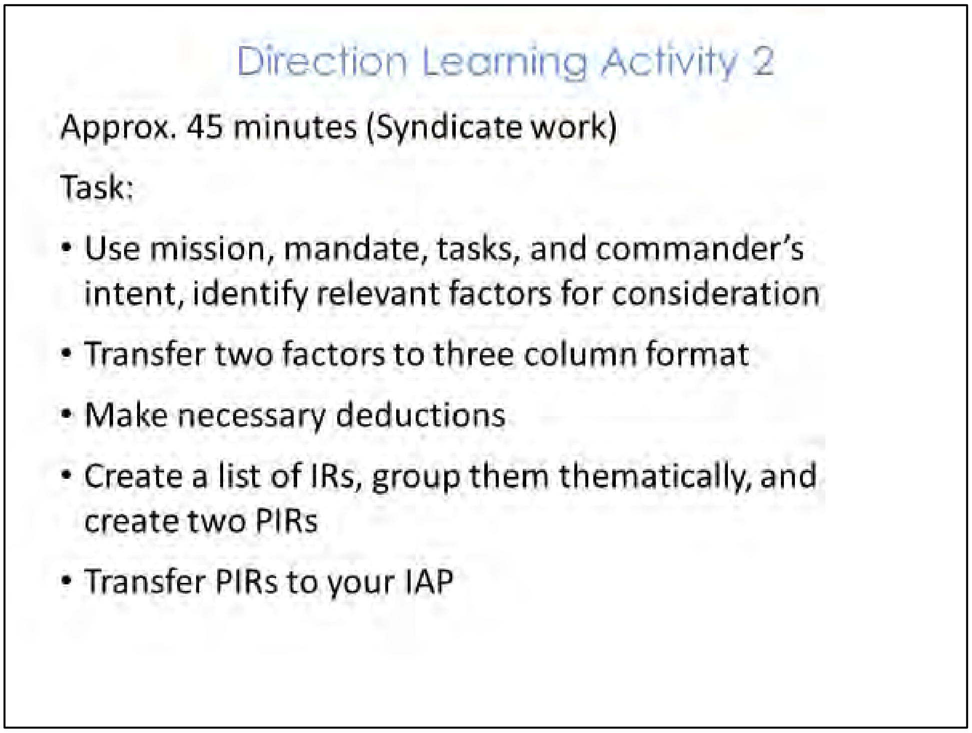
PIR: Priority intelligence requirement
NLT: Not later than
NAI: Named area of interest

IR: Information requirement
RFI: Request for Information.
LTIOV: Latest time information of value

Priority: Mission Critical (MC)
Mission Essential (ME)
Mission Desirable (MD)

Here is an example of the location of PIRs on the IAP. Shown in the red circles, here is where we place their PIRs on their own IAP as they construct it throughout the course.

Slide 23



Direction Learning Activity 2

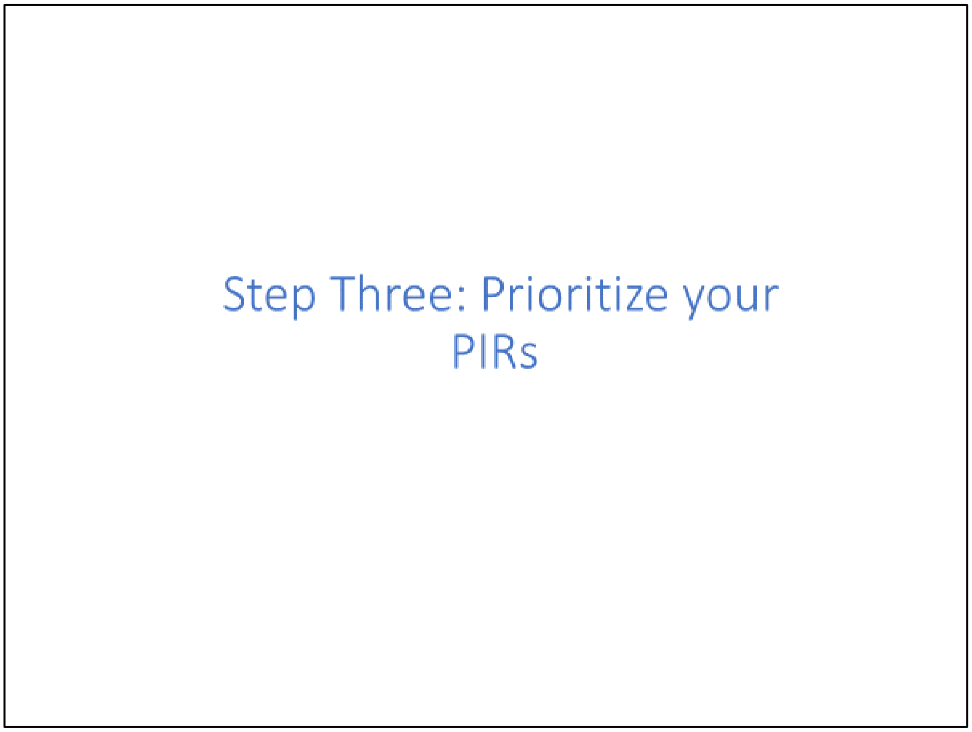
Approx. 45 minutes (Syndicate work)

Task:

- Use mission, mandate, tasks, and commander's intent, identify relevant factors for consideration
- Transfer two factors to three column format
- Make necessary deductions
- Create a list of IRs, group them thematically, and create two PIRs
- Transfer PIRs to your IAP

Interaction/learning activity: Let us now do a learning activity to reinforce what we have learned. The slide shoes the tasks. We will discuss as a class in about 45 minutes your solutions/outcomes. Requirements. Whiteboards and pens for students. A laptop for each group with a blank IAP. Handouts for mission, mandate, tasks, and commander's intent for each syndicate. Ensure that students focus on factors related to UN Force Protection and the Protection of Civilians. Good PIRs would include something like 'what threat does threat actor A pose to the UN?', 'what are the threats to the civilian population'.

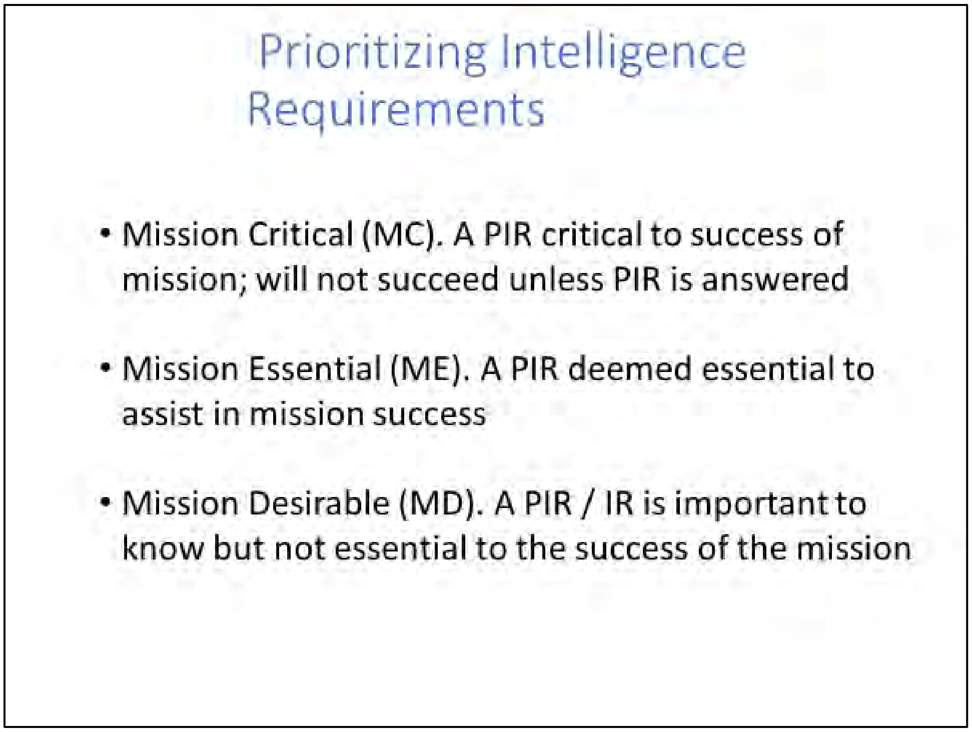
Slide 24



Step Three: Prioritize your PIRs

MPKI cells and units will have limited acquisition assets, and limited time during which to acquire information. Therefore, PIRs must be prioritised. However, students should be aware that PIRs relating to POC and UN Force Protection will always be in the top two PIRs. They will always be mission-critical, which means that the mission will fail unless we have access to information and intelligence about them.

Slide 25

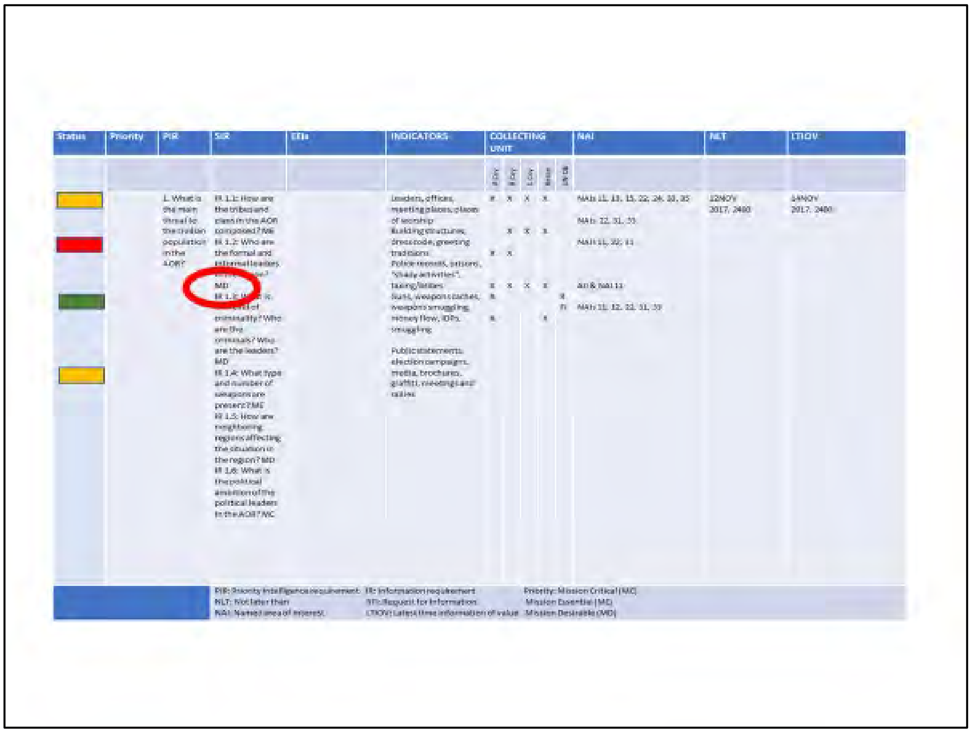


Prioritizing Intelligence Requirements

- 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

Which Priorities should the MPKI cell focus most effort on? The response is MC, followed by MD, followed by MD. Who prioritises these PIRs? The response is that the commander should, but if he/she does not react, then the MPKI cell should work jointly with the operations cell to do this.

Slide 26



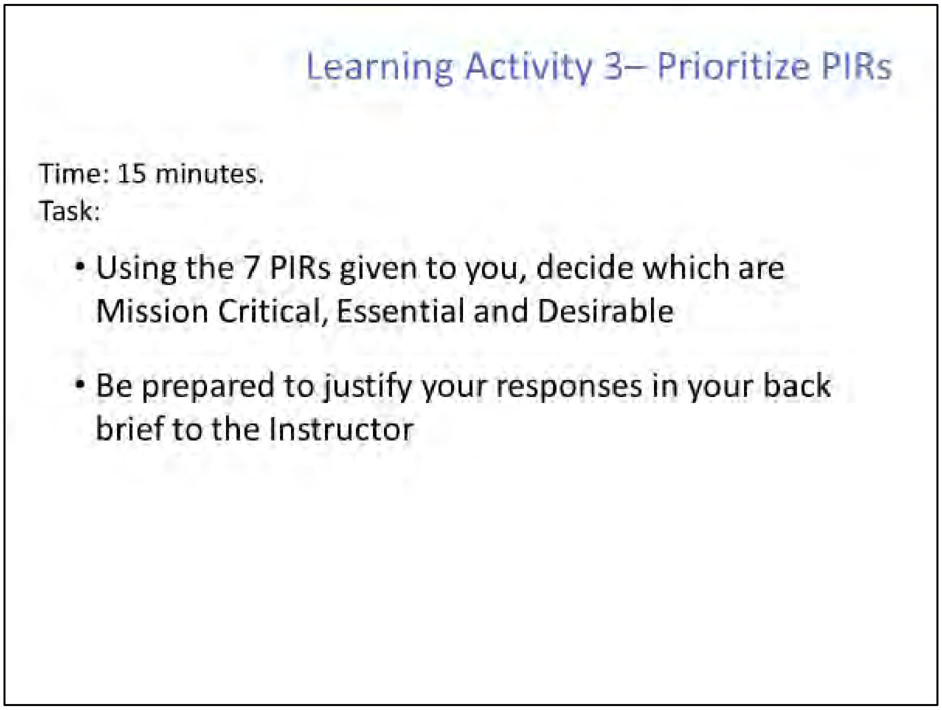
Status	Priority	PIR	SIR	EEIs	INDICATORS	COLLECTING UNIT					NAI	NLT	LTIOV
						A Coy	B Coy	C Coy	Recce	UN CB			
🟨 🟥 🟩 🟨		1. What is the main threat to the civilian population in the AOR?	IR 1.1: How are the tribes and clans in the AOR composed? ME IR 1.2: Who are the formal and informal leaders [illegible]? MD IR 1.3: What is the level of criminality? Who are the criminals? Who are the leaders? MD IR 1.4: What type and number of weapons are present? MC IR 1.5: How are neighboring regions affecting the situation in the region? MD IR 1.6: What is the political ambition of the political leaders in the AOR? MC		Leaders, offices, meeting places, places of worship Building structures, dress code, greeting traditions Police records, prisons, "shady activities", taxing/levies Guns, weapon caches, weapons smuggling, money flow, IDPs, smuggling Public statements, election campaigns, media, brochures, graffiti, meetings and rallies	X X X X X	X X X X	X X X	X X X X	X X	NAIs 11, 13, 15, 22, 24, 33, 35 NAIs 22, 31, 33 NAI 11, 22, 13 AO & NAI 13 NAIs 11, 12, 22, 31, 33	12NOV 2017, 2400	14NOV 2017, 2400

PIR: Priority intelligence requirement IR: Information requirement Priority: Mission Critical (MC)
NLT: Not later than RFI: Request for information Mission Essential (ME)
NAI: Named area of interest LTIOV: Latest time information of value Mission Desirable (MD)

We record MC, MD, and ME rating beside the questions that we acquire information on. These ratings can be put beside a PIR, a SIR, or an EEI. They are recorded as shown on the screen with the red circle. In this example, a SIR is rated as being Mission Desirable.

Interaction. Ask the students *what does mission desirable mean. Response- It is important to know, but not critical or essential to mission success.*

Slide 27



Learning Activity 3– Prioritize PIRs

Time: 15 minutes.
Task:

- 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

Interaction / learning activity:

Hand out 8 PIRs to the students.

- *What challenges are there to 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 organisations?*
- *What are the threats to the Civilian Population?*
- *What are the threats to mandate implementation?*

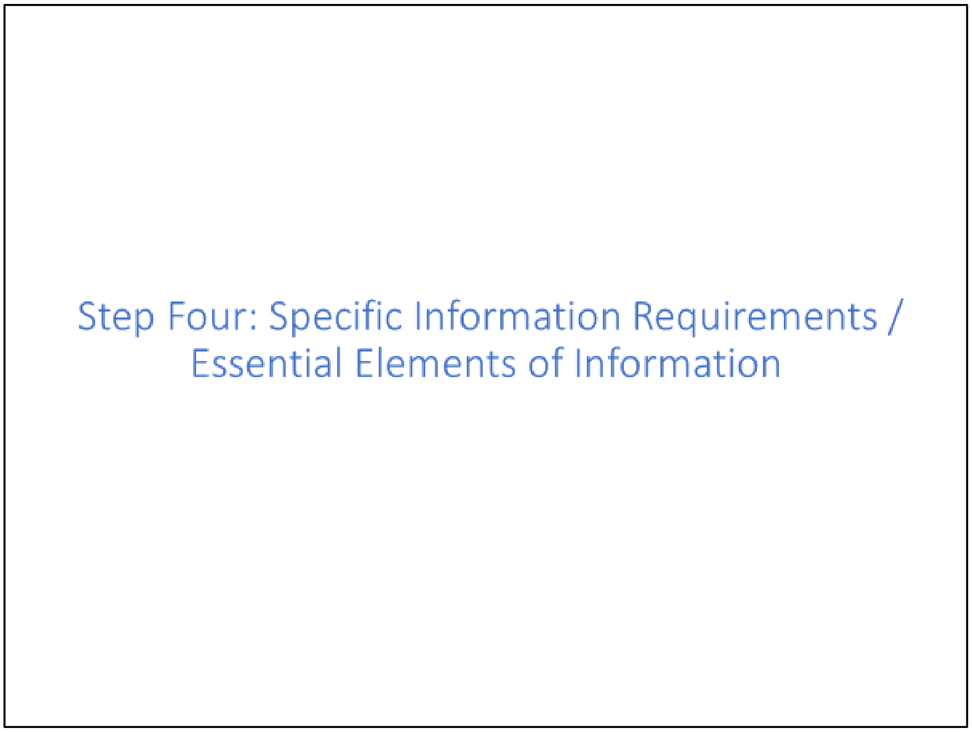
Ensure that the back brief takes place in front of the whole class to encourage debate. Select a few students and have students brief the class on the PIRs. They do NOT describe all PIRs as MC or ME; instead, have them choose at least one that is MD. Assessed responses are:

- *(ME) What challenges are there to Freedom of Movement?*
- *(MD) What is the capacity of national partners?*

- *(MC) What are the threats to UN Forces?*
- *(MD) What hazards are in the UN AO?*
- *(MD) What is the capacity of international organisations?*
- *(MC) What are the threats to the Civilian Population?*
- *(MC) What are the threats to mandate implementation?*

Approx. Total time 15 minutes.

