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.

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

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

© UN 2020

Integrated Training Service

Department of Peace Operations

United Nations

New York, NY, 10017, USA

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

M o d u l e
1

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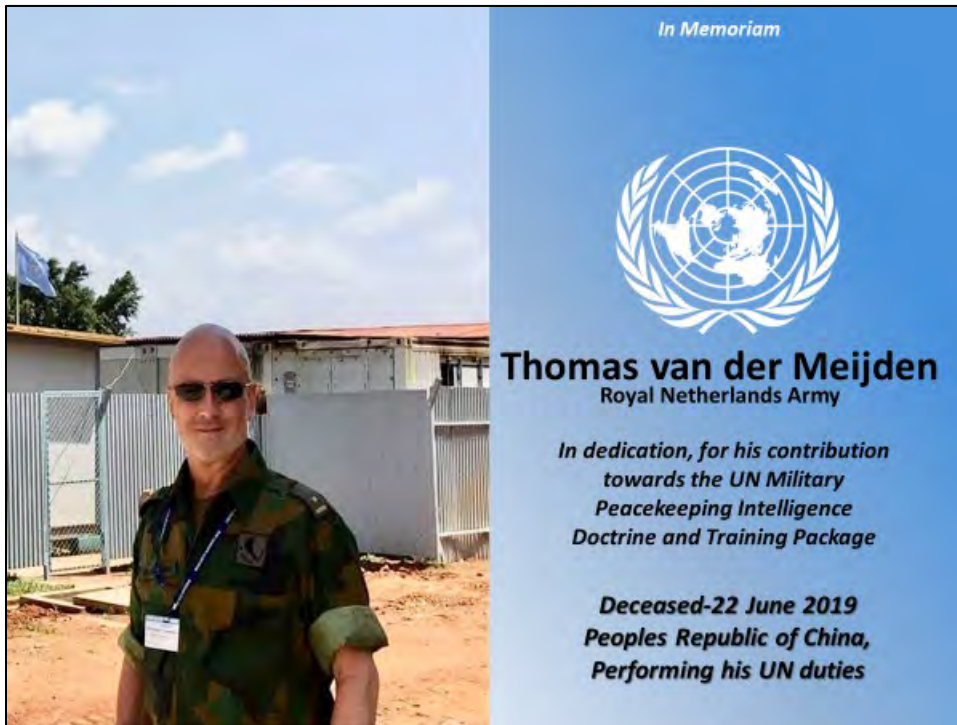
Thomas was a true professional who was involved in the early stages of development of the Military Peacekeeping Intelligence handbook and training materials. His broad experience enabled him to actively support other Peace Operation projects. Our heartfelt thoughts go to his family and friends; Thomas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

Slide 2

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

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.
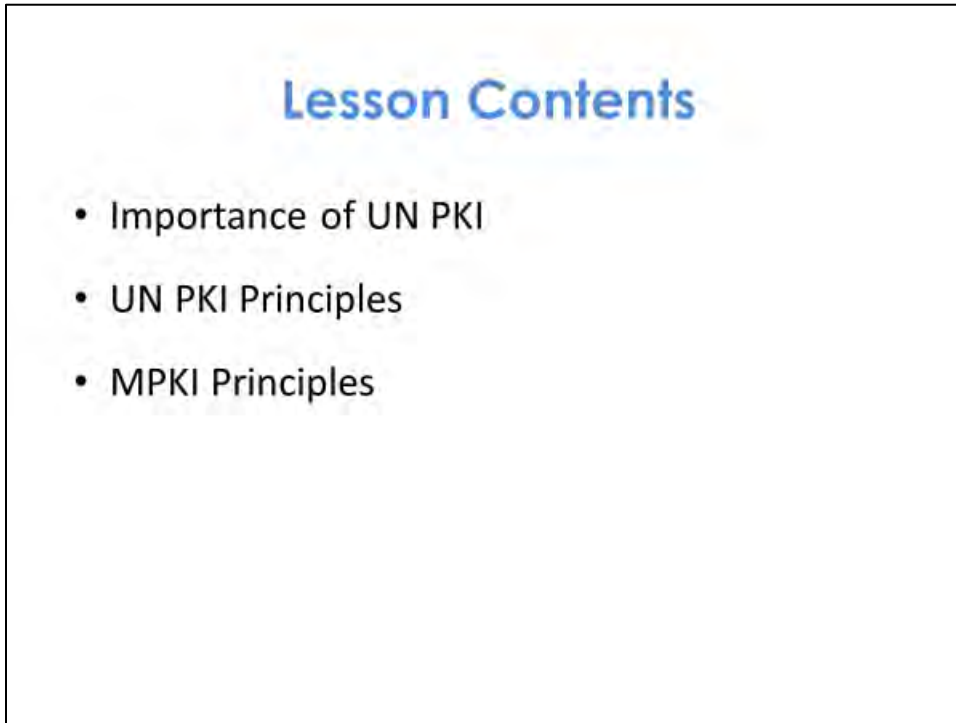
Slide 4

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.
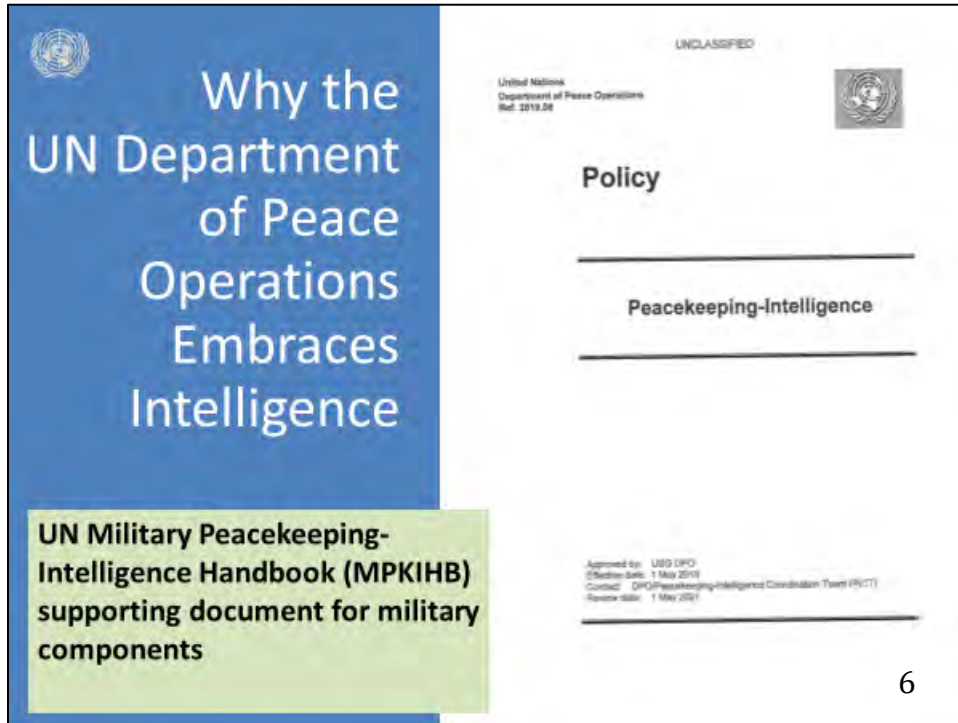
Slide 6

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

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.

Slide 13

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

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

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

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

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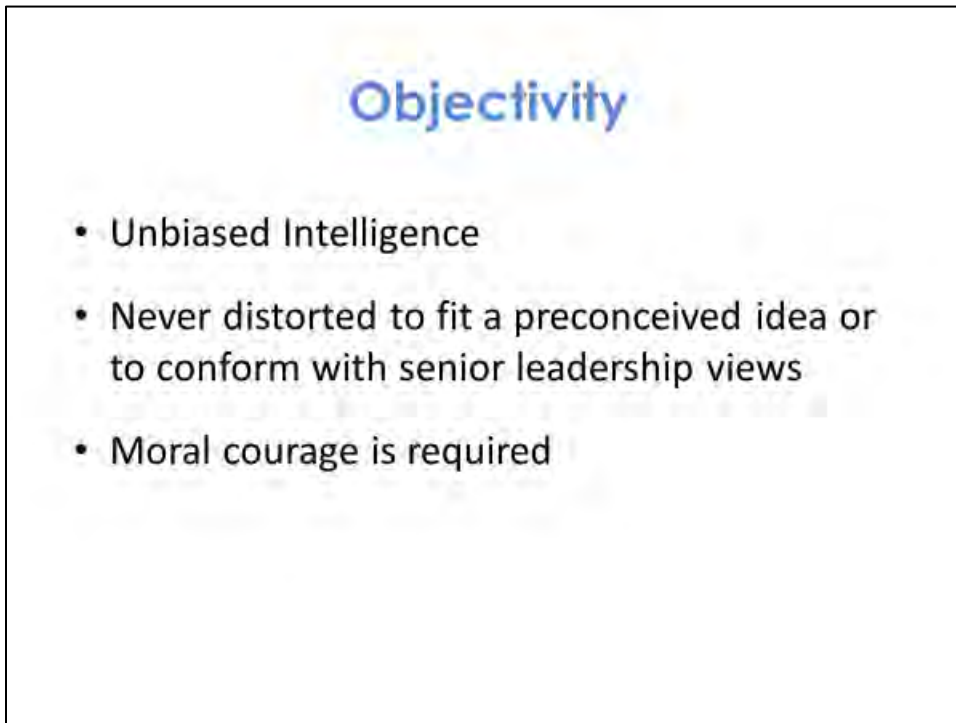
Centralised control also means that unwanted duplication of acquisition effort is avoided.

☞ *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

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

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

Slide 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.
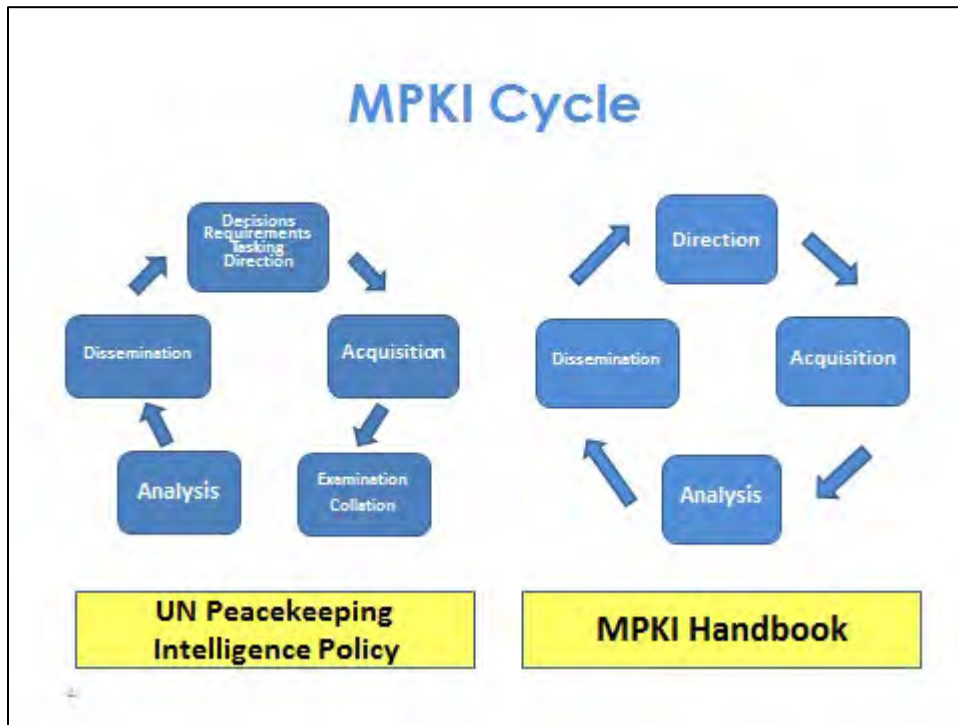
Slide 3

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

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

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

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

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

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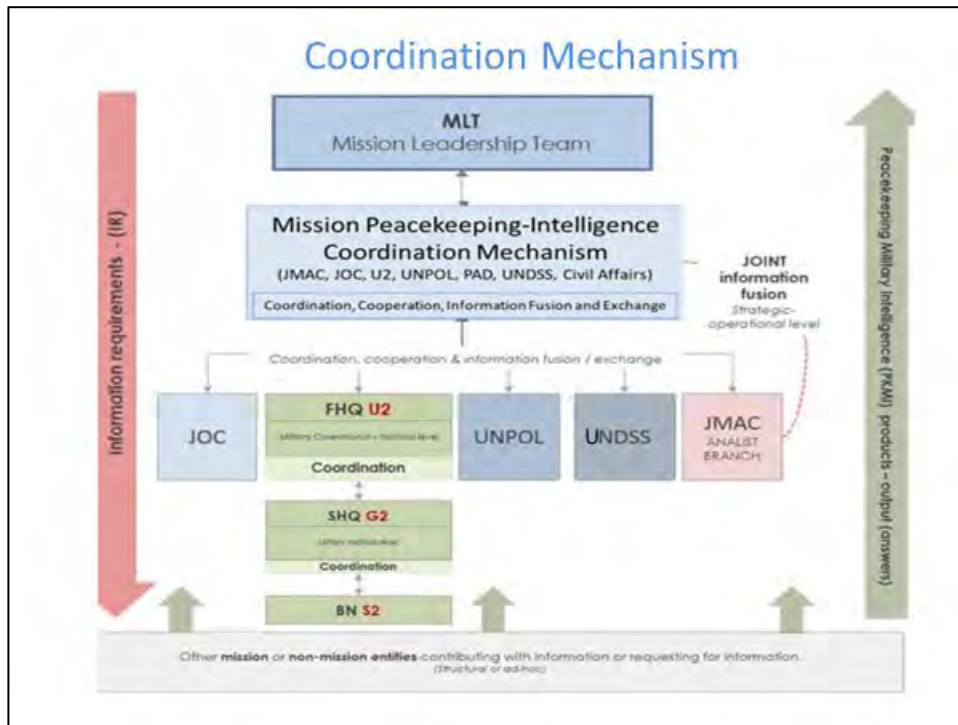
As you can see, there are various peacekeeping-intelligence entities in a UN peacekeeping mission, each with its own roles and responsibilities.

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 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

<div style="border:1px solid #000; padding:1em;">

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
</div>

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.

L e s s o n
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

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

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

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

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.

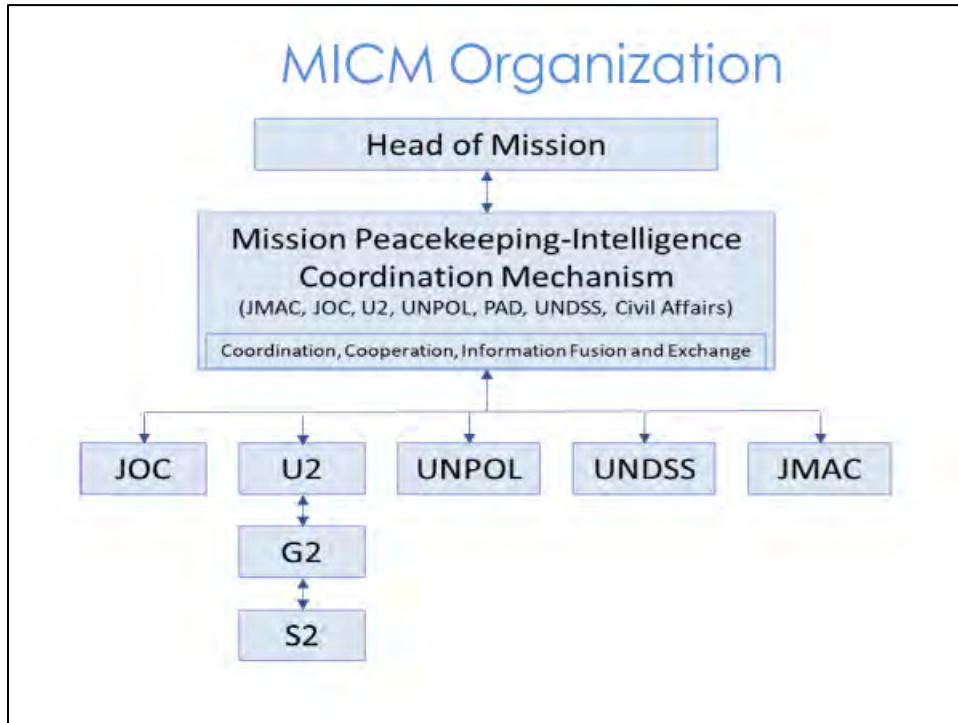**Slide 7**

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

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

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
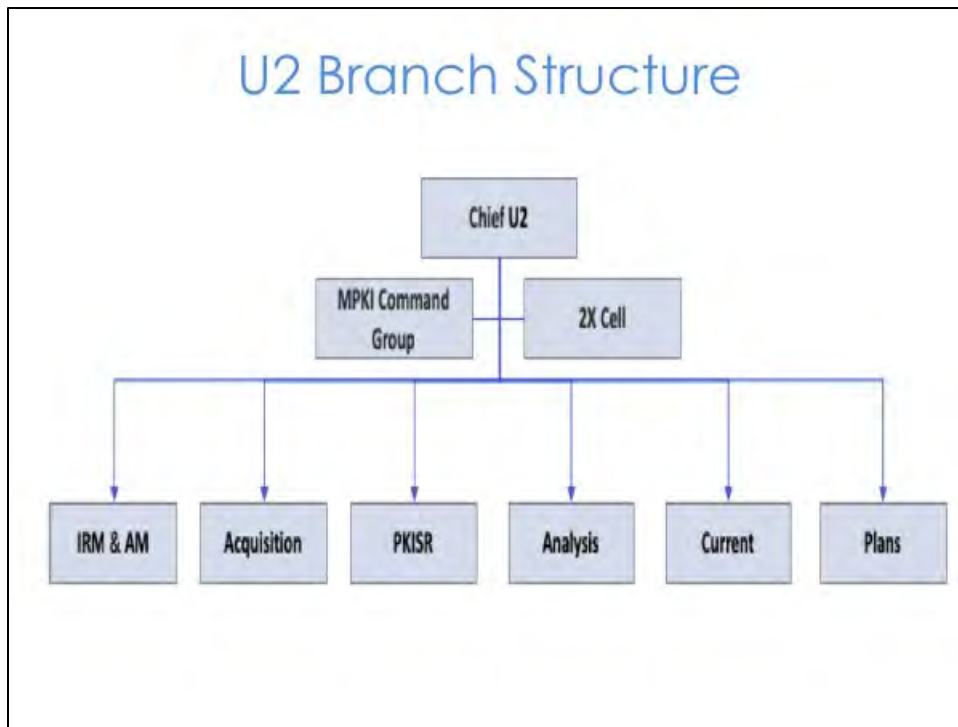
Key Message: The structure of the U2 Branch varies from mission to mission, but it is always part of the military component. The structure and staffing of the U2 cell will change according to the mission's mandate, the Status of Forces Agreement (SOFA) in place between the Host State and the UN, the 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
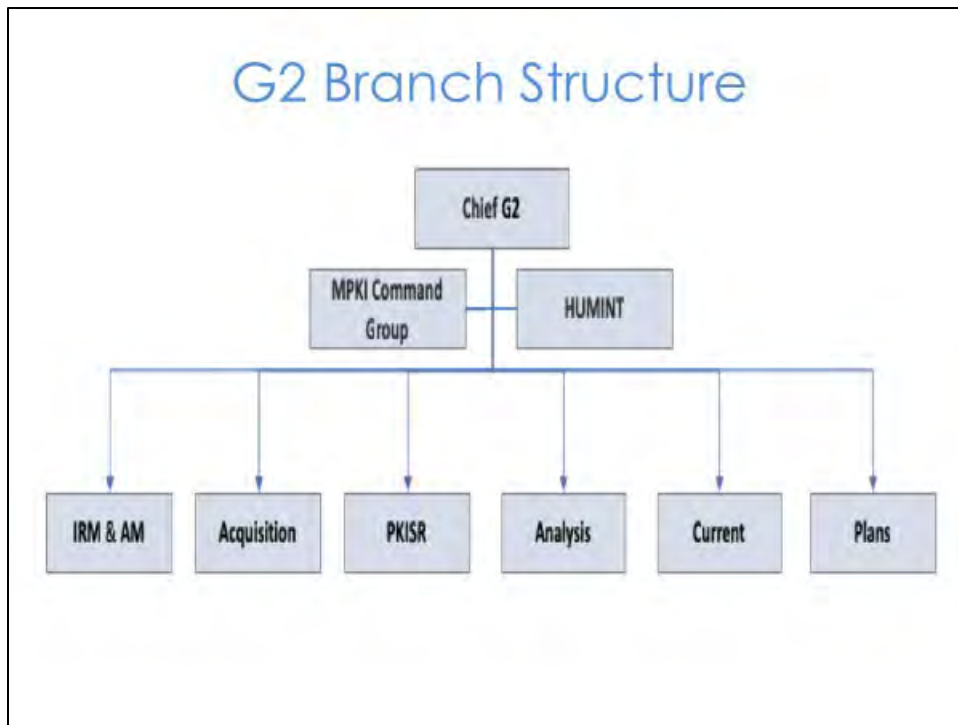
The G2 peacekeeping-intelligence branch in a Sector deals with all matters concerning peacekeeping-intelligence and military security operations at tactical/ operational level within the battalion AOR. Its recommended structure is depicted above, and roles and functions for the cells/sections are like the U2 sections/cells.

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

Slide 15

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

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

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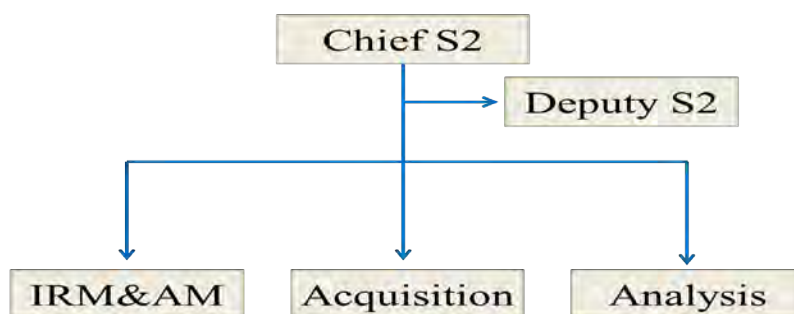
Chief S2: Head of S2 MPKI command group
Deputy S2: Counterintelligence and information security
IRM & AM: Information requirement and acquisition management

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

L e s s o n
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

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

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

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

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

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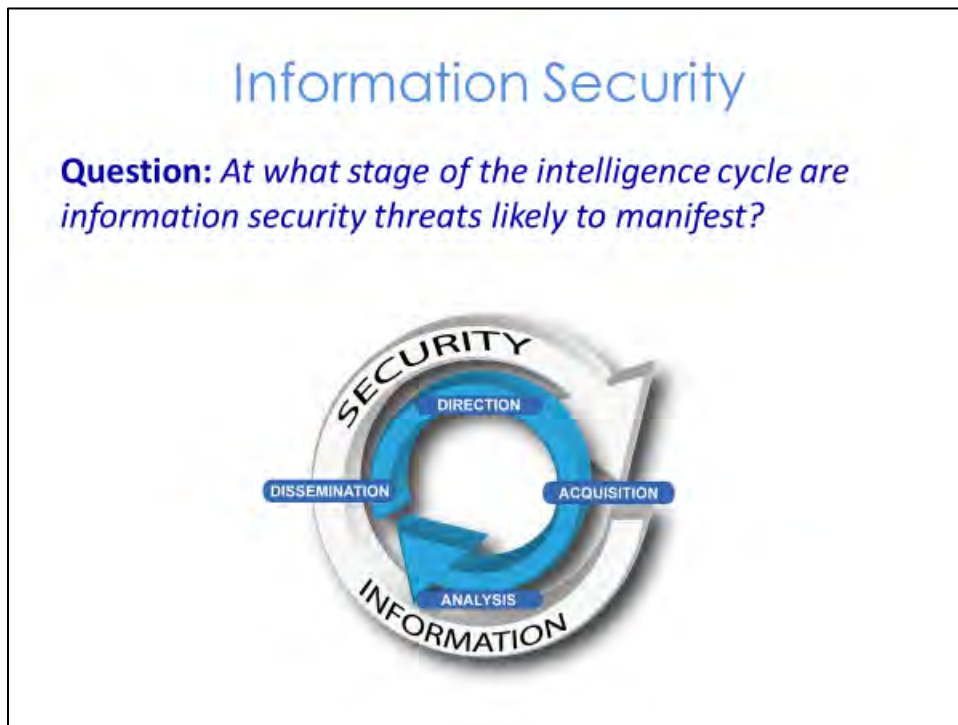
Information security must be achieved during the whole knowledge production process (intelligence cycle). In order to keep the information secure, the MPKIO must be aware of the possible threats, who should be handling the information, how to disseminate it, and who should be aware of the information.

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

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

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

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.*

M o d u l e
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

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

Slide 2

Here are the learning objectives for this lesson.
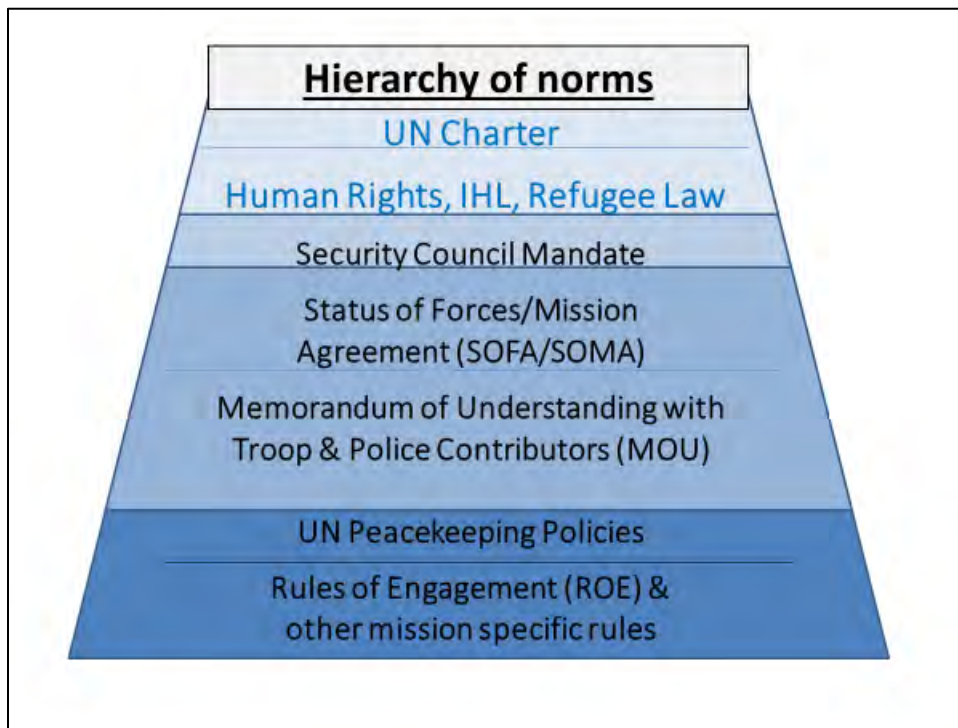
Slide 3

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 <u>could not be mandated</u> 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
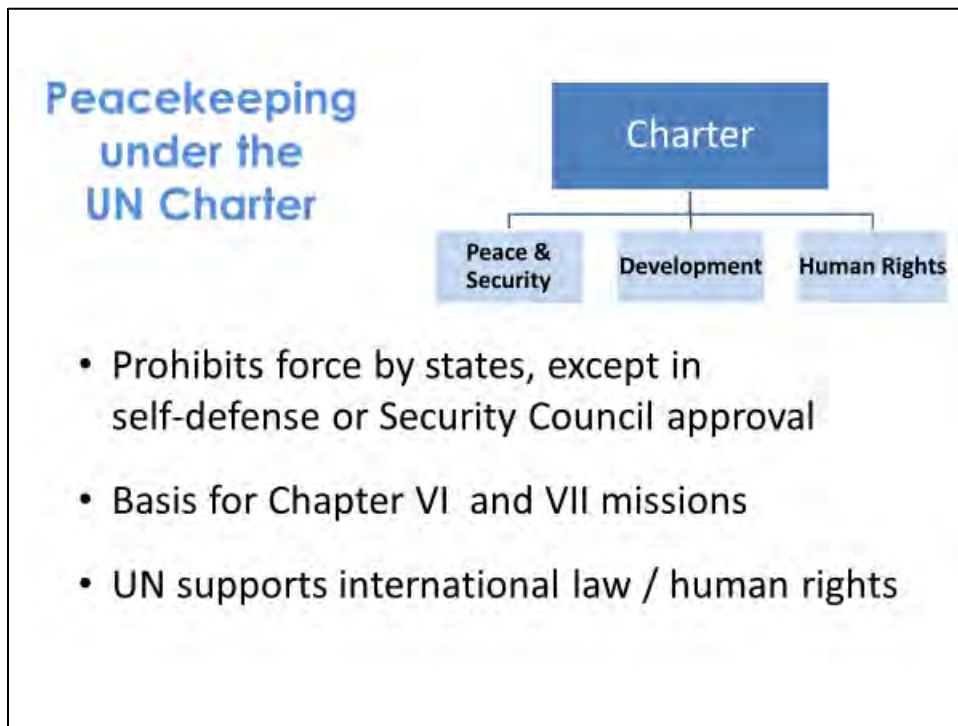
The Charter of the UN is the founding document of the Organisation and the basis of all the Organisation's work. The UN was established to "save succeeding generations from the scourge of war" and it, therefore, prohibits force between states, except in self-defence or with Security Council approval.

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

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 <u>respect</u> human rights and <u>protect</u> 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

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

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

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

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

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

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:

  o Before launching an assault, no effort is made to verify that the target is a military target

  o 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

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

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

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

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) 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

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

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

Slide 2

Here are the learning objectives for this lesson. Take a minute to read over the objectives.

Slide 3

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

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

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

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

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

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

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

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

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

M o d u l e
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

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

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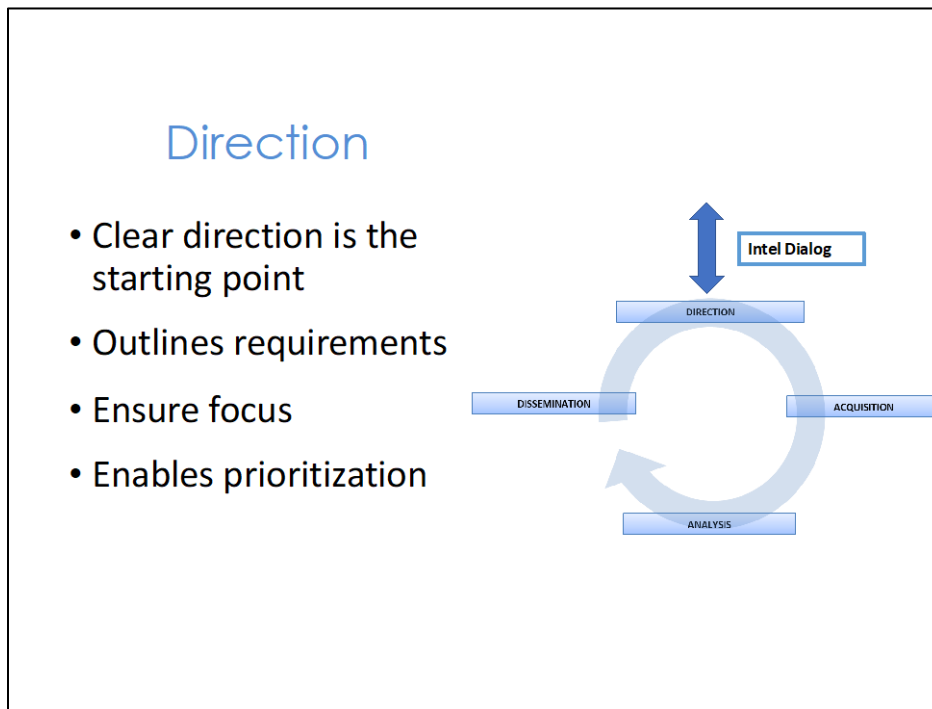
Key Message: The MPKI Cycle is the process that will – if used correctly – perpetually increase our understanding of the operational environment, in a structured manner, in order to support the MDMP. It contains four Intelligence Functions:

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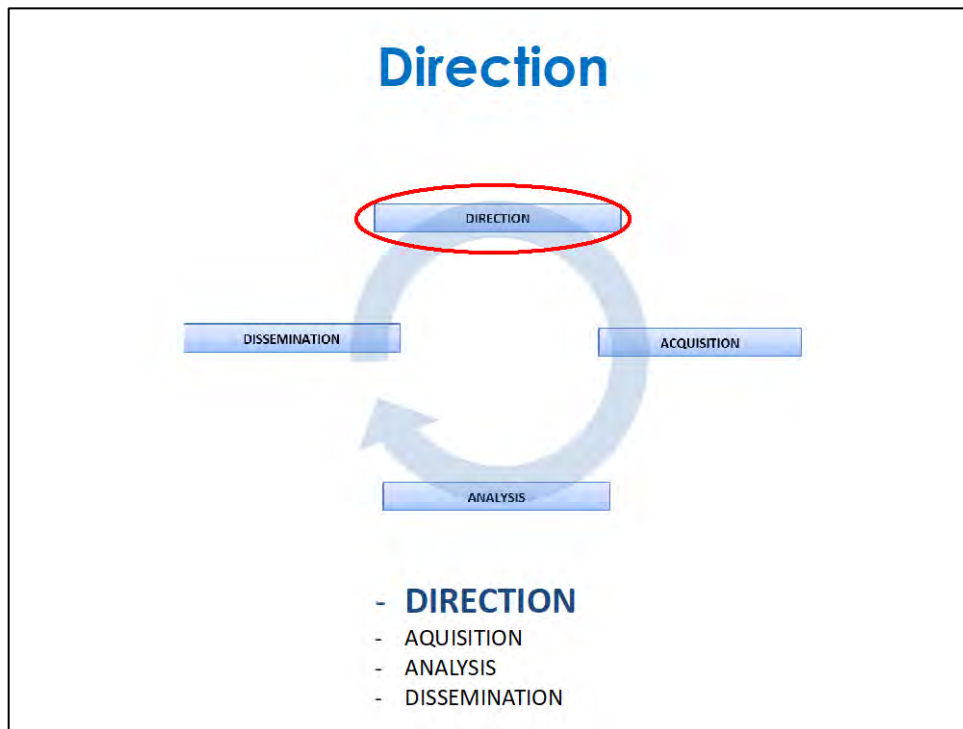
The direction is the starting point of intelligence dialogue. The direction is the Intelligence Function that shall assure that the Peacekeeping Intelligence Community always conducts its activities in support of the mission. Without direction, there exists a risk of irrelevant activities and poor resource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

Slide 8
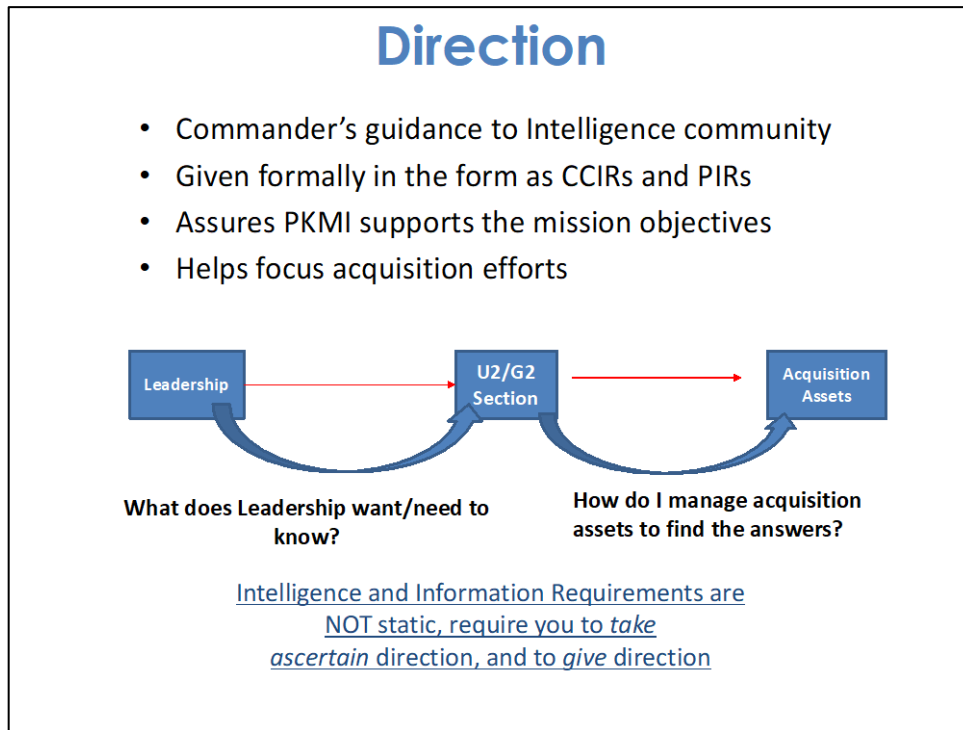
The commander may often require assistance in formulating his/her direction so that the intelligence community can produce a feasible and *relevant* product.

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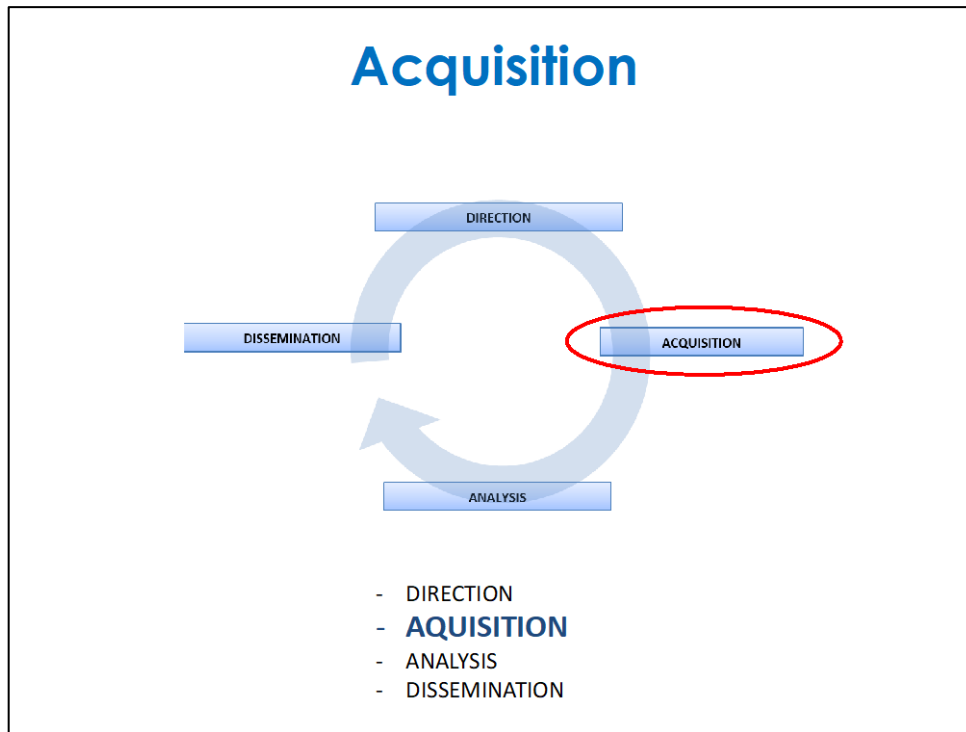
Key Message: This is the actual collection of data and information. The focus of acquisition comes from the previous stage in the cycle.

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

<div style="border:1px solid black; padding:10px;">

Acquisition

- Operationalized through the IAP

- Limited by capacity to collect (scarcity of acquisition assets)

- Requires an understanding of given Direction

</div>

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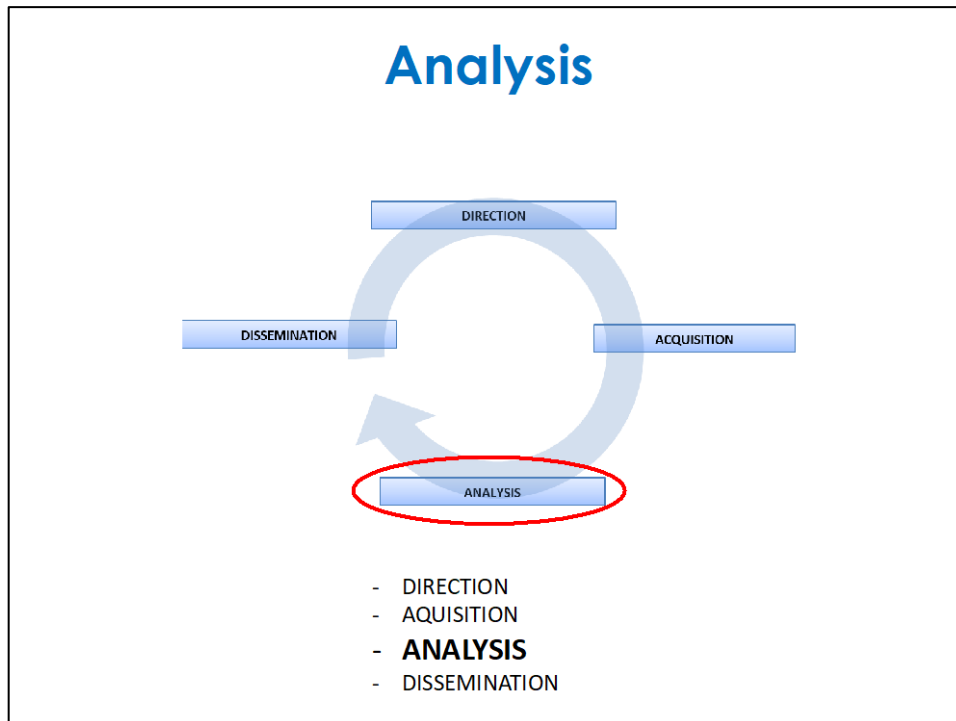
This Intelligence function is the most complex part of the PKMI Cycle.

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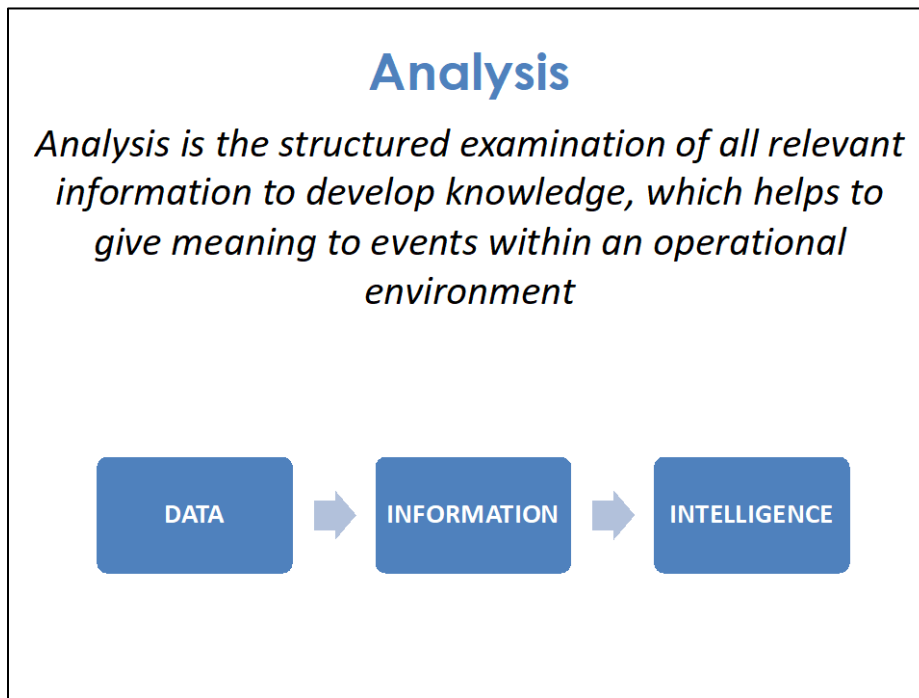
Key Message: Without analysis, there will be a mass of raw data floating around randomly, leaving the leadership to make decisions based on whatever unprocessed data available to them at the time. This will reduce the leadership's capability to make unified and well-supported decisions.

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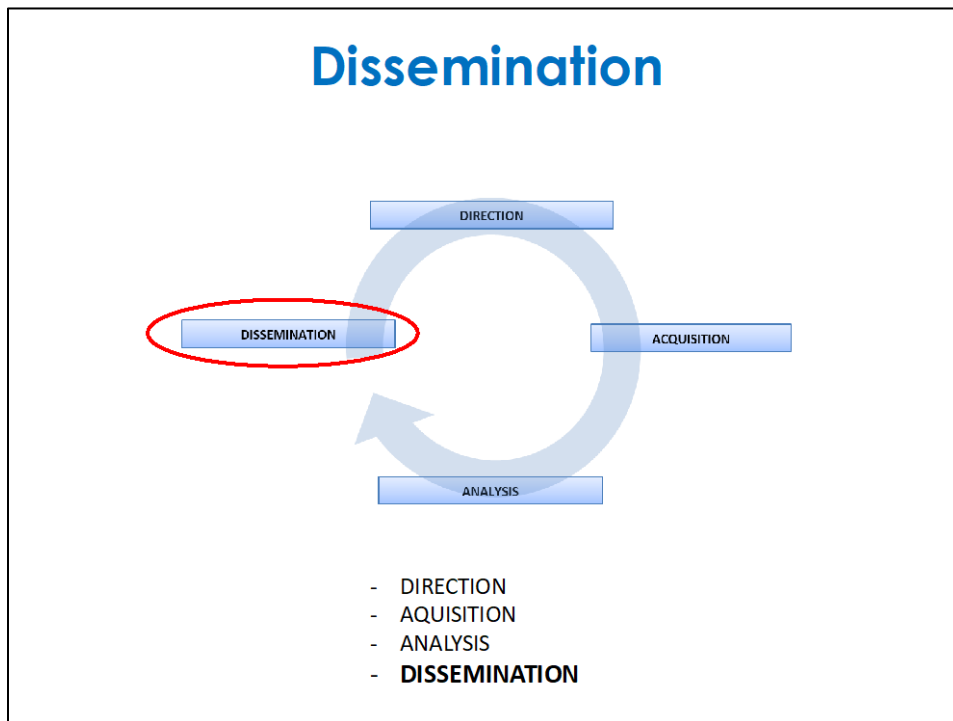
The production of Intelligence has no purpose unless the output is disseminated to those who need for it. To stay relevant, it is important that proper dissemination-directives are given and followed.

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
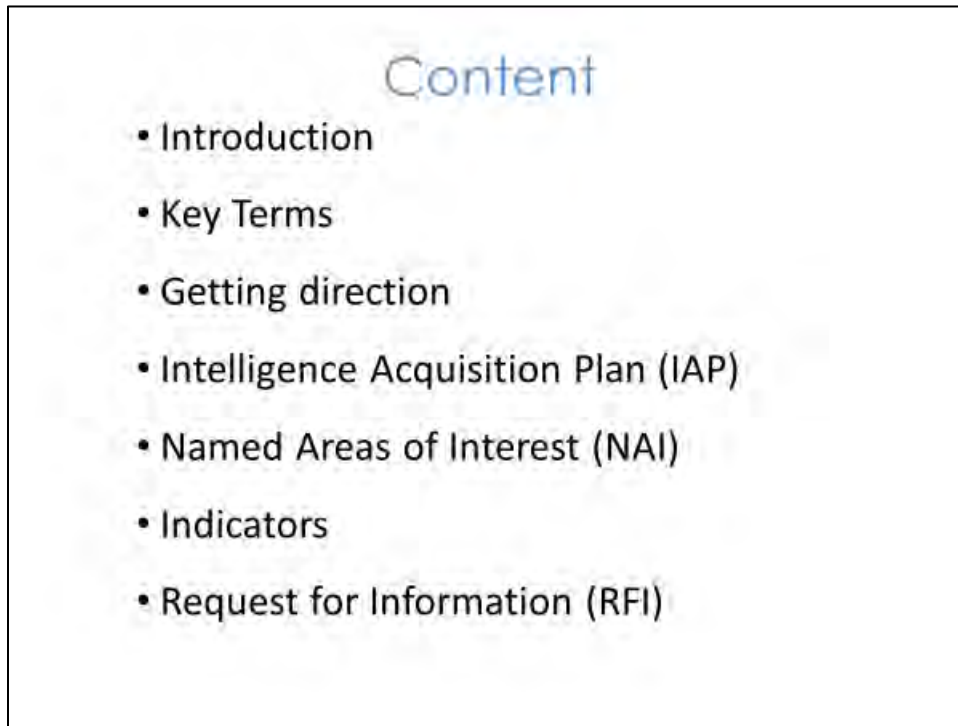
Slide 1

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

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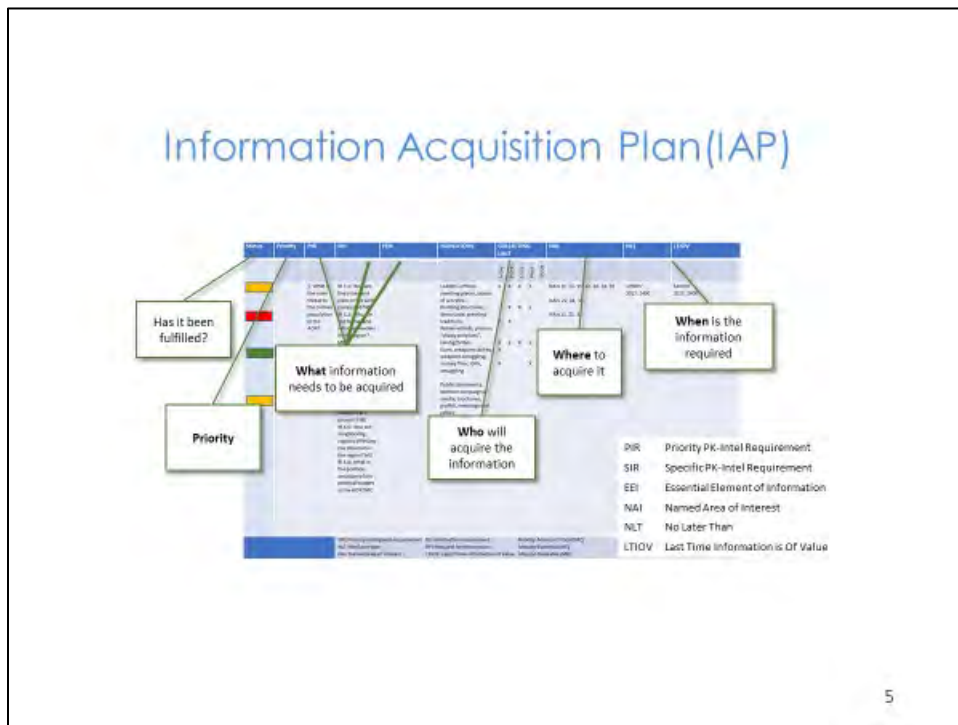
This is what we want you to construct at the end of this lecture series.

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
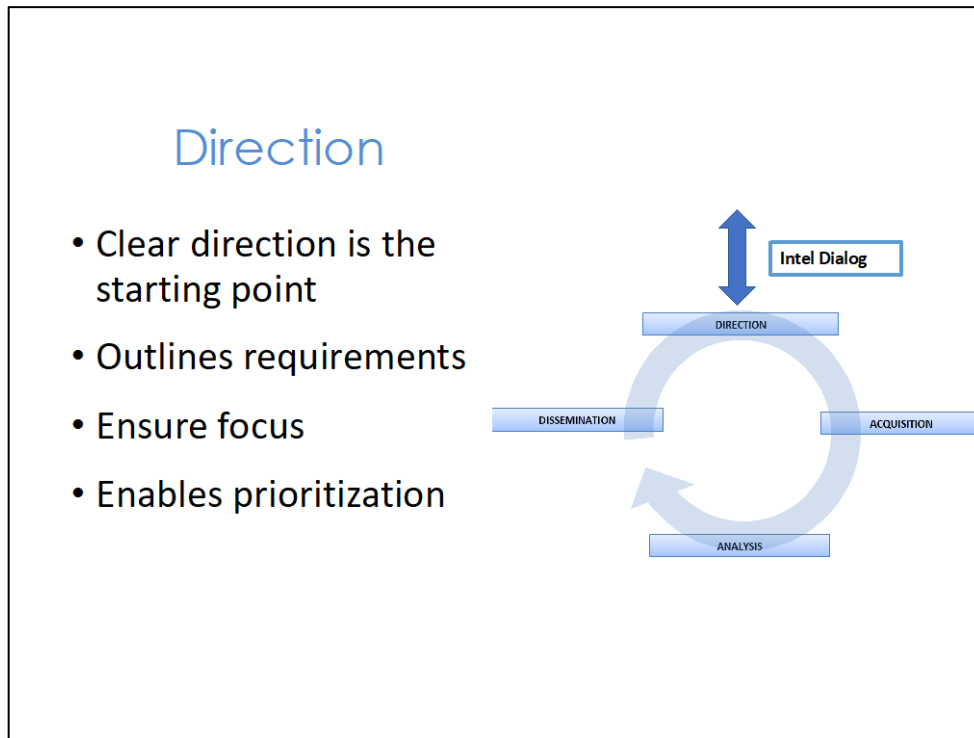
Key Message: Clear direction from the Commanders, at all levels, is the start point for the MPKI Cycle. The direction outlines to the MPKI staff what the commander wants/needs to know and ensures that the MPKI staff have a clear focus for their efforts. It is also important to understand that MPKI assets 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
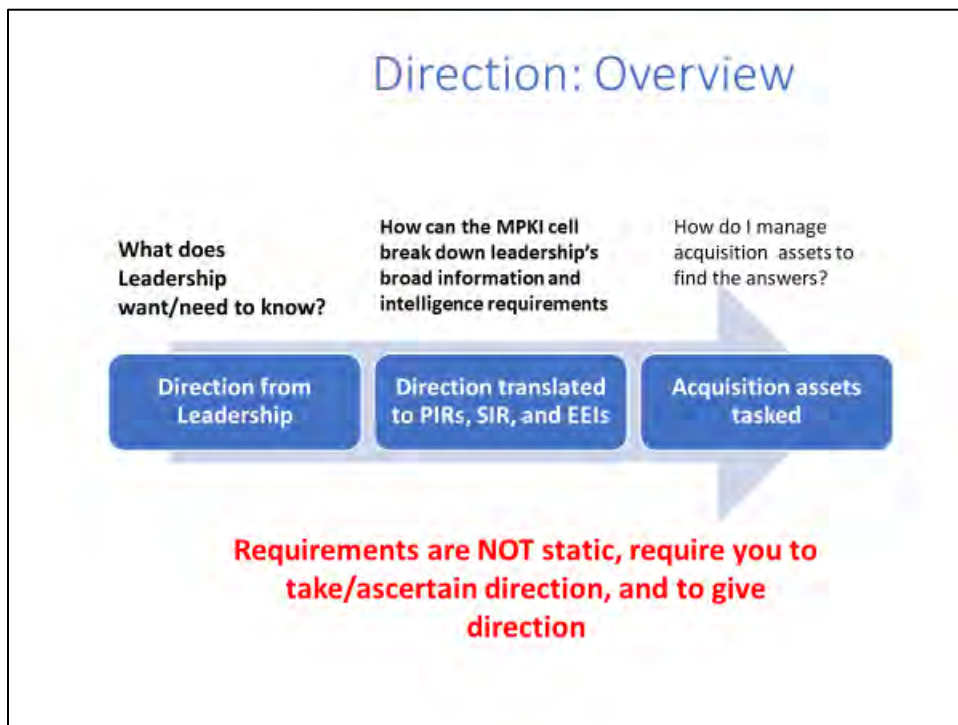
This slide is a visual graphic to support student understanding of the direction and acquisition process. Leadership first outlines its information and intelligence requirements to the MPKI cell at force, sector or battalion level. The MPKI cell then takes these requirements and breaks them down into 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
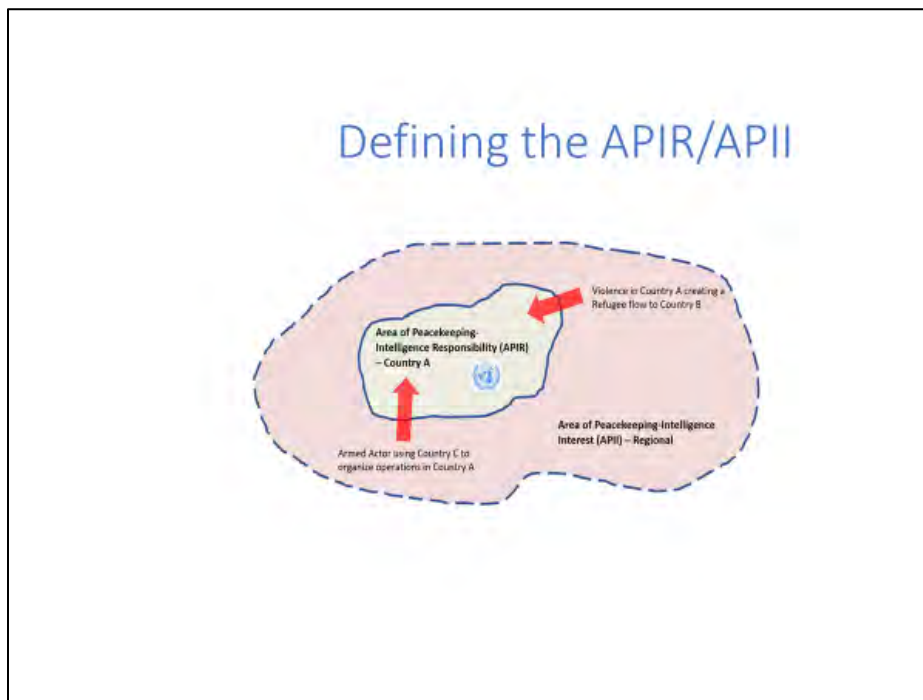
This graphic visually depicts a possible UN APIR and an APII. The key point here is that incidents and events in one country can have an impact on the situation in a UN AO.

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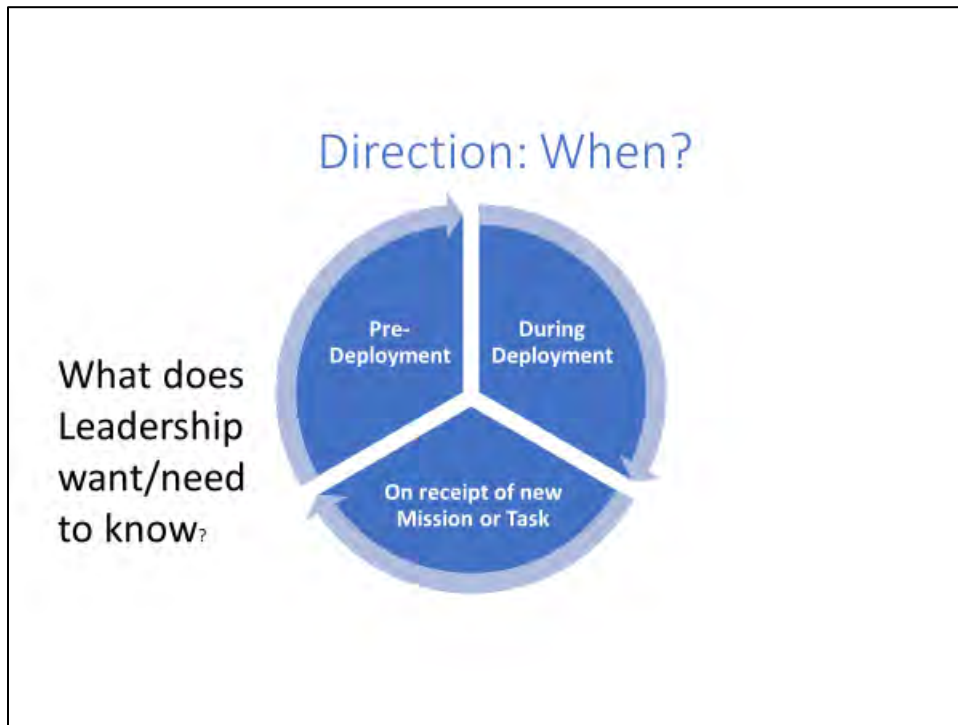
The direction is a continuous process, and it happens at all stages of the operational cycle, including before deployment, on deployment, and on receipt of a new mission.

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
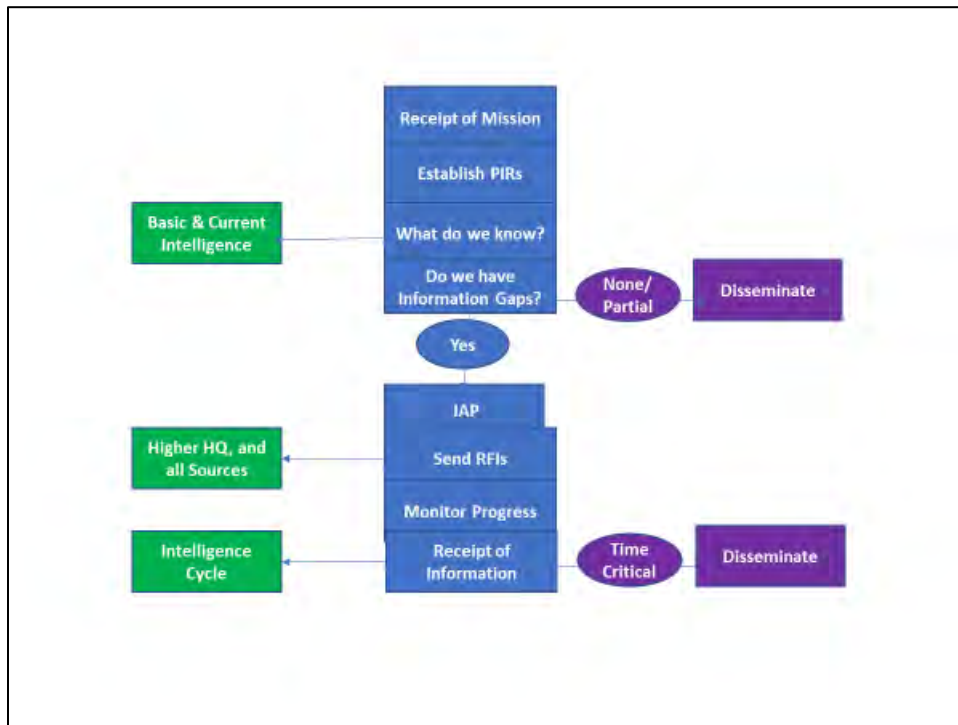
The key element is as follows. On receipt of the mission, PIRs are ascertained and broken down into IRs. The MPKI cell then searches its databases to find out what is already known and whether these PIRs/IRs can be immediately responded to. If we have no information gaps, then the intelligence product 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

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

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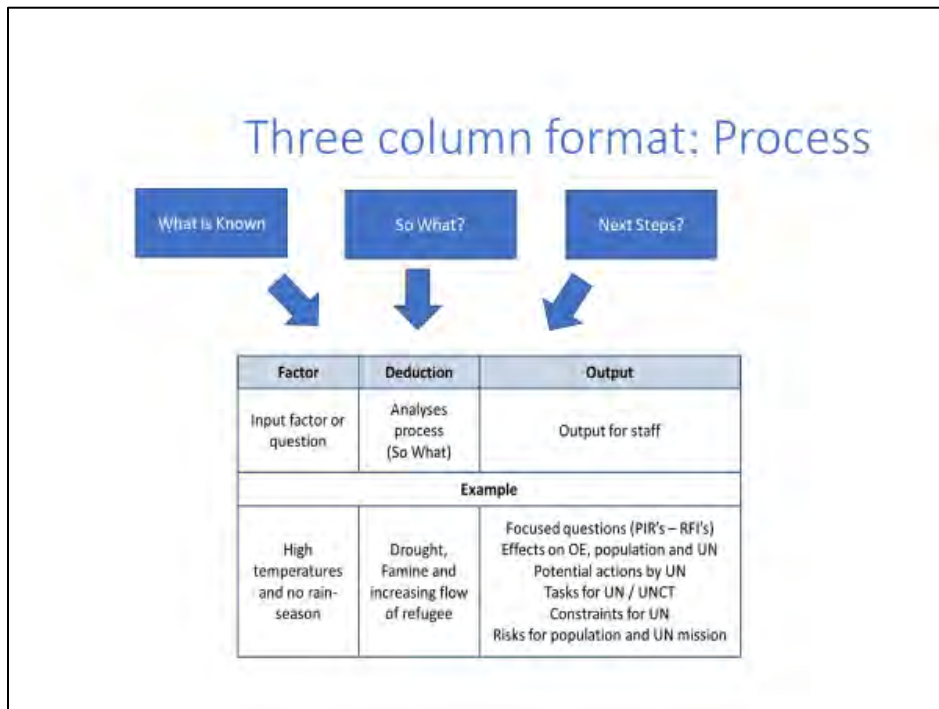
These factors will then be worked through using the three-column format methodology, which will create several deductions from each factor. These deductions should uncover information requirements.