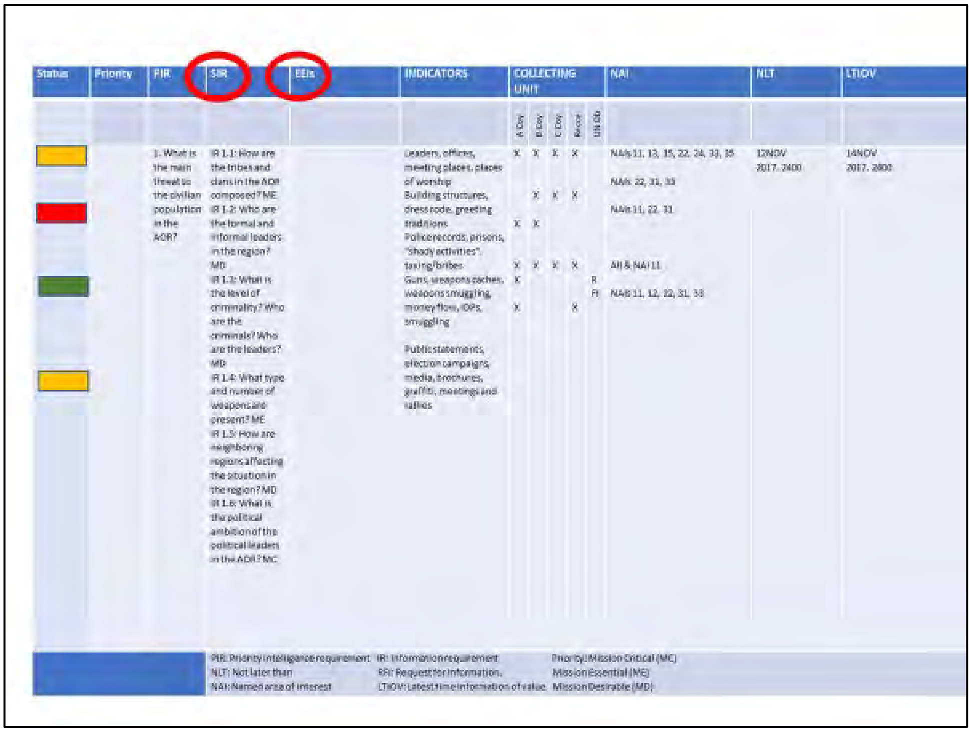
Slide 28



Step Four: Specific Information Requirements / Essential Elements of Information

We now move to demonstrate how to break broad PIRs into smaller sub-questions, which can be responded to by acquisition assets.

Slide 29

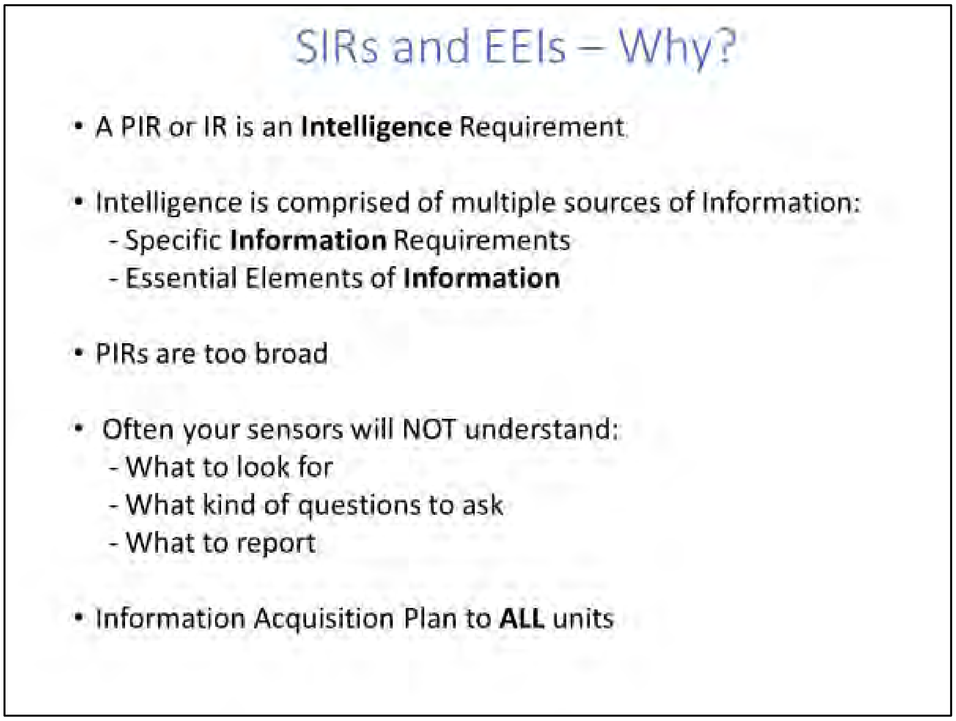


Status	Priority	PIR	SIR	EEIs	INDICATORS	COLLECTING UNIT					NAI	NLT	LTIOV
						A Coy	B Coy	C Coy	Recce	UN Ob			
🟨		1. What is the main threat to the civilian population in the AOR?	IR 1.1: How are the tribes and clans in the AOR composed? ME IR 1.2: Who are the formal and informal leaders in the region? MD IR 1.3: What is the level of criminality? Who are the criminals? Who are the leaders? MD IR 1.4: What type and number of weapons are present? ME IR 1.5: How are neighboring regions affecting the situation in the region? MD IR 1.6: What is the political ambition of the political leaders in the AOR? MC		Leaders, offices,	X	X	X	X		NAIs 11, 13, 15, 22, 24, 33, 35	12NOV	14NOV
					meeting places, places							2017. 2400	2017. 2400
					of worship						NAIs 22, 31, 33		
					Building structures,		X	X	X				
🟥					dress code, greeting						NAIs 11, 22, 31		
					traditions	X	X						
					Police records, prisons,								
					"shady activities",								
					taxing/bribes	X	X	X	X		All & NAI 11		
🟩					Guns, weapons caches,	X				R			
					weapons smuggling,					FI	NAIs 11, 12, 22, 31, 33		
					money flow, IDPs,	X			X				
					smuggling								
					Public statements,								
					election campaigns,								
🟨					media, brochures,								
					graffiti, meetings and								
					rallies								

PIR: Priority intelligence requirement IR: Information requirement Priority: Mission Critical (MC)
NLT: Not later than RFI: Request for Information. Mission Essential (ME)
NAI: Named area of interest LTIOV: Latest time information of value Mission Desirable (MD)

We now move to the right of the PIRs on the IAP. The location of SIRs and EEIs is designed in this manner in order to show that they are linked to the parent PIR. For example. PIR one is broken down to several SIRs, and each SIR is broken down to several EEIs. The information from several EEIs will come together to respond to a SIR, and all SIRs will come together to respond to a PIR.

Slide 30



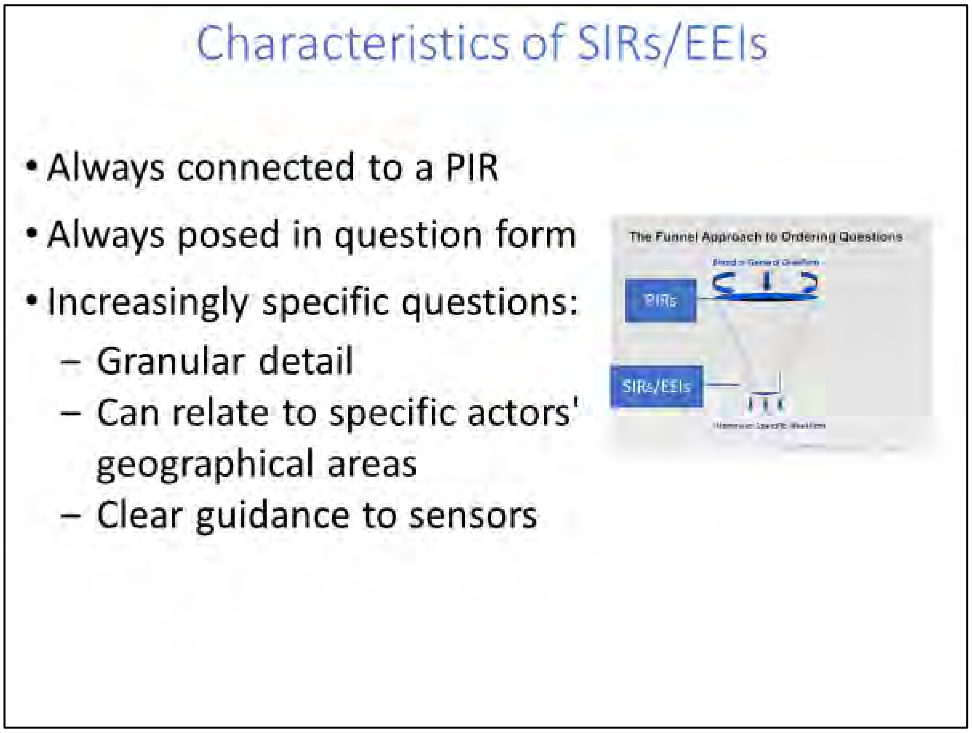
SIRs and EEIs – Why?

- A PIR or IR is an **Intelligence** Requirement
- Intelligence is comprised of multiple sources of Information:
  - Specific **Information** Requirements
  - Essential Elements of **Information**
- PIRs are too broad
- Often your sensors will NOT understand:
  - What to look for
  - What kind of questions to ask
  - What to report
- Information Acquisition Plan to **ALL** units

Key Message: A significant amount of data is required to produce a valid response to an Intelligence Requirement. This data is acquired by acquiring responses to numerous SIRs and EEIs, each of which links back to one PIR.

PIRs are broad, vague questions, which are not designed for acquisition assets. Rather, a PIR is designed to be broken down into sub-questions. This stimulates the thinking of an MPKI cell. Acquisition assets would not be able to acquire a suitable response to a PIR, but they can acquire a suitable response to a SIR or EEI.

Slide 31



Characteristics of SIRs/EEIs

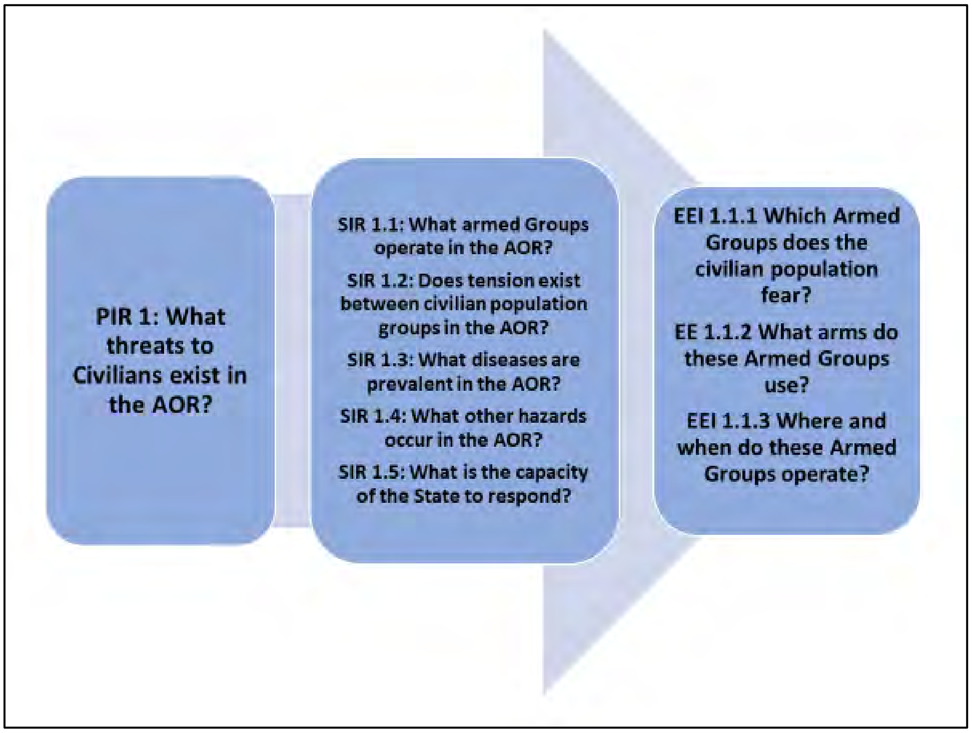
- Always connected to a PIR
- Always posed in question form
- Increasingly specific questions:
  - Granular detail
  - Can relate to specific actors' geographical areas
  - Clear guidance to sensors

The Funnel Approach to Ordering Questions
Broad or General Question
PIRs
SIRs/EEIs
Numerous Specific Questions

Key Message: The sum of the responses to the SIRs and EEIs is designed to deliver a response to a PIR. Students should be reminded that Intelligence is only created by processing numerous elements of information.

As shown by the graphic onscreen, PIRs are broad questions, which become numerous smaller questions, the answers to which combine to form intelligence. SIRs and EEIs can relate to specific areas and actors.

Slide 32



PIR 1: What threats to Civilians exist in the AOR?

SIR 1.1: What armed Groups operate in the AOR?

SIR 1.2: Does tension exist between civilian population groups in the AOR?

SIR 1.3: What diseases are prevalent in the AOR?

SIR 1.4: What other hazards occur in the AOR?

SIR 1.5: What is the capacity of the State to respond?

EEI 1.1.1 Which Armed Groups does the civilian population fear?

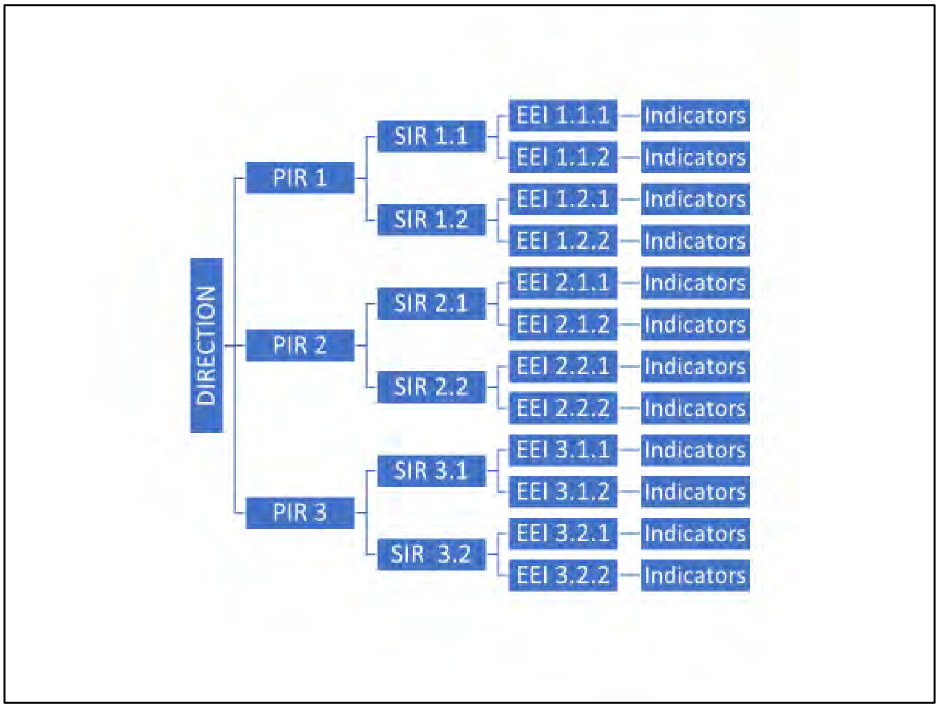
EE 1.1.2 What arms do these Armed Groups use?

EEI 1.1.3 Where and when do these Armed Groups operate?

This is an example of how one PIR is broken into several SIRs. Each SIR is then broken down to several EEIs. Each SIR on the screen relates to the parent PIR, while each EEI relates to SIR 1.1. As you can see, there will be many EEIs for each PIR. Generally, EEIs are what acquisition assets will be tasked to deliver on. It is important to note that while SIRs will generally be broken down to EEIs, this will not always be the case.

A general rule is that if you must elaborate on a SIR to say what the MPKI cells require from it, then it should be broken down to EEIs. For example, 'what armed groups operate in the AOR' is not a good SIR in this context as you need much more detail, such as 'what arms and ammunition do the group have', and other questions relating to its capabilities and intent. If an SIR speaks for itself, then it does not need to be broken down further.