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

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

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

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

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

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

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
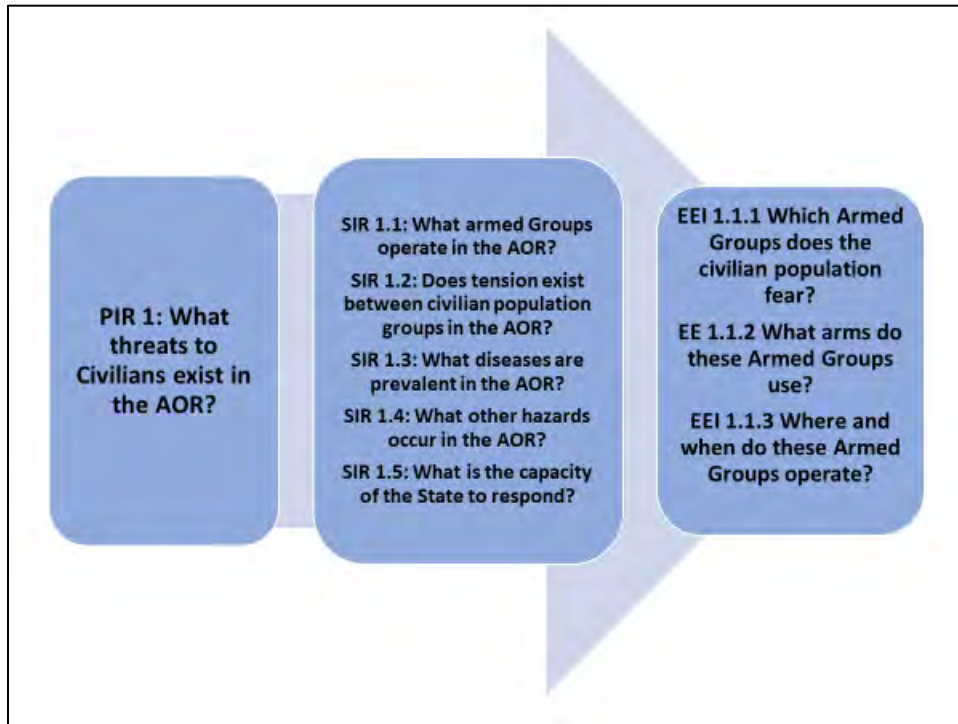
This is an example of how one PIR is broken into several SIRs. Each SIR is then broken down to several EEIs. Each SIR on the screen relates to the parent PIR, while each EEI relates to SIR 1.1. As you can see, there will be many EEIs for each PIR. Generally, EEIs are what acquisition assets will be tasked 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
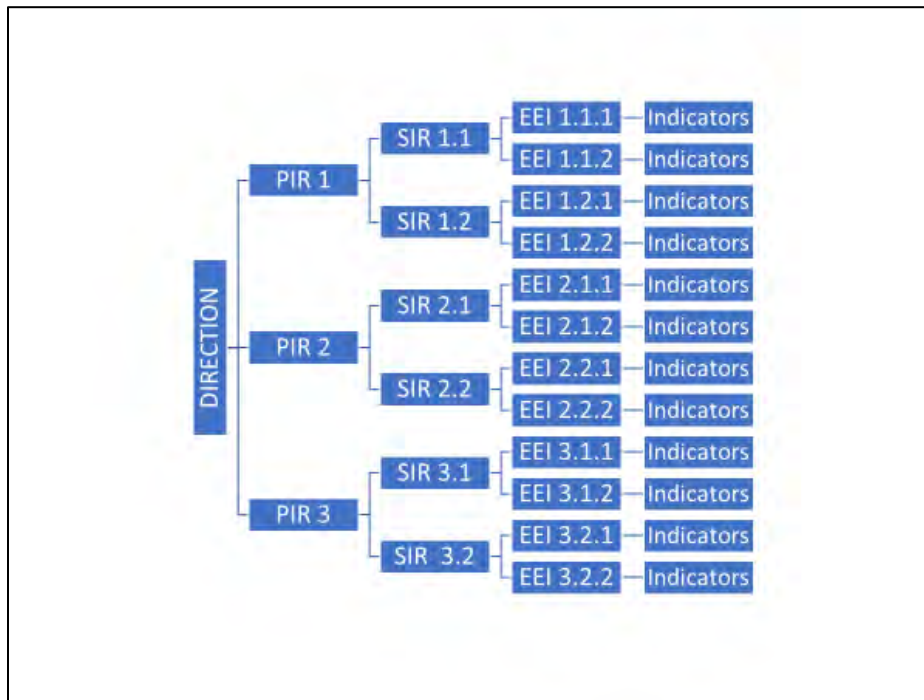
This is an example of how any given question can be broken down. Note that there is no actual limit to how many PIR's you can have, but it will normally be limited by the actors and factors that can affect the mission at hand. If you find yourself in a situation where the number of PIR's exceed 10, you 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

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

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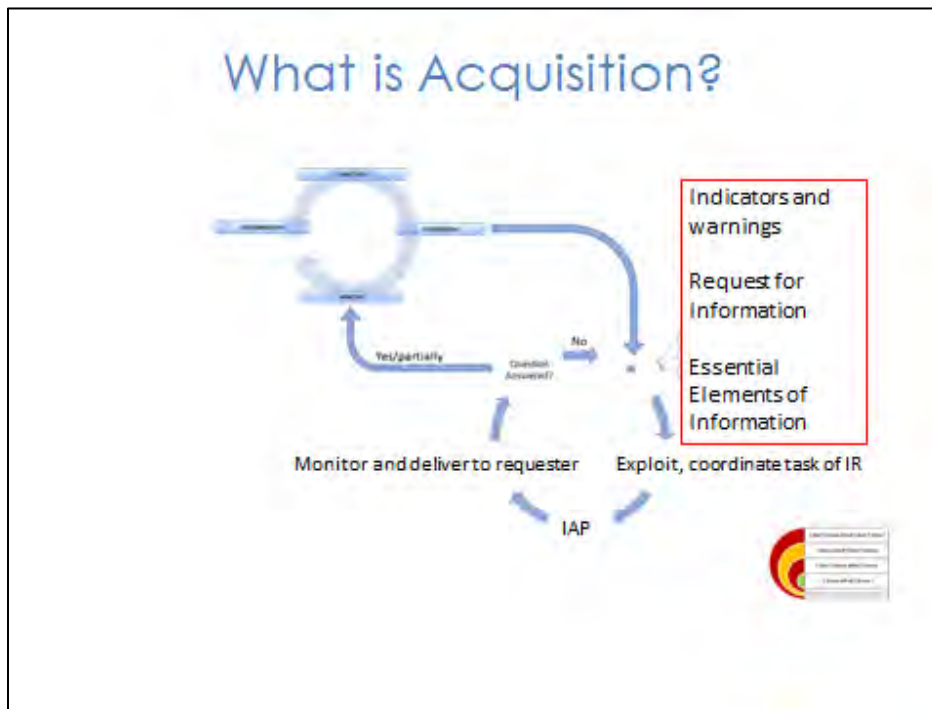
Key Message. The acquisition is the exploitation of sources of information by collection units and assets, and the delivery of this information to the proper intelligence processing unit for the use in the production of intelligence.

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
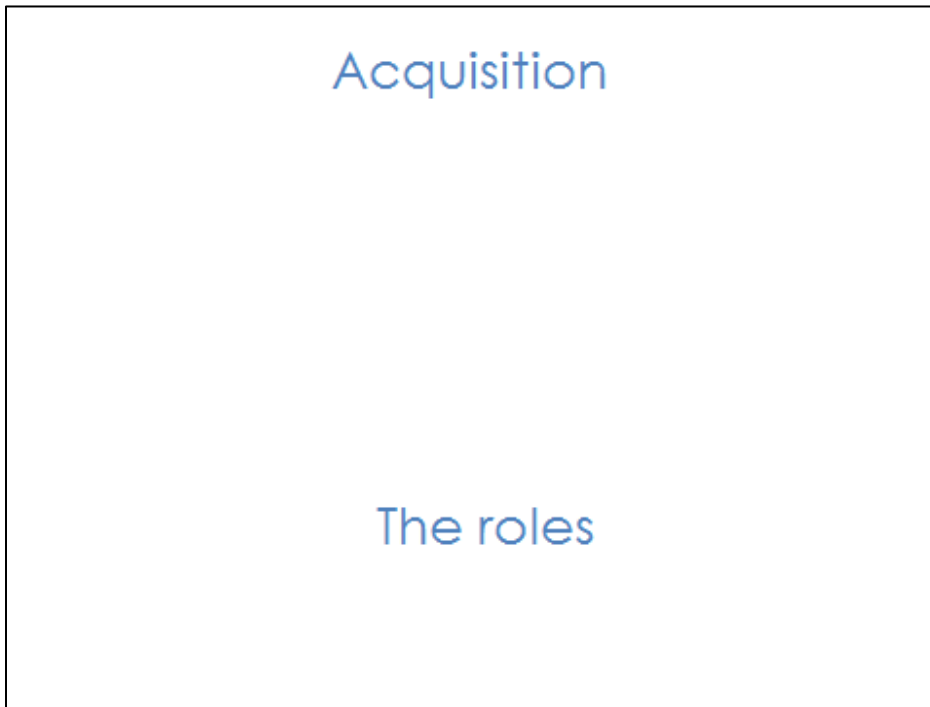
Acquisition

The roles

Slide 8

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

Slide 9
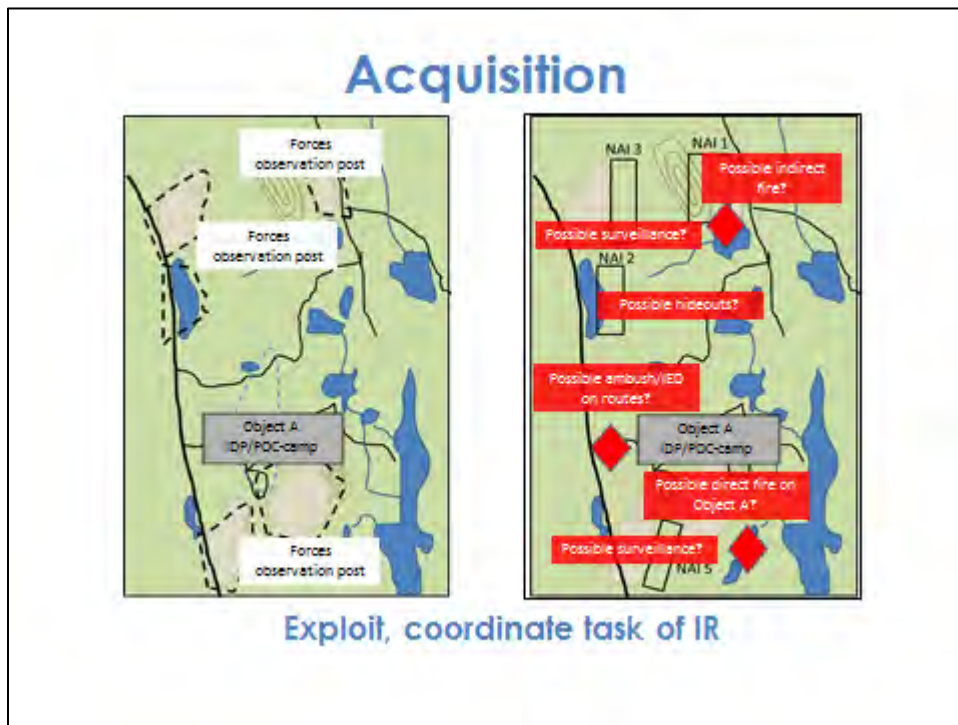
While the IAP is a very important part of the process, and it exists due to the knowledge gaps within the mission, it cannot be the only focus of the acquisition process. The mission will also be conducting operations on humanitarian efforts that must also be supported to enhance decision making. It 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

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

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

Slide 12

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

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

	Daily INTSUM	Weekly INTSUM	Monthly INTSUM	CIMICREP	MRAT (PHT)	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 TP 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

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

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
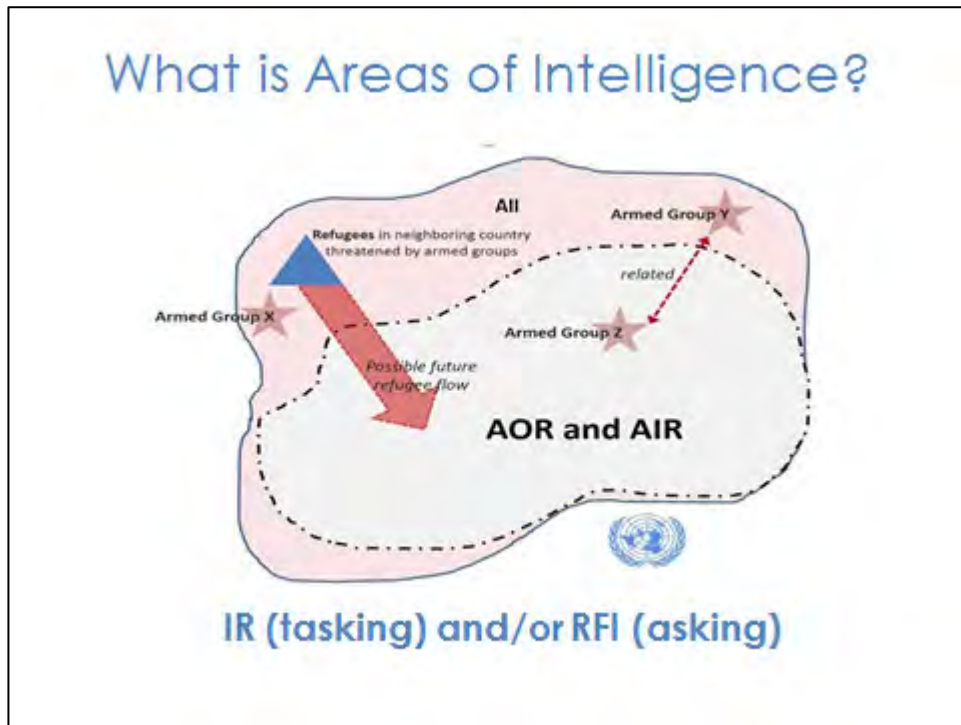
The Operating Environment is that geographical area (including the physical elements, the information environment and actors) that has been given to a Commander in order for him to conduct his given mission within the context of a UN Mandate. There are 2 sides to the management of Acquisition: Peacekeeping-Intelligence 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

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

Slide 20

Acquisition

Sources of information

Slide 21
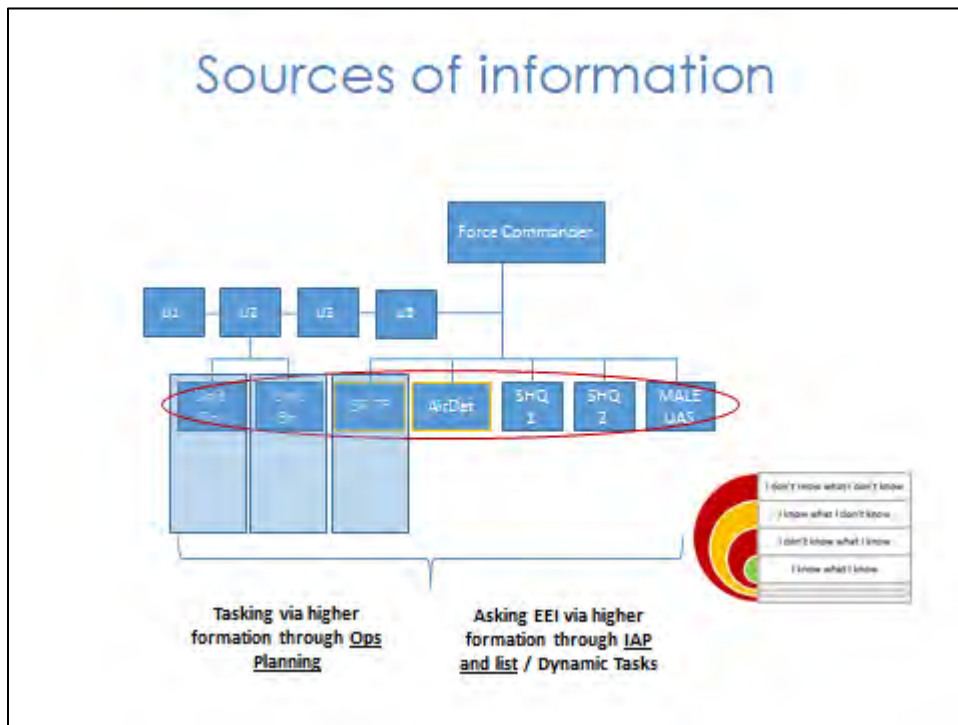
Key Message: The various acquisition capabilities that are controlled have their own procedures and methods appropriate to the exploitation of their sources. Planning and liaison are key terms of success.

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
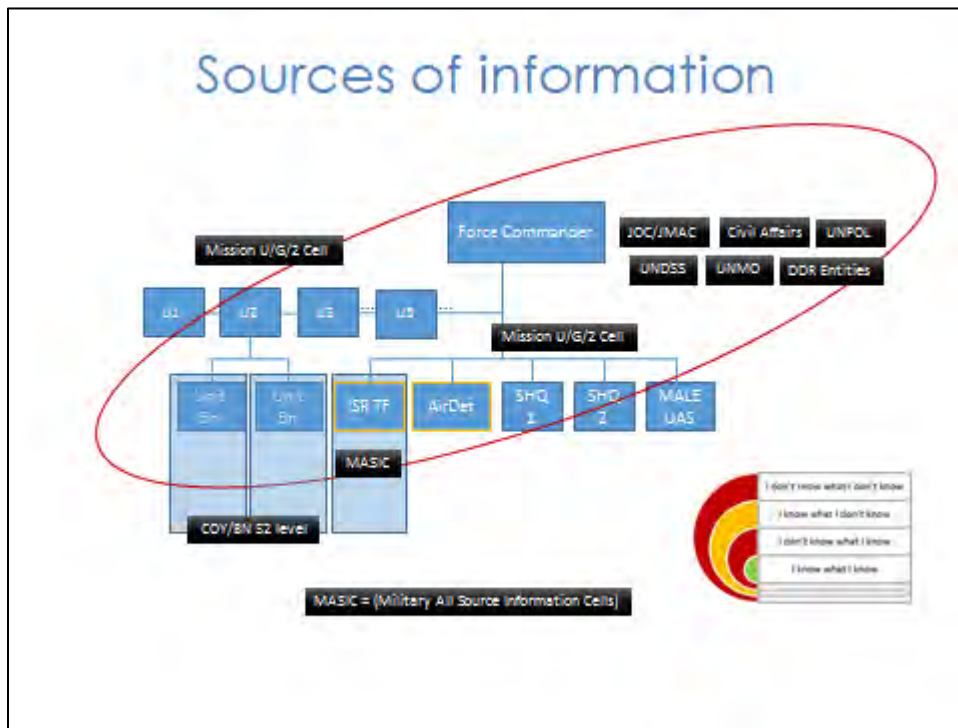
Key message: Good communication is the single most important factor that will underpin success in managing Acquisition. The communication within the U2 section filling the various roles, communication between the U2 and the customers, and, critically, communication with the mission's leadership helps 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
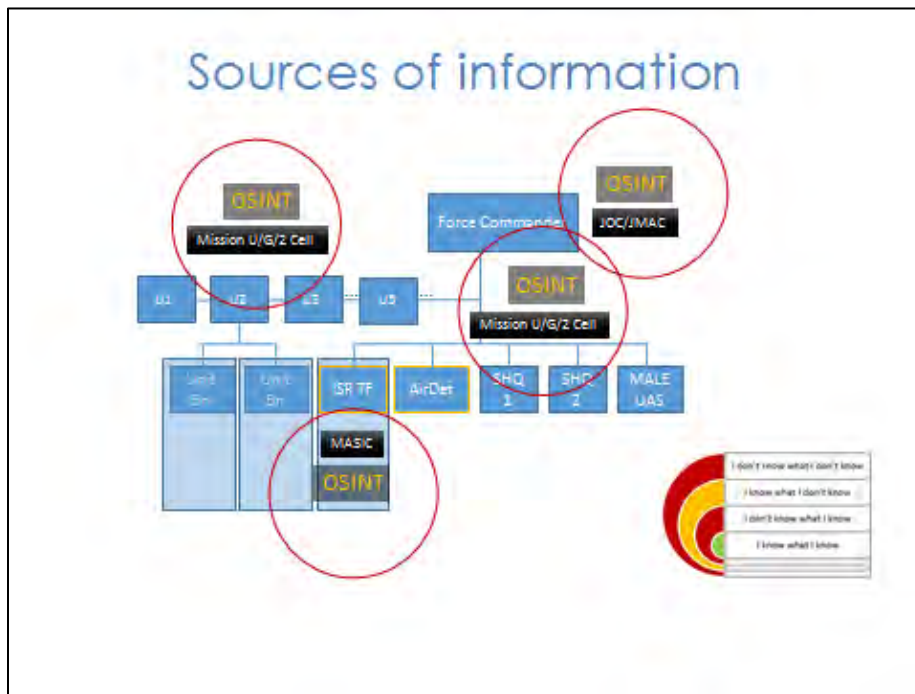
Key message: Acquisition/IRM/CM officers at all levels must recognize potential uncontrolled sources (such as new publication or broadcast on a new wavelength) and arrange for the recording and reporting of such information through the correct channels so that the source can be exploited.

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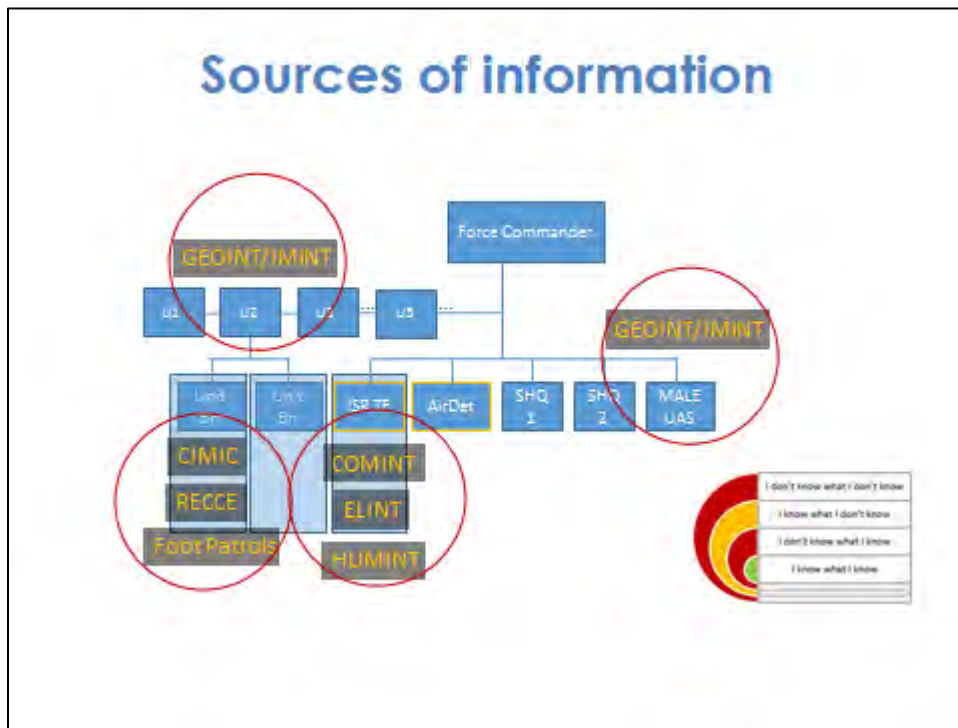
The acquisition should be a "System of Systems" approach to the employment of acquisition assets. This requires the assets to be used as a holistic entity rather than as a series of stovepipes. It seeks to provide a robust mix of assets at each level of command and to ensure the essential interplay between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

.

Slide 26

Acquisition Cycle

The way of an IR
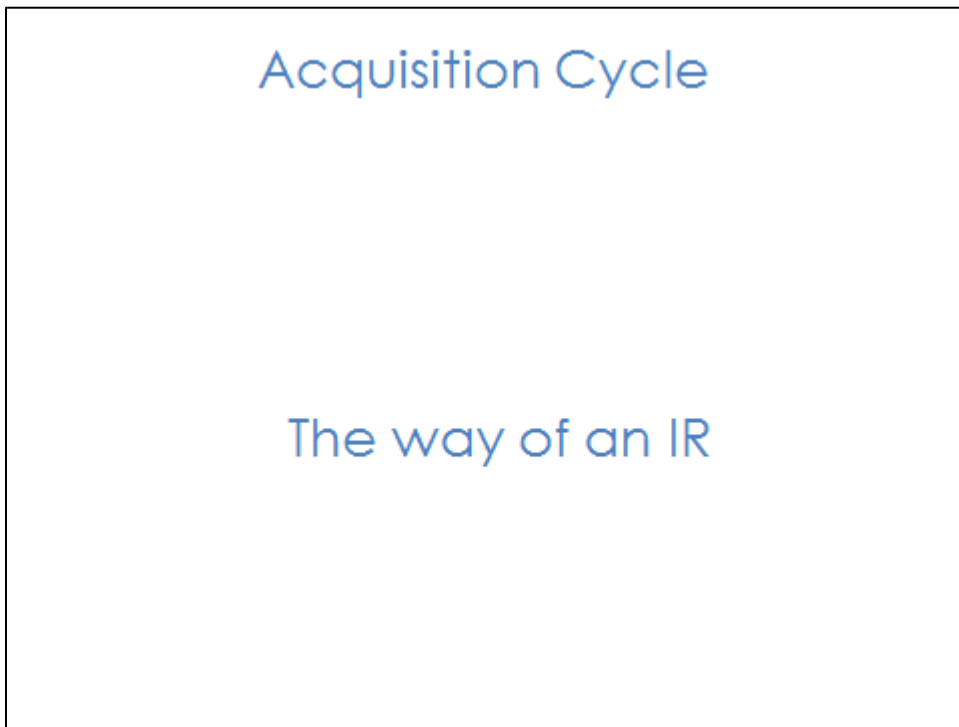
Slide 27
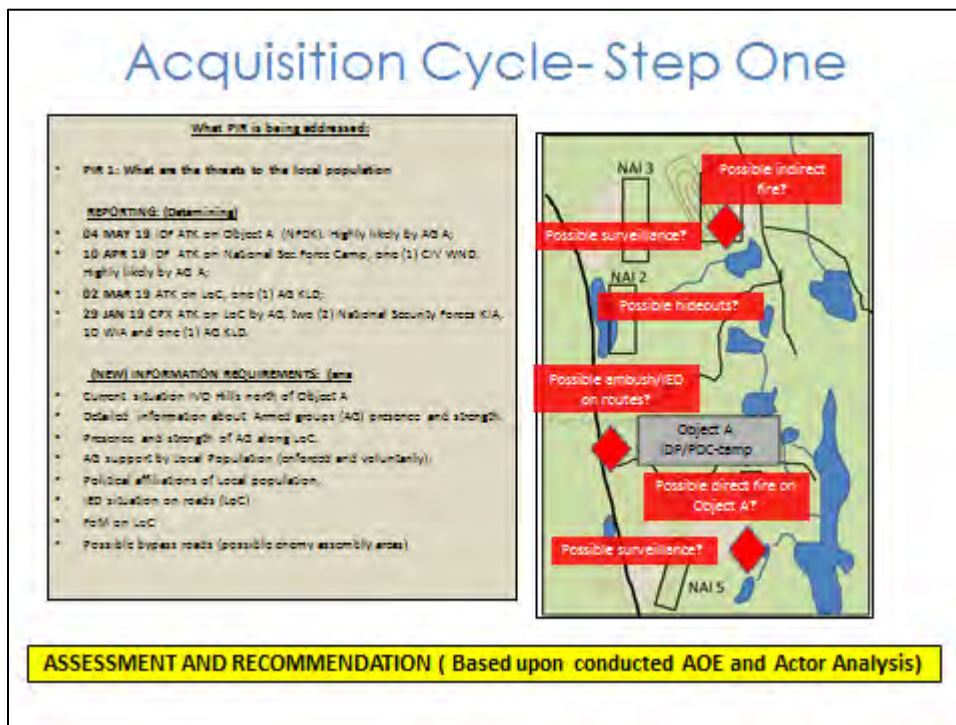
Step One: is a review of available information to see which IRs can be satisfied with information already stored on file by the mission. This is often referred to as basic or current information or intelligence. It should be noted that there will be few occasions that IRs can be entirely satisfied with 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
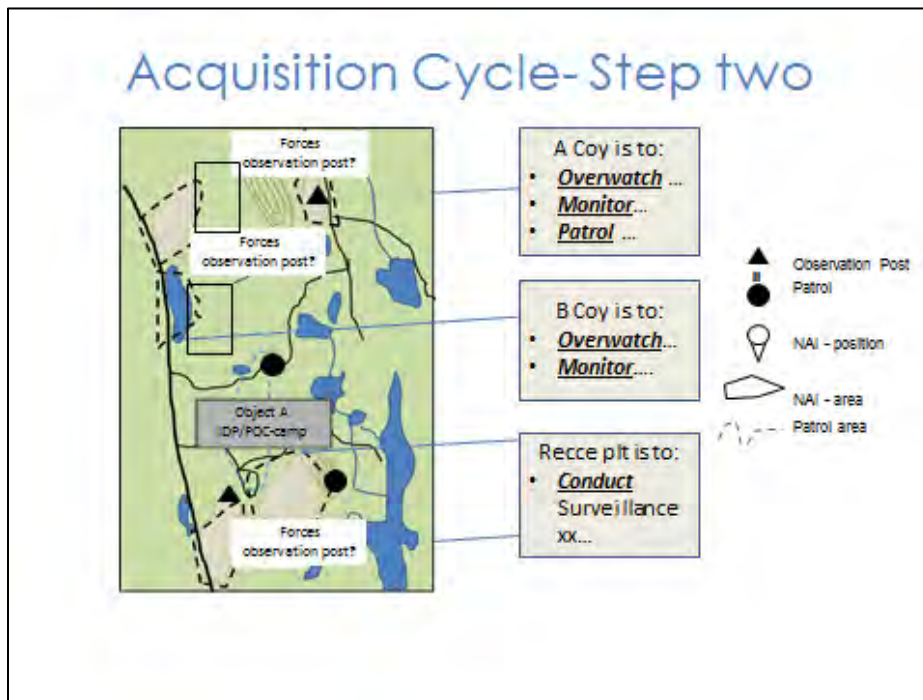
Key Message. The exploitation of acquisition assets (units) is often recognised through MDMP, the operation planning, ending up in an operations order/ Frag O via the mission U/G/S3 section including Air Ops sections.

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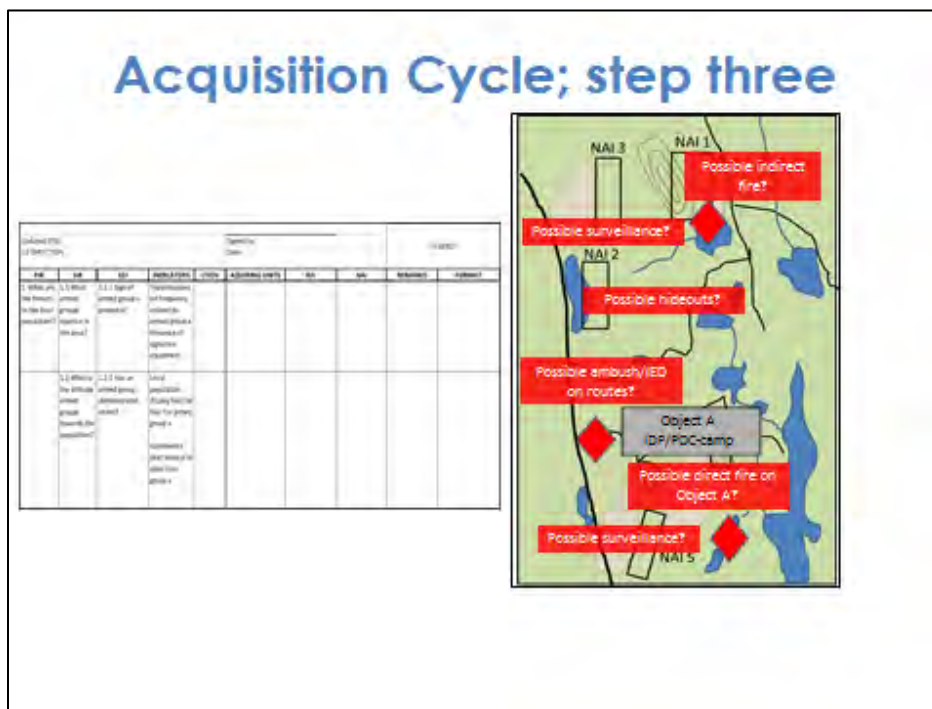
Key message: Close coordination and good communication between Acquisition Manager, IRM Manager and the Intel Function Direction, who direct the IR s.

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

Slide 31

Slide 32

Slide 33

Acquisition

Best practise; example from a mission

Slide 34

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

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

Lesson
3.3a

Analysis Introduction, Collation and Evaluation

The Lesson

Starting the Lesson

Slide 1

Lesson 3.3a
Analysis Introduction,
Collation and Evaluation

An essential component of a MPKIO work is to conduct ongoing analysis of threat situations within the UN mission area.

Slide 2

Here is the lesson content.

Slide 3

Learning Outcomes

- Explain the importance of Analysis

- Explain the importance of Collation and Evaluation

- Explain that collation systems are adaptable

- Explain how to evaluate information, include : Reliability and Credibility

Upon completion of this lesson, participants will be able to accomplish these outcomes.

Slide 4
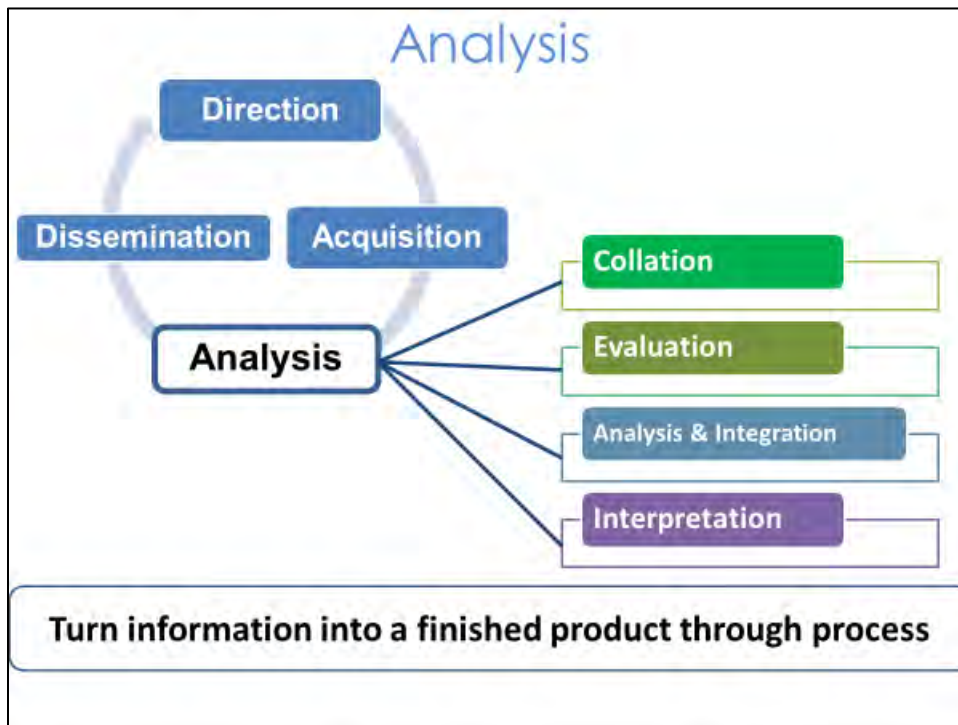
Key message: The Analysis phase answers the following questions: So What? Why is the information important?

To be useful, information must go through the analysis process before its dissemination. The analysis phase is broken down into four steps: Collation; Evaluation; Analysis and Integration; and Interpretation.

At this stage, you all know that the third phase of the MPKI cycle is Analysis. It is defined as the methodical breaking down of information into its component parts. The examination of each part to find interrelationships, and application of reasoning to determine the meaning of the parts and the whole is crucial.

During this phase, the acquired information turns into a finished product that ideally gives meaning to the individual pieces of information and is, therefore, more than the sum of its parts.

Ultimately, you as MPKI analysts are required to provide predictive analysis and scenarios on the evolving tactical and operational situation that go beyond establishing capabilities of the threat and other actors to determine their intentions and probable actions and scenarios.

For analysis to be predictive, it should consider an event/incident, trend or a threat and establish why such a thing is occurring, what is likely to come next, and what the implications for the UN Mission are.

The analysis itself is broken down into four steps: the first two are collation and evaluation, which we will go through in this lesson. The third one is analysis and integration and then interpretation.

Slide 5

Key message: The primary objective of this step is to make sure that no information is lost and information is easy to retrieve. To do so, it is very important to ensure that all information is recorded and sorted in a common format.

Collation is the first step of the analysis phase. It is a set of procedures for receiving, recording, and grouping all information acquired. Well trained, efficient collators are vital to the effectiveness of peacekeeping intelligence cells.

The primary job of a collator is to ensure that no piece of information is lost. It is of high importance that every piece information is registered, sorted and recorded, and most importantly, can be retrieved by the analysts at will. Indeed, it is really of no use if you can identify vital information, but you cannot retrieve it promptly.

Collation consists of:

- Assimilation of a large volume of information

- Identifying and registering each piece of information without compromising source security. Often a human source will be given a nickname

- Recording the reliability of the source. We will see how to do this in a few minutes

- Categorise each piece of information in a way to retrieve it by knowing its date of acquisition or reception, its type, its source type and name, and its reliability and credibility

What is good about this step is that when you become familiar with the information you are collating and aware of the IRs, you will be able to provide, at your level, the first analysis as you receive the information.

Slide 6

Key message: Appropriate use of tags (date, source, subject, location, etc.) is essential in the collation mechanism and makes it easy to retrieve information.

Now that you have understood the importance and the principles of the peacekeeping-intelligence collation, we will see how it is done. It is very important to have an established collation format before the information flow starts. There is no specific agreed-upon format, but whatever format you choose to work with, it must allow you to sort the acquired information according to:

- **Date of information** which is the date that the event occurred on
- **Date of** the information **acquisition,** or that date that you received the information
- In the **Source** box, you indicate its nature and name (SIGINT, OSINT, IMINT, HUMINT...) if it is a HUMINT source, don't give your source's real name. A nickname is often used instead
- For the **source grading**, we will see how it is done in the evaluation lesson
- In the **Subject** of the information box, give a summary (a few words) or a title if suitable
- **Location** acquired in the location box – this is where you provide information on the location of the source at the time the information was

acquired. E.g. the elevation of an aircraft providing aerial imagery, the distance an OP was from the incident reported, etc.

- And a link to given PIRs, IRs if appropriate

- In the last box, you put a **hyperlink** to the original document so that it can be located on the system

If information is received in a language other than the working language for your UN mission, ensure that it is translated, and the translation is attached to the original information so that it is usable when retrieved by other analysts.

In terms of personnel, only an experienced intelligence person can do this job. Ideally, a senior intelligence NCO would be chosen for this role.

The software that is most widely available for use in a collation database is Microsoft XL. An example is shown on the next slide.

Slide 7

Key message: The use of Excel to create a collation log is highly recommended.

To Microsoft Excel is a common programme that offers an effective platform for peacekeeping collation. Excel is easy to populate with information and to search for content if it is set up well. You can run a single collation worksheet, or create specialised worksheets for specific time frames, sources, threat groups, incident types, etc. If you are not familiar with Excel, it is recommended that you learn how to use it.

The key to a successful collation database is that information can easily be accessed and sorted. Central to this is the ability to quickly filter information. The location of the filter function is on the next slide.

Slide 8
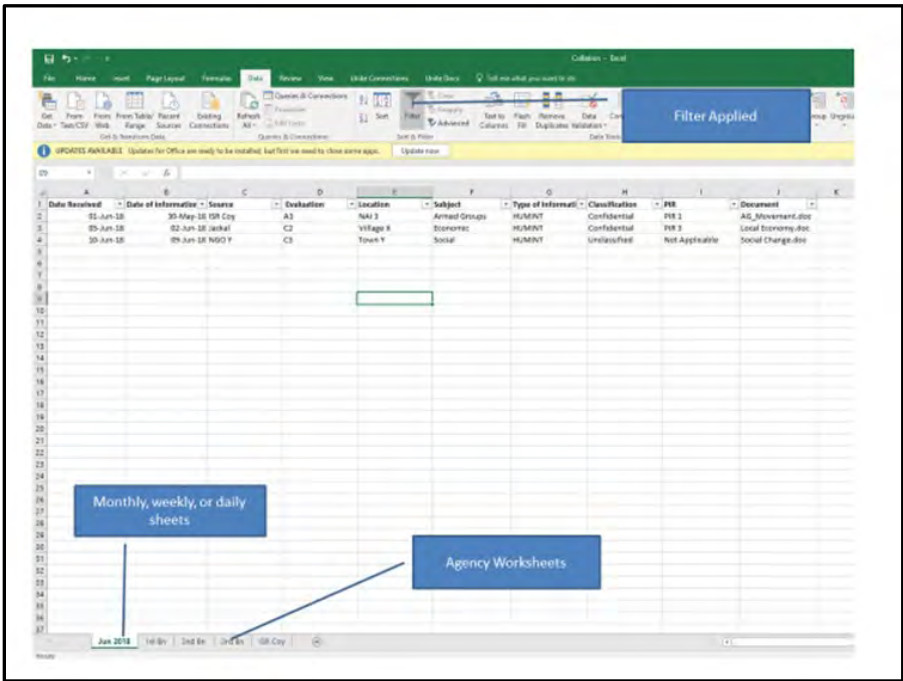
This slide shows the filter on MS XL.

Slide 9

Interaction, The purpose of this exercise, is for the students to decide how they would collate incoming data. Prompt the students to begin a discussion within their syndicates as to how they would record information as it comes into their MPKI cell. Responses should include:

- Date of information acquisition
- Date information comes to MPKI cell
- Location information was acquired
- Type of information; the subject of the information
- Source; source grading
- Link to PIR, SIR, or EET

If possible, this should be placed on an XL file format, as outlined above.

Slide 10

Key message: An analyst needs to anticipate and prepare for physical problems be pragmatic in prioritising data and creative in using recording and visual aids.

You should always keep in mind the following considerations:
A collation system based on Information Technology is vulnerable to certain difficulties.

Interaction *What might those difficulties be?   Get answers from the audience and comment on them briefly with "correct" or "not that much".*

To sum up, what you just said, the difficulties are related to:
Shortage of power, unavailability of software, insufficiency of communication, security clearance restrictions, system incompatibility, limited memory and lack of skilled operators.

As facilities are not generic in UN missions, you will need to consider whether these difficulties might impact your ability to collate information in your and think of how you might deal with the potential loss of IT.

Always ensure that your collation data is backed-up. If your power supply and/or computer systems are unreliable, keep updated hard copies of your collation sheet to ensure that collation data is not lost.
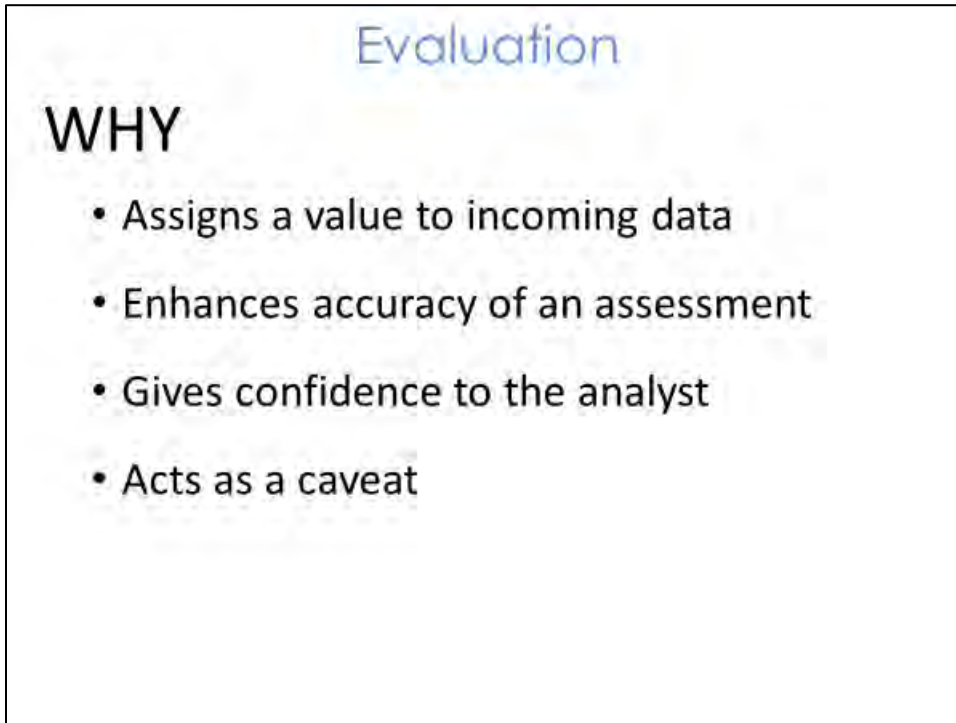
Also, be pragmatic. It is not possible to collate in detail every piece of information, and peacekeeping intelligence received. A compromise between what is desirable and what is possible is required, focusing on collating the most relevant information (i.e. information that best contributes to answering PIRs). Any information that is not immediately relevant can be retained for future review.

To prioritise information, collators must consider their relevance to PIRs and IRs.

Relevant recording and visual aids can be linked to the collation log so that analysts can quickly find them. They include, but are not limited to:

- Annotated Maps

- Incident maps

- Situation maps

- Order of battle (ORBATs) threat groups

- MS Excel or Word documents with hyperlinks to data files

- Timelines

- Diagrams

- Matrices

Slide 11

Key Message: Properly evaluated source reports increase the confidence of the analyst in his/her product and increase the confidence of the commander in the product.

If information is passed to the commander, particularly in single-source format, he/she needs to understand how reliable the source is and how credible the information is. This is so as the commander may base an operational decision based on this information.

Slide 12

Evaluation - How

- Information is examined
- Regard to reliability of source
- Regard to credibility of content
- Acquisition normally evaluates
- Caveat – sources registered, higher HQs may assign different reliability
- Source registration limits circular reporting / better assessments
- Credibility – often not apparent to collector, usually a HQ role

Key message: Knowledge of the reliability of previous information and sources helps in verifying, comparing and therefore rating every piece of information or peacekeeping intelligence.

Evaluation is defined as the step of the analytical process where every item of information is examined regarding the reliability of its source and the credibility of its content.

Step 1 Assess the reliability of the source. Factors in this regard include carefully evaluating the reliability of the information that the source has provided in the past. If this information has been accurate, then the source will be judged as more reliable than a source that has provided less reliable information.

It is worth noting that the MPKI cell will normally accept the human source evaluation of the acquisition asset. However, it can change this evaluation if it has additional information about the source. For example, if the same source is reporting less reliable information to another acquisition agency, then his/her rating may be changed on that basis. A caveat to this is that sometimes a source may have excellent access to some types of information, and reduced access to other types of information. For example, a source 'Erik' could have excellent access to political information, but his access to military information may be limited. MPKI cells should refer to organic assets by unit, and to open source information as OSINT.

Step 2 – Evaluated the credibility of the information. This is accomplished by comparing the new information with information already on file.

Comparison is carried out by:

- Cross-checking the information to check if it is derived from multiple sources. The information has greater credibility if multiple sources support it, and especially if those sources are distinct and independent (e.g. two siblings reporting the same incident is less reliable than two strangers with no relationship reporting the same incident)

- Checking its coherence with previously processed data

- Assessing its conformity with previous knowledge about the operational environment, including the potential threats and risks

Remember that verification and comparison of information provides an indication of its credibility, but there is no guarantee that just because a piece of information cannot be verified or seems out of step with other known information that it is not reliable.

For example, threat groups are not always predictable. They might be innovative, and nonconformist, so consider this possibility and use verification and comparison as a guide.

Rating is a means of combining the reliability of the source with the credibility of the information to reflect the level of confidence in the material.   We will discuss this in detail in the next three slides.

Slide 13

Key Message: Sources need to be evaluated for their reliability based on a scale from reliable to unreliable (A-E), with an option for showing that reliability cannot be judged (F).

When evaluating the reliability of a source, the closest HQ to the source is ordinarily, the best judge of its reliability.   Keeping track of the source reliability is important and must be updated. A source might be upgraded or downgraded.

Information is rated in the form of an alphanumeric code whereby the Letter indicates the reliability of the source and the Figure indicates the credibility of the information.   In this table, the letters go from A to F ranging from "reliable" to "cannot be judged".

- For "Reliable" there is No doubt of the authenticity, trustworthiness, or competency of the source as it has a history of complete reliability

- For "Usually Reliable" there is a Minor doubt about its authenticity, trustworthiness, or competency and it has a history of valid information most of the time

- For "Fairly Reliable" there is a doubt of its authenticity, trustworthiness, or competency but has provided valid information in the past

- For "Not Usually Reliable" the doubt is significant, but the source has provided valid information in the past

- For "Unreliable", the source lacks authenticity, trustworthiness, and competency and has a history of invalid information

- The letter "F" is attributed to the source when there is no basis that permits evaluating its reliability

Please note that the acquisition agency is the one that usually rates the source. The caveat to that is that the source must be registered, but higher HQ might assign a different level of reliability. When evaluating a source, you are letting analysts know how much you think this source can be relied upon. It is okay if different people have different opinions on the source's reliability, so long as you have offered a considered evaluation.

Slide 14

Key message: Evaluate credibility independently from source reliability to avoid mutual influence. Even the most reliable source can provide wrong information.

In this table, you can see that the Figures go from 1 to 6 ranging from "confirmed" to "cannot be judged "going through "probably true ", "possibly true ", "doubtfully true "and "improbable".

A higher HQ normally accepts the reliability evaluation offered by a reporting headquarters. However, it might change its grading if incorrect grading cases were registered in the past; or when it has access to an overall source register.

If you are to serve in a U2 Branch, you will have the responsibility of maintaining the 'theatre source register'. Therefore it is very important to evaluate the credibility of the information with no regard to its source.

There is a natural tendency to take what is reported by a reliable source as confirmed or probably true. But keep in mind that even the most reliable source can provide wrong information.

Slide 15

Key message: Rating is the combination of the source reliability and the information credibility grading; a letter and a number.

By combining the reliability of the source and the credibility of the information, we can attach a rating to a piece of information that is a combination of a letter and a number.

For example, information coming from a B-graded source (minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time) that has 'not been confirmed but is logical and consistent with other information on the subject, must be graded as B2

Please keep in mind that a reliable source can deliver improbable information in which case the rating would be A5. in such a case the figure is more important than the letter as it reflects the confidence level attributed to the information.

Slide 16

Take Away

- The primary objective of collation is to make sure that no information is lost, and all information is easy to retrieve

- All information needs to be recorded and sorted in a common format

- Always consider issues around IT, pragmatism and the use of recording and visual aids

- Evaluation is achieved through: Verification, Comparison and Rating

- To rate a piece of information, its credibility and source reliability is assessed

Summary

The aim of this lesson was to provide you with the necessary information to understand and apply the fundamentals of Collation and Evaluation.

- The primary objective of collation is to make sure that no information is lost, and that all information is easy to retrieve

- All information needs to be recorded and sorted in a common format

- Always consider issues around IT, pragmatism and the use of recording and visual aids

- Evaluation is achieved through: Verification, Comparison and Rating

- To rate a piece of information, its credibility and source reliability is assessed.

Learning Activity

RESOURCES
Whiteboards, chalkboards or butcher/chart paper
Markers and chalk, computers or pens and papers.

Approx. TIME
15-20 minutes

Task:
Students have 10min to read these reports and collate them according to the projected format. See the slide below.

NOTE TO INSTRUCTORS:

Hide this slide below and use it as a tool to discuss the trainee's answers, eventually project it at the end of the discussion. Reinforce the learning outcomes and assess the knowledge of the group and individuals.

Learning activity possible answers

Serial number	Date of information	Date of acquisition	Source	Rating	Subject
1.1	06 Jul 18	07 Jul 18	A Garland Armed Forces (GAF) officer	A/2, A/3,A/4 Or B/2, B/3,B/4	4x4 vehicles entering Garland along un approved roads
1.2	07 Jul 18	08 Jul 18	Grant,	A/1, A/2 Or B/1, B/2 Or C/1, C/2,	the price of weapons and ammunition in the local markets has doubled

L e s s o n
3.3b

Introduction to Analysis and Integration

The Lesson

Starting the Lesson

Interaction. *Have the student break into a few groups. Assign each group a few of the questions below and have them address the class:*

- *Why does our analysis need to align with the commander's requirements?*
- *Why does our analysis need to follow the PKI process?*
- *What do we do to fill information gaps?*
- *Why do we need to deliver analysis on time?*
- *Why does our analysis need to be audible by another analyst?*
- *Why should we draw our analysis from multiple sources?*

Slide 1

We are now going to cover an introduction to Analysis and Integration.

Slide 2

Here is the lesson content. These topics will provide MPKIO / peacekeepers with an understanding of the analysis fundamentals and standards.

Slide 3

At the end of this lesson, you should be able to explain analysis and integration and explain the fundamentals and standards of analysis, as discussed in this lesson.

Slide 4
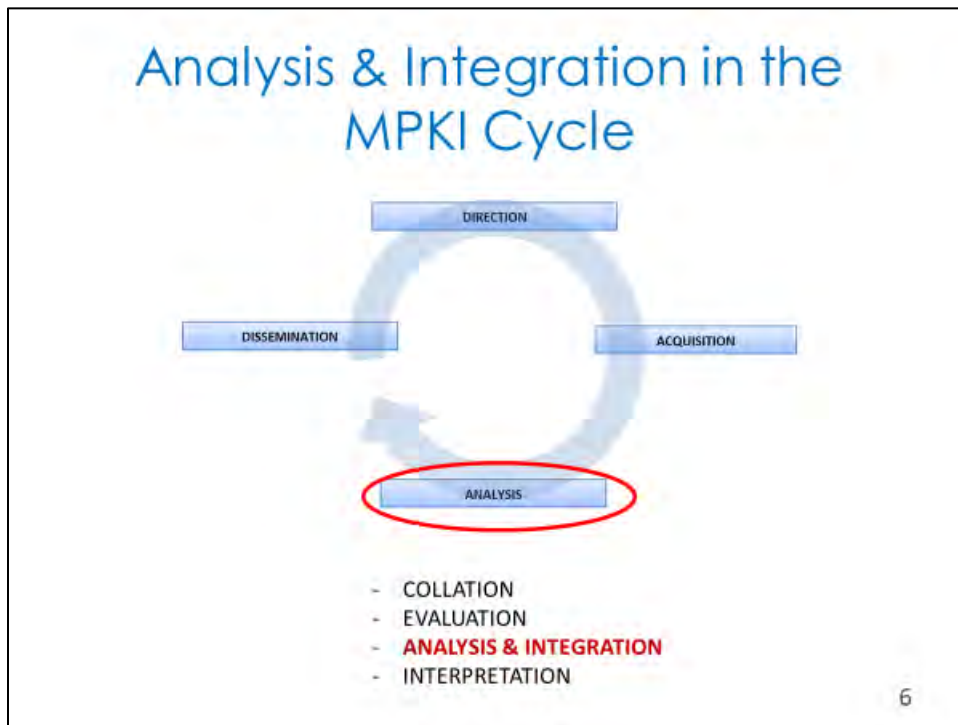
Analysis and Integration is the third step in the Analysis phase of the MPKI Cycle. Let us recap what we have already covered. We had lessons and learning activities on the direction and acquisition phases of the MPKI management cycle. We also covered the first two steps of the analysis portion of the management cycle. In this lesson, we will discuss and apply the 3rd step of the analysis phase, which is analysis and integration.

Slide 5

Key message: Analysis follows a deliberate, structured process or processes that integrate all that we learn intending to enhance our understanding of the operational environment meaningfully.

Analysis Definition:

There are two key elements of the definition of analysis:

- The analysis is structured; it is not intuitive. Analysts use a disciplined process to examine, break down, test and refine the information that leads to reliable assessments; they do not make things up based on gut feelings

- The analysis must develop understanding by revealing the meaning of events in the operational environment that the supported commander is responsible for. This meaning must be predictive, that is forward-looking. However, the PKI analysis needs to help decision-makers understand what events mean for the future, not just what they meant at the time they occurred

Analysis and Integration:

During the Analysis and Integration step of the MPKI Cycle, the methodical and structured breaking down of information into its parts to understand the meaning of events is not enough to support the mission or protect civilians.

An analyst must also consider all the analysed parts and fit them together (integrates them) in order to create an overall picture of what is happening and, more importantly, what is likely to happen in the future.   Only then the analysis will be able to assist decision-makers in achieving the mission better and/or protect civilians.

Why are we so deliberate with our analysis and integration? It is because the peacekeeping environment is always going to have degrees of complexity, and we do not want to overlook important factors.

Slide 6

Analysis Fundamentals

- Aligned with commander's requirements and PKI processes
- Must accept a degree of ambiguity
- Timeliness is more important than perfection
- Must be auditable/replicable
- Deals with quantitative and qualitative information
- Multiple sources of data (avoid single sources)
- Objectivity

Key message: Applying fundamental analysis principles ensures that the quality and timeliness of PKI effectively aids the achievement of mission goals, particularly POC.

No matter how clever it might be, any analytical effort that does not align with achieving the commander's requirements is wasted, so an analyst must understand the commander's requirements before commencing the analysis process.

Also, PKI processes, as outlined in the MPKI HB, have been designed to deliver the best intelligence that supports the UN MDMP. These processes ensure that an analyst can pick up someone else's work and continue it – analysts should therefore follow proper PKI processes as much as possible.

An analyst must be able to accept some ambiguity because, ordinarily, no analyst can achieve complete clarity by removing all ambiguity. An analyst demonstrates their professional competency and courage by offering assessments based on imperfect understanding.

Timeliness is important, good analysis delivered too late can cost lives – it is much more important to meet decision deadlines with incomplete analysis than to withhold information from decision-makers.

It is important that your analysis can be audited and replicated. An analyst needs to be able to show what information they have drawn their analysis from so that other analysts can follow their reasoning and use it.

Analysts may deal with both qualitative and quantitative information, noting that quantitative information is primarily objective and easily measurable. In contrast, qualitative information is primarily subjective and difficult to measure but is necessary to support predictive analysis, so should not be avoided.   For example, if we see a group of fighters we can easily count how many there are and how many weapons they have (quantitative), but we also need to make a qualitative assessment on how effective they might be as a fighting force to predict the level of threat they represent and to whom. For example, if they are all over 70 years old and have trouble walking, we can assess that they will not be very effective.

Single sources of data should be avoided due to the risk of being deceived by a threat source who wants us to believe something that is not true.   By seeking to confirm data through multiple sources, we can gain improved confidence in our analysis, and expose potential deceptions.

While the information we deal with may be subjective (e.g. qualitative), analysts themselves need to remain as objective as possible.   This requires a high level of self-awareness, especially understanding our biases.   Everyone has biases that can affect how we interpret information. Still, if we are aware of what those biases might be (e.g. cultural or family inherited perspectives on ethnicity, gender, religion, social status, dress, courtesy, etc.), we can guard against allowing our biases to affect our analysis. One way to check ourselves is to regularly list and challenge any assumptions we might make (e.g. because of our cultural background we may assume that women are always subordinate to men, and as a result, we may misidentify a woman actor as being insignificant when she may, in fact, be a key decision-maker/influencer in her culture).

Slide 7

All UNPKI analytical product is expected to meet the identified standards to best support the UN MDMP.

- Analysis fundamentals are focused on the analyst, and analysis standards are focused on the product, so they naturally overlap

- The product needs to be objective in that it does not contain bias that will mislead decision-makers

- The product needs to be delivered in time to make a difference

- The product needs to be accurate so that it is reliable, including noting what we don't know (information gaps). Information gaps should then be added to the IAP or sent as RFIs to relevant units

- Products need to be relevant, and they should directly support the achievement of the commander's mission and/or support CPOC. The analysts need to be aware of the commander's requirements and any threats to civilians

- Analysis should be based on information derived from the maximum number of relevant sources that can be practically drawn from in the time available.   As a

rule, the more sources that contribute to the analysis, the more confident we can be in the analytical product

- Appropriate. Analytical tools provide disciplined processes to analyse information in ways that force analysts to consider different perspectives and possibilities.   Analysts should become familiar with a range of analytical tools (found in chapters 7 and 9 of the MPKI HB) so that they can select and use appropriate tools to test and refine information

- Products need to be evaluated. While sources (persons) may not be named in the analytical product, source evaluations should be marked against sourced information (e.g. A man on a green bicycle rode through the crossroad at approximately 1025 Hs [Source: B:3]). What does B:3 tell us about the source and information? Usually reliable and or possibly true.