Slide 33



DIRECTION

PIR 1

SIR 1.1

EEI 1.1.1 — Indicators

EEI 1.1.2 — Indicators

SIR 1.2

EEI 1.2.1 — Indicators

EEI 1.2.2 — Indicators

PIR 2

SIR 2.1

EEI 2.1.1 — Indicators

EEI 2.1.2 — Indicators

SIR 2.2

EEI 2.2.1 — Indicators

EEI 2.2.2 — Indicators

PIR 3

SIR 3.1

EEI 3.1.1 — Indicators

EEI 3.1.2 — Indicators

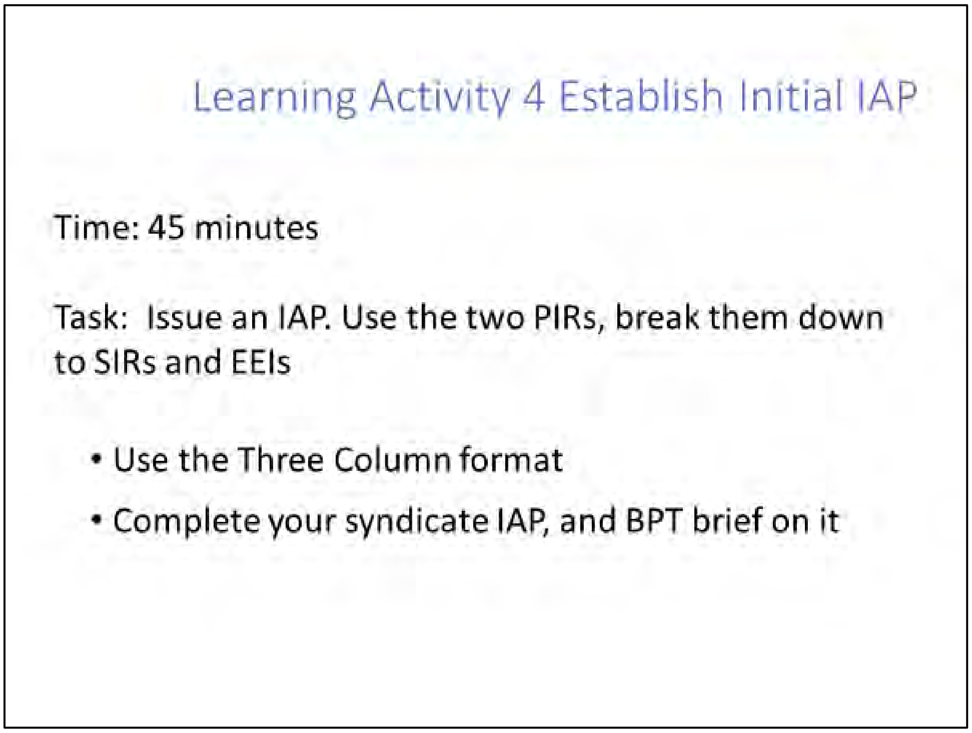
SIR 3.2

EEI 3.2.1 — Indicators

EEI 3.2.2 — Indicators

This is an example of how any given question can be broken down. Note that there is no actual limit to how many PIR's you can have, but it will normally be limited by the actors and factors that can affect the mission at hand. If you find yourself in a situation where the number of PIR's exceed 10, you might want to reassess them. You will note that we link some EEIs to indicators in this example. This will not always be the case. However, if an EEI is something like 'will threat actor A lay an IED to target UN forces?' then there may be several indicators which acquisition assets should focus on. For example, indicators of IED emplacement could include ground disturbance, the absence of local civilian traffic on a particular route etc.

Slide 34



Learning Activity 4 Establish Initial IAP

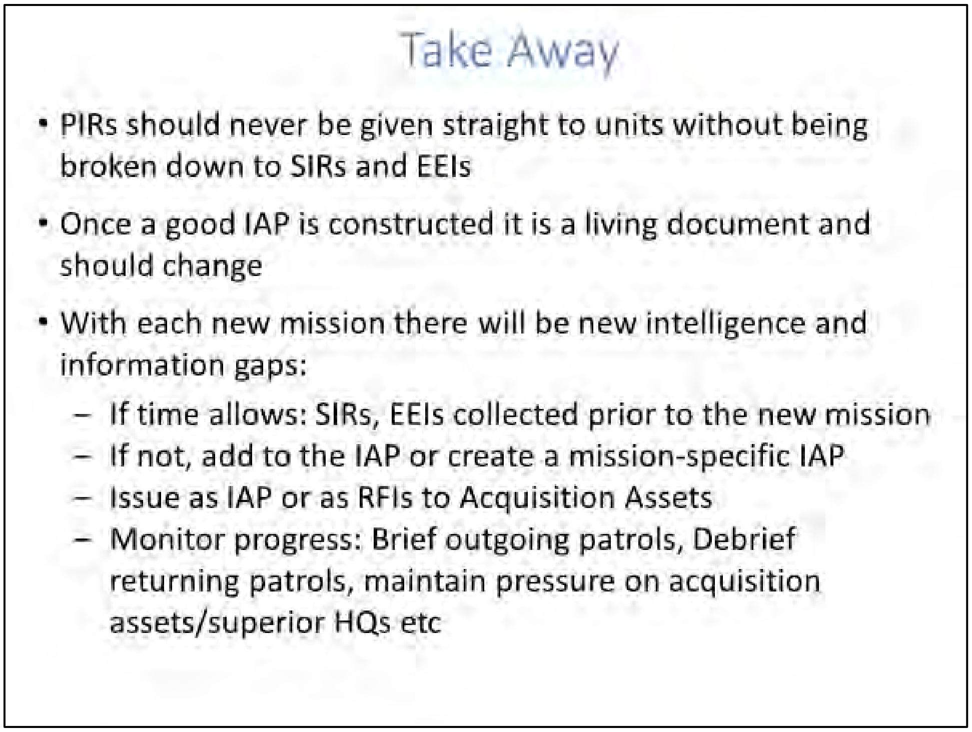
Time: 45 minutes

Task: Issue an IAP. Use the two PIRs, break them down to SIRs and EEIs

- Use the Three Column format
- Complete your syndicate IAP, and BPT brief on it

Interaction/learning activity: *This is a syndicate room activity. Resources will include a laptop for each syndicate containing the IAP that students have already worked on. Students are expected to use the three-column format to uncover SIRs and EEIs. Let the students take approximately 45 minutes (your judgement)? Reminded the students as they move through the lessons in the training packet that they identified IRs, and they should continuously add/update their IAP. Instructors must ask to see student IAPs at regular intervals to ensure they are keeping it updated.*

Slide 35



Take Away

- PIRs should never be given straight to units without being broken down to SIRs and EEIs
- Once a good IAP is constructed it is a living document and should change
- With each new mission there will be new intelligence and information gaps:
  - If time allows: SIRs, EEIs collected prior to the new mission
  - If not, add to the IAP or create a mission-specific IAP
  - Issue as IAP or as RFIs to Acquisition Assets
  - Monitor progress: Brief outgoing patrols, Debrief returning patrols, maintain pressure on acquisition assets/superior HQs etc

Summary

Always remember to get clear direction and guidance from the Commander and read back your work. This is a starting point for the intelligence dialogue, which must run continuously throughout the MPKI Cycle.

Remember to utilize the full potential of the UN information community, and other entities as approved by the HoM (or those delegated responsibility for this). Continuous external – and internal dialogue is vital for the success of the MPKI output. Always remember to utilize the full information community available in the UN Mission, including outside inlets as appropriate.

Lesson 3.2

Acquisition

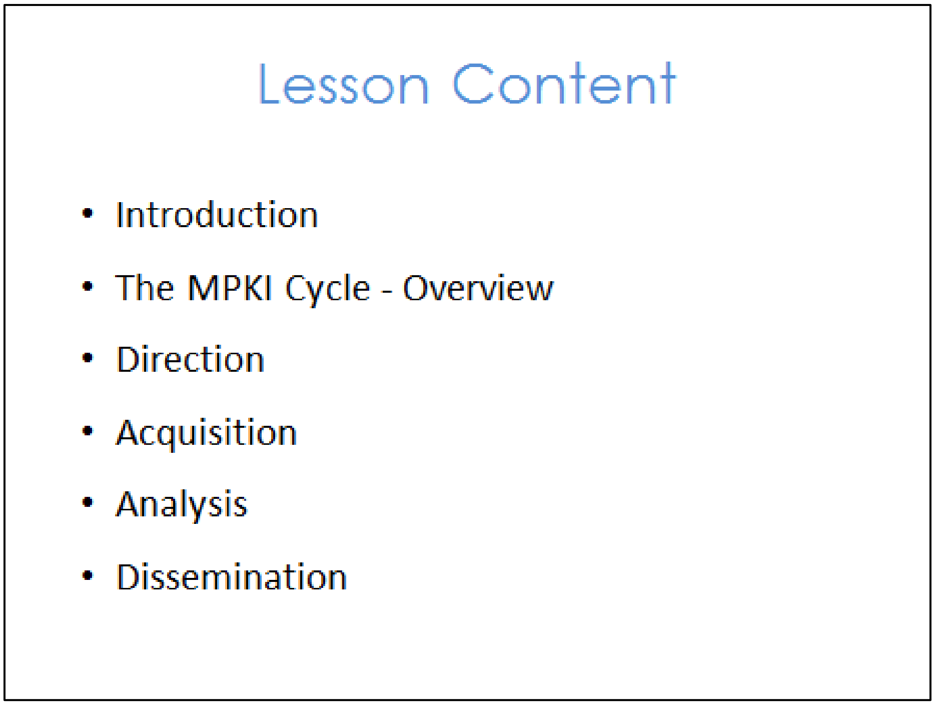
The Lesson

Starting the Lesson

Slide 1

Lesson 3.2
MPKI Acquisition

Slide 2

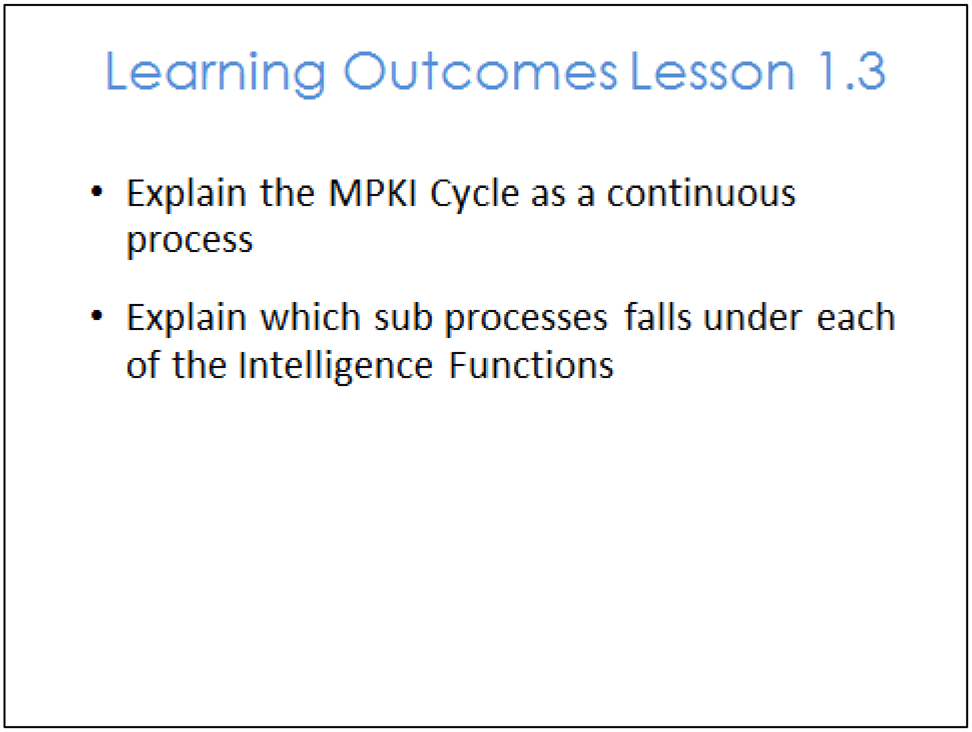


Lesson Content

- Introduction
- The MPKI Cycle - Overview
- Direction
- Acquisition
- Analysis
- Dissemination

We will cover the following topics during this lesson:

Slide 3

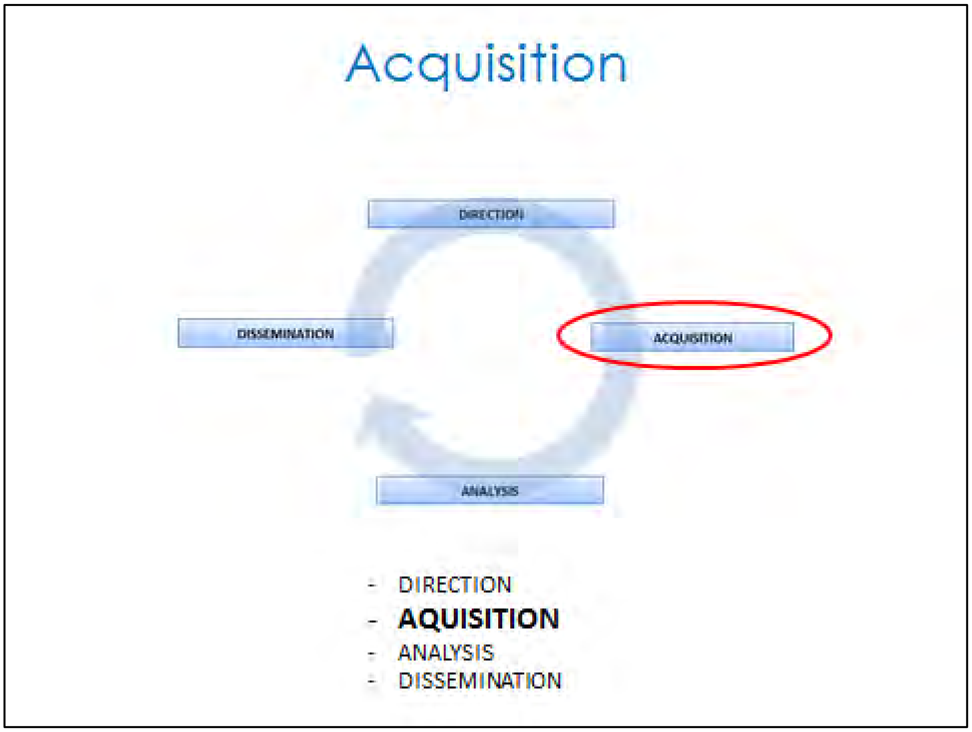


Learning Outcomes Lesson 1.3

- Explain the MPKI Cycle as a continuous process
- Explain which sub processes falls under each of the Intelligence Functions

Let’s review the Learning Outcomes for this lesson. At the end of this lesson, you should be able to perform these outcomes.

Slide 4



Acquisition

DIRECTION

DISSEMINATION

ACQUISITION

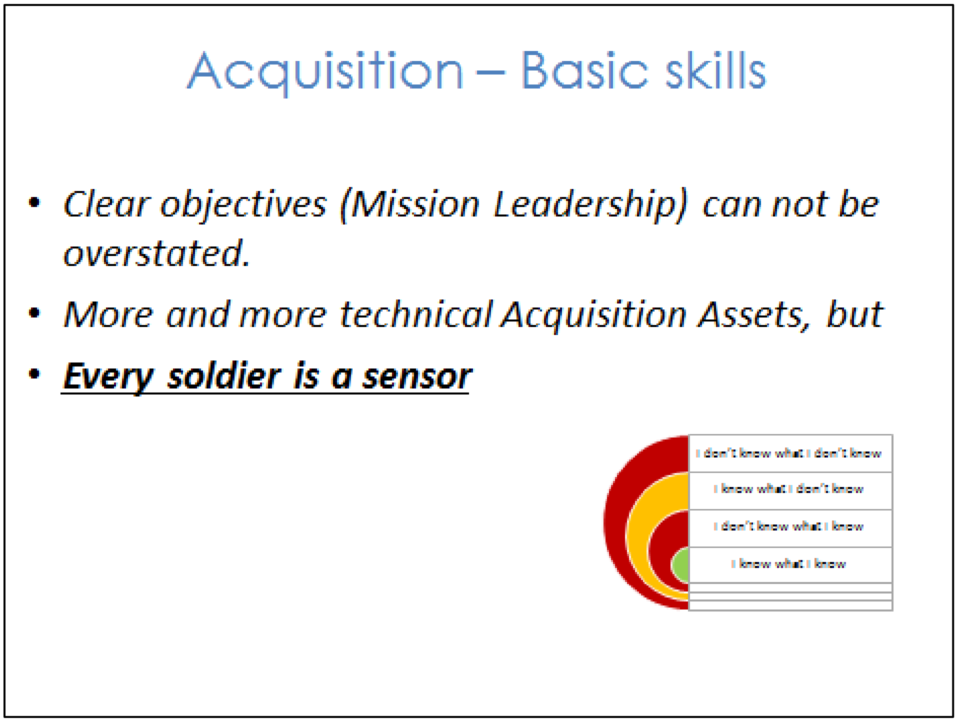
ANALYSIS

- DIRECTION
- **AQUISITION**
- ANALYSIS
- DISSEMINATION

After ascertaining the requirements and sorting them according to priority, the next step is the acquisition of the data or information, which is required to feed the analytical step of the cycle. Many PKMI acquisition resources will be the same across missions, (e.g. UN Military patrols and observers); however, some acquisition capabilities will only be available in certain mission areas.

PKMI personnel must develop the fullest awareness of all the sources and agencies they are able to task with the acquisition. It should be noted that data and information should be sought from the broadest sources available and be sourced from women as well as men.

Slide 5



Acquisition – Basic skills

- *Clear objectives (Mission Leadership) can not be overstated.*
- *More and more technical Acquisition Assets, but*
- ***Every soldier is a sensor***

I don't know what I don't know
I know what I don't know
I don't know what I know
I know what I know

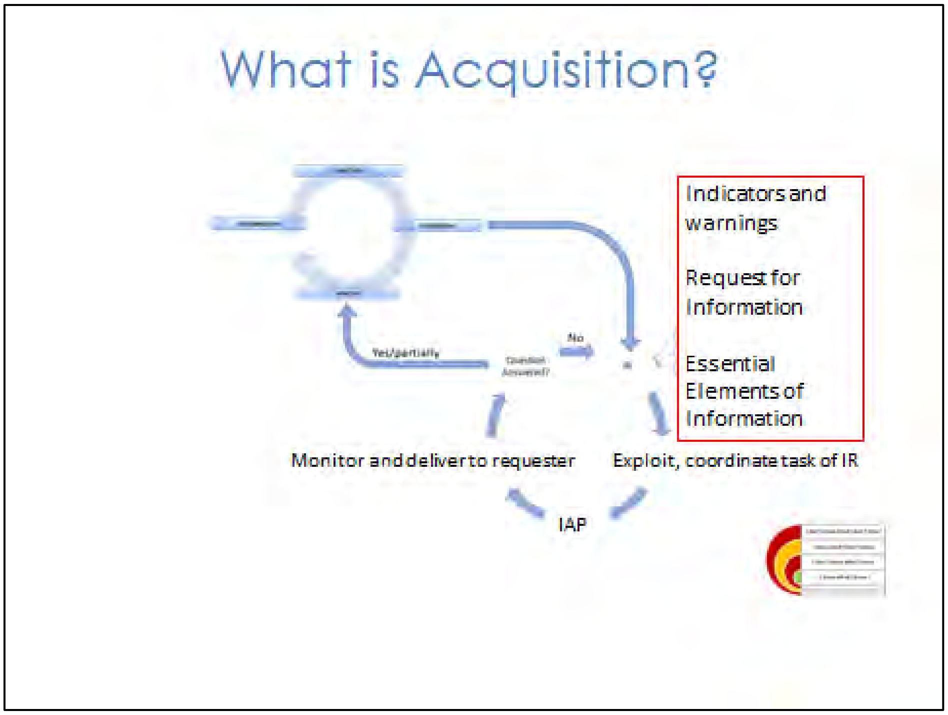
Key message: Acquisition is the Intelligence Function that contains the planning, focusing, prioritisation and tasking of acquisition assets to support the Commander's CCIRs and PIRs. Every Intel Requirement should be broken down into questions that everyone will understand, as shown in the chapter on the direction. These lecture aims to visualise how to make a collection cycle of it.

Every soldier is a sensor. The most readily available and best acquisition capability UN missions have military personnel. The phrase 'Every Soldier is an acquisition sensor' is key to the success of UN acquisition. Soldiers may acquire information through patrolling, through the manning of observation posts, by conducting base security patrols and during most routine operational activity. Further information may be acquired if they positively interact with the local population.

Information gathering can be conducted by static and mobile surveillance supported by technical systems such as documentation equipment, manned observation posts or mobile ground units. Overhead surveillance is conducted from existing Unmanned Aerial Vehicles (UAV) systems which have the capability to conduct surveillance against a static position or a moving actor. The acquisition is also conducted through interaction with human sources; this acquisition skill will make it possible to reveal the intent of an actor.

Therefore, the Force Intelligence Acquisition Plan (IAP) must be communicated to all personnel in a manner that makes it understandable. For example, broad, strategic PIRs should be broken down into questions that everyone will understand, as shown in the chapter on the direction.

Slide 6



What is Acquisition?

Indicators and warnings

Request for Information

Essential Elements of Information

Monitor and deliver to requester

Exploit, coordinate task of IR

IAP

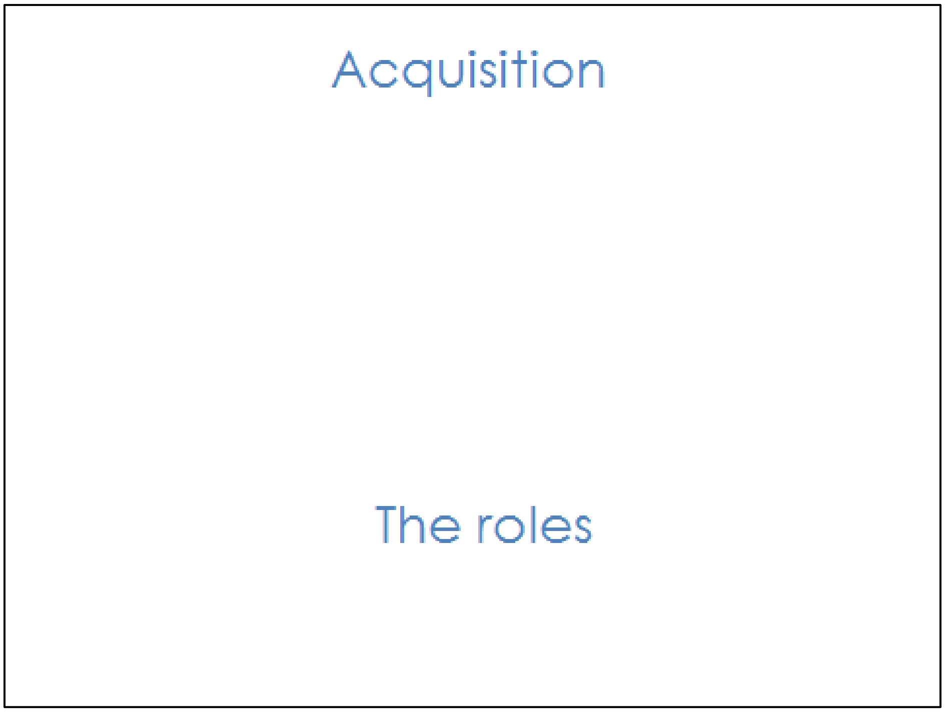
Key Message. The acquisition is the exploitation of sources of information by collection units and assets, and the delivery of this information to the proper intelligence processing unit for the use in the production of intelligence.

Information acquisition follows on from Direction, and the two (functions) are very closely linked. Direction determines what information requirements, while acquisition is the actual collection of the information in pieces.

Most UN mission has many acquisition assets, such as individual soldiers, specialist intelligence personnel, and Intelligence Surveillance and Reconnaissance (ISR) capabilities such as UAVs. It is also worth noting that searching the internet (open source information acquisition) or by searching through the information that is already known (some countries refer to this as datamining).

Regardless, the information must be acquired and passed to the Analytical elements (the following Intel Function) of PKMI in the right format and at the right time.

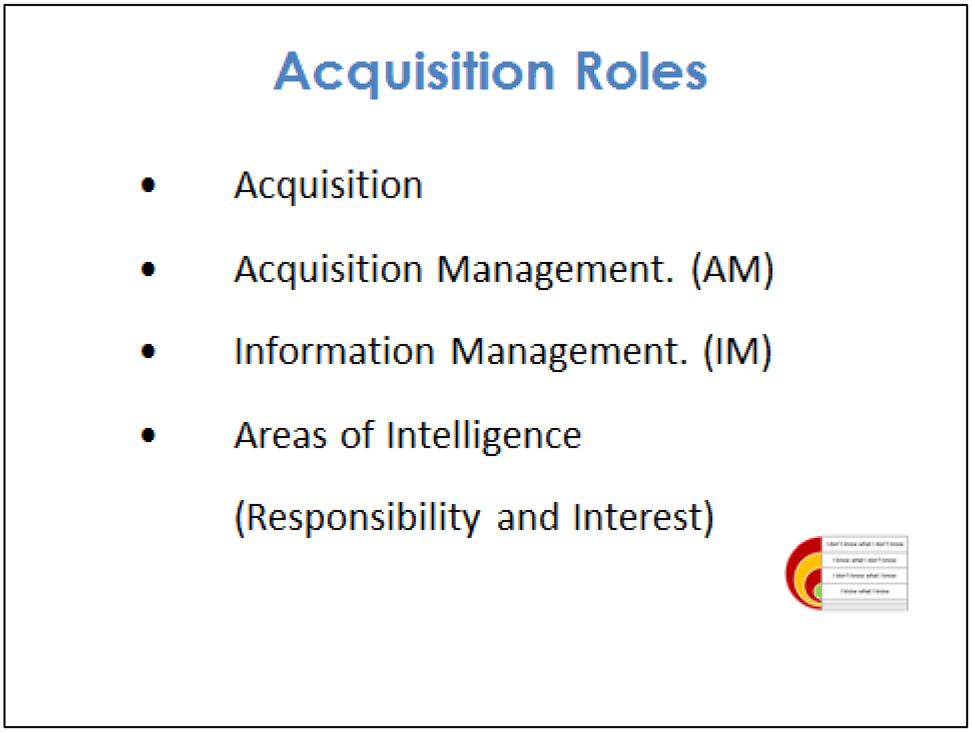
Slide 7



Acquisition

The roles

Slide 8



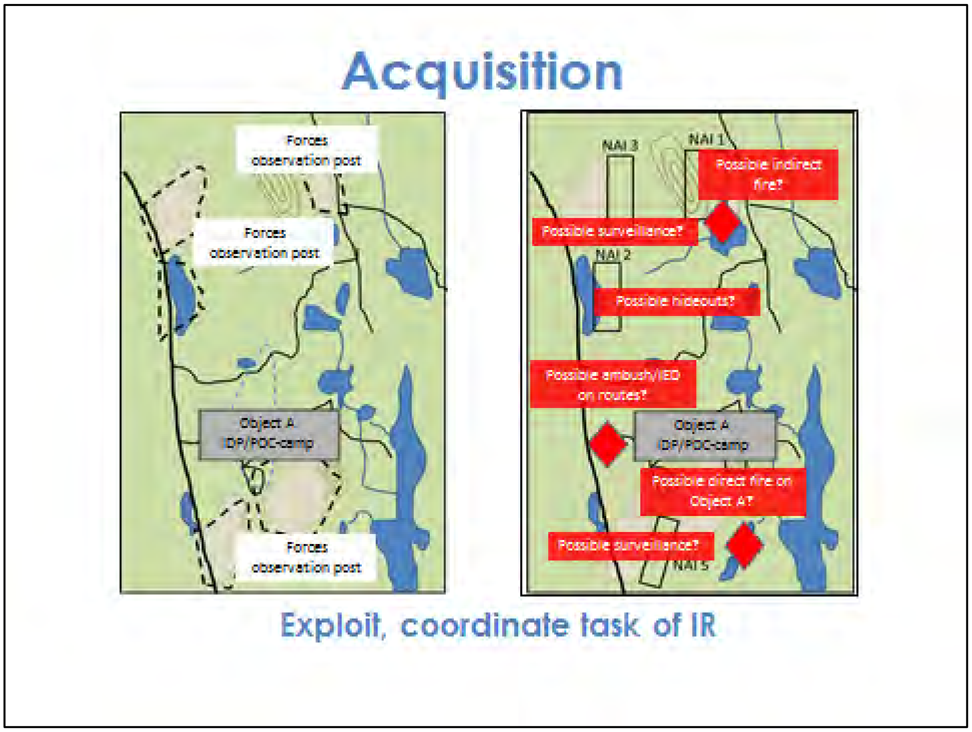
Acquisition Roles

- Acquisition
- Acquisition Management. (AM)
- Information Management. (IM)
- Areas of Intelligence

  (Responsibility and Interest)

The acquisition is the Intelligence Function that contains close coordination in these areas.

Slide 9



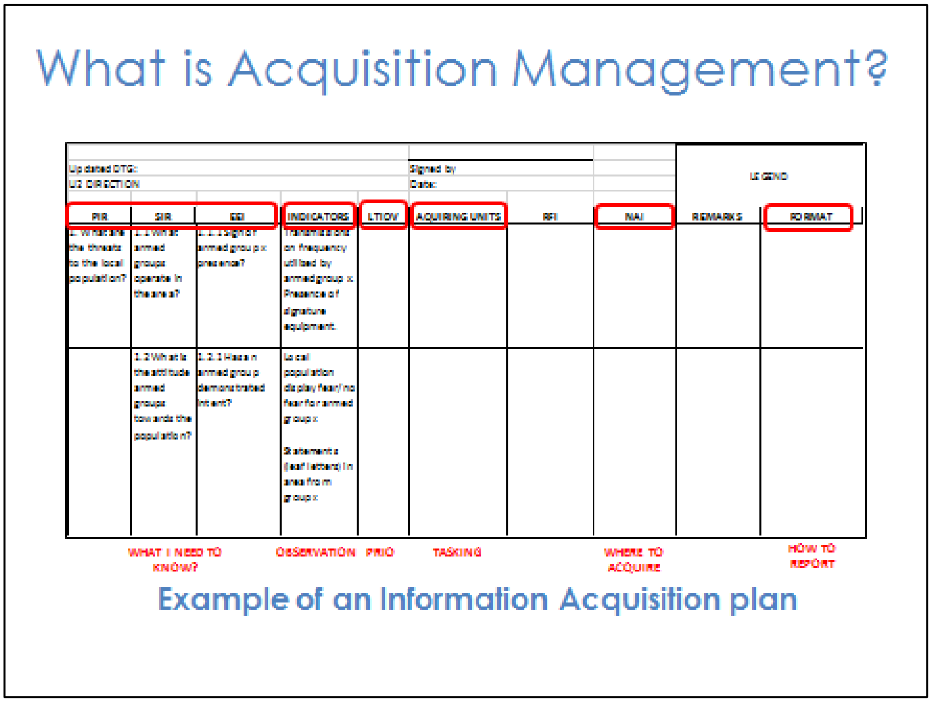
Acquisition

Exploit, coordinate task of IR

While the IAP is a very important part of the process, and it exists due to the knowledge gaps within the mission, it cannot be the only focus of the acquisition process. The mission will also be conducting operations on humanitarian efforts that must also be supported to enhance decision making. It is very important within the roles of the Acquisition section to be represented during mission planning and update meetings to ensure that there is a clear understanding of mission priorities.

The example above: As the PKMI staff conducts AOE, there will be a constant identification of intelligence and acquisition gaps. These gaps are to be annotated in the Intelligence Acquisition Plan and are to initiate the production of RFIs and IRs (as detailed in previous chapters).

Slide 10



What is Acquisition Management?

Updated DTG:					Signed by			LEGEND	
U2 DIRECTION					Date:				
PIR	SIR	EEI	INDICATORS	LTIOV	AQUIRING UNITS	RFI	NAI	REMARKS	FORMAT
1. What are the threats to the local population?	1.1 What armed groups operate in the area?	1.1.1 Sign of armed group x presence?	Transmissions on frequency utilised by armed group x. Presence of signature equipment.						
	1.2 What is the attitude armed groups towards the population?	1.2.1 Has an armed group demonstrated intent?	Local population display fear/ no fear for armed group x Statements (leaf letters) in area from group x						

WHAT I NEED TO KNOW? OBSERVATION PRIO TASKING WHERE TO ACQUIRE HOW TO REPORT

Example of an Information Acquisition plan

Key message: The IAP is the most important direction tool and is the catalyst for the MPKI Cycle.

Acquisition Management is the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection units or assets, monitoring results and re-tasking as required. Acquisition Management and coordination must be conducted at every staff level. The Acquisition Plan is a tasking matrix that links information acquisition with the sensor assets. It lists the information requirements with the organisations or databases that might hold the information or with the sensor assets that might be used to gather the information. The Intelligence acquisition plan is not a static document frozen in time but a continuous process. It will react and respond to changes in the operational situation and the information gathered by the assets tasked.

The aim is to coordinate **prioritisation in time and where the collection is acquired.** The prioritisation of IRs is important to make the acquisition effort more efficient and focused. Prioritisation is the ordering of IRs according to whether they are mission-critical, essential, or desirable. IRs can also be time-sensitive and often include a 'Not Later Than' (NLT) or **'Last Time Information is of Value' (LTIOV) label.** This also helps the PKMI cell to focus its acquisition effort.

Most RFIs adhere to the same system, and will always have an NLT or LTIOV label. There should also be a review process that assesses the degree of fulfilment of the requirement, so that if fulfilled, so it can be removed from the list.

Having broken down, the various IR's results are populated in the IAP. The IAP, when approved by the Commander, can be regarded as an executive order. This is preferably attached as an Annex to a FRAGO. Each level of units has to develop its own IAP, always incorporating the overarching requirements of the higher level(s). However, various levels will have individual differences depending on which actors are present in the operational area, the human terrain, and other factors.

We have been through PIR/SIR/EEI, but there are some other entries in the IAP:

- LTIOV is "Latest Time Information is Of Value", meaning that in order to underpin an operation or planning process the answer needs to be given before the stated date
- Acquiring Unit is the unit that we wish to task with the acquisition on a specific requirement. This could be geographical, such as Sectors/Battalions; or acquisition discipline, such as OSINT/SIGINT/HUMINT. Several units can be tasked with fulfilling the same requirements
- RFI: When a level is unable to fully, or partially fulfil a requirement, they can use RFI to neighbouring units or higher levels.
- NAI: Named areas of Interest is where one can expect to find answers to a requirement. The NAI helps Acquiring units focus its efforts geographically.
- Remarks: This is a free-text portion where amplifying instructions and guidance can be provided if necessary.