- Products need to be clear. Clarity is defined as clearly differentiating between fact and assessment – all product needs to be clear on what is known or reported as fact, and what is assessed by the analyst.   For example, it was reported that a man on a green bicycle rode through the crossroad at approximately 1025 Hs.   It is assessed that the man is likely to be John Smith, who owns a green bicycle.   The product should include, where appropriate, explanations of any concerns about the reliability of the information, any reasons for confidence and/or any possible alternative explanations for what has been reported, e.g.,   Source is suspected of being colour blind, therefore it may also have been John Brown who owns a red bicycle

- The product should identify any changes in the analysis since the last time analysis was communicated.   An analyst may be tempted to hide changes if new information arises, and their original assessment is proven to be false. However, a good analyst always seeks to provide the best possible analysis to decision-makers, so should always demonstrate professional courage by identifying changes to assessments, explaining why it has changed

- Lastly, perspectives can often differ between genders offering analysts a useful opportunity to gain a broader understanding of the operating environment. Hence analytical processes and product should always incorporate the perspectives of both genders.   For example, during a riot, men will likely notice other men whom they consider to be a threat to themselves and their families and be focused on them, but women may also notice what is happening to other women and any children in the area and will generally remember supporting details with better clarity than men.

Slide 8

Summary

Analysis that does not support the UN MDMP and decision makers is of no value, therefore an analyst needs to keep in mind that their job is to provide the best possible assessments to decision makers in time to have a positive effect on the protection of civilians and mission personnel, and on the achievement of the mission.

Learning Activity

Exercise

Tasks:

Explain the importance of:

  Timeliness

  Multiple sources (including different genders)

Answer the following question:

If an analyst discovers information that they previously missed, how do they demonstrate professional courage

Approx. Time: Discuss 10

LEARNING ACTIVITY

RESOURCES
Pen and paper, UNPKI HB

TIME
Approx. 10-15 minutes

NOTE TO INSTRUCTOR:

Have the class break into a few smaller groups and have them discuss the above questions (5 minutes).   Ask each group to answer one question for 1-2 minutes and if you think it will not cause disruption, encourage the other groups to challenge the answers given, testing their assumptions and logic (10 minutes).

Questions:

If you provide advice to a decision-maker too late for the advice to affect the plan, all your analytical effort is wasted.   It is critical to delivering an analytical product with sufficient time for the decision-maker to consider it and integrate it into their decision making, even if the product is incomplete or you don't feel like you have a complete understanding (in fact, you should always expect to have an incomplete understanding).   If you do have incomplete understanding, you provide any analytical insights that you have generated in the available time and identify the areas that you feel are incomplete, which will naturally lead to IRs.

2.   Explain the importance of multiple sources (include gender).

An effective analyst will use every available source to add as many perspectives to their understanding as they can to create as complete an understanding as they can in the time available.   An obvious, but sometimes overlooked perspective, is that of gender, so an effective analyst will always consider the perspectives of both gender, which means actively seeking both men and women as sources, if possible in all the represented groups (e.g. if refugees are providing information, be sure to seek information from both the men and women in the refugee group).

3.   If an analyst discovers information that they previously missed; how do they demonstrate professional courage?

An analyst should always seek to offer the best available truth to decision-makers.   This means that if an analyst has previously assessed a likely threat course of action, but new information shows that this is no longer likely, they demonstrate professional courage by immediately amending their assessment and communicating what has changed to decision-makers.

Lesson
3.3c

3 Column Format

The Lesson

Starting the Lesson

Interaction: Break the students into small groups and assign the following questions. Have the students answer the questions and report to the class their answers.

- What is end state/ contribution of our tasks / products?

- Why do we call our products planning guidance?

Slide 1

Slide 2

Here is the lesson content

Slide 3

On completion of this lesson, you will be able to explain the 3 Column Format and accurately derive, identify and fill in relevant factors, deductions and outcomes.

Slide 4

Key message: The 3 Column Format is a simple analytical tool that all analysts need to be able to use to draw deductions and outcomes from factors.

The 3-column format is the cornerstone of PKI analysis – you have already seen it as a tool to derive PIRs, and it is the basic building block of the Peacekeeping-Intelligence Estimate, so if you are not already familiar with it, you must understand it as you will get to use it again, many times.

In very simple terms, it takes what is known or reported as fact (noting that sources may report things that need to be tested and may not be fact) and asks so what, and what are the next steps, that is what we should do about this information and the deductions that we have drawn from it?

A 3-column format is a tool for making deductions and determining outcomes, but it also provides a useful logic trail that you and other analysts can use to test assessments. Most analysts have no problem identifying factors, but many struggles to fully deduce what it means and so can struggle to know what the outputs should be – in this lesson we will help you to avoid those challenges.

As is always the case, such analytical tools are more easily applied as one knows or learns more about the operating environment. It is not easy to make deductions about an operating environment that one is unfamiliar with.

Slide 5

Key message : Factors lead to a relevant result or an output - if a circumstance, fact or influence has no bearing on our mission or the protection of civilians, we can discard it.

The Oxford English Dictionary provides a sound definition of a factor for us, noting that a factor must contribute to a result. Otherwise, it is just an interesting piece of information. Because our analysis must support the mission and/or the protection of civilians, the factors we consider must contribute to a result that supports the mission and/or the protection of civilians.

Example: If we note that next to a refugee camp, there is a historical building that is an excellent example of early architecture, that is interesting, but not a factor we should consider.   If we note that that building is placed on the only high ground that overlooks the refugee camp, we should deduce immediately that its position offers a security advantage to whoever occupies it, and so it impacts on the protection of civilians and potentially our ability to achieve our mission, so it should be considered.

Slide 6

> # Identifying Factors Exercise
>
> **Tasks:**
>
> Identify a factor we should consider if our mission is to secure a refugee camp, and why:
>
> - The rainfall in the region this year conforms to the average over the last 10 years
> - Historically, rain falls in the area of the Refugee Camp in intense downpours during the late afternoon lasting up to 30 minutes, reducing visibility
>
> **Approx. Time:** Consider 3 minutes, answer 2 minutes

Working in syndicate groups have participants review the slide and then discuss. Then have syndicate groups report back brief the plenary. Below are a few areas to assist in facilitating the discussions.

- *Ask which groups identified factor 1 as needing to be considered, and which groups identified factor 2 as needing to be considered.*

- *Ask any group who identified fact 1 why they did so.*

- *Ask any group who answered the fact 2 why they did so.*

Possible solution sets to assist you in facilitation:

Fact 1 is an interesting piece of information, but it has no meaningful impact on the mission or protection of civilians so it does not need to be considered (though allow for some imaginative reasons why someone might include it for consideration) – it only suggests that it is business as usual in the area of the camp.

If the year had had lower than normal rainfall, you could consider whether or not there might be a shortage of water for the refugees, or if it was higher than normal, you could consider whether or not there was a risk of flooding and what impact that might have on living conditions, hygiene and/or waterborne

disease threats, but conforming to the average suggests that the ground is unlikely to be significantly affected.

Fact 2 should be considered as the type of rain reduces visibility for up to 30 minutes, which could provide cover for criminals such as human traffickers or smugglers to move in and out of the camp undetected.   There may also be a risk of flooding if the presence of tents or stores blocks the drainage routes in the camp.

Slide 7

Key message: Deductions produce outputs from factors by repeatedly asking "So what?" until the output is reached.

A deduction is produced when we take a factor and pass it through an analytical process. In the case of the 3 Column Format, we use a very simple process where we repeatedly ask the question, "So what?", each time producing a deduction that leads us closer to output.

An analyst needs to keep asking "So what?" until the output is reached, and not give up too early resulting in a dead-end with no output or output that does not support the mission and/or protection of civilians.

Slide 8a
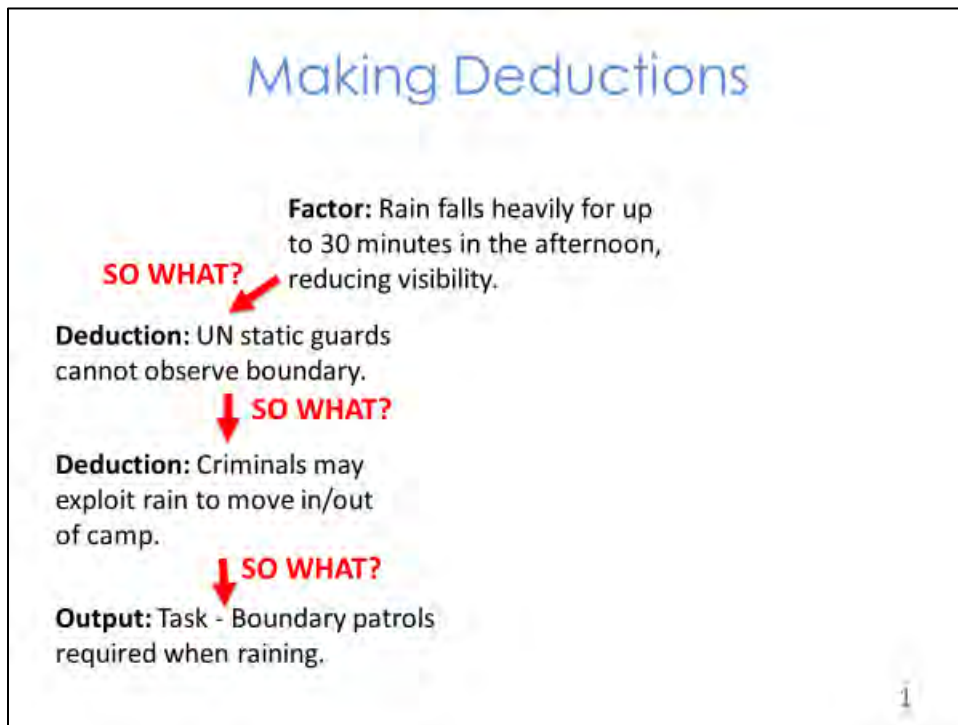
On this slide let us visit an example of this line of deductions. If we start with the factor that rain falls heavily for 30 minutes most afternoons, which reduces visibility, we can ask the question, "So what?". Our deductions might then follow like this:

- Deduction 1 – UN forces may not be able to observe movement in and out of the camp for up to 30 minutes per day. So what?

- Deduction 2 – Criminal elements may exploit this 30-minute window to move in and out of the camp. So what?

- Output – Extensive boundary patrols need to be carried out during rainstorms in order to interdict/discourage potential criminal movement

Slide 8b
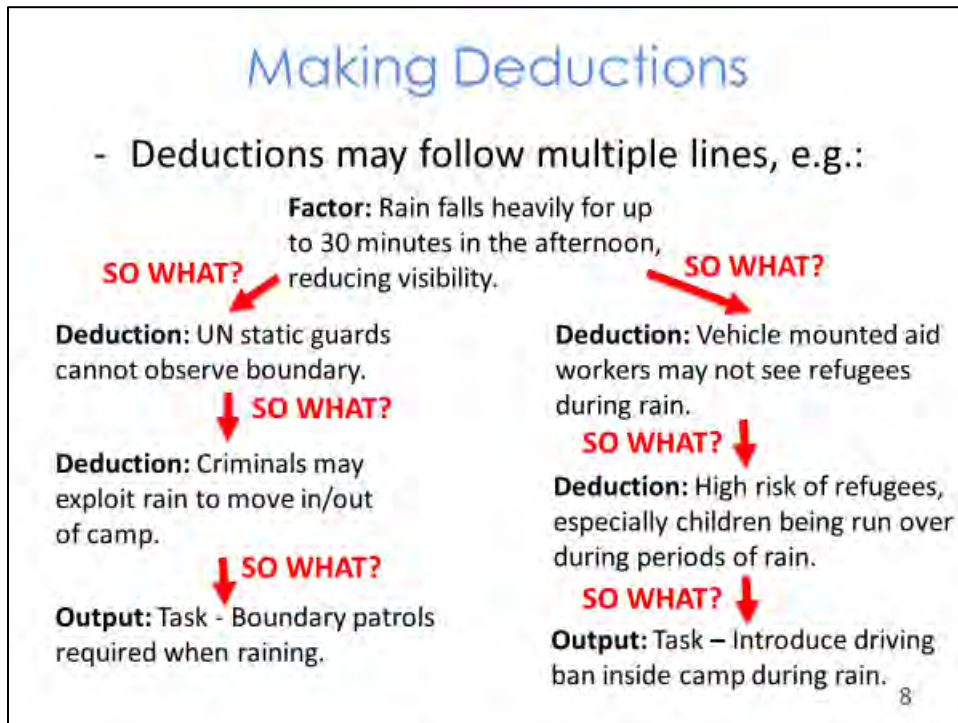
Key message: Multiple lines of deductions and outputs may come from single factors.

Once we have considered a line of deductions that result in a relevant output, be sure to go back to the factor and consider whether or not other lines of reasoning might follow from the same factor, as in the example shown where poor visibility due to heavy rainfall may result in criminal activity AND may place refugees at risk.

Slide 9

Making Deductions

- Deductions may follow multiple lines, e.g.:

Factor	Deduction	Output
Rain falls heavily for up to 30 minutes in the afternoon, reducing visibility	1.1 - UN static guards cannot observe boundary. 1.2 - Criminals may exploit rain to move in/out of camp.	TASK (T) – Task - Boundary patrols required when raining.
	2.1 - Vehicle mounted aid workers may not see refugees during rain. 2.2 - High risk of refugees, especially children being run over during periods of rain.	TASK (T) – Introduce driving ban inside camp during rain.

This is what those two lines of deductions might look like in the 3 Column Format.
From this slide, now we can see how this also provides a good way for other analysts to audit your analysis; that is, they can follow your reasoning so that they can test or build on your initial analysis.

Slide 10

Working in syndicate groups have participants review the slide and then discuss.
Then have syndicate groups report back brief the plenary. Below are a few
areas to assist in facilitating the discussions.

- *Ask two or three groups to explain their deductions*

- *If you can see their logic, complement them, if you can't see their*
  logic, ask them to expand on their deduction

- *Complement any imaginative deductions*

- *Complement anyone who also offers a relevant output*

Possible solution sets to assist you in facilitation:

- *Refugees may block drainage routes with rubbish. [Possible output: Task –*
  Provide rubbish bins]

- *Rubbish may spread through the camp and spread disease. [Possible*
  output: Task - Clear drainage routes daily]

- *Toilets may overflow and spread disease. [Possible output: Planning*
  Guidance – Toilets to be constructed on the high ground]

- *Children playing in the water will be exposed to diseases. [Possible output: Task – Impose a rain curfew]*

- *Standing water poses a drowning threat to small children. [Possible output: Task – Impose a rain curfew]*

- *Some accommodation may be flooded, causing dampening of bedding and a health risk. [Possible output: Planning Guidance – Plan to hold dry bedding in reserve]*

- *Family food stores may be flooded, causing food to rot and health risk when eaten. [Possible output: Planning Guidance – Consider a food swap option to exchange rotten food]*

- *Snakes may be flushed out of holes posing a threat to refugees, especially children. [Possible output: Task – Impose a rain curfew]*

Slide 11

Key message: Outputs are the natural result of exhausting a string or line of deductions.

When you have exhausted a line of deductions, the natural product is output. You can recognise an output because it identifies something that must be done, rather than a deduction that is further information derived from a factor or a previous deduction but does not require you to do anything. Deductions build understanding, but outputs require an action to do something.

Multiple outputs can be derived from a single factor, for example, a series of deductions from the single factor that rain reduces visibility may produce a clear task (such as patrolling the refugee camp boundary during rain) and a Request For Information (such as "What routes do known criminal groups use to enter and exit the refugee camp?")

Outputs come in several forms, which we will discuss in more detail on the next slide.

Slide 12

> ## Types of Outputs
>
> - **Task**. Action needs to be taken
> - **Planning Guidance**. Advice on to consider during planning
> - **Information Requirement**. A requirement for internal answer
> - **Request for Information**. A request to an external audience for an answer
> - **Constraint**. A factor preventing freedom of action during a mission
> - **Freedom**. A factor providing physical or conceptual room for action during a mission

Key message: Outputs take several forms, but each requires a tangible response.

Ask the students to explain these types of outputs. Use the narrative below to facilitate or explain.

The following are common outputs:

- Task – something that needs to be done in order to protect civilians or ensure the success of the mission

- Planning Guidance – something that decision-makers should consider including in their plans in order to protect civilians or ensure the success of the mission

- Information Requirement – A question that needs to be resolved by UN staff.

- Request for Information – A question that is asked of external sources (e.g. local police), the answer to which provides information that will help to answer an Information Requirement or that provides a new factor to analyse

- Constraint – a factor that reduces the UN's ability to protect civilians or complete their mission, which requires action to avoid or address [this output identifies things that slow down the UN's ability to act therefore should result in corrective adjustments to the plan]

- Freedom – a factor that creates an opportunity for the UN to act more freely in the protection of civilians and/or the completion of the mission [this output identifies things that speed up the UN's ability to act, therefore should result in additional or accelerated actions]

These are the standard types of outputs; however, an analyst can use their own judgment to identify an output that may not fit neatly into one of these headings but does help decision-makers to better protect civilians of achieving the mission. For example, an analyst may deduce that there is a significant risk to either civilians or UN personnel, and so could simply identify a risk that needs to be urgently considered as an output.

Slide 13

Take Away

• The 3 Column Format is the cornerstone of PKI analysis, understand how to use it

• The keys to the 3 Column Format are:

— Identify factors that are relevant to the mission and/or protection of civilians

— Produce deductions by asking "So what?" repeatedly until you reach an output

— Produce outputs that result in something that needs to be done

13

Summary

Given that the 3 Column Format is the cornerstone of PKI analysis, analysts need to ensure that they can use it.   To do so they need to be able to identify factors and make relevant deductions that produce outputs that support the achievement of the UN mission and protection of civilians.

Learning Activity

RESOURCES:

Exercise Instructions (MPKIO.RTM LA 190918_20_Three_Column_Format_Exercise_TTT_UNUC.docx)
Threat Profile: ENLF (190828_06_Eyrian_Independent_Movement_Fighters_Threat profile_TTT_UNUC.docx)
Class notes
MPKI HB
Pen and paper

TIME:

Approx: 45 Minutes

TASKS:

- Practice using the 3 Column Format for analysis of the Eyrian Independent Movement Fighters.

- Produce draft 3 Column Format product.

Instructor Notes-

- Ensure that the students have the Exercise Instructions and Threat Profile

- Encourage the class to start at the beginning of the Threat Profile and draw out facts as they go and make deductions (tell them not to try to read and absorb the whole document before beginning to make deductions, this will take too much time).

- Emphasize that you are looking for identification of factors, good deductions and logical outputs – they should not rush through the document at the expense of the quality product.

- Look for students who are not writing and coach them to get them writing.

- After approximately 30 minutes, spend 10 minutes to:

  - Ask students what difficulties they had and help them to resolve them.

- Invite students to offer up key deductions and outputs – discuss the quality of those deductions and outputs and complement and/or suggest improvements.

- Inform students that they will have an opportunity to practice the format again as part of the lessons on Analysis of the Operating Environment (AOE)

3-column Format Exercise: Threat Evaluation EIMF

Task (20 minutes):
Use the Three-Column Format to analyse the EIMF using the Threat Profile below.
- **Focus on:**
  - Selecting relevant factors

  - Making deductions that lead to outputs

  - Producing outputs that require a response

- **Use the following process:**
  - Start at the beginning of the document

  - Identify a factor and record it in the first column

  - Draw out deductions and record them in the second column

  - Produce outputs and record them in the third column

  - Continue in the document, identify the next factor and repeat the steps above

Threat Profile - EIMF

Name		Eyrian Independent Movement Fighters (EIMF)
Classification		Ethnic-based Eastarian Separates
Bases of Operation		South Eri Province
Date formed		2012
Strength		1,500 – 3,000 (active and inactive) members
Organisation	Organisation al Structure	While EIMF forces are likely following a traditional, hierarchical military structure, there is little further verifiable information about the group's specific order of battle. Platoon-sized units (30-40) operating under the leadership John Sparrow in the towns/villages of South Eri Province. Like the Eri National Liberation Front (ENLF), EIMF maintains a decentralised structure, as a means of both

		retaining operational security and avoid set-piece conventional warfare with the more powerful Garland Armed Forces (GAF). It is suspected that there is cross-membership between EIMF and ENLF members residing along the provincial borders along White Lake.
	Command & Control	Leader: John Sparrow. Like his ENLF counterpart, Le Pew, John Sparrow is a shadowy figure who is suspected of maintaining his HQ across the border in Eastland. Sub-unit commanders do NOT meet openly, and it is suspected that most do not even know who the other sub-unit commanders are. They communicate through Whatsapp and couriers.
	Financial sources	Information is limited, and EIMF is known to collect taxes in areas under its control, mainly South Eri Province and suspected to receive funding from the Government of Eastland and the Eastarian diaspora. The group also controls some artisanal mines in South Eri Province. EIMF maintains links to lower-level GAF commanders and uses these links to sell what it mines. It also trades with businessmen in Eastland.
	Assets	Vehicles mounted with light machine guns (LMG); AK-series assault rifles; Mounted anti-aircraft guns; Rocket-propelled grenades (RPG); 60mm Mortars; and Improvised Explosive Devices (IEDs)
Intention	Founding Philosophy	The EIMF (South Eri Province) separated from the ENLF in 2012 and operated independently. The group maintains an operational philosophy of defending the Eastarian mountain culture from Dotan and Sunka influence. In their view, the only means to defend the culture is to secede from Garland and form an autonomous nation-state, but with free trade with Eastland. To achieve this, they maintain the identical position as ENLF - bleeding the GAF through "death by a thousand cuts." They also see victory as a multi-generational goal and will "shame all who attempt to control them."
	Mission Stated	In November 2012, an unidentified EIMF spokesperson announced the formation of the group as the 'Eriyan Independent Movement Fighters.' Their mission is to restore the independent tribal lands confiscated during the War of One Hundred Moons (circa 1080-1100).
	Current Goals	The creation of an autonomous state of ERI, separate from both Eastland and Garland. It appears the EIMF is attempting to further their cause through

		political dialogue, having suspended military operations in 2016.
	Evolution of the Group	The group originally constituted the northern branch of the Eriyan fighters against GLA. When Garland gained independence in 1983, with the GLM becoming the ruling party in Garland, the remnants of the ENLF started a campaign to fight for Eastarian rights in Garland. During the Garland invasion of Eastland in 1988, the ENLF conducted guerrilla raids on GAF lines of communication and supply. Between 1990 and 1991, ENLF forces split geographically between North and South Eri Provinces, under the command of Joseph Le Pew and John Sparrow respectively. After the 2012 attempted coup, the EIMF (South Eri Province) separated from the ENLF. The majority of the ethnic-Eastarian officers who attempted the coup came from SOUTH ERI Province. To show solidarity, the EIMF was formed and officially separated from the ENLF on friendly terms. However, the two (2) groups have different political agendas (the ENLF wants to secede from Garland and join with Eastland, whereas the EIMF wants to establish an autonomous nation-state) and compete for resources in some areas, particularly along the border between North and South Eri Province.
Linkages	Allies/Support	ENLF
	Influence	South Eri Province
	Opposition group	GLM/GPF and GAF
Threat Assessment	TTPs	Small unit raids and ambushes. Known to kidnap foreigners supporting the government (usually released for ransom, seldom murdered).
	Capability	Co-ordinated military operations at the squad (8-12 fighters) platoon (20-40 fighters).
	Weakness	Little cohesiveness beyond village/town militia units. Influence limited to South Eri Province.
	Greatest strength	Cross-border safe havens in Eastland; mountainous terrain as inhibiting context, decentralised command and control; and access to resources at the artisanal level.
UN Operational Implications	Threat level	
	Benefit	UN Humanitarian Support for the people of South Eri Province. UN reports on human rights abuses by the GAF.

Related to EIMF	Harmful	UN reports on human rights abuses by the EIMF. UNODC surveys on black market smuggling operations. UN removal of illegal tax collection checkpoints. UN interruption of information trade across EIMF controlled border crossings.
	Assets Against the UN	Vehicles mounted with light machine guns (LMG) (Technicals); AK-series assault rifles; Mounted anti-aircraft guns; Rocket-propelled grenades; 60mm Mortars; Improvised Explosive Devices (IEDs)
	Vulnerability	Roadside IEDs; Collateral effects of GAF/EIMF operations
Operational History		**2012** EIMF separated from the ENLF and began operating independently in South Eri Province. **2013-2015** No reliable database exists on EIMF activities between 2013 and 2015. According to government sources, over 80 "acts of terror" occurred throughout the province of South Eri Province, with GAF suffering 20 killed and 18 injured in clashes with the group. The Government of Garland confirmed 11 hostage incidents within the Eri National Park, with all incidents successfully resolved. According to the independent think-tank South Eri Observatory for Human Rights (SEOHR), GAF has lost over 130 soldiers killed and 200+ injured. Seven (7) international mining offices were raided with 19 hostages (foreign nationals) held for ransom in the Eri National Park. SEOHR analysts reported widespread reprisals and detentions by GAF against the families of "identified" EIMF members, as well as surviving family members of those executed for planning and participating in the failed 2012 coup. **2016** While no attacks were attributed to the EIMF in 2016, the stall of the talks in Garville coincided with a few of attacks in the South Province adjacent to South Eri Province, with at least six (6) attacks taking place against military targets over the course of 2016. OHCHR reports that ERI villages along the border of South and South Eri Provinces were the targets of midnight raids by GAF in the search for weapons and evidence of EIMF involvement.

	2017

There were NO reports of EIMF activities throughout 2017. GAF released a statement saying, "the EIMF no longer poses a threat to the peaceful people of SOUTH ERI Province, who have endured untold hardships under their yoke." The Government of Garland asked the UN to conduct a DDR Programme

2018

As general election approaches, EIMF has stated that it continues to maintain the peace in South Eri Province, but that it expects talks on the establishment of an autonomous state to recommence in the short-term. EIMF welcomed the deployment of the 7CF and UNMMIG 01, and no clashes occurred.

EIMF has stated that it will not enter the UN-led DDR program until its political goals are satisfied.

EIMF clashed with the ENLF over control of border crossing points to Eastland.

There have been reports that EIMF is recruiting fighters at Protection of Civilian (POC) sites along the border with North and South Eri Provinces.

There have been reports that EIMF is short of resources to sustain operations.

There have been reports of some EIMF violations of Human Rights at POC sites. |

Lesson
3.3d

Other Analytical Tools

The Lesson

Starting the Lesson

Slide 1

This lesson aims to provide MPKIOs with information on the principles and basic skills of other major analytical tools used in the MPKI framework.

Slide 2

Here is the content of the lesson

Slide 3

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

Introduction

- Analytical tools assist us to see information from different perspectives

- There different tools other than 3-column format

- Graphical tools help us absorb information quickly and give us briefing tools

- Two key categories of graphical tools:

    - Pattern analysis-Timeline, Time Event Chart, Event Mapping

    - Link analysis- Association Matrix, Link Diagram

4

Key Message: While the 3 Column Format will be the tool we will most commonly use, we need to be aware of other analytical tools that can enhance the quality of our analysis.

Tools other than the 3 Column Format need to be considered for use by analysts as they can offer different ways of looking at problems that help us to understand meaning better.

Tools that represent information graphically are particularly helpful for making sense of complex issues involving multiple factors, both for the analyst to be able to identify the meaning of events and information more quickly and to help brief information in a way that decision-makers can quickly integrate intelligence into their decision making.

In this lesson, we will look at two key categories of graphical tools – Pattern analysis and Link analysis.

Pattern analysis uses graphical tools to display information that depict patterns in time, activity, location and any other information that can be graphically represented to reveal patterns.   The key to pattern analysis is that its ultimate purpose is to reveal patterns that allow analysts to make predictions that assist decision-makers in achieving the mission and protect civilians.   We will cover the timeline, time event chart and event mapping as basic pattern analysis tools.

Link analysis uses graphical tools to facilitate greater understanding of the relationships between entities (individuals and organisations) and activities or events (p.56).   The key to link analysis is that its ultimate purpose is to reveal linkages that allow analysts to make predictions that assist decision-makers in achieving the mission and protecting civilians.   We will cover the link diagram and association matrix as basic link analysis tools.

It is always important to remember that pattern analysis becomes far more difficult if the analyst does not have deep contextual knowledge of the operating environment. Such knowledge will help the analyst to make the necessary connections.

Slide 5
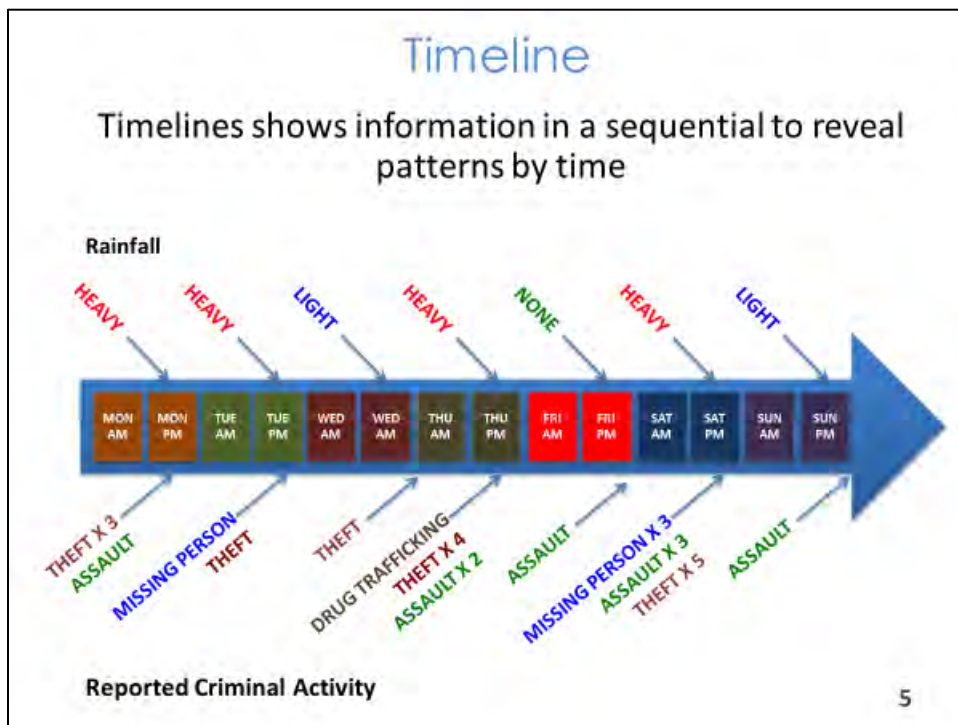
Key Message: Timelines order information in a meaningful way along a line.

Timelines are one of the simplest pattern analysis tools to use and can reveal meaning with minimal effort for the analyst.

For example, this timeline shows the relationship between rainfall and reported criminal activity in a refugee camp that the UN is protecting. By simply ordering the events in line with the heaviness of the rain on the top and reports of criminal activity below, we can quickly see a pattern of the majority of criminal activities occurring during times of heavy rain, presumably due to the loss of visibility during heavy downpours and therefore opportunity to carry out activities of a criminal nature.

If you extend this out to cover several weeks, then the pattern would become clearer, or the analyst may discover that it is not a consistent pattern.