Slide 11

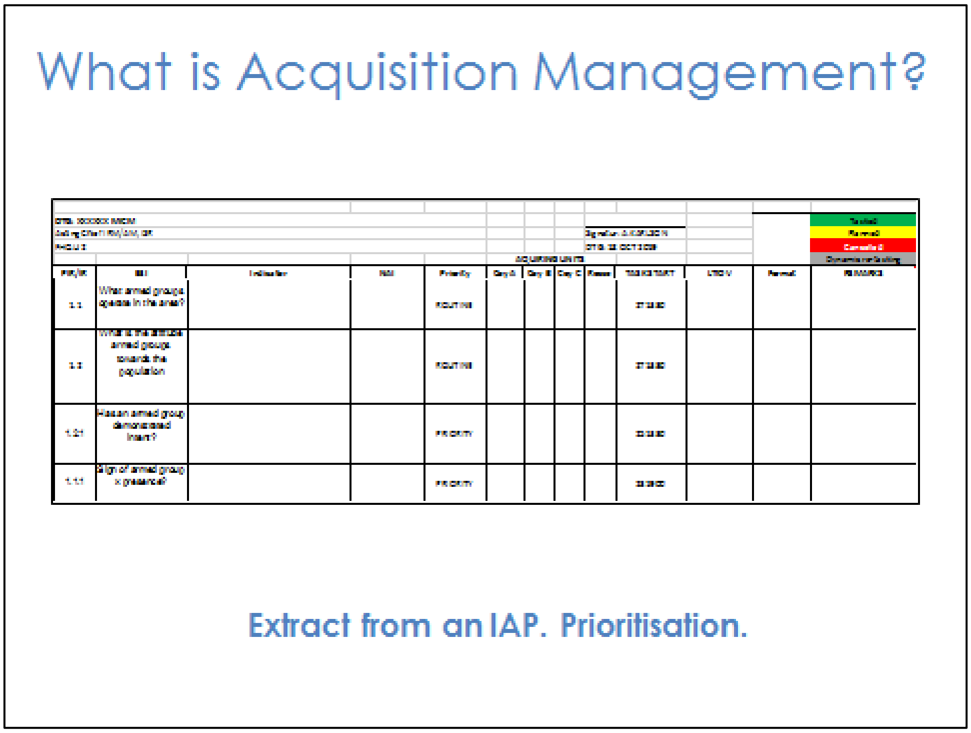
What is Acquisition Management?

MILITARY INFORMATION ACQUISITION PLAN

A full Intelligence Acquisition plan. Too BIG!

Key Message. The IAP is the most important direction tool and is the catalyst for the MPKI Cycle.

Slide 12



What is Acquisition Management?

DTG: [illegible]
[illegible]
[illegible]

Signature: [illegible]
DTG: [illegible] OCT [illegible]

🟩 Tasked
🟨 Planned
🟥 Cancelled
▨ Dynamic re-tasking

					ACQUIRING UNITS							
PIR/IR	EEI	Indicator	NAI	Priority	Coy A	Coy B	Coy C	Recce	TASK START	LTIOV	Format	REMARKS
1.1	What armed groups operate in the area?			ROUTINE					[illegible]			
1.2	What is the attitude armed groups towards the population			ROUTINE					[illegible]			
1.2.1	Has an armed group demonstrated Intent?			PRIORITY					[illegible]			
1.1.1	Sign of armed group x presence?			PRIORITY					[illegible]			

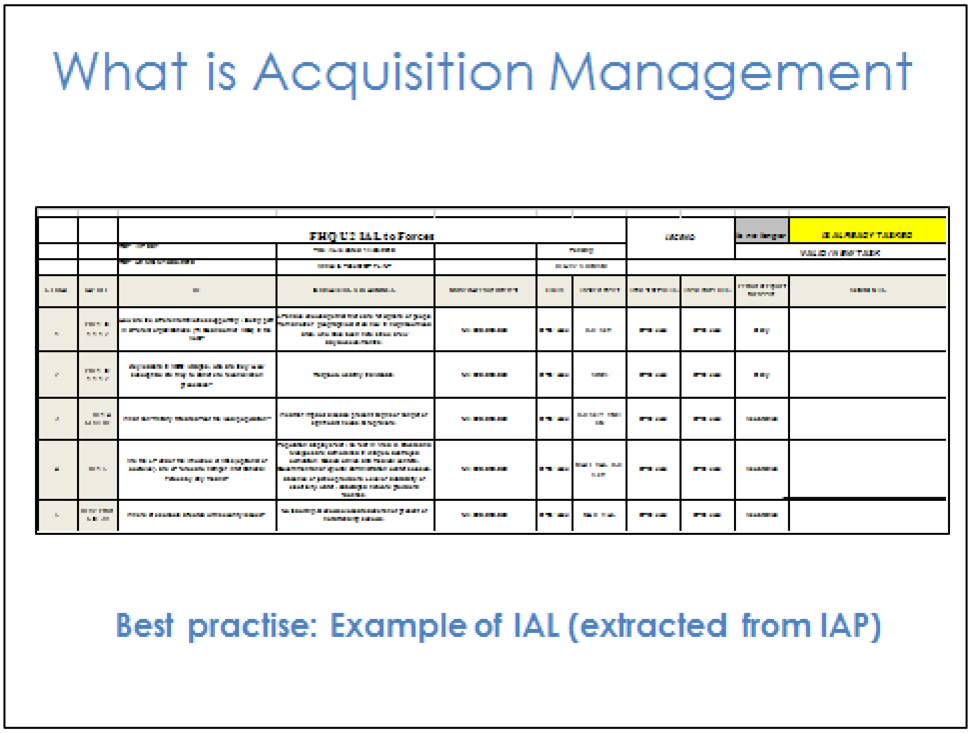
Extract from an IAP. Prioritisation.

Key message: Do not disseminate the IAP as a total, other than to units/sections, that have Military All sources capability, G2/S2/ ISR Units.

Best practice of not sharing the IAP is to disseminate a list of prioritisations. The IAL is the daily/weekly list of all the IRs that are planned to be acquired on given periods/patrols or within an operation. It is a combination of the EEIs, RFIs and I&W, which have become IRs in the acquisition process and have been prioritised accordingly.

The column to the left is showing the EEI to be answered by units or sensors, and these questions are to be referred to - and valid - to the PIR´s. The example shows both SIR and EEI, in this case. The IAL is a list of IRs that is then tasked against the variety of units/sensors across the mission. The prioritisation is very important as it allows those who have been tasked to easily understand what should be acquired first, to start their planning to achieve answers and reports.

Slide 13



What is Acquisition Management

FHQ U2 IAL to Forces

Best practise: Example of IAL (extracted from IAP)

Key message: A good IAP fits into and supports the overall operations plan or order. The acquisition is based on the commander's direction/intent and the PIRs / IRs received. IAL to Force level is an extraction out of IAP to Force-level.

Once areas (NAI) are identified and acquired units are tasked, broad PIR/IRs will not normally be passed directly to units and assets.

The life of an IR starts as an EEI, an I&W or an RFI within the IAP. The IAP is explained in chapter five! Once the daily IAL has been extracted from the IAP, the IR will then be assigned to the appropriate acquisition capability. See an example of IR based upon the IAP in chapter five. These are highlighted to the left column

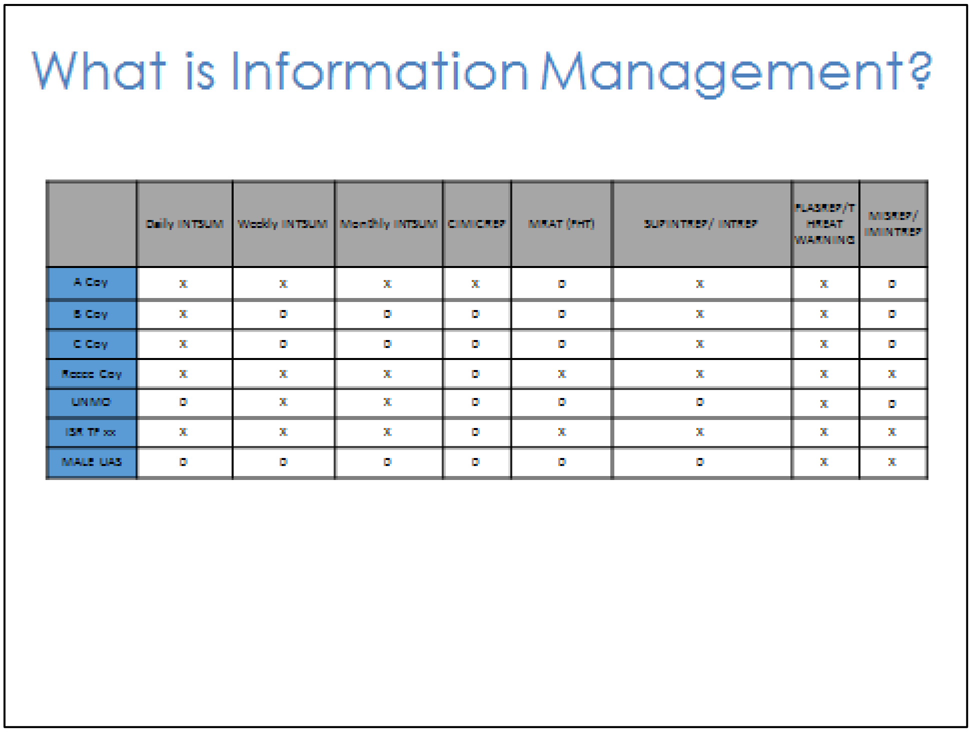
Once dissemination is complete, the IAP must be updated to reflect open and complete IRs to ensure that an effective IAL is generated for the next day. Once the process is established, IALs can be generated in several days in advance with only minor adjustments taking into account IRs that were not able to be acquired on a given day. While it is a dynamic process, it does not need to be last minute.

Often the IAP will task several units to collect the same information. This is done to ensure that high-priority information is collected and to ensure that information is not just a single source.

The IAP itself should be updated regularly to firstly ensure that the priorities remain in line with the mission leader's intent. This can be achieved through a quarterly meeting with the leadership to discuss their requirements. The IAP must also be updated when information gaps are closed to ensure that assets are not being misemployed on tasking. For example, an EEI could relate to a specific village that is under threat of attack. If that village is destroyed by armed groups then unless there is new reporting perhaps relating to people returning, there will be no requirement to continue to monitor the village.

Units that are tasked throughout the IAL, to collect information, should be represented on the Force-level IAP with a simple tick or another symbol. This will allow the information acquisition manager to follow-up on acquisition taskings. A simple example of a completed Force – level IAL is shown above.

Slide 14



What is Information Management?

	Daily INTSUM	Weekly INTSUM	Monthly INTSUM	CIMICREP	MRAT (FHT)	SUPINTREP/ INTREP	FLASREP/T HREAT WARNING	MISREP/ IMINTREP
A Coy	X	X	X	X	O	X	X	O
B Coy	X	O	O	O	O	X	X	O
C Coy	X	O	O	O	O	X	X	O
Recce Coy	X	X	X	O	X	X	X	X
UNMO	O	X	X	O	O	O	X	O
ISR TF xx	X	X	X	O	X	X	X	X
MALE UAS	O	O	O	O	O	O	X	X

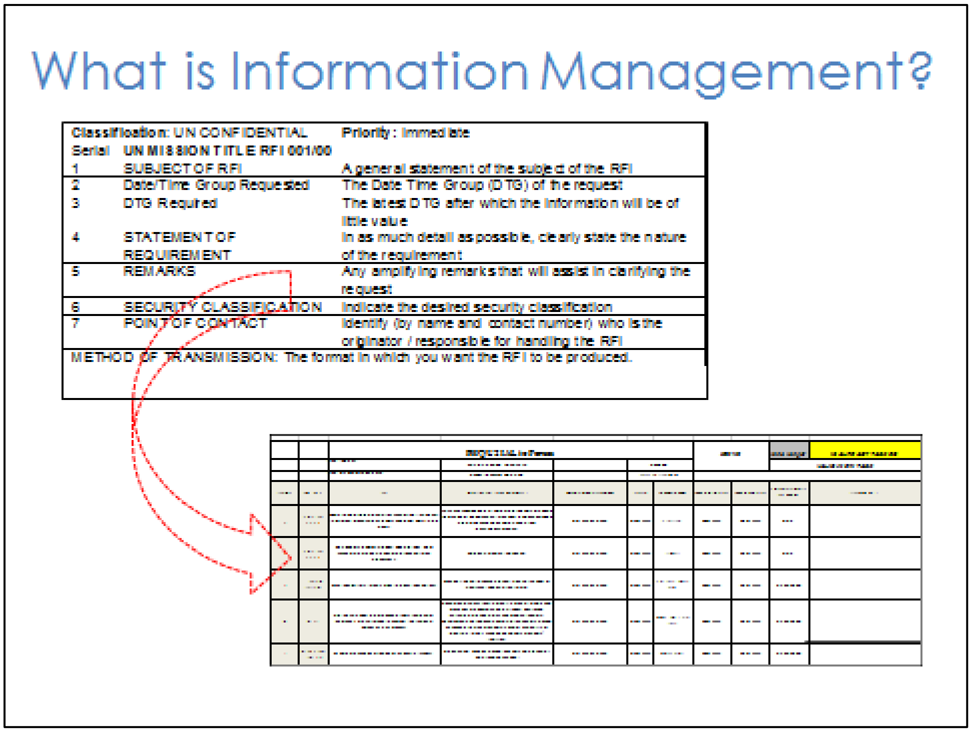
Key Message. Information management is the process designed to ensure that operational intelligence reaches those who need it, efficiently and promptly, while units and assets are exploited to optimum effect.

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

Intelligence IM responsibilities include:

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

Slide 15



What is Information Management?

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

Key Message. Communication between the two entities is essential to ensure the most effective employment of what are finite resources.

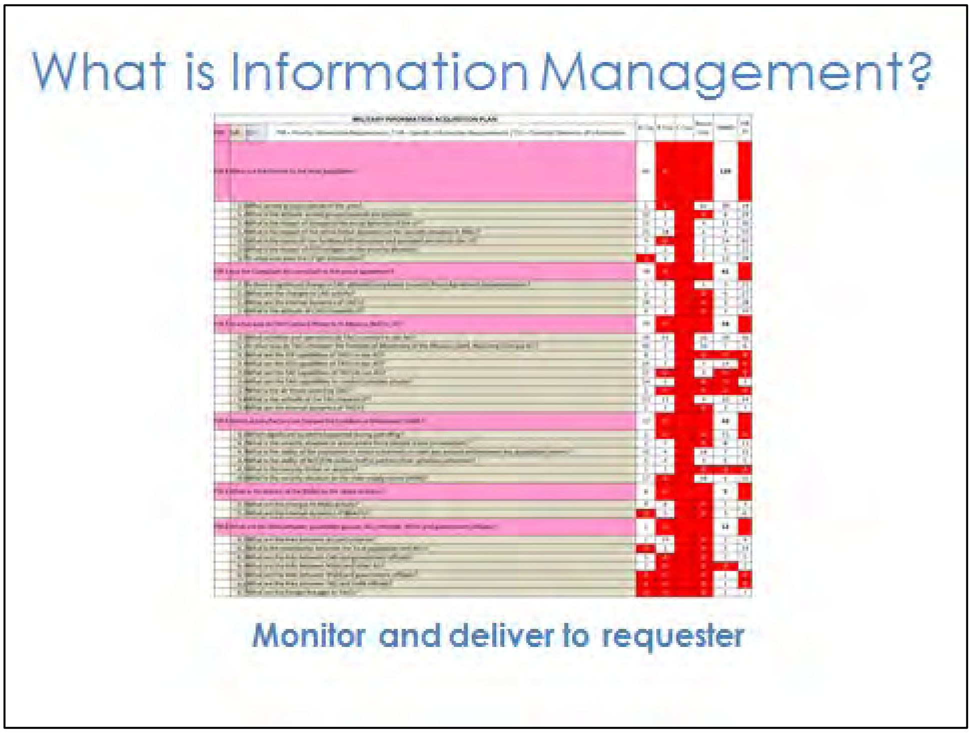
There are two sides to the management of IR, Intelligence Requirements Management (IRM) and Acquisition Management (AM). The IRM part deals with the RFIs and manages the IAP whereas the AM side deals with the planning and tasking side of the operation.

The RFI Manager's first task is to review each RFI received to ensure that all information has been filled out correctly by the customer. Essential elements of the RFI include a location of where the acquisition is required in as much detail as possible, ideally with geolocation included, date and time that the information is required by and how the information is to be disseminated. This is particularly important for requests to support activity that will require real-time updates. For example, a UAS overwatching of a convoy must include the ability to communicate with the convoy. If the UAS team observe an IED being set up ahead of the convoy, then there must be a means to warn the convoy of the activity. RFIs without dissemination information must be rejected and returned to the customer to be updated.

Once the manager has accepted the RFI, the first task should be to determine if the information already exists. One of the fundamental principles of Acquisition is to "acquire once, use many", meaning that instead of acquiring new information against every request, if the answer already exists then this should be sent to the customer to determine if it meets their needs. It is recognised that in some missions, it will be a challenge to know if the information already exists, but if databases are in use, this will be the place to check.

If the information does not exist already, the RFI Manager should consult the IAP to determine if the RFI relates to any of the EEIs, which will assist in the **prioritisation** process. If the RFI is a PKI request that does not relate directly to an EEI, then the topic should be recorded and when the IAP is updated this information should be reviewed to determine if the IAP properly reflects the mission's PKI requirements. RFIs should not be rejected if they do not relate to EEIs, there will be times when the capabilities are required for operational purposes rather than PKI. It is, however, important to track the operational use of assets to assess over time if the mission is focused on closing PKI gaps.