Note that by colour coding days and activities, the timeline further uses a visual representation to help absorb information.

Timelines can take many different forms, and cover any period an analyst chooses, so long as they order events over an identified period (e.g., week, month, year, or between set dates or times) and that they identify meaningful patterns that give meaning and assist in predicting future events.

Slide 6
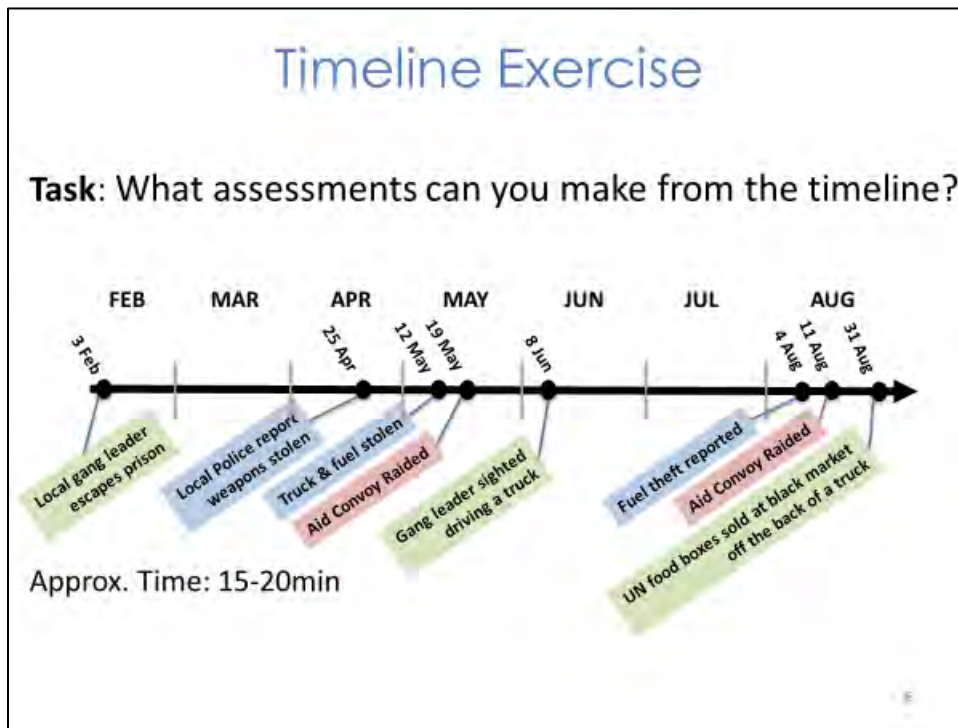
Working in syndicate groups have participants review the slide and then discuss. Then have syndicate groups report back brief the plenary. Here are a few areas to assist in facilitating the discussions. Emphasise the pattern of fuel theft a week before convoy raids may help them to predict future criminal actions and when / how best to protect convoys.

Note to Instructor- Possible answers:

The gang leader is likely involved in the thefts and convoy raids if there were no raids before the gang leader escaping prison.

The stolen truck is likely the one the gang leader was seen driving and the one the assumed stolen UN food was sold from.

Fuel is stolen one week before the convoy raids, so the fuel was likely stolen to use in the truck to assist in the convoy raids.

When fuel is stolen in the future, additional security should be provided for convoys in anticipation of a raid.

The most likely meaning to these events is that the escaped gang leaders stole weapons and a truck to raid UN convoys to steal food for sale on the black market, potentially planning a raid every 11 weeks.

Interaction. Ask the student what other information would have helped them in their analysis. The responses should include additional data on previous criminal activity. This added context is essential to effective pattern analysis.

Slide 7
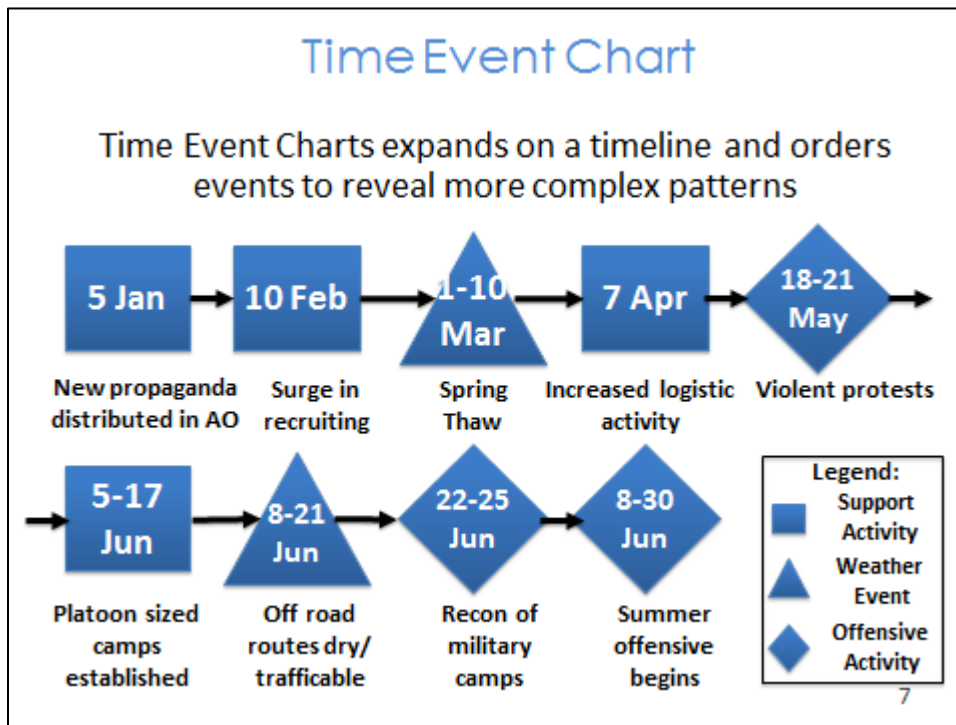
Key Message: Time Event charts order events by time, but using a chart and symbol format, they reveal patterns in activities and time from more complex data than would be practical in a simple timeline.

Time event charts take more effort than timelines but are well worth it to reveal patterns that timelines may not reveal clearly. A time event chart would be used when there is more data or more complex data than a timeline could usefully display.

For example, this is a simple time event chart showing an observed sequence of events that helps decision-makers to predict when a northern hemisphere insurgent group might start their summer offensive. Note that the symbols represent different types of information.

The Time Event Chart is read from left to right and top to bottom in a linear fashion over 6 months. Here it is displayed, and we can see and follow how the insurgent group prepared last year for their summer offensive, becoming more active as the weather improved. While it most likely not be the same this year, it provides a useful framework to make a predictive analysis.

Slide 8
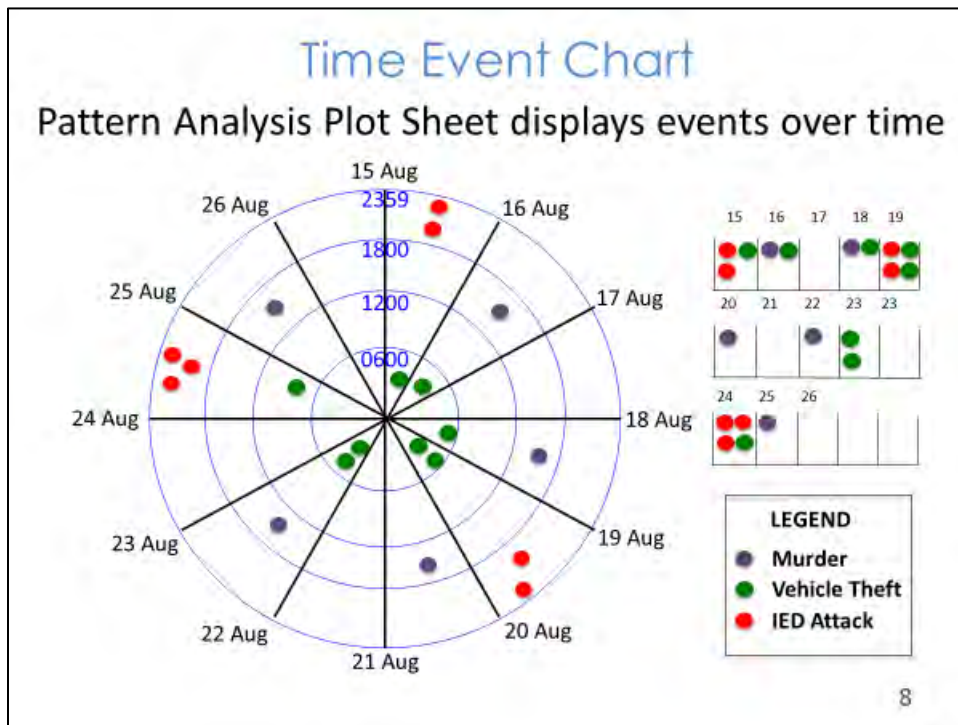
Key Message: This circular type of Time Event Chart reveals patterns by displaying events by type, date and time, which hopefully reveals patterns that allow us to predict future events.

Narrative: This circular Time event chart is also called a Pattern Analysis Plot Sheet, a Pattern/Time Analysis Tool, or just a Time Event Chart.   It displays events by type, date and time, which hopefully reveals patterns that allow us to predict future events.

This Pattern Analysis Plot Sheet has divided the circle into 12 segments representing the days from 15-26 August.   The four concentric circles, each increasing in size from the centre out, divide up time blocks from 0000 to 0600, 0600-1200, 1200-1800 and 1800 to midnight.

The events are colour coded by type (shown in the legend, bottom-right) and they are plotted in the date/time segments that the events occurred in, and in a calendar (top-right) for cross-checking.   Footnotes may be added on the chart or attached to the chart for extra explanation.

In this example, the patterns that can be identified are:

- Murders happened at least every second day [do murders require a day of planning/movement between them?

- Murders all happened on days that there were no IED Attacks [are murders and IED attacks carried out by the same groups and therefore cannot occur on the same day?

- Vehicle thefts occur in the early morning, generally before 0600 [is this when most vehicles are left unattended by their owners and hence are easier to steal]

- Vehicle thefts occur most days [are vehicles being used for activities only once and then discarded or are they being sold to raise funds?

- IED attacks occurred in the evening or late night [is this time chosen to target commuter traffic or to use the cover of night for attacks?

Slide 9
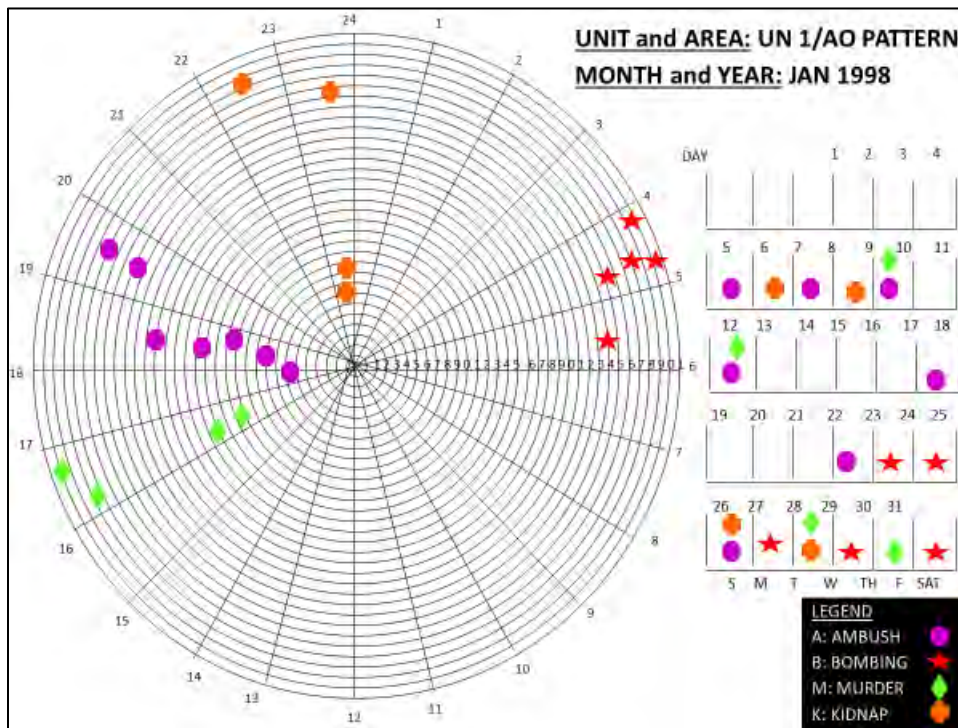
Key Message: You can adapt Pattern Analysis Plot Sheets to cover whichever timeframes are of value in your analysis.

Narrative: Pattern Analysis Plot Sheets can be adapted to suit your analytical needs.

For example, this Pattern Analysis Plot Sheet covers insurgency activity in AO Pattern across the month of January 1998.

The analyst who constructed this chart decided to make the segments the hours in the day (1-24) and the concentric circles the dates (starting in the centre with 1 Jan, noting that to save space, they use the pattern 1-9, 0-9, 0-9, 0-1 to show the 31 days in January, this instead of using 1-9, 10-19, 20-29, 30-31).

This reveals the following patterns:

- All bombings occurred between 0400 and 0600 and after 23 Jan

- All murders occurred between 1600 and 1700

- All ambushes occurred between 1700 and 2000 with a minimum of 1 day between events

- All Kidnappings occurred between 2200 and midnight, two at the beginning of the month, two at the end of the month

You should play with the way you structure these charts to display events in a way that best reveals the patterns.

Slide 10
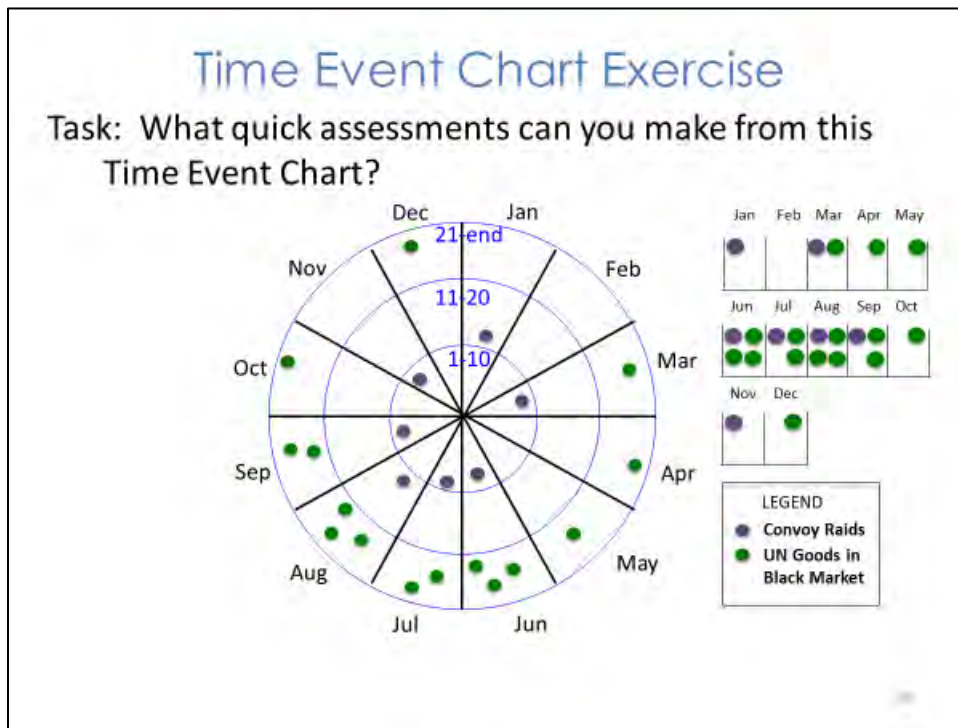
*Working in syndicate groups have participants review the slide and then discuss.
Then have syndicate groups report back brief the plenary. Here are a few areas
to assist in facilitating the discussions. Total TIME 5-10 minutes.*

Possible answers:

*Convoy raids occur early in the month. UN goods are sold on the black market
10-20 days after raids [stolen goods are possibly hidden until police/UN give up
looking for them].*
*Convoy raids are every month over the warmer months, every two months over
cooler months [possibly due to difficulty moving goods over winter, or lower
demand on the black market?]*

*Remember, it is important to note that drawing real meaning from such patterns
is more difficult without having a deep understanding of the operational
context. For example, we assume that the period from June to October is a
summer period, but in the southern hemisphere, this might not be the case.*

Slide 11
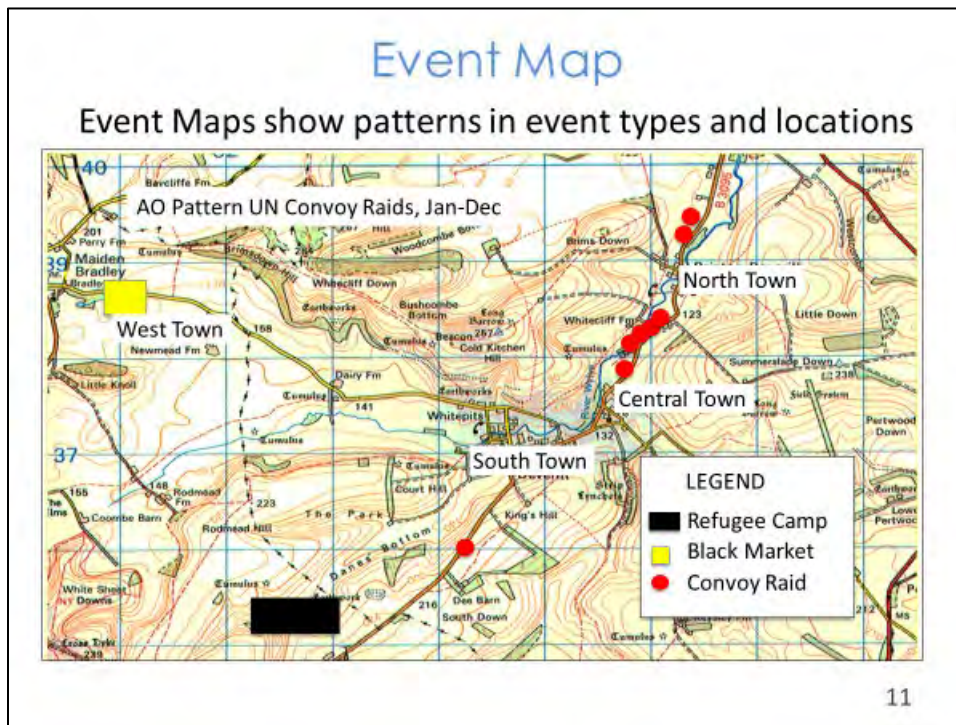
Key Message: An Event Map is simply events plotted on a map that reveals patterns in locations and event types.

Event maps are a common intelligence tool, so most of you are probably familiar with them in one form or another. We display events on a map in a way that reveals patterns and assists us in predicting future events.

In this example that displays locations where raids by insurgents on UN convoys have occurred over 12 months concerning the black-market locations where UN goods have been seen for sale.

Interaction. What patterns can be identified here? Facilitate discussion using the following possible solution sets.

- *Insurgents prefer the northern road to conduct their ambushes, primarily between North Town and Central Town [is this the best terrain for ambushes?]*

- *Insurgents avoid raid locations near South Town [stolen goods may be stored in South Town, and they wish to avoid Police attention there?]*

Event Maps are very useful for displaying graphical patterns from which predictions can be made, and, of course, they are also very useful briefing aids to help decision-makers absorb information.   You can add notes and, potentially, dates and times to your Event Map if it does not become so cluttered that it becomes confusing. Of note, if the tool you are using makes things more complex and confusing, you should find a tool that gives more clarity and simplifies the analysis process.

Slide 12

Working in syndicate groups have participants review the slide and then discuss. Then have syndicate groups report back brief the plenary. Here are a few areas to assist in facilitating the discussions.

☞ **Note to Instructor-**

Possible answers: (Complement imaginative observations):

- Anti-election violence was concentrated around North Town and Central Town [possible stronghold for insurgents?]

- West Town and South Town have no violent events [possibly to avoid compromising black-market insurgent activity in those two towns?]

- Some attempts to intimidate refugees [possible insurgent supporters in the refugee population?]

- Are we missing context here? What more would the students like to know? This **missing data should become RFIs/IRs**

This is the last of the three Pattern Analysis tools that we will look at, and now we will look at two Link Analysis tools.

Slide 13
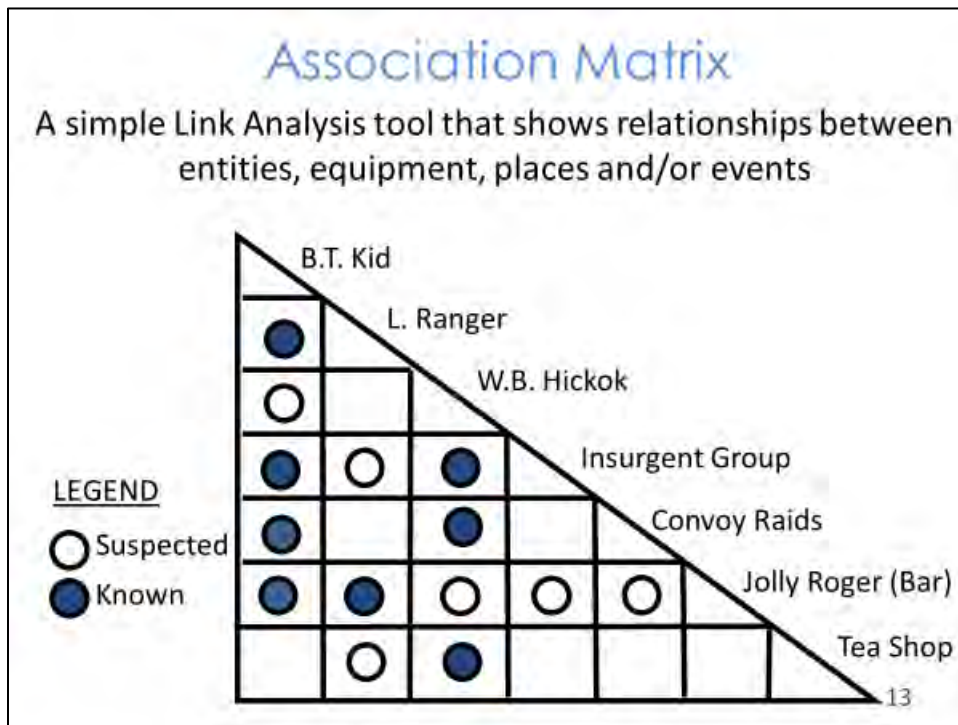
Key Message: An Association Matrix (sometimes referred to as a Relational Matrix) is a simple Link Analysis tool that reveals linkages between entities and events.

An Association Matrix is one of the simplest Link Analysis tools to use and help to make sense of relationships between entities, that is individuals or organisations, and events.

The circles on this Association Matrix show whether the association is known or only suspected, i.e. there has not been enough reporting to be sure of the association, but there is enough to be suspicious.

For example, this Association Matrix suggests the following:

- B.T. Kid is connected (or suspected to be connected) to everyone/thing else, except for the Tea Shop, and so may have a leadership role

- The Jolly Roger Bar is likely to be a meeting place for planning and preparation for insurgent activities such as the raids on UN convoys

Slide 14
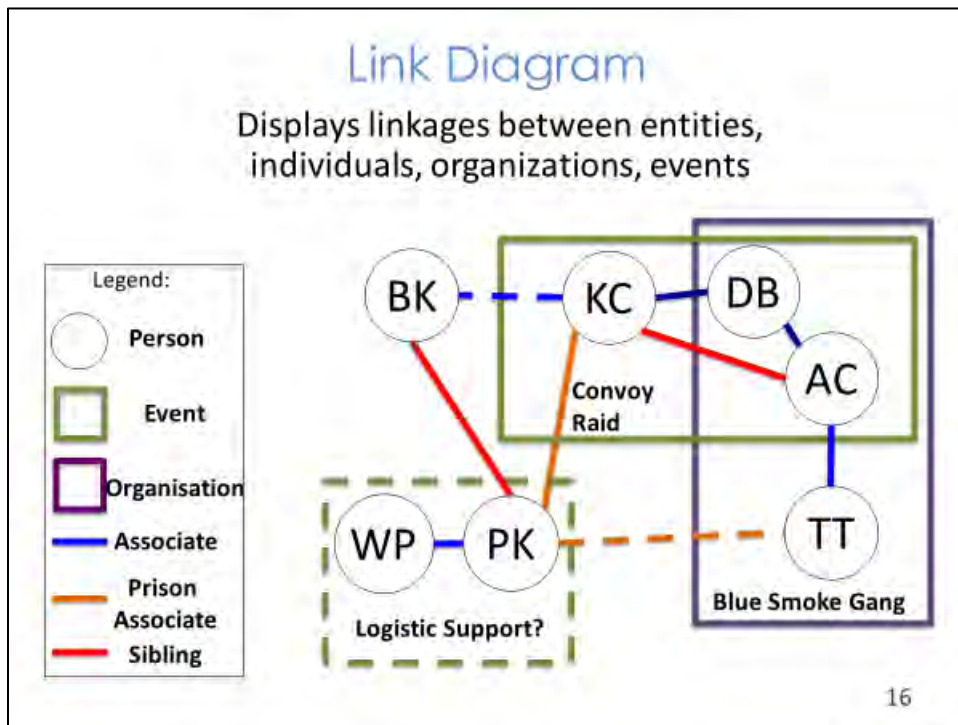
Key Message: A Link Diagram (sometimes referred to as a Link Chart) is a more detailed Link Analysis tool (than the Association Matrix) that reveals linkages between entities and events, and can show types of entities, events and relationships.

A Link Diagram is a Link Analysis tool that includes more detail in the relationships between entities and events than an Association Matrix allows. Symbols are used to denote the type of information displayed, and solid lines show confirmed linkages while dotted lines show suspected linkages.   Symbols and lines can be colour-coded to display additional information such as the type of event or type of relationship.

For example, this Link Diagram shows who was identified as raiding a UN convoy, and the known members of a local insurgent group (the Blue Smoke Gang. What can we deduce from this? Here are a few suggested deductions:

- DB and AC are confirmed insurgent group members and involved in the raid
- KC and AC, being siblings strengthen the linkage between the gang and raids
- The person with more connections is KC, makes it possible that KC is a leader
- BK is yet unconnected to events, but they will be a person of interest due to their links to both KC and PK, even though the link to KC is not yet confirmed

The tool here is constructed by the analyst to assist in the understanding of complex relationships. The analyst continues to populate and adjust the diagram to help reveal linkages that have meaning.

Slide 15

Additional Analytical Tools

- You have been exposed to a small number of possible tools
- Explore additional analytical tools:
  - mind-mapping
  - brainstorming
  - ACH, SWOT analysis
  - COG analysis
  - gender analysis

Reference: MPKI HB, pp. 55-57, 81-84, 88-89   18

Key Message: As a part of their professional development, analysts should explore the use of additional analytical tools.

In this lesson, we only cover a few tools, but there are others in the UN MPKI Handbook, that you should review once you have mastered the basic tools.

Remember that each tool can help you discover different aspects of the operational environment. It is important to regularly step back and integrate all your analysis products and outputs to ensure that you are visualizing the whole picture, not just part of one or two analytical tools reveal.

Slide 16
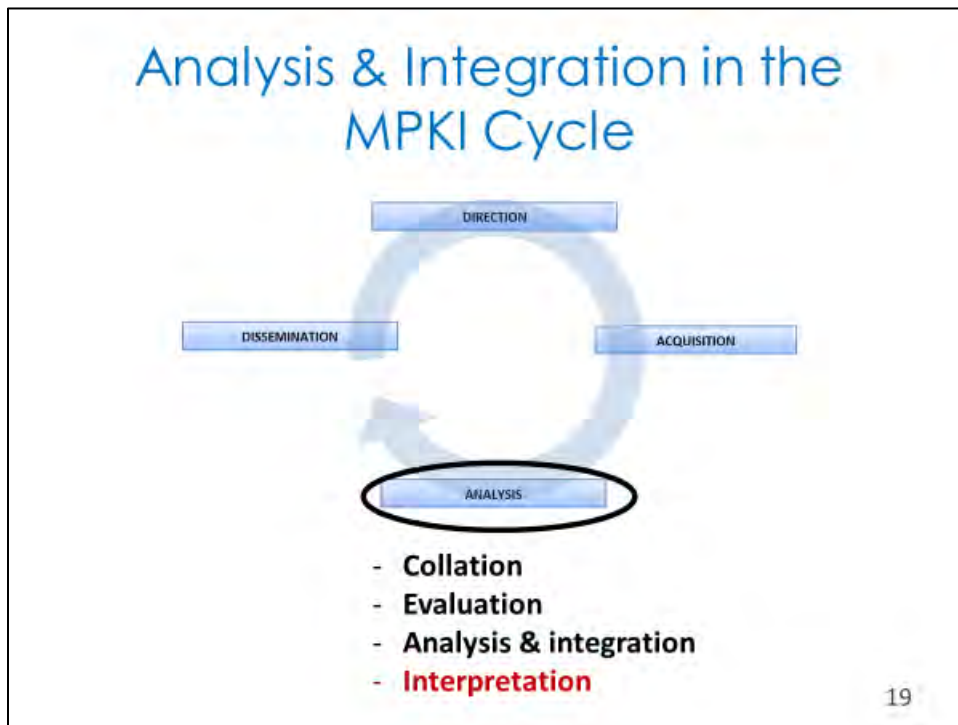
Key Message: Interpretation is the last step in the Analysis phase of the MPKI Cycle.

Before we practice using an analytical tool, let's quickly cover the final step in the Analysis Phase of the MPKI Cycle.

After collating and evaluating the information we have acquired, we then analyse and integrate this information using analytical tools, and then the last step in the Analysis phase of the MPKI Cycle is to interpret the new information, delivering peacekeeping-intelligence.

Slide 17
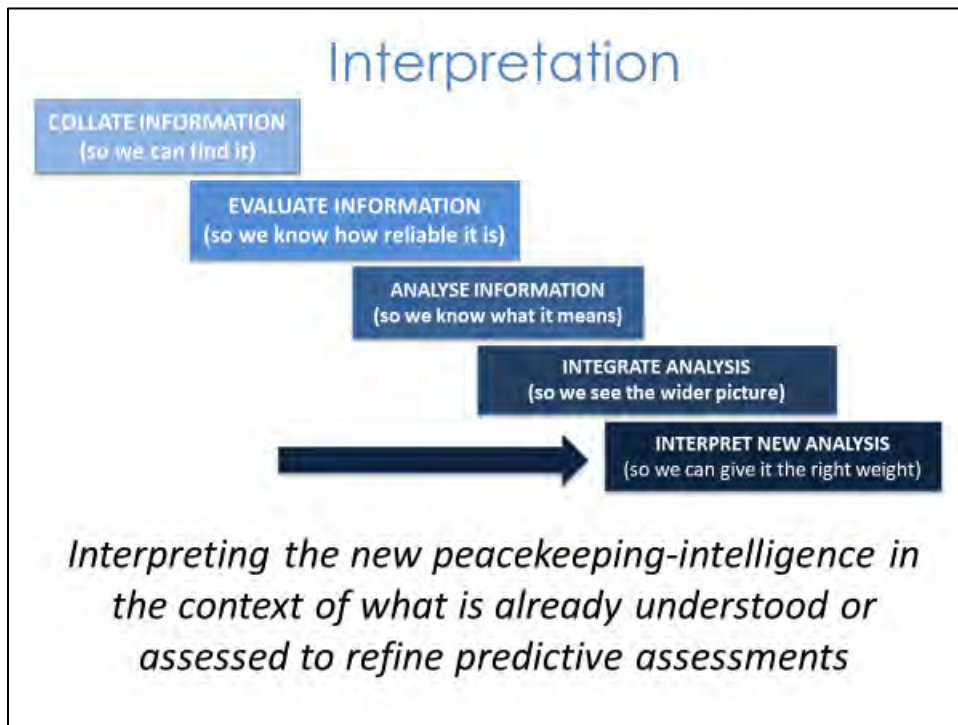
Interpretation is effectively a validation check to ensure that our analysis meets two criteria:

1. It contributes to the commander's priorities to achieve their mission, help contribute to a secure environment, and assist in CPOC planning
2. Predictive in nature to support the commander and staff in planning operations

Slide 18

> ## Take Away
>
> - In addition to the 3 Column Analysis tool, Pattern Analysis and Link Analysis include analytical tools:
>   - Timeline
>   - Time Event Chart
>   - Event Map
>   - Association Matrix
>   - Link Diagram
> - Analysts should become conversant with a range of analytical tools in order to provide the best possible analysis to decision makers
> - The final step in the Analysis Phase is to interpret new intelligence, relating it to previous assessments
>
> 21

Summary

Analysts should become conversant with a range of analytical tools in order to provide the best possible analysis to decision makers.

The final step in the Analysis Phase of the MPKI Cycle is to interpret the intelligence that has been collated, evaluated, analysed and integrated. This is done by critically considering its weight considering previous assessments. Of note, analytical tools do not produce analysis; instead, they assist the analyst in the process and helps them visualize the process.

Learning Activity 1

RESOURCES:
Exercise Instructions (MPKIO RTM TTX
190821_18_Pattern_Analysis_Exercise_TTT_UNUC.docx)
Class notes
MPKI HB
Pen and paper

TIME:
Approx. 1 hour

TASKS:

- Produce a Timeline

- Identify patterns

- Present conclusions

-

Instructor Notes-

- Ensure that the students have the Exercise Instructions.

- Instruct the students to begin with the Timeline, then work on the Association Matrix.

- Emphasise that they are looking for identification of patterns, so quickly place the information on the Timeline or in the Association Matrix, then spend time discussing in their syndicates what patterns they can see.

- You may need to suggest coach students construct a triangular Association Matrix and group

  – Produce Timeline

  – Discuss patterns, make notes

  – Produce Association Matrix

  – Discuss patterns, make notes

- After 45 minutes, spend 15 minutes to Ask students what difficulties they had and help them to resolve them.

- Invite students to offer up any patterns they discovered – complement their use of the tools and suggest improvements

Learning Activity 2 (optional if time permits)

RESOURCES:
Exercise Instructions (MPKIO.RTM TTX 191030_20_Link_Analysis_Exercise_TTT_UNUC
v2.docx)
Class notes
MPKI HB
Pen and paper

TIME:
Approx. 1 hour

TASKS:

- Produce a Link Diagram

- Identify patterns

- Present conclusions

Instructor Notes-

- Ensure that the students have the Exercise Instructions.

- Instruct the students construct a link diagram.

- Emphasize that they are looking for identification of linkages between people, organisations and events, so work on rough drafts of the link diagram that best display the linkages, then spend time discussing in their syndicates what ties they can see.

- Time allocation is:

  - 10 minutes – produce draft link diagram

  - 25 minutes – refine and redraw the link diagram to best show linkages

  - 10 minutes – discuss linkages, make notes

  - After 45 minutes, spend 15 minutes to: ask students what difficulties they had and help them to resolve them; and invite students to offer up any patterns they discovered – complement their use of the tools and suggest improvements

- The diagram can look very different from the suggested possible answer if it does the following:
  - Shows the incidents
  - Shows the organisations
  - Identifies the relational links
  - Identifies the association links
  - Uses dotted lines to show suspected but unconfirmed links correctly
  - Possible link diagram

The syndicates may produce a diagram similar to this:

1

- Complement any syndicate that:
  - Shows AS (the missing correctional officer) but does not link them to anyone (we don't know why he is missing).
  - Shows FK as possibly the driver in the Prison Attack (there is no positive identification of her being there).
  - Notes that OK and BD are not positively identified, and therefore their associations are not confirmed
- Possible deductions from this link diagram:
  - HD and BD most likely facilitate the connection between Ansar al-Dine and the FLM

- FK is also likely to be the driver in the Prison Attack, given her strong links with HD and OK, and she is expected to have FLM allegiance if not a formal member

- MK is likely involved in supporting FLM given his criminal record and relational links to known members

- The Keita family is central to insurgent activity in this area (some effort should go into further investigating this family)

- Ansar al-Dine publicly claimed responsibility, but FLM has potentially provided the bulk of the support for the attacks

- Blood relationships appear to play a substantial role in tying the groups together

The students may produce a diagram similar to this one below:
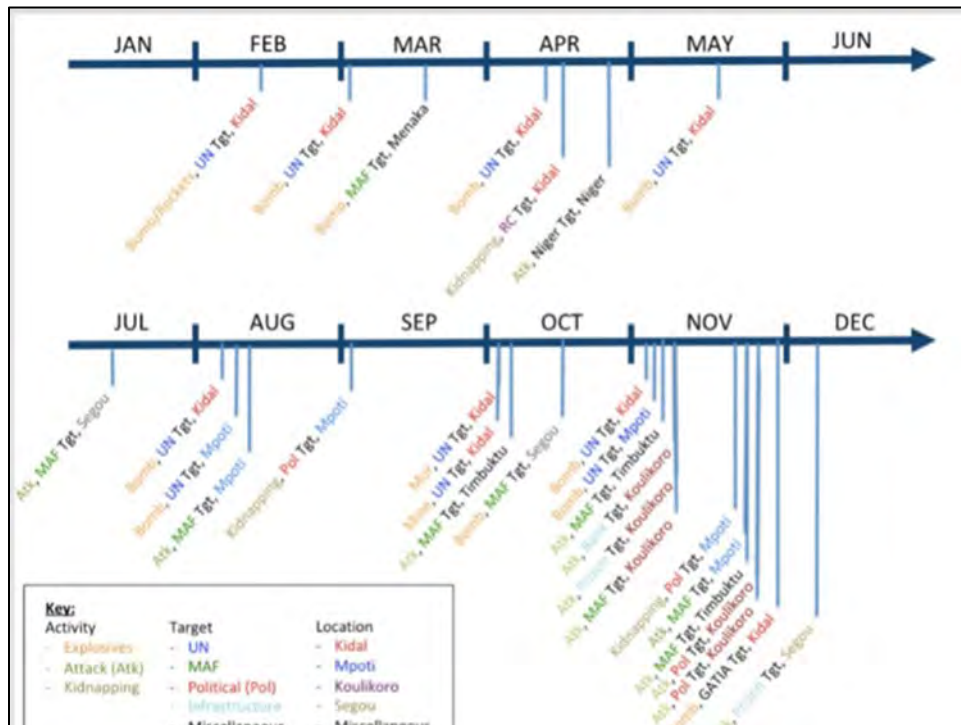
-----------------------Student Handout for Learning Activity 1-----------------

Pattern Analysis: 2016 Attacks by Ansar al Dine (MALI)

Instructions (Assume that all attacks were carried out by Ansar al Dine)

- **The attacks are already arranged in a sequence in MM/DD/YYYY format;**
- **Search for patterns:**
  - **By date (use a timeline over 12 months and look at a frequency related to each month);**
  - **By attack type (hint – use a relational matrix to sort the data by type);**
  - **By attack location (hint – use a relational matrix to sort the data by location);**
  - **By target set (use a relational matrix).**

- **What does this tell you about the group? What is the so what for your commander?**

INCIDENT SUMMARY:

12/06/2016: Assailants attacked a prison and freed 93 inmates in Niono, Segou, Mali. Two prison guards were injured in the attack. Ansar al-Dine (Mali) claimed responsibility for the incident, though sources also suspected the involvement of the Macina Liberation Front (FLM).

INCIDENT SUMMARY:

11/30/2016: An explosive device detonated targeting a Tuareg Imghad and Allied Self-Defense Group (GATIA) vehicle in Adjelal, Kidal, Mali. At least five GATIA members were killed in the blast. No group claimed responsibility for the incident; however, sources suspected that Ansar al-Dine (Mali) carried out the attack.

INCIDENT SUMMARY:

11/21/2016: Assailants raided the residence of the sub-prefect in Dilli, Koulikoro, Mali. This was one of three related attacks in Dilli on this date. One civilian was killed across the three events. No group claimed responsibility for the incidents; however, sources attributed the attacks to Ansar al-Dine (Mali).

INCIDENT SUMMARY:

11/21/2016: Assailants raided the city hall building in Dilli, Koulikoro, Mali. This was one of three related attacks in Dilli on this date. One civilian was killed across the three events. No group claimed responsibility for the incidents; however, sources attributed the attacks to Ansar al-Dine (Mali).

INCIDENT SUMMARY:

11/21/2016: Assailants raided the sub-prefecture building in Dilli, Koulikoro, Mali. This was one of three related attacks in Dilli on this date. One civilian was killed across the three events. No group claimed responsibility for the incidents; however, sources attributed the attacks to Ansar al-Dine (Mali).

INCIDENT SUMMARY:

11/20/2016: Assailants opened fire on an army convoy transporting ballot boxes in Timbuktu region, Mali. At least four soldiers were killed, and four soldiers were injured in the assault. This was one of two related attacks targeting electoral convoys on this date. No group claimed responsibility for the incidents; however, sources attributed the attacks to Ansar al-Dine (Mali).

INCIDENT SUMMARY:

11/20/2016: Assailants opened fire on an army convoy transporting ballot boxes between Bambara Maoude and Douentza, Mopti, Mali. At least five soldiers were killed, and an unknown number of soldiers were injured in the assault. This was one of two related attacks targeting electoral convoys on this date. No group claimed responsibility for the incidents; however, sources attributed the attacks to Ansar al-Dine (Mali).

INCIDENT SUMMARY:

11/19/2016: Assailants abducted Saibou Barry, a PRVM-FASAKO candidate, in Koro, Mopti, Mali. The outcome of the kidnapping is unknown. No group claimed responsibility for the incident; however, sources attributed the attack to Ansar al-Dine (Mali).

INCIDENT SUMMARY:

11/07/2016: Assailants attacked a National Guard camp in Banamba, Koulikoro, Mali. No casualties were reported in the attack. This was one of four related attacks in the area on this date. Ansar al-Dine (Mali) claimed responsibility for the incident; however, sources also attributed the attack to the Macina Liberation Front (FLM).

INCIDENT SUMMARY:

11/07/2016: Assailants attacked a prison in Banamba, Koulikoro, Mali. No casualties were reported in the attack; however, a prison guard was reported missing. This was one of four related attacks in the area on this date. Ansar al-Dine (Mali) claimed responsibility for the incident; however, sources also attributed the attack to the Macina Liberation Front (FLM).

INCIDENT SUMMARY:

11/07/2016: Assailants attacked the Mali Development Bank in Banamba, Koulikoro, Mali. No casualties were reported in the attack. This was one of four related attacks in the area on this date. Ansar al-Dine (Mali) claimed responsibility for the incident; however, sources also attributed the attack to the Macina Liberation Front.

INCIDENT SUMMARY:

11/06/2016: Assailants attacked a military camp in Gourma Rhaous, Timbuktu, Mali. No casualties were reported in the attack. Ansar al-Dine (Mali) claimed responsibility for the incident.

INCIDENT SUMMARY:

11/06/2016: An explosive device detonated, and assailants opened fire targeting a United Nations Multidimensional Integrated Stabilisation Mission in Mali (MINUSMA) convoy in Ngouma, Mopti, Mali. One Togolese peacekeeper and two Malian civilians were killed, and seven peacekeepers were injured in the attack. Ansar al-Dine (Mali) claimed responsibility for the incident.

INCIDENT SUMMARY:

11/04/2016: An explosive device detonated near a French Armed Forces convoy in Kidal region, Mali. At least one soldier was killed, and another was injured in the blast. Ansar al-Dine (Mali) claimed responsibility for the attack.

INCIDENT SUMMARY:

10/13/2016: Multiple explosive devices detonated near a Malian Army vehicle in N'Goma Coura, Segou, Mali. Following the blast, assailants then opened fire on the vehicle. At least four soldiers were killed, and seven others were wounded in the attack. Ansar al-Dine (Mali) claimed responsibility for the incident.

INCIDENT SUMMARY:

10/05/2016: An explosive device detonated near a Malian Armed Forces convoy near Bambara Maounde, Timbuktu, Mali. At least two soldiers were killed, and two others were injured in the blast. Ansar al-Dine (Mali) claimed responsibility for the attack.

INCIDENT SUMMARY:

10/03/2016: A landmine detonated targeting two United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) vehicles in Aguelhoc, Kidal, Mali. This was one of two related attacks targeting MINUSMA personnel in Aguelhok on this date. At least two MINUSMA peacekeepers were killed, and seven others were injured across both attacks. Ansar al-Dine (Mali) claimed responsibility for the incidents.

INCIDENT SUMMARY:

10/03/2016: Assailants fired mortars at a United Nations Multidimensional Integrated Stabilisation Mission in Mali (MINUSMA) camp in Aguelhoc, Kidal, Mali. This was one of two related attacks targeting UN personnel in the area on this date. At least two MINUSMA peacekeepers were killed, and seven others were injured across both attacks. Ansar al-Dine (Mali) claimed responsibility for the incidents.

INCIDENT SUMMARY:

09/02/2016: Assailants raided Boni, Mopti, Mali. Several buildings were burned, and a deputy mayor was abducted in the assault; the outcome of the kidnapping is unknown. No group claimed responsibility; however, sources attributed the incident to the Macina

Liberation Front (FLM). Sources also suspected that Ansar al-Dine (Mali) might have carried out the attack.

INCIDENT SUMMARY:

08/08/2016: Assailants attacked a Malian military position between Tenenkour and Sevare in Mopti, Mali. An assailant was killed, and five soldiers were reported missing and were later found dead. Ansar al-Dine (Mali) claimed responsibility for the attack.

INCIDENT SUMMARY:

08/07/2016: An explosive device detonated near a United Nations Multidimensional Integrated Stabilisation Mission in Mali (MINUSMA) patrol outside Kidal town, Mali. There were no reported casualties in the blast. This was one of two attacks targeting MINUSMA peacekeepers in Kidal region on the same day. Ansar al-Dine (Mali) claimed responsibility for the incidents. Source also suspected that the attacks were carried out by Al-Qaida in the Islamic Maghreb (AQIM).

INCIDENT SUMMARY:

08/05/2016: An explosive device detonated targeting Chadian peacekeeper near Kidal, Mali. One peacekeeper was injured in the blast. Ansar al-Dine (Mali) claimed responsibility for the attack.

INCIDENT SUMMARY:

07/19/2016: Assailants opened fire on a Malian Army base in Nampala, Segou, Mali. At least 17 soldiers were killed, and 35 others were injured in the assault. Additionally, six soldiers were reported missing, and their whereabouts are unknown. Ansar al-Dine (Mali) claimed responsibility for the incident and stated that it was holding five soldier's hostage in a video posted on August 4, 2016. The National Alliance for the Protection of the Fulani Identity and the Restoration of Justice (ANSIPRJ) separately claimed responsibility for the incident. Sources also attributed the attack to the Macina Liberation Front (FLM).

INCIDENT SUMMARY:

07/09/2016: Assailants attacked a military checkpoint in Dinangorou, Mopti, Mali. At least two soldiers were killed in the attack. Al-Qaida in the Islamic Maghreb (AQIM) claimed responsibility for the attack. Additionally, sources suspected the involvement of Ansar al-Dine (Mali).

INCIDENT SUMMARY:

05/18/2016: Assailants detonated an explosive device and opened fire targeting a United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) convoy in Aguelhoc, Kidal, Mali. Six Chadian peacekeepers were killed, and two peacekeepers were injured in the ambush. Ansar al-Dine (Mali) claimed responsibility for the incident.

INCIDENT SUMMARY:

04/28/2016: Assailants attacked a Niger Army vehicle in Tchin-Tabarade district, Tahoua, Niger. At least one soldier was killed, and another was injured in the incident. No group claimed responsibility; however, sources suspected that the attack was carried out by either the Movement for Oneness and Jihad in West Africa (MUJAO) or Ansar al-Dine (Mali).

INCIDENT SUMMARY:

04/16/2016: Assailants abducted four International Committee of the Red Cross (ICRC) employees near Abeibara, Kidal, Mali. One of the hostages was released on April 18, 2016, and the three remaining hostages were released on April 22, 2016. Ansar al-Dine (Mali) claimed responsibility for the incident and demanded the release of one of their members in exchange for the victims.

INCIDENT SUMMARY:

04/12/2016: An explosive device detonated near a French military convoy in Tessalit, Kidal, Mali. At least three French soldiers were killed, and two others were injured in the blast. Ansar al-Dine (Mali) claimed responsibility for the attack.

INCIDENT SUMMARY:

03/22/2016: An explosive device detonated near a Malian Armed Forces vehicle in Menaka, Gao, Mali. At least one soldier was injured in the blast. No group claimed responsibility for the attack.

INCIDENT SUMMARY:

03/01/2016: An explosive device detonated targeting a United Nations Multidimensional Integrated Stabilisation Mission in Mali (MINUSMA) vehicle on the road between Aguelhoc and Tessalit in Kidal, Mali. Six peacekeepers were injured in the blast. Ansar al-Dine (Mali) claimed responsibility for the attack.

INCIDENT SUMMARY:

02/12/2016: Two suicide bombers detonated an explosives-laden vehicle and assailants launched rockets at a United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) base in Kidal town, Kidal region, Mali. In addition to the two bombers, seven Guinean peacekeepers were killed, and 29 others were wounded in the attack. Ansar al-Dine (Mali) claimed responsibility for the incident and sources also suspected that the attack might have been carried out by Al-Qaida in the Islamic Maghreb (AQIM).

---Handout Learning Activity 2------------------------

Link Analysis: 2016 Attacks by Ansar al Dine (MALI)
Instructions (<u>Assume that all attacks were carried out by Ansar al Dine</u>)
- **You have been tasked to investigate three incidents in greater depth and determine what links the actors involved have with each other.**
- **Construct a Link Diagram and search for links:**
  - Between actors (include all the identified actors on your Link Diagram);
  - Between actors and known organisations (include the identified organisations on your Link Diagram);
  - Between actors and incidents (include the three incidents in your Link Diagram).

  - What does this tell you about the links? What are the "so what" deductions for your commander?

INCIDENT SUMMARY:

11/07/2016, 0900: Assailants attacked the Mali Development Bank in Banamba, Koulikoro, Mali. No casualties were reported in the attack.   Ansar al-Dine (Mali) claimed responsibility for the incident; however, sources also attributed the attack to the Macina Liberation Front (FLM).
Among the assailants, CCTV footage positively identified two known members of Ansar al-Dine, Moussa Arby (MA) and Seydou Bagayogo (SB).   An eyewitness positively identified Fanta Kieta (FK) as the driver who drove the van transporting the assailants, a green Renault Master with no windows.   Two other assailants remain unidentified.
Adama Kone (AK), the local Ansar al-Dine commander, claimed responsibility for the attack via a local radio station.

INCIDENT SUMMARY:

11/07/2016, 1320: Assailants attacked a prison in Banamba, Koulikoro, Mali. No casualties were reported in the attack; however, a prison guard, Amadou Sacko (AS), was reported missing.   Ansar al-Dine (Mali) claimed responsibility for the incident; however, sources also attributed the attack to the Macina Liberation Front (FLM).
CCTV footage positively identified known member of Ansar al-Dine, Seydou Bagayogo (SB), and one assailant who is suspected to be Oumar Keita (OK), a known member of the Macina Liberation Front (FLM).   Three other assailants were not identifiable on the CCTV footage.

A fairly reliable HUMINT source (C), provided a report that is probably true (2) from February 2016 reporting that Oumar Keita (OK) is brother to Fanta Kieta (FK) and that there is another brother, Moussa Keita (MK) who has a criminal record (violent robbery), but as yet has not been identified as active in any insurgent group.

An eyewitness identified a green, windowless van on the road outside the prison. The eyewitness believed that a woman was driving the van.

A prison guard positively identified Hawa Damba (HD) as an assailant.   Damba is a known member of the Macina Liberation Front (MLF) and a known associate of Fanta Kieta (FK).   The women attended high school together and were detained together in 2013 by Police on shoplifting charges.

A usually reliable HUMINT source (B), provided a report that is probably true (2) from July 2016 reporting that Hawa Damba (HD) married Moussa Keita (MK) in March 2019.

During the attack, one assailant was heard calling for help from someone called "Seydou".   A man (assumed to be "Seydou") replied, "be quiet Boubacar".

Note: Boubacar Damba is a known member of Ansar al-Dine and cousin of Hawa Damba.

Lesson
3.4a

Introduction to Dissemination

Starting the Lesson

Slide 1

In this lesson, we will give you an introduction and overview of the MPKI dissemination function.

Slide 2
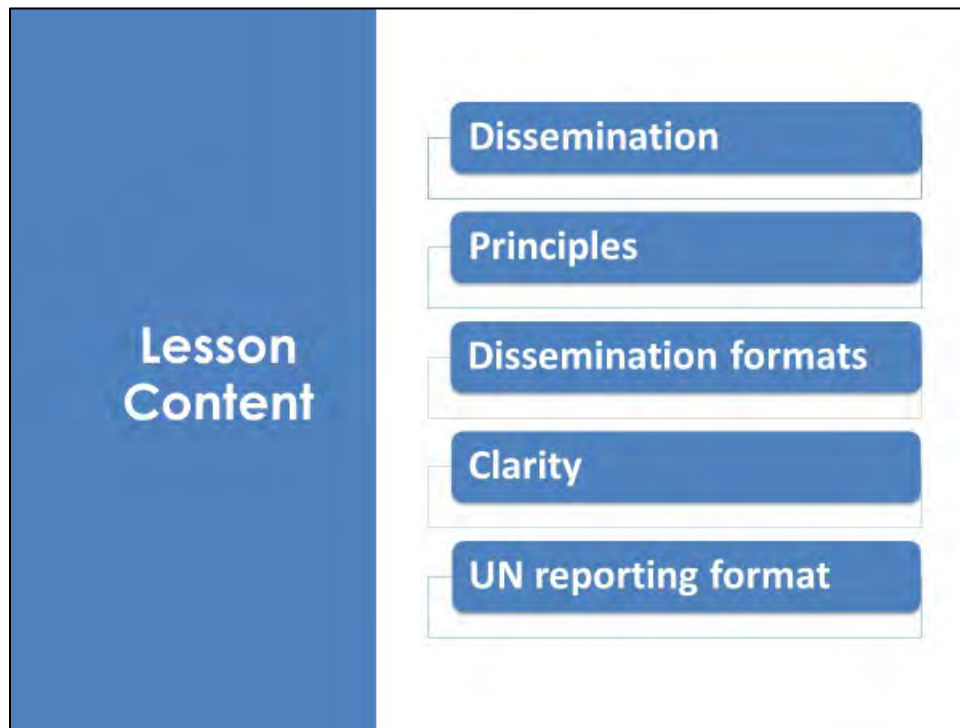
Here is the lesson content.

Slide 3

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

Slide 4

Dissemination is the process of conveying peacekeeping-intelligence to mission decision-makers and other relevant mission personnel.

Dissemination is the final phase of the Peacekeeping-Intelligence cycle. The Commander's information requirements are acquired, and the relevant information is analysed and integrated to produce peacekeeping-intelligence, which is then disseminated to the right people, to enable decision-making and initiate further direction.

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

Slide 5

The dissemination of peacekeeping-intelligence products shall follow the concepts as stipulated in either the Peacekeeping-Intelligence Support Plan and/or relevant SOPs. Mission level documents should be replicated at Force and below levels.

The ISP supports the Peacekeeping-intelligence production and dissemination providing regulation on:

> - Details the positions responsible for ensuring generation and dissemination of products through various channels, including releasing authorities for the dissemination of products within and outside the mission.

> - Details the media and information technology, management and communications systems through which peacekeeping-intelligence products are to be released.

The initial Intelligence Dialogue will determine methods, timeframes, and formats of products in terms of dissemination. So the initial Intelligence Dialogue is the starting point but needs to be continuously revisited as circumstances and requirements change.

The Production Plan (MPKI HB, 5.5) that can be part of a Mission or Force SOP ensures the direction to produce peacekeeping-intelligence products per the decision-makers' needs. The responsibility for developing the production plan is with the Chief of the peacekeeping-intelligence branch at a specific level. This plan lists:

- Regular products (daily, weekly, monthly), timings, formats and who has responsibility;

- Ad hoc products per situation, formats and who has responsibility;

- Release authority for different products (i.e., checking quality, content and relevance before dissemination)

Preferred dissemination (when, how and to whom). The production plan is a living, dynamic, situational, flexible and internal peacekeeping-intelligence production tool that normally is based on more static Reporting Directives and SOPs.

Slide 6

> ## How to Disseminate
>
> - Compliance with the "need to know/need to share" concepts
> - Mandatory reporting requirements
>   - human rights and humanitarian law violations including trafficking, combat-related sexual violence (CRSV) and crimes against children

 The dissemination of peacekeeping-intelligence products shall be done in compliance with the "need to know/need to share" concepts to minimize unauthorized disclosure, as well as the below organisational requirements for information classification, security, handling, ownership and sharing. An assessment of the risks associated with the disclosure thereof should be done.

The delegation of authority to disseminate peacekeeping-intelligence products shall be identified as part of the mission's Peacekeeping-Intelligence Support Plan and internal guidance for participating mission entities.

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 MPKI cycle must be reported through the appropriate channels.

Slide 7

 As seen in the Acquisition lesson, Information Management (IM) is a crucial element for effective intelligence delivery. One of the most important functions is to ensure that all relevant information is disseminated to the right organisations at the right time. Intelligence IM responsibilities include, among others:

- 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

Slide 8
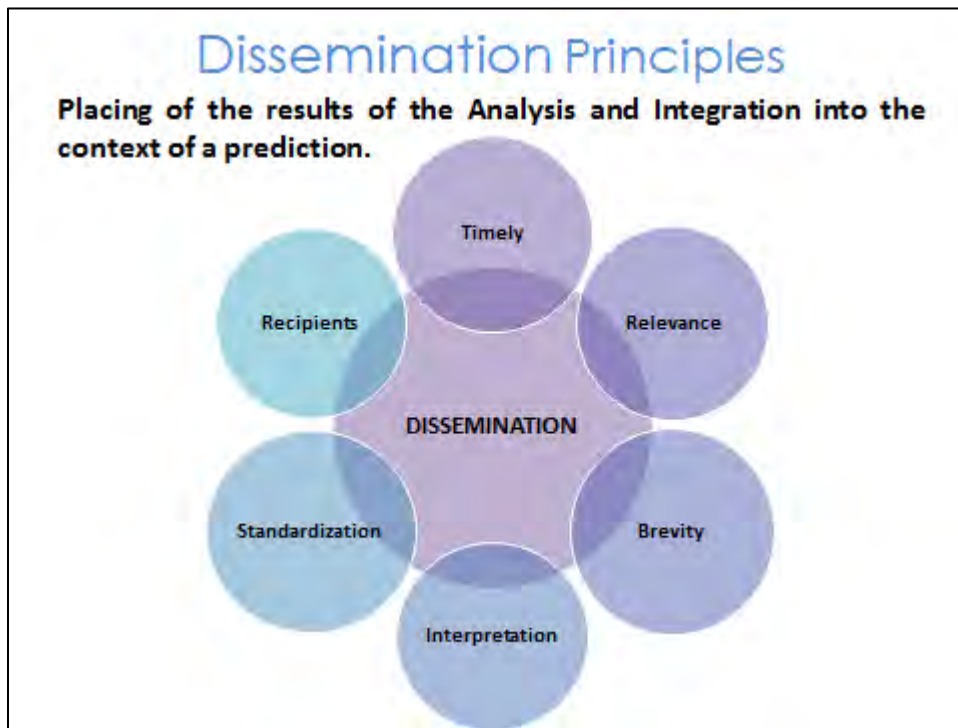
Peacekeeping-intelligence should be disseminated with relevancy, timeliness and in a standardized way. The final phase of the peacekeeping-intelligence cycle is dissemination. Your information has been analysed and turned into a finalized intelligence. If the previous steps in the MPKI Cycle have been followed correctly, this output will be relevant, and hopefully timely.

However, it has absolutely no value if it is not disseminated, is not understood or not delivered promptly. It also has no value if it is not delivered in the relevant quantity and quality to the right recipients.

Slide 9
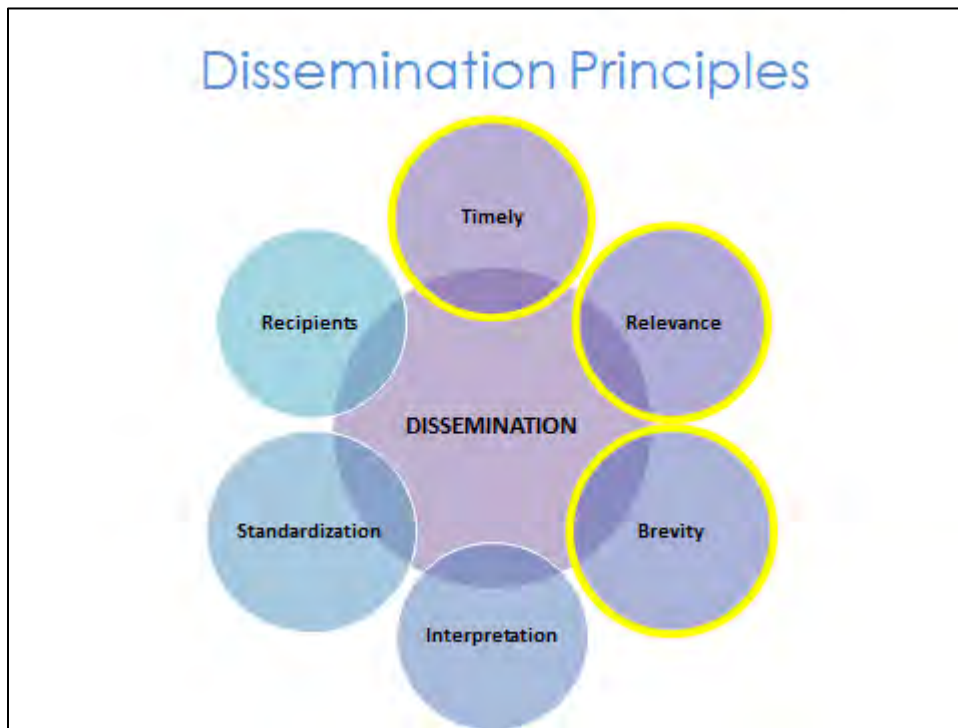
Key message: intelligence should be disseminated with timeliness, relevance and brevity.

Timeliness: Intelligence must be delivered timely so planners and decision-makers can act rather than react, thus keeping the initiative. Some acquisition assets can disseminate collected information on a real-time or near real-time basis, vastly increasing their timeliness. This sometimes conflicts with the quality of the decision support, as the direct input from acquisition assets should be processed, collated and evaluated to enhance the quality of the decision support.

Relevance: Is determined by the needs and objectives of the recipients as defined in the Direction phase of the Intelligence Cycle. If an element of intelligence does not answer a question in the IAP, it may not be necessary to report it. Remember that commanders and planners deal with large amounts of information and that they have already made it clear as to what they would like to know in the IAP.