Slide 16



What is Information Management?

MILITARY INFORMATION ACQUISITION PLAN

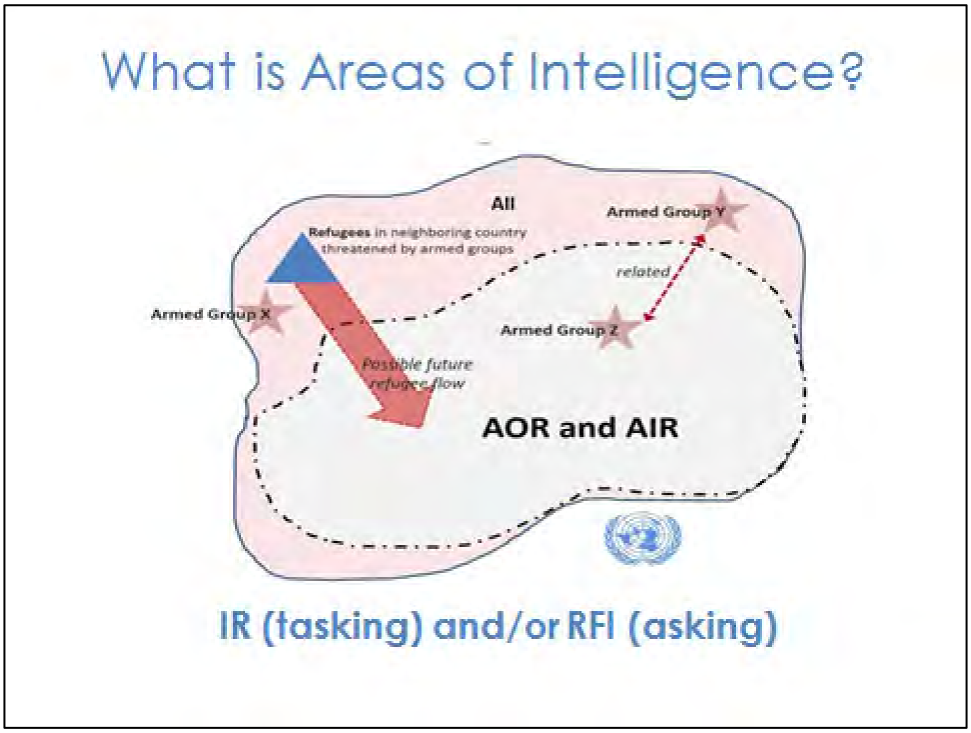
Monitor and deliver to requester

Key Message: Once the IR has been answered in accordance with the IAL, the next step within the process is to receive a report from acquisition units.

In all instances, information acquisition authorities must receive generated products to allow the update of the IAP. Where the IR related to an EEI or I&W, the verified completion of the task can be done by an acquisition manager. If an RFI generated the IR, then only the demander can confirm if the response meets their requirement.

One of the most important functions of an Information Manager is to ensure that all relevant information is disseminated to the right organisations at the right time. This is particularly the case with threat reporting and Indicators & Warnings but applies to all intelligence. Handling the dissemination effectively requires experienced oversight and collation of incoming reporting with the experience to understand who needs to see what elements of information.

Slide 17



What is Areas of Intelligence?

AII
Armed Group Y
Refugees in neighboring country threatened by armed groups
related
Armed Group X
Armed Group Z
Possible future refugee flow
AOR and AIR

IR (tasking) and/or RFI (asking)

The Operating Environment is that geographical area (including the physical elements, the information environment and actors) that has been given to a Commander in order for him to conduct his given mission within the context of a UN Mandate. There are 2 sides to the management of Acquisition: Peacekeeping-Intelligence Requirements Management (IRM) and Acquisition Management (AM) as described earlier in this lecture. The IRM part deals with the RFIs and I&W and manages the IAP, whereas the AM side deals with the planning and tasking side of the operational coordination. Communication between the 2 entities is essential to ensure the most effective employment of what are finite resources.

The effective acquisition greatly depends on the clarity of requirements to ensure that resources are used most effectively. Experience suggests that some requirements warrant one specific type of acquisition, whereas others may require several different types of acquisition. It is important to highlight that PKMI acquisition can be broken down into two types, IR and RFI.

Area of Intelligence Responsibility (AIR). The AIR is an area allocated to a commander, at any level, in which he is responsible for intelligence production. This area is limited to the range of his organic collection assets. If deemed necessary, it is possible to task multiple Company patrols through IRs and also request support from a higher formation – perhaps one that owns a specific capability such as a UAS – through an RFI.

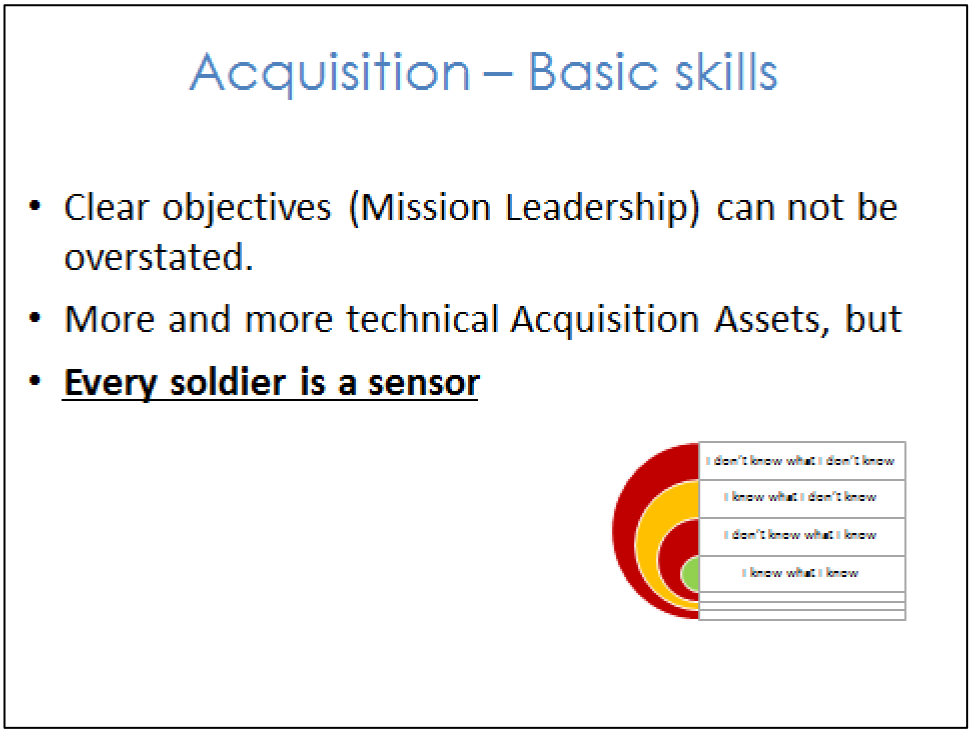
RFI: When a level is unable to fully, or partially fulfil a requirement, they can use RFI to neighbouring units or higher levels.

Area of Intelligence Interest (AII). The AII is an area in which a commander requires intelligence on those factors and developments likely to affect the outcome of his current or future operations. This is an area beyond the control of a Commander and is outside of his AIR, but one that has relevance to the conduct of the Commander's mission and therefore must be considered and evaluated. It is important to note that more than one acquisition capability can be applied against a requirement.

- An IR where the PKMI entity owns the capability required to acquire the information. The acquisition assets are considered organic to the organisation. e.g. a Battalion S2 tasking a Company patrol

- An RFI is made when the PKMI entity does not own the assets required to acquire the needed information, and thus must send an external request to another part of the PKMI architecture in the form of an RFI. All RFIs must receive a response, even if it is a nil response from those asked

Slide 18



Acquisition – Basic skills

- Clear objectives (Mission Leadership) can not be overstated.
- More and more technical Acquisition Assets, but
- **Every soldier is a sensor**

I don't know what I don't know
I know what I don't know
I don't know what I know
I know what I know

The phrase 'Every Soldier is an acquisition sensor' is key to the success of UN acquisition. Soldiers may acquire information through patrolling, through the manning of observation posts, by conducting base security patrols and during most routine operational activity.

Further information may be acquired if they positively interact with the local population. Therefore, the Force Intelligence Acquisition Plan (IAP) must be communicated to all personnel in a manner that makes it understandable. For example, broad, strategic PIRs should be broken down into questions that everyone will understand, as shown in the chapter on the direction.

Slide 19

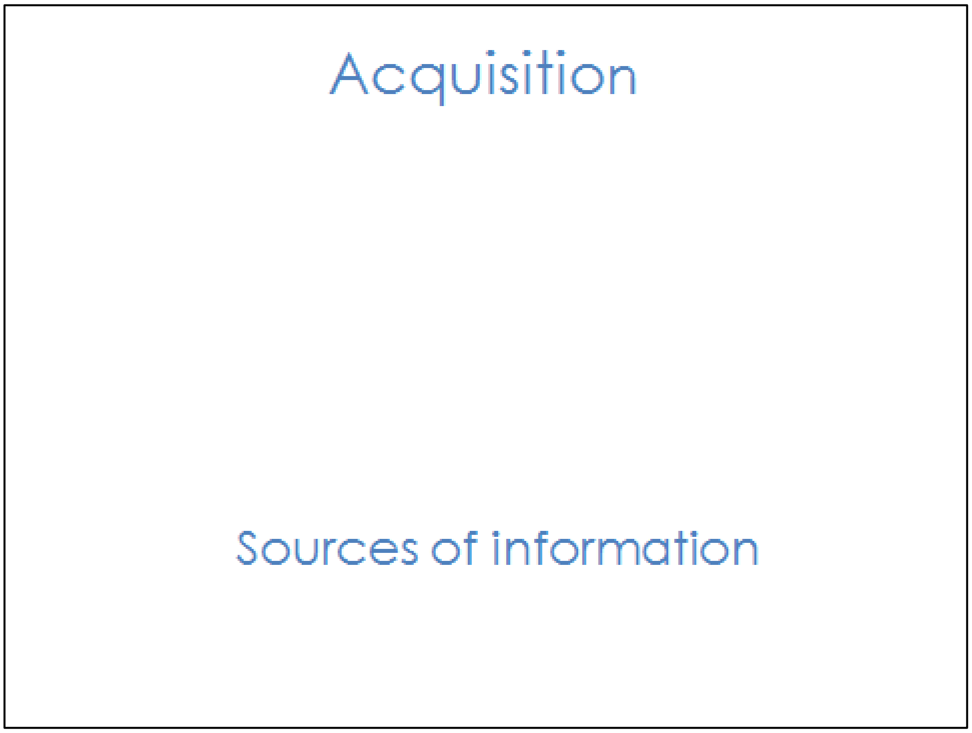
I don't know what I don't know

I know what I don't know

I don't know what I know

I know what I know

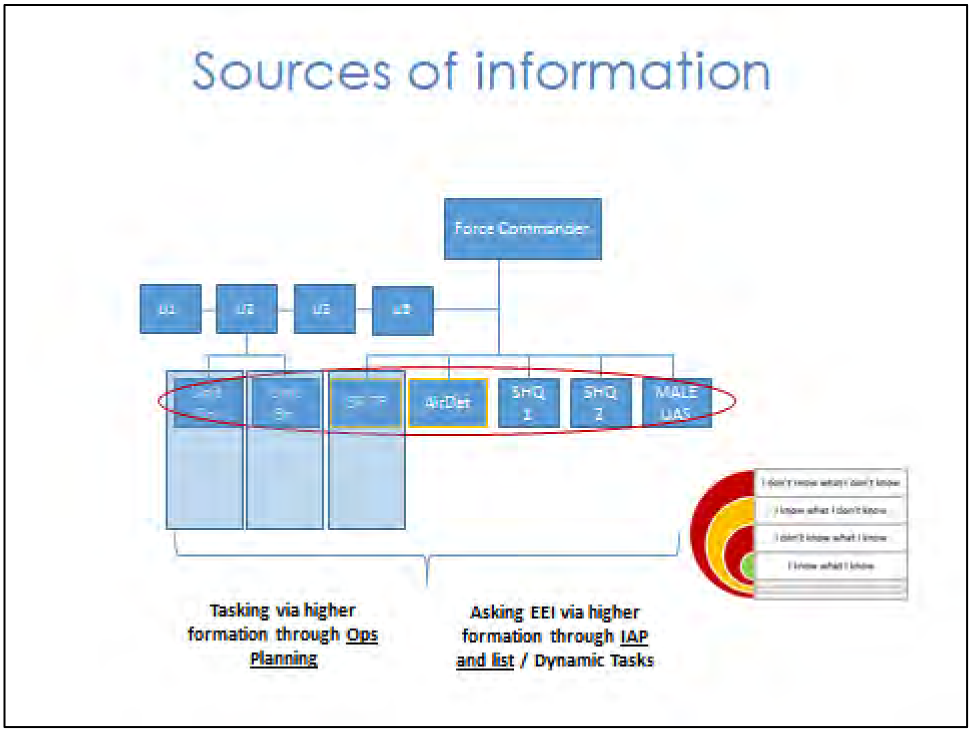
Slide 20



Acquisition

Sources of information

Slide 21



Sources of information

Tasking via higher formation through Ops Planning

Asking EEI via higher formation through IAP and list / Dynamic Tasks

Key Message: The various acquisition capabilities that are controlled have their own procedures and methods appropriate to the exploitation of their sources. Planning and liaison are key terms of success.

Source of Information. There are three types from which information can be obtained, and these are listed below:

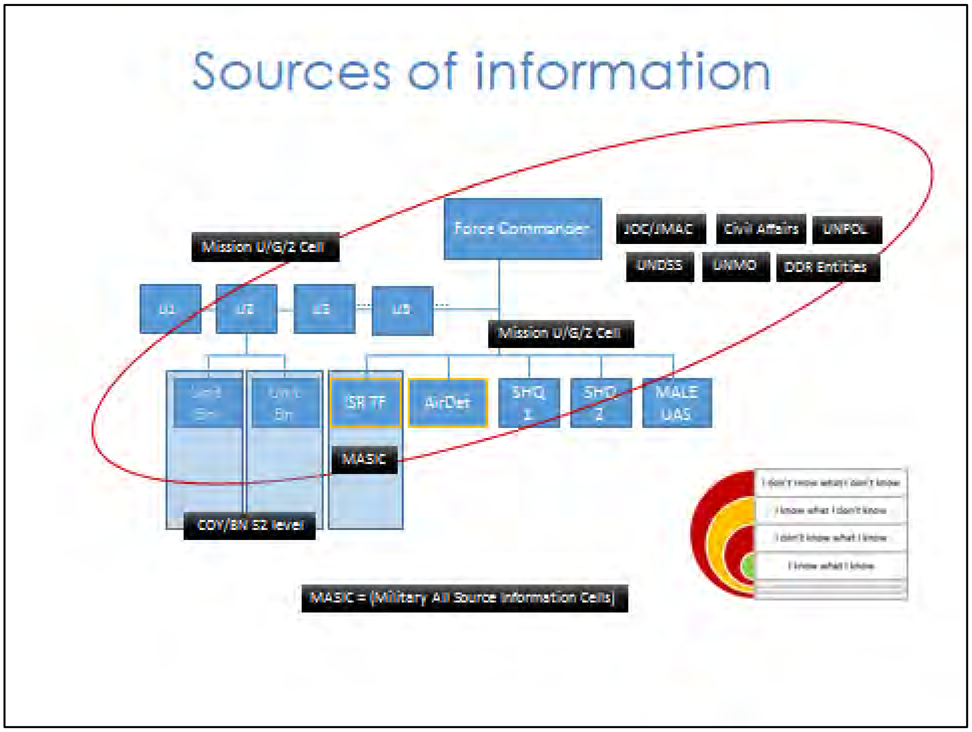
- Controlled. Units or assets which can be tasked by an Acquisition Management Officer (or ISR) officer to provide answers to his questions
- Uncontrolled. Units, assets, sources or agencies which provide information, but an ISR officer has no control over them. (can only 'ask', not 'task')
- Casual. Sources or agencies which may or may not be known to exist and which provide useful information unexpectedly

The slide above shows an organigram of controlled sources. The principal controlled units and assets available to an Acquisition officer at a higher command level in UN field formations are:

- Observation posts.

- Foot patrols.
- Reconnaissance patrols.
- Aircraft.
- Surveillance devices and sensors, both ground and airborne

Slide 22



Sources of information

Key message: Good communication is the single most important factor that will underpin success in managing Acquisition. The communication within the U2 section filling the various roles, communication between the U2 and the customers, and, critically, communication with the mission's leadership helps to ensure that priorities are very well understood.

The exploitation of sources of information by collection units and assets and the delivery of this information to the proper intelligence processing unit for the use is important in the production of intelligence and processed periodicals.

The exploitation of other controlled sources of information by collection units and assets, and the delivery of this information to the proper intelligence processing unit for the use in the production of intelligence and processed periodicals. In formatting, a collection strategy collection staffs will normally rely on controlled units and assets to obtain their Priority Intelligence Requirements (PIRs) within the specified time limit.

Information from uncontrolled sources will normally be received in the form of intelligence summaries from higher formations, or reports from specialist agencies, which is of value in preparing assessments or intelligence estimates. Information from casual sources is unpredictable, and in the absence of collateral information or confirmation from a reliable source, it is difficult to establish its authenticity

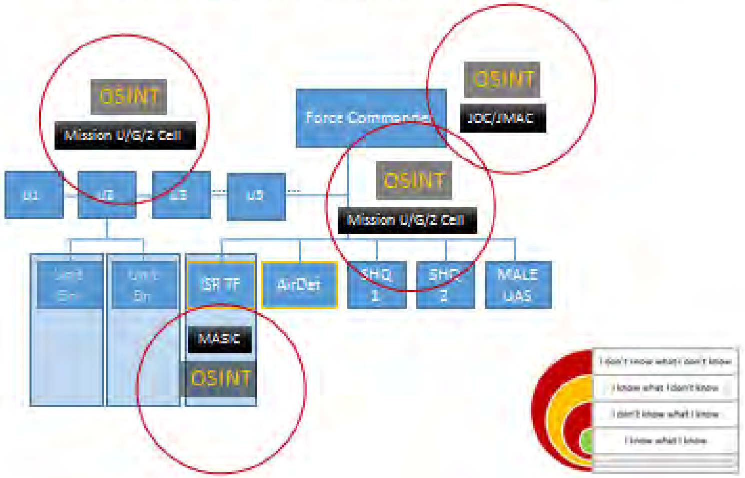
The principal controlled units and assets available to an Acquisition officer at a higher command level in UN field formations are:

- Dissemination JOC/JMAC products.
- Dissemination PKMI (U2/G2/S2) products.
- Civil Affairs, UNPOL, UNMO, UNDSS, DDR entities products.

The synchronisation with other collection at field level and/or flanking units, SF, FHT (Humint) is important.

Slide 23

Sources of information



Key message: Acquisition/IRM/CM officers at all levels must recognize potential uncontrolled sources (such as new publication or broadcast on a new wavelength) and arrange for the recording and reporting of such information through the correct channels so that the source can be exploited.

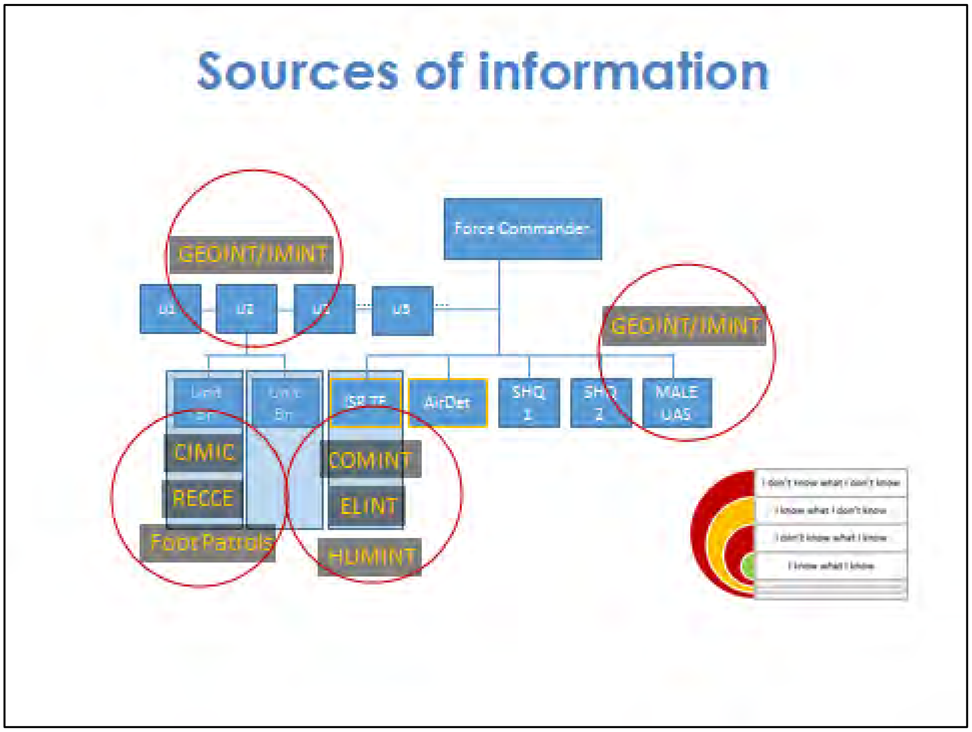
The Uncontrolled Sources. In general, uncontrolled sources consist of written material of all sorts and radio or television broadcasts, relating to forces and areas of operations, actual or potential, which may contain useful information, and so cannot be ignored. Examples of this are:

- Newspapers and periodicals - containing details of personalities and current events, or political and economic developments
- Maps, Charts, town plans, guidebooks, directories and tide tables - containing detailed topographical information
- Annual reports of commercial concerns, state-owned and private commercial agencies, international enterprises etc. - containing indications of industrial and economic capabilities, growth and development potential
- Scientific and technical journals and papers - containing detailed studies of activities in their respective fields
- Reference books - containing a variety of detail, from lists of naval vessels and aircraft types to the professional, technical and academic qualifications and positions held by individuals

- Monitored radio broadcasts - containing information on current events, future intentions, morale and administration, in general

Open Source information (OSINT) section must exist at U2 and G2 level. If manpower is enough, S2 and C2 sections should also endeavour to establish such a section. If this is not possible, both the S2 and C2 sections should request a daily Open Source summary from Higher HQ. Ideally, the Open Source section should focus on the region, the country, and then on individual sectors

Slide 24



Sources of information

The acquisition should be a "System of Systems" approach to the employment of acquisition assets. This requires the assets to be used as a holistic entity rather than as a series of stovepipes. It seeks to provide a robust mix of assets at each level of command and to ensure the essential interplay between them, avoiding reliance on any one type of asset.

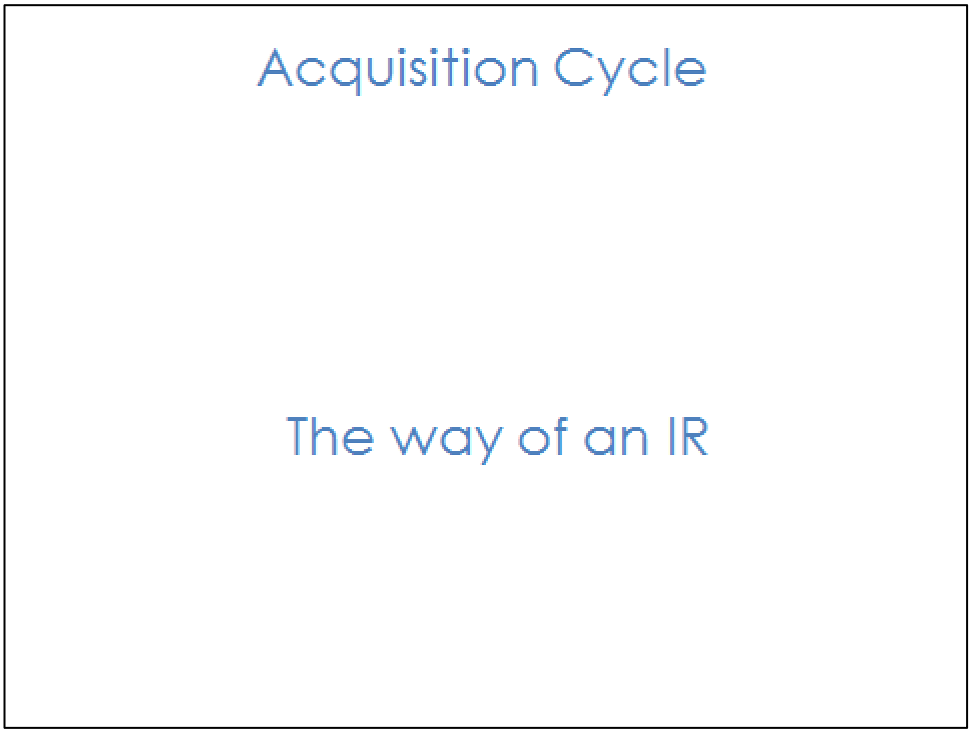
Within the Land Component, ground-based manned reconnaissance is now considered to be a core capability at each level of command. This combined with other systems such as Unmanned Aerial Systems (UAS), Communication interception (COMINT/ELINT) and Human Intelligence (HUMINT) within an ISR TF, provides the ingredients for this robust mix.

Slide 25

I don't know what I don't know
I know what I don't know
I don't know what I know
I know what I know

.

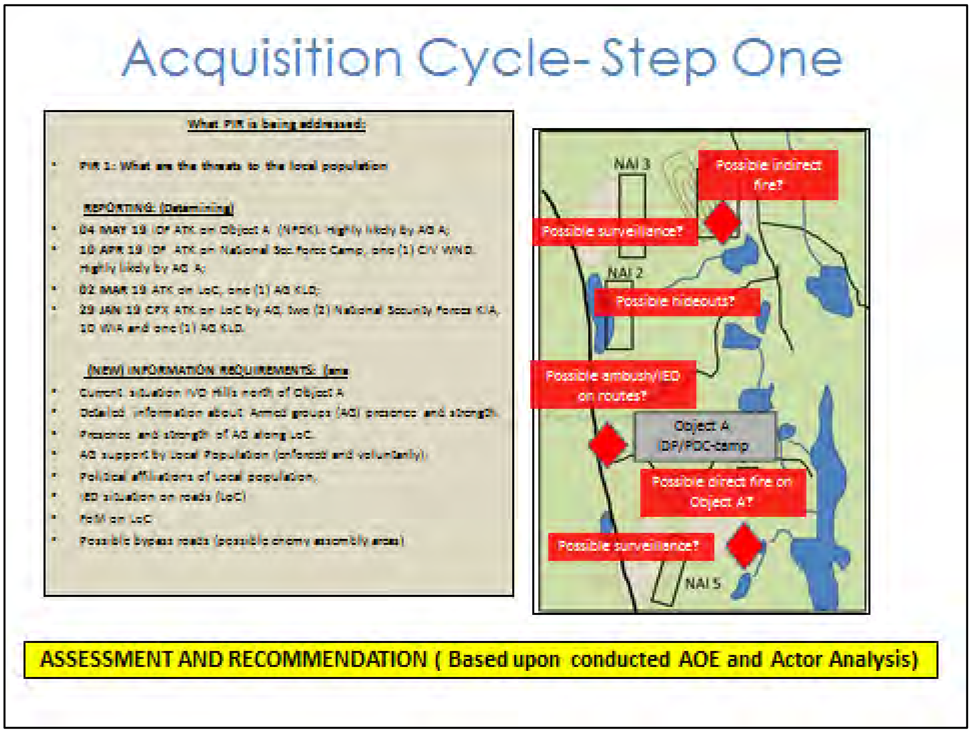
Slide 26



Acquisition Cycle

The way of an IR

Slide 27



Acquisition Cycle- Step One

What PIR is being addressed:

- PIR 1: What are the threats to the local population

REPORTING: (Determining)

- 04 MAY 19 IDF ATK on Object A (NPDK). Highly likely by AG A;
- 10 APR 19 IDF ATK on National Sec.Force Camp, one (1) CIV WND. Highly likely by AG A;
- 02 MAR 19 ATK on LoC, one (1) AG KLD;
- 29 JAN 19 CPX ATK on LoC by AG, two (2) National Security Forces KIA, 10 WIA and one (1) AG KLD.

(NEW) INFORMATION REQUIREMENTS: (ans

- Current situation IVO Hills north of Object A
- Detailed information about Armed groups (AG) presence and strength.
- Presence and strength of AG along LoC.
- AG support by Local Population (enforced and voluntarily).
- Political affiliations of local population.
- IED situation on roads (LoC)
- FoM on LoC
- Possible bypass roads (possible enemy assembly areas)

ASSESSMENT AND RECOMMENDATION (Based upon conducted AOE and Actor Analysis)

Step One: is a review of available information to see which IRs can be satisfied with information already stored on file by the mission. This is often referred to as basic or current information or intelligence. It should be noted that there will be few occasions that IRs can be entirely satisfied with information already on file.

When there is insufficient data available to answer the intelligence requirement, the new acquisition must occur. Those information requirements that cannot be satisfied are then collated and laid out in a logical sequence that will form the basis of the Intelligence Acquisition Plan.

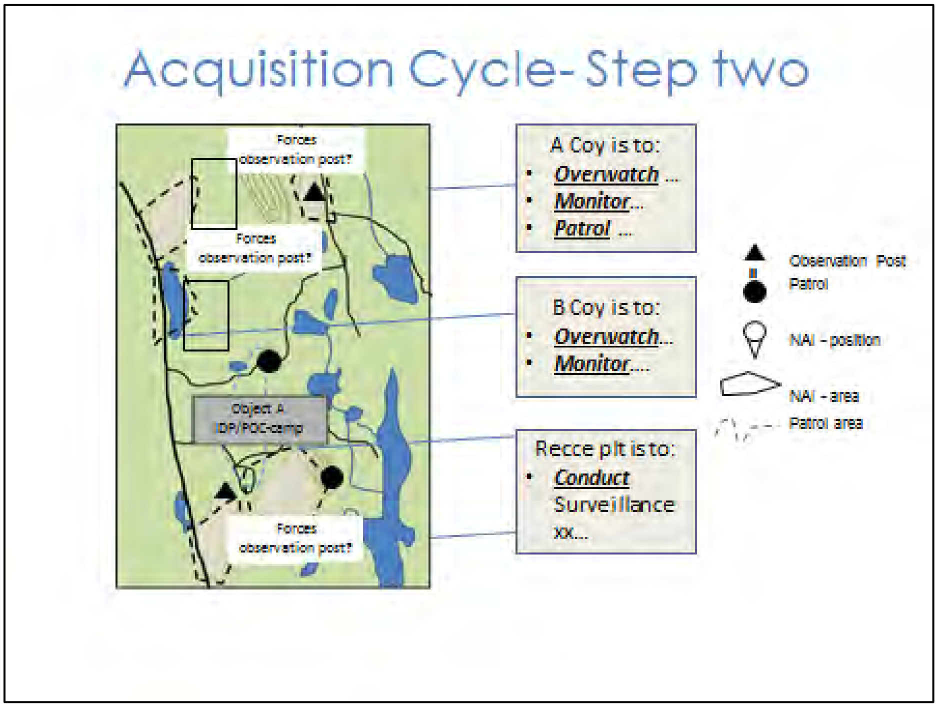
After ascertaining that there is no data available the requirements and according to priority, the next step is to the task of the data or information acquired, which is required to feed the Analytical step of the cycle.

Due to weak presence of Nation Security Forces and a total absence of Mission forces, it is highly likely AG will expand their influence in the area IVO Object A. Other camps in AOR and the Mission convoys along LoC will highly likely be attacked continuously, as long as AG possesses FoM.

Hence, the Mission has to employ forces into the area IOT:

- Gather information about the current situation with the main focus on AG & TAG activities and FoM along LoC
- Gather information on AG presence and political affiliation of Local population
- Link up with local authorities and Nations Security Forces
- Show presence towards LP

Slide 28



Acquisition Cycle- Step two

A Coy is to:

- ***Overwatch*** ...
- ***Monitor***...
- ***Patrol*** ...

B Coy is to:

- ***Overwatch***...
- ***Monitor***....

Recce plt is to:

- ***Conduct*** Surveillance xx...

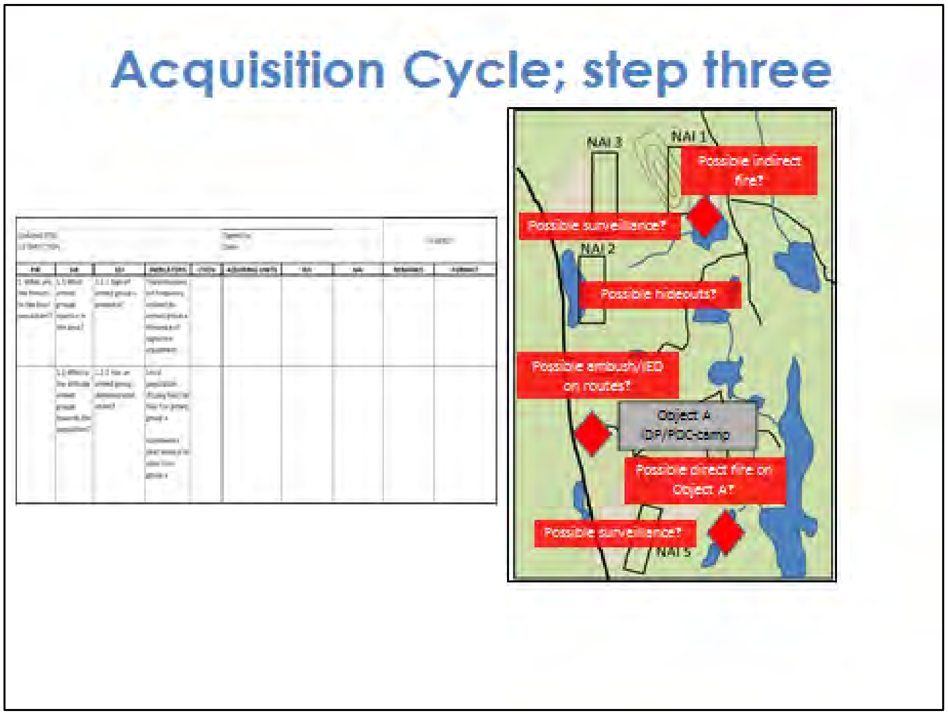
▲ Observation Post
● Patrol
NAI - position
NAI - area
Patrol area

Key Message. The exploitation of acquisition assets (units) is often recognised through MDMP, the operation planning, ending up in an operations order/ Frag O via the mission U/G/S3 section including Air Ops sections.

Step two: is an Assessment of the Operating Environment that provides a general indication of the location to which acquisition assets need to be deployed to gather the necessary information. These areas are often referred to as Named Areas of Interest (NAIs). The acquisition process also includes the identification of the assets that can most effectively meet the various Information Requirements. The acquisition assets are tasked through an operations order via the mission U/G/S3 section. Remember: the acquisition assets are then tasked through via mission U/G2 Branches or S2 input, such as IAP or the extract IAL. Examples are followed below.

If subordinate units are using sources, then all sources must be registered with higher HQ. This avoids circular reporting.

Slide 29



Acquisition Cycle; step three

Key message: Close coordination and good communication between Acquisition Manager, IRM Manager and the Intel Function Direction, who direct the IR s.

Step three: The U2 cell or subordinate PKMI cells should take the IAP, which lists all PIRs, IRs, SIRs, and EEIs on the left-hand side of a spreadsheet or word document, and should then list all controlled (military sources) in columns to the right-hand side. This should be done in conjunction with the U3 cell.

In conjunction with the U3 cell, controlled, subordinate units (depending on the mission assets, structure, role, SOPs, and mandates, these units can include: HUMINT, SIGINT, IMINT, Air assets, ISR units, and all military formations), are tasked to acquire specific information, based on their unique capabilities.

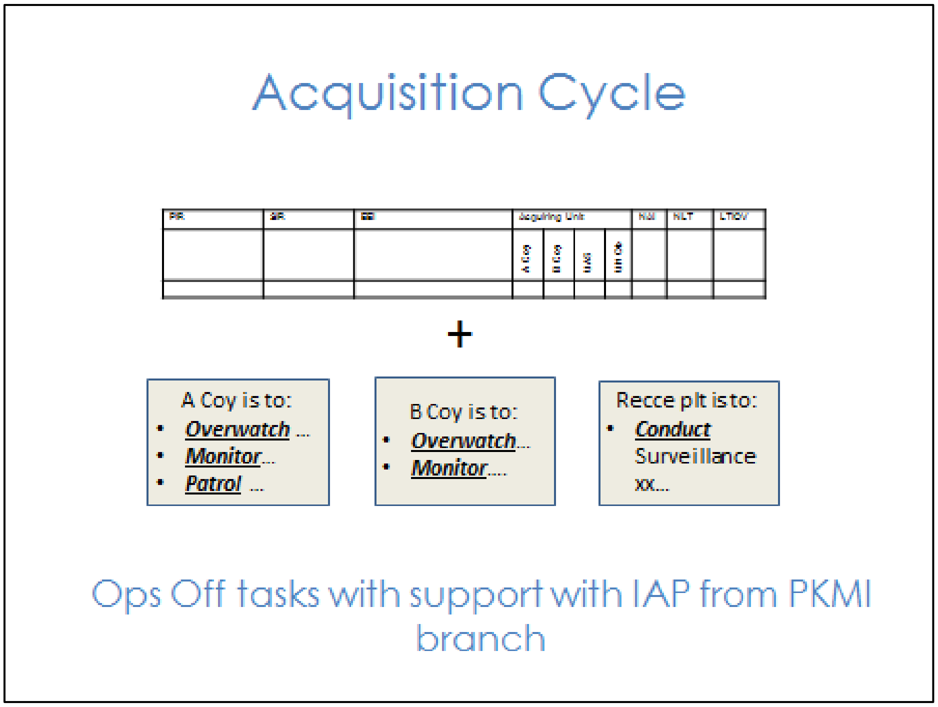
Often the IAP will task several units to collect the same information. This is done to ensure that high-priority information is collected and to ensure that information is not just a single source.

Units that are tasked to collect information should be represented on the Force-level IAP with a simple tick or another symbol. This will allow the information acquisition manager to follow-up on acquisition taskings. A simple example of a completed Force – level IAP is shown below.

If subordinate units are using sources, then all sources must be registered with higher HQ. This avoids circular reporting.

Information Requirements, however, will not normally be passed directly to units and assets. Rather, as outlined in the direction chapter, each will be broken down into smaller, more Specific Information Requirements (SIRs) and Essential Elements of Information (EEIs) or Indicators & Warnings. It will be these SIRs, EEIs, and/or indicators which the units and assets will be expected to look for. All acquisition assets and resources must be placed into a single plan to capitalise on different capabilities. This plan is known as the Force-level Intelligence Acquisition Plan (IAP). The plan synchronises and coordinates acquisition activities. A good information acquisition plan fits into and supports the overall operations plan or order.

Slide 30



Acquisition Cycle

PIR	SIR	EEI	Acquiring Unit				NAI	NLT	LTIOV
			A Coy	B Coy	[illegible]	[illegible]			

+

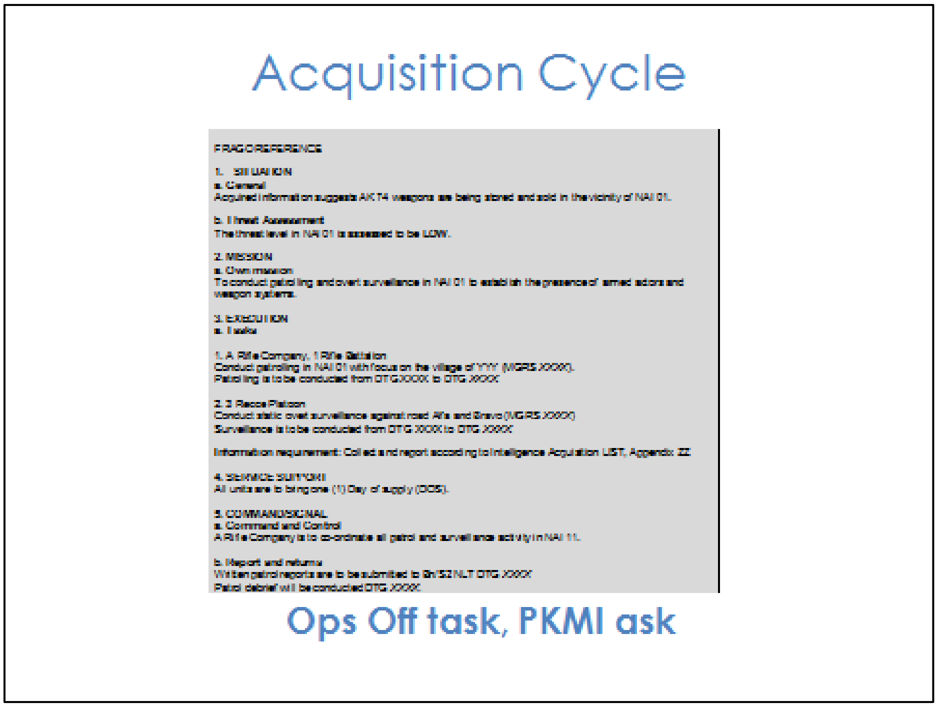
A Coy is to:
- ***Overwatch*** …
- ***Monitor***…
- ***Patrol*** …

B Coy is to:
- ***Overwatch***…
- ***Monitor***….

Recce plt is to:
- ***Conduct*** Surveillance xx…

Ops Off tasks with support with IAP from PKMI branch

Slide 31



Acquisition Cycle

FRAGO REFERENCE

1. SITUATION
a. General
Acquired information suggests AK 74 weapons are being stored and sold in the vicinity of NAI 01.

b. Threat Assessment
The threat level in NAI 01 is assessed to be LOW.

2. MISSION
a. Own mission
To conduct patrolling and overt surveillance in NAI 01 to establish the presence of armed actors and weapon systems.

3. EXECUTION
a. Tasks

1. A Rifle Company, 1 Rifle Battalion
Conduct patrolling in NAI 01 with focus on the village of YYY (MGRS XXXX).
Patrolling is to be conducted from DTG XXXX to DTG XXXX

2. 3 Recce Platoon
Conduct static overt surveillance against road Alfa and Bravo (MGRS XXXX)
Surveillance is to be conducted from DTG XXXX to DTG XXXX

Information requirement: Collect and report according to Intelligence Acquisition LIST, Appendix ZZ

4. SERVICE SUPPORT
All units are to bring one (1) Day of supply (DOS).

5. COMMAND/SIGNAL
a. Command and Control
A Rifle Company is to co-ordinate all patrol and surveillance activity in NAI 11.

b. Report and returns
Written patrol reports are to be submitted to Bn/S2 NLT DTG XXXX
Patrol debrief will be conducted DTG XXXX

Ops Off task, PKMI ask

.

Slide 32

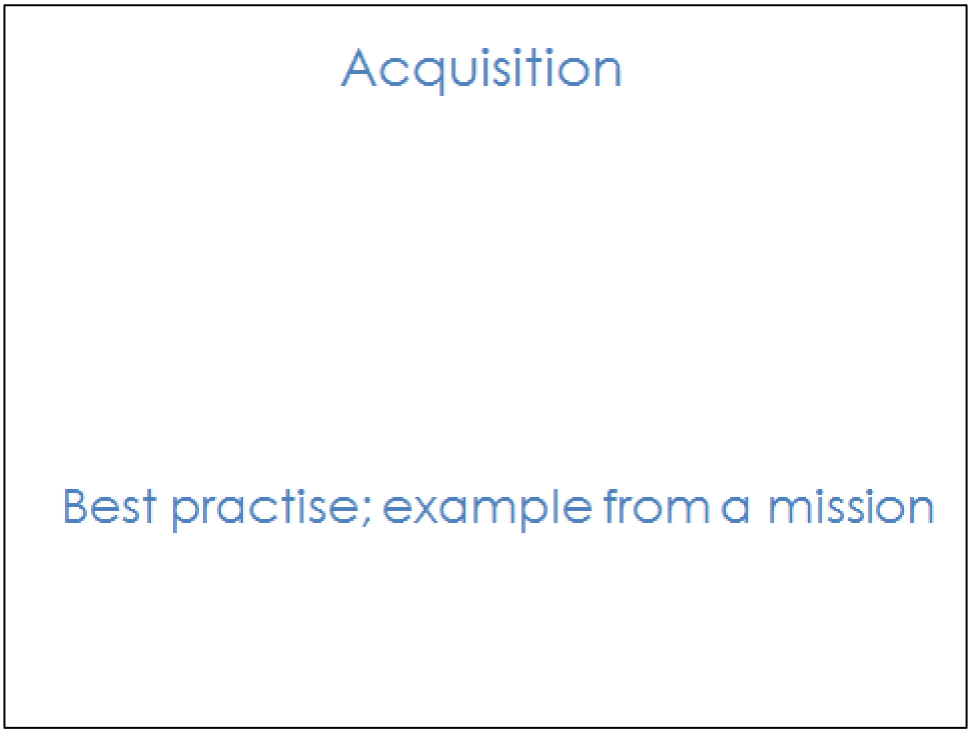
I don't know what I don't know

I know what I don't know

I don't know what I know

I know what I know

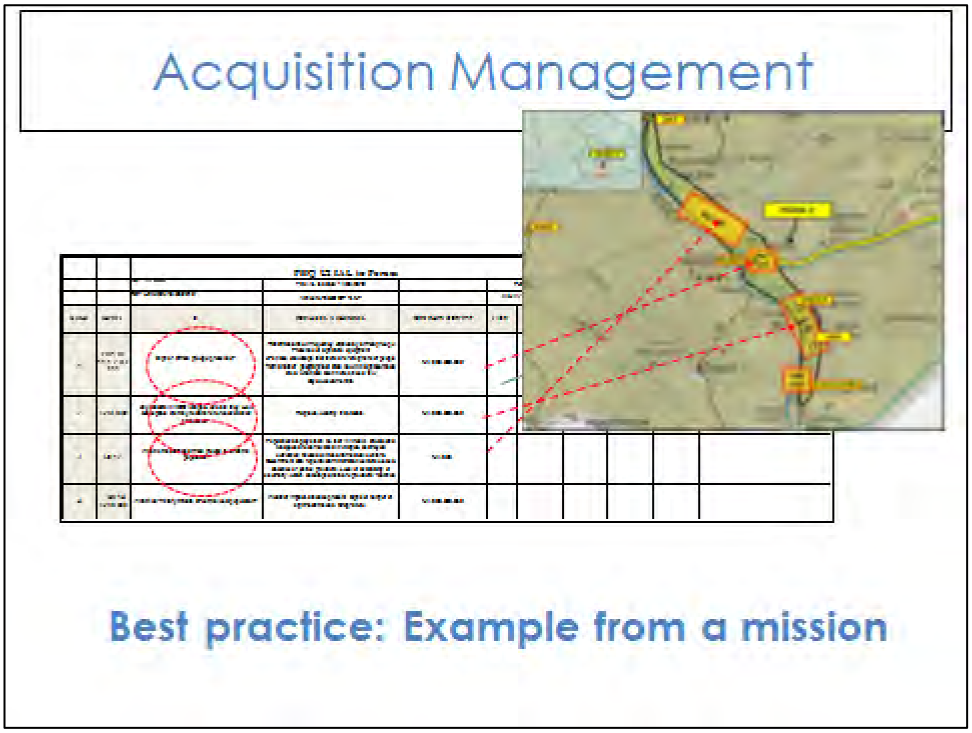
Slide 33



Acquisition

Best practise; example from a mission

Slide 34



Acquisition Management

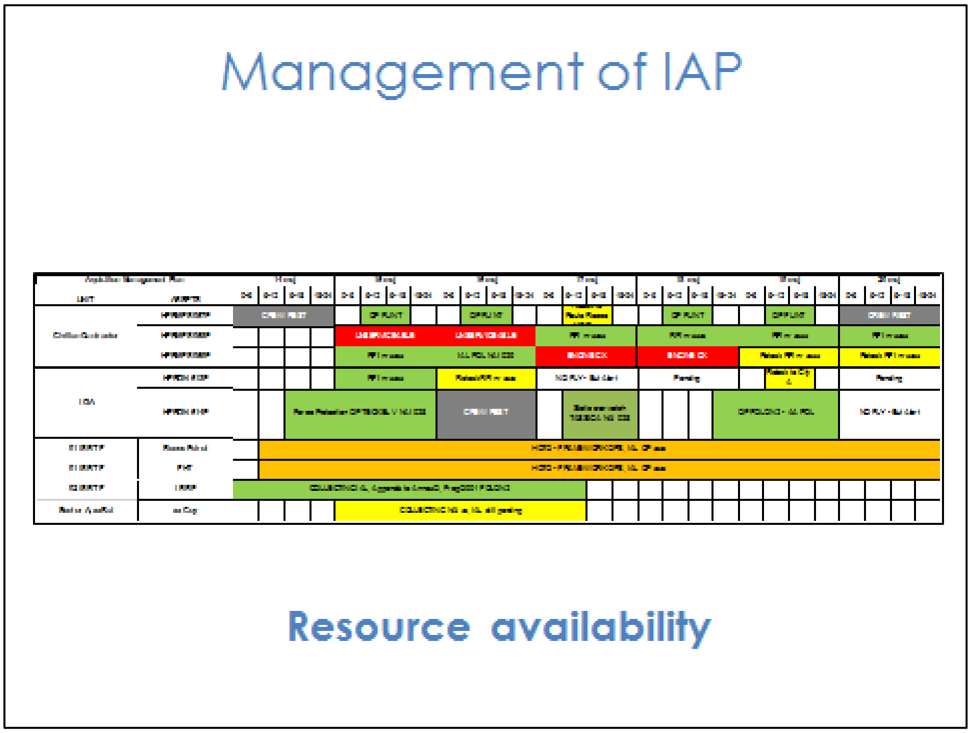
Best practice: Example from a mission

Key message: A good Acquisition fits into and supports the overall operations plan or order.

This example shows the IR that are highlighted within the example IAP. Each level must develop its own IAP, always incorporating the overarching requirements of the higher level(s). However, various levels will have individual differences depending on which actors are present in the operational area, the human terrain, and other factors.

The U2 Branch or subordinate MPKI cells should take the IAP, which lists all PIRs, IR, SIR and EEI on the left hand of a spreadsheet or word document and should then list all controlled (military sources) in columns to the right-hand side. This should be one in conjunction with the mission U/G3 Branch. It is good practice to link SIR, and EEI to geographic areas where information can acquire. As outlined, these areas are known as NAIs (Named Area of Interest).

Slide 35



Management of IAP

Resource availability

Key message: A helping tool to support best Practice in step two, all acquisition assets and other acquisition resources are included in a single plan to maximise the different capabilities. The plan synchronises and coordinates acquisition activities in the overall scheme of manoeuvre.

While many PKMI Acquisition resources will be the same across missions (e.g. UN Military patrols and observers) some acquisition capabilities will only be available in certain mission areas. The PKMI personnel must develop the fullest awareness of all the sources and agencies they can task with Acquisition.

The list above is a result of coordination at every staff level and especially between planning sections mission U/G2/S2. In conjunction with the U3 planning section, controlled, subordinate units (depending on the mission assets, structure, role, SOPs, and mandates, these units can include: HUMINT, SIGINT, IMINT, Air assets, ISR units, and all military formations), are tasked to acquire specific information, based on their unique capabilities.

An important aspect of the AM authority is that it allows the tasking of acquisition capabilities at higher, flanking or lower elements within the mission. For example, assets that might operate within a sector can be tasked by the Mission, U/G2 level as a result of the authority conferred AM.

This is not the tasking matrix, but an overview to support in producing the IAP. The spreadsheet is a result of inputs from