Brevity: Reports must be kept as brief as possible, but at the same time include everything that the recipient needs to know. Commanders seldom have time to wade through long documents or listen to verbose oral briefings. Full use of traces, annexes, and facsimile processes should be made to cover additional detail. Always create a BLUF (Bottom Line Up Front) Paragraph or Executive Summary if you submit a lengthy product.

Slide 10
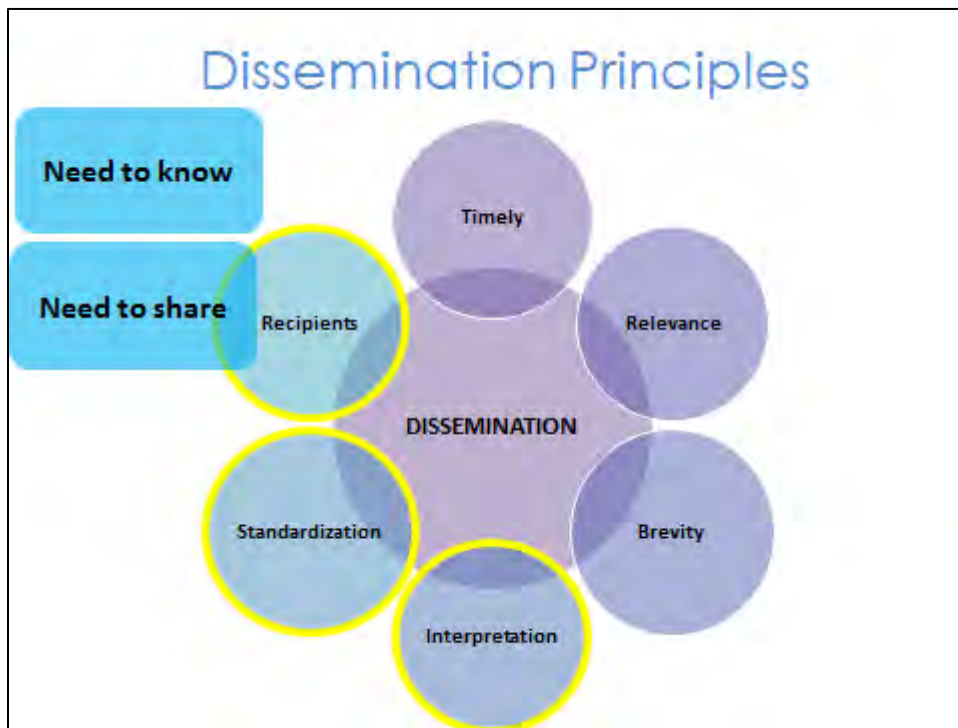
Key Message: After interpretation, intelligence should be standardized and disseminated to recipients.

Interpretation: Wherever possible, all facts must be correctly evaluated, and their significance interpreted before dissemination. In all intelligence reports, whether oral or written, a clear distinction must be preserved between facts and the deductions, assumptions, and assessments made from them. In written reports and oral briefs, such interpretation must be made clear.

Standardisation: Reports are understood more quickly if they are laid out in a logical sequence under convenient standard headings, using the same language of probability. The format should be covered in standing operating procedures. This also enables all producers and users of intelligence to recognize the product and to more quickly extract what is most relevant to them in the product.

Recipients: Distribution is based on a thorough knowledge of the Intelligence requirements of units, planners and decision-makers. This knowledge is based on the Intelligence Acquisition Plan (IAP) and Requests for Information (RFI). Remember, if it's not relevant to the recipient, it can add to the confusion and ambiguity for understanding the operational environment.

Access to classified intelligence should be strictly limited to those who have a need-to-know to carry out their duties. Intelligence can be shared within the UN and with non-UN entities in accordance with the Mission policy. The source of information might be protected, and the intelligence itself might be sanitized to protect the source from sharing information with others.

Slide 11
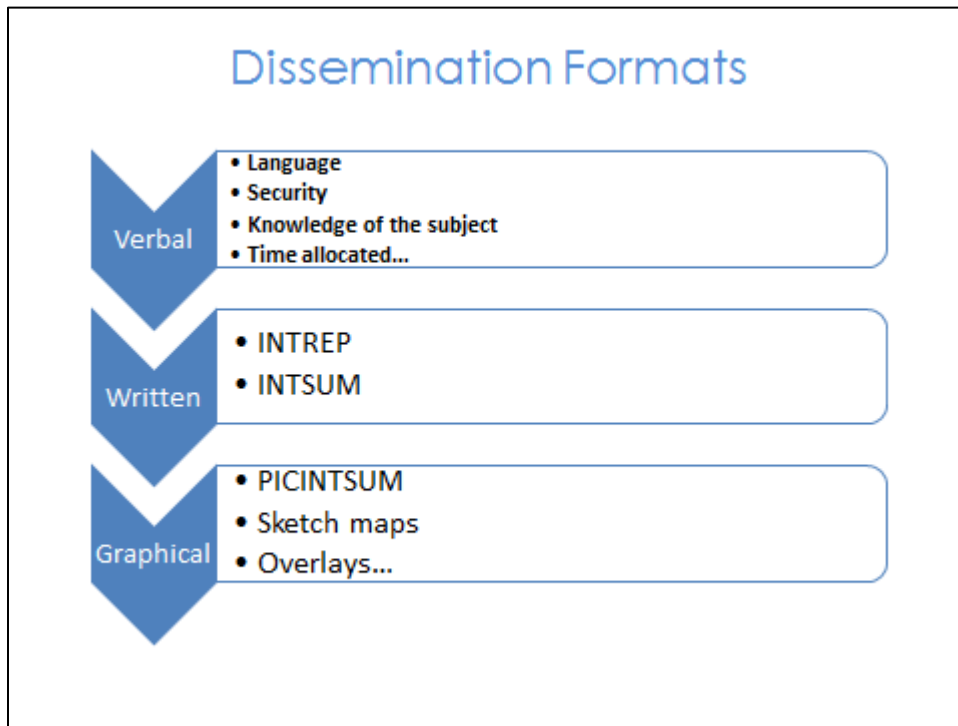
Key Message: Dissemination can be verbal, written or graphical.

How you disseminate the peacekeeping intelligence depends on both « push » and « pull » concepts. The push concepts being the high command pushing the peacekeeping intelligence to a lower level of command.

The pull factor involves direct electronic access to web pages, databases, peacekeeping intelligence files, or other repositories (where applicable).
With, peacekeeping intelligence must be delivered in a format that the recipient readily understands and is readily usable. It can be:

Verbal: Verbal briefings are useful for timeliness and for providing an opportunity to emphasize significant issues, as well as providing the briefer with immediate feedback and the potential for further direction. A Verbal presentation can be organized and supported by a PICINTSUM. When preparing a verbal presentation, should be considered the language, the level of security clearance and the level of knowledge the recipients have. Time allocated, use of visual aids and IT capabilities in the briefing room should also be considered.

Written: Written dissemination encompasses Intelligence Reports, Intelligence Summaries and Thematic Reports. Intelligence summaries should be disseminated at

regular intervals relevant to the situation. Time-sensitive material is disseminated using INTREP.

Dissemination can also be Graphical like PICINTSUM, sketch maps, physical, human, and information overlays, link charts. Please remember that maximum use of graphical dissemination is highly recommended in peacekeeping-intelligence.

In any case, keep in mind that Intelligence indicating an imminent assessed threat to life must be conveyed immediately. The source and any classified information may be left out / protected as required, but the threat to life must be passed on by the fastest means.
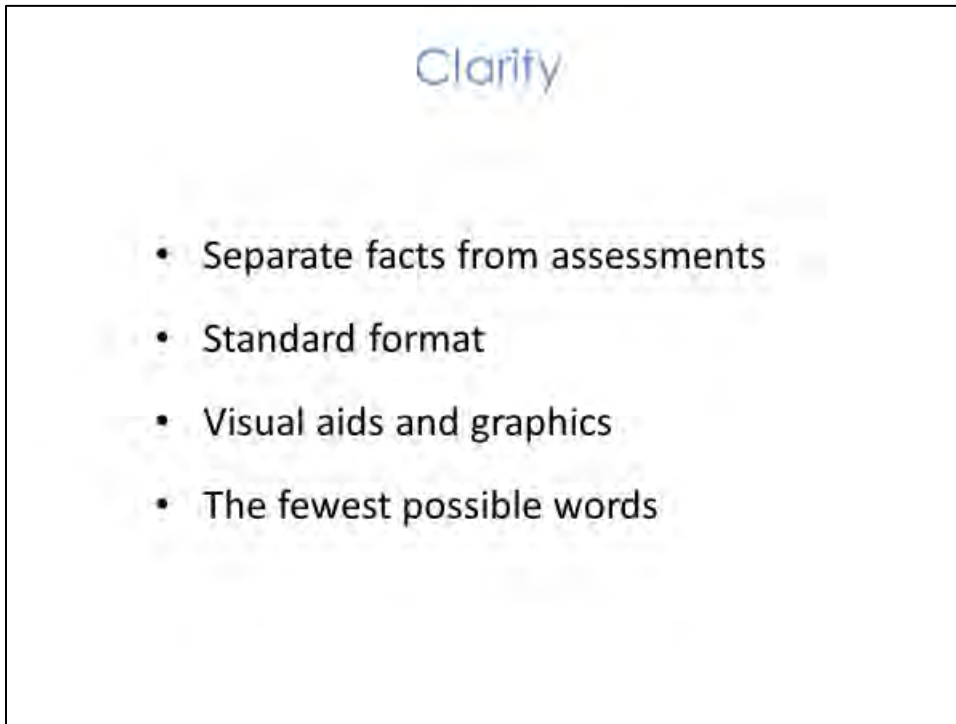
Interaction *Ask the students which other products not in the slide that was delivered during the course and can be disseminated and by which format. Answers should point to SPIE and Phase 1 Brief. RFI and IAP can also be mentioned.*

Narrative: As identified in its specific lesson, the SPIE is a method of disseminating the AOE in written and graphical form using the same logical process as the AOE and ends with detailed assessments of the ACOAs. SPIE is more easily disseminated.

The initial IAP is disseminated at the early stages of the mission or after its completion. As the IAP is a living document and should be managed in all levels (Mission, Force, Sector and Unit), new IRs, SIRs and EEI can be disseminated as part of intelligence annexes of FRAGOs, WARNOs and other documents. Also, as explained in the Acquisition lesson, the Information Acquisition List should be distributed to subordinate assets. It is a combination of the EEIs, RFIs and I&W, which have become IRs in the acquisition process and have been prioritized accordingly.

Slide 12

Key Message: Avoid ambiguity and separate facts from assessments while disseminating peacekeeping intelligence.

Both briefings and reports should be characterized by clarity and brevity. Intelligence should be presented unambiguously – clearly separating facts from assessments.

The originator must ensure that he has focused his thoughts before briefing or writing. Always rehearse briefings. The briefings and reports should follow a standard format and sequence of slides. The use of visual aids, maps, drawings and diagrams will enhance the verbal briefing and clarify the intelligence being discussed. To be brief and precise is the key to the successful dissemination of intelligence. The good presentation – verbal or written - is the one which contains the most information in the fewest possible words.

Disseminating intelligence through known reporting formats also enhances clarity. Always assure that you do not place elements of reports in the wrong place in the format. The release authority will normally conduct a final quality assurance check of a report before it's distributed.

☞ *Instructor note: If possible, draw examples from your experience as an intelligence officer on how clarity can be achieved when conveying intelligence products.*

Slide 13

Dissemination
- UN Reporting Formats -

- Peace keeping Intelligence reports called INTREP
- Peace keeping Intelligence summary called INTSUM
- Thematic reports

Key Message: Always use a UN format in Peacekeeping Intelligence cells.
The UN uses standard report formats in order to guarantee multinational interoperability.

Here are a few examples of reporting formats:

Peace Keeping Intelligence Reports or INTREP: The INTREP will be covered in a subsequent lecture. It is in short, a way of conveying intelligence of immediate importance that cannot wait for the regularly published products.

Peacekeeping-Intelligence Summary also called INTSUM: The INTSUM will be covered in a subsequent lecture. It is in short, a collection of the intelligence reporting received over a period defined. An INTSUM may be written in prose or with graphics, called Picture Peacekeeping-Intelligence Summary (PICINTSUM)

Thematic reports: Thematic reports are created as required, often as an answer to a Request for Information (RFI). The Thematic Report is always useful when providing a deeper understanding of a specific topic and draws on all intelligence gained until the time it is released.

Slide 14

Key Message: The following points should be considered for all dissemination products.

To attend the brevity principle, an executive summary can be required. The executive summary is a summary paragraph highlighting the main events or reporting themes. This will also include the main deductive and predictive assessments. Should be written in continuous narrative or in bullet points to provide the customer with a concise summary of what has happened, why, and what will occur next.

The critical factual detail is taken from the reporting usually comprising Date-Time-Group (DTG), location, and what occurred.

The classification should follow UN regulations and Mission SOPs.

The distribution will be done following ISP, SOP and need to know and need to share principles.

When required, a title should cover the main topic/issue covered by the document.

Slide 15

Important contents
- **Situation**
  - Report briefly what happened
  - Provide only relevant information
  - Consider recipient background – provide additional information (footnotes, annex) if required
  - Follow logic sequence of facts (time, location, actor)
  - Relevant information - unevaluated / unconfirmed sources
- **Comment**
  - Factual and provide context
  - Relation to something happening or TTPs or can support
  - Comment Ends

The situation must provide the critical facts of the situation and the required background. Focus on reporting facts briefly relating to the main topic covered. Consider audience background, what they already know/understand about situation/topic covered.

References with a footnote and or an annexe so the customer can go direct for further information. Facts should be presented following a logical sequence that can be a timeline or grouped by areas/sectors or relevant actor involved. Check inconsistencies and understanding.

Relevant information from unevaluated facts or unconfirmed sources will be disseminated but requires the highest care to state its nature. Although the information is not confirmed, can bring attention to leadership and planner about a change of trends or TTPs, per instance. The instructor should provide examples.

Comment on implications of the situation, draw linkages. Alternatively, this section can provide additional background to the situation, or a deep dive into particular issues raised.
A comment must be factual and provide context. This could include previous reporting, your knowledge, data or reference material.

At the end of the comments should be written to make clear to the recipients.

Slide 16

An evaluation of what has happened to explain why and whether it will occur again based on your analysis of the information you have.

Should include both deductive and predictive assessment. Deductive - What just happened and Why? Predictive - What will happen in the future? Include an assessment of likelihood (uncertainty yardstick), usually at the end of the document.

Assessment should also tell the commander/audience what information is still missing. This will again move the cycle and provide new IRs.

The instructor can provide examples (e.g. "no group has yet claimed responsibility for this attack. However, it is consistent with known Al-Shabaab TTPs…" or "the number of displaced has not been confirmed at this time, however, given the scale of fighting is likely to have been significant…").

The assessment should use predictive language, including an assessment of its likelihood. The uncertainty yardstick supports the audience's better understanding of the level of confidence for each portion of your assessment. Best practices show that including the uncertainty yardstick enhance the comprehension in commanders. A summary of threat levels seen in Actor Evaluation lesson can also be used in threat assessments.

Slide 17

Important contents

Outlook

- Predictive, including second and third order effects
- Can be broken down into three time periods
  - Short term
  - Medium term
  - Long term
- Vary depending if at the tactical, operational or strategic level

The outlook is a result of predictive analysis of a situation visualized in the future for a specific period.   An outlook can be included in the assessment part of an intelligence product. The assessment is predictive, looking to a point in the future and might consist of second and third-order effects.

Interaction Present the following situation and ask which are the second and third-order effects:

Situation- A farmer killed a Fulani herder because Fulan cattle destroyed the farmer's crops. Comment: during the transhumance season there's a historical increase of ethnic violence involving local self-defence militias and armed Fulanis.

Answers should vary Second-order: revenge acts against farmers, crops destruction. Third-order: robbery/killing of Fulanis or cattle, resumption of ethnic clashes

The outlook can be broken down into three time periods.   These periods will vary depending on if at the tactical, operational or strategic level.
Tactical example:
Short term - Immediate threats, typically looking at the next 24hours / reporting period.
Medium-term - Typically looking at the following 24-96hrs.

Long Term - Horizon scanning, 96hrs plus.

The strategic level can vary from Short term – few months to Long Term – some years ahead.

Slide 18

Interaction: *In this interaction, have the students read the report and, in a group, highlight the main points covered.*

Situation – brief report of the fact.

Comment – explanation of the ethnic background and referring to the previous observation of similar facts.

Assessment – likelihood per each specific idea/inference, not overall. Predictive for a particular period.

Second-order effects – gaining confidence, demonstrations continuing

So What? How this relates to the UN

Logic narrative assessment first that demonstrations can continue and then about the use of violence during the rallies.

Student can be asked about the need for an Executive Summary, and the answer should be no, as the assessment is clear and concise.

Slide 19

Interaction. Have the students read the following INTREP (provide a hard copy). Then discuss it for five minutes.

Ask them to comment on where this report does not adhere to the principles of dissemination. Time: Approx. 15 minutes

Expected outcome:
The students should be able to recognize where a report deviates from the dissemination principles to be able to self-correct when creating intelligence products.

Slide 20

Take Away

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

- Peacekeeping intelligence indicating an assessed threat to life must be conveyed immediately

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

Summary

Remember that:

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

- Peacekeeping intelligence indicating an assessed threat to life must be conveyed immediately

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

Lesson
3.4b

Dissemination-INTREP

The Lesson

Starting the Lesson
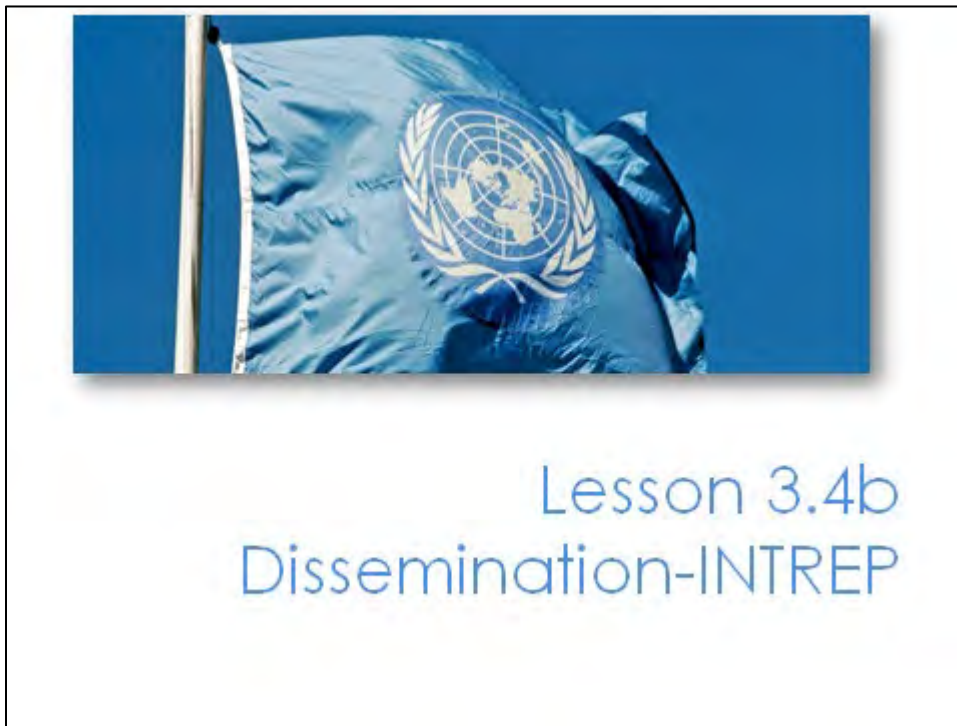
Slide 1

In this lesson, we will give you an overview of the INTREP used for MPKI dissemination.

Slide 2

Here is the lesson content. This lesson will give an overview of what an INTREP is in the UN-context. The format contains the elements recognizable from most national military equivalent products. There will be a short learning activity to allow the syndicates to create an INTREP based on information provided.

Slide 3

Learning Objectives

- Explain why the INTREP is sent without regard to a time schedule

- Describe the INTREP format

- Describe the INTREP content and how it helps portray information

Here are the learning objectives for this lesson. After this lesson, you should be able to do these objectives.

Slide 4
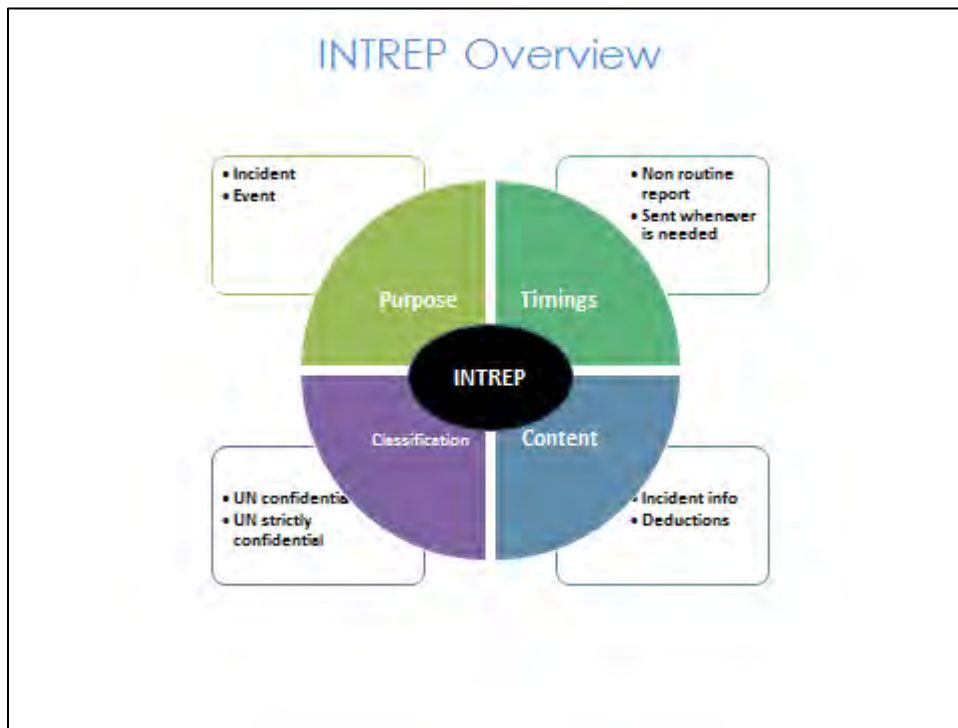
Key Message: The INTREP is one of the core products of intelligence staffs supporting current operations.

A peacekeeping intelligence report, commonly called INTREP is a document that can be originated at any level of command and is a non-routine report; it is sent as required.

The INTREP is used to report essential elements of intelligence information. The INTREP provides timely information regarding incidents/events that could influence current or pending operations.

An INTREP is sent without regard to a specific time schedule, and whenever the information it contains is considered likely to require the urgent attention of the receiving commander or his staff.

An INTREP relates incidents/events issued as soon as possible after their occurrence, allowing for the time it takes to process the information correctly. It can be quite challenging to strike a balance between the quality of the report and the urgency of communicating the information.

It should include any information that may be relevant to the information/intelligence requirements of any commander to whom it is disseminated. It should consist of the issuing Intelligence staff's deduction of the significance of the information. The INTRERPs you will produce shall be classified per content, either UN CONFIDENTIAL or UN STRICTLY CONFIDENTIAL.

Slide 5

INTREP Format

Classification: UN CONFIDENTIAL		Precedence: IMMEDIATE.
SUBJ:	INTREP 001/00 241200 C DEC 17	
1	DETAILS	• Who • What • Where • When • Why/How • Own CoA or response
2	COMMENT	The Intelligence staff's deduction of the implications of the incident or event.
ORIGINATOR: U2/UN Mission XX. Releasing officer:		

Key message: The INTREP is created in a fixed format so that it will be recognizable and comprehensive. It may not be complete according to format, especially if the information provided does not cover all the 5WH in the "DETAILS" box.

Line The report should include as a minimum:

1. DETAILS (The "Improved and Quality Assured Incident Report")

This is where you go through the Incident Report to deliver the best possible description of the incident. Remember that the Incident Report very often consists of individuals' perception of what transpired or that person's subjective take on events. There should be some effort made to get more information and clarification from the originator before issuing the INTREP if time allows.

On the slide is an example of how to put these questions into an INTREP format. You can see that it contains classification and a level of precedence. These are important for both procedural and operational reasons. For instance, the priority tells the transmitter of the report where it should be placed in the transmission queue, based on the time-sensitivity of the information. This, in turn, can be essential when forming our response.

The questions what, where, when, why, how and own CoA or response if applicable are answered in the details box

Who: which actors were involved, name of individuals, groups and factions that are associated with the INTREP

What: what happened and the sequence of events. Form a timeline to list the events chronologically

Where: the location (s) where the incident took place; Use map-references, if available, at very least give the location name(S).

When: DTG of the incident, if possible specify when the incident started and when it ended

Why/How: Report what has instigated or triggered the incident, and what was the desired end-state of the instigator of the incident.

Own COA or response: What were own forces actions in response to the incident, which actions have been initiated, and that may still be ongoing?

2. COMMENT:

In the comment box, you place any relevant deductions made in the time available, or all pertinent context (previous applicable reporting or known TTP).

An INTREP is usually issued without assessment, due to the time constraints, but if you have a CoA analysis, you can refer to it here; Example: "This information/incident is consistent with the actor adhering to the MOST LIKELY COA".

3. ORIGINATOR:

The Originator/Releasing Officer box is essential as it enables the recipient to ask follow-up questions and to provide feedback on the INTREP.

☞ *Instructor note:*   *The template is a guide. You can diverge from it, as required to meet the commander's requirements.*

Slide 6

> ## Take Away
>
> - The INTREP is a *non routine* report sent as required
>
> - The INTREP is made to provide clarity on current incidents/events where the information can not wait for the INTSUM (next lesson)
>
> - The INTREP should include the issuing intelligence staff's evaluation of significance and relevance of the information

Summary
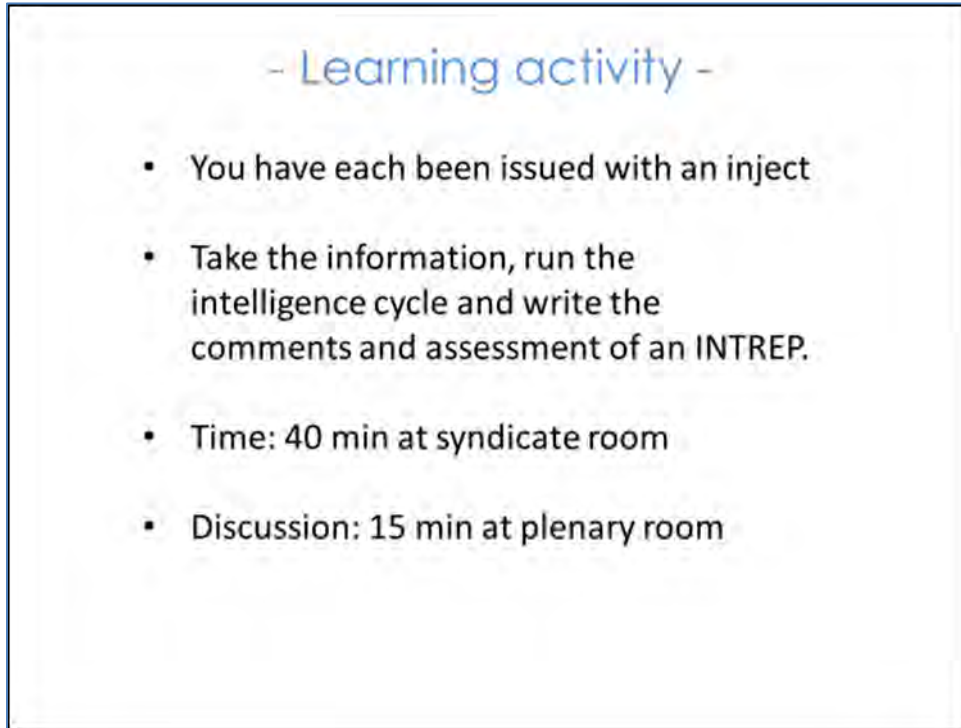
Remember:

- Peace keeping intelligence Report is a non-routine report sent whenever is needed

- Peace keeping intelligence Report about incidents/events assessed to influence current or pending operations must be conveyed immediately

- Peace keeping intelligence Report should include the issuing Intelligence staff's deduction of the significance of the information

Learning Activity

Slide 7

Task:
Create an INTREP based on the inject provided to the Syndicate

Resources:
A computer with a blank INTREP format (.doc-file); Additionally, a flip-chart paper can be used.

Approx. Time:
55 minutes

Learning activity:
The activity is conducted in two stages:

- 40 minutes: each student works individually to produce comments and assessment of an INTREP from the information his/her syndicate has been given, mainly the comments and assessment parts.

- 20 minutes: students will provide their INTREPs to the discussion group.

Students will receive 3 BATT INTREP 296/18, printed and digital copy.

Expected outcome:
Students are to produce an INTREP containing the 5W&H, including a short assessment (optional).

Lesson
3.4c

Dissemination-INTSUM

The Lesson

Starting the Lesson

Slide 1

In this lesson, we will give you an overview of the INTSUM used for MPKI dissemination.

Slide 2
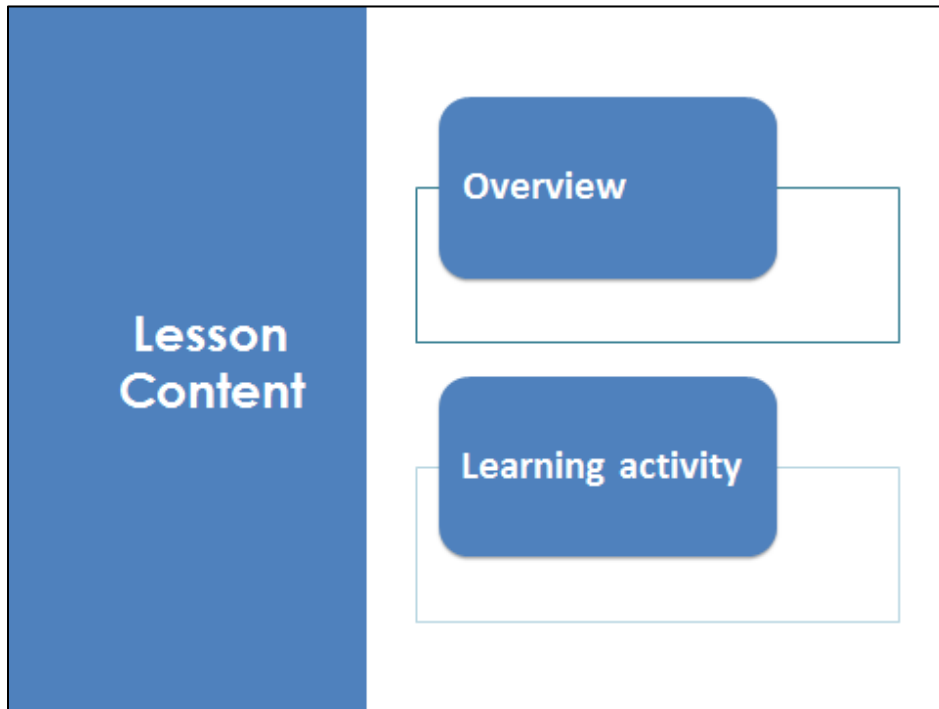
Here is the lesson content. This lesson will cover an introduction and overview of the ITSUM as a key output from an intelligence staff section. There will be a brief learning activity, where information in the form of INTREPs will be integrated into an INTSUM.

Slide 3

Here are the learning objectives for this lesson. After this lesson, you should be able to do these objectives.

Slide 4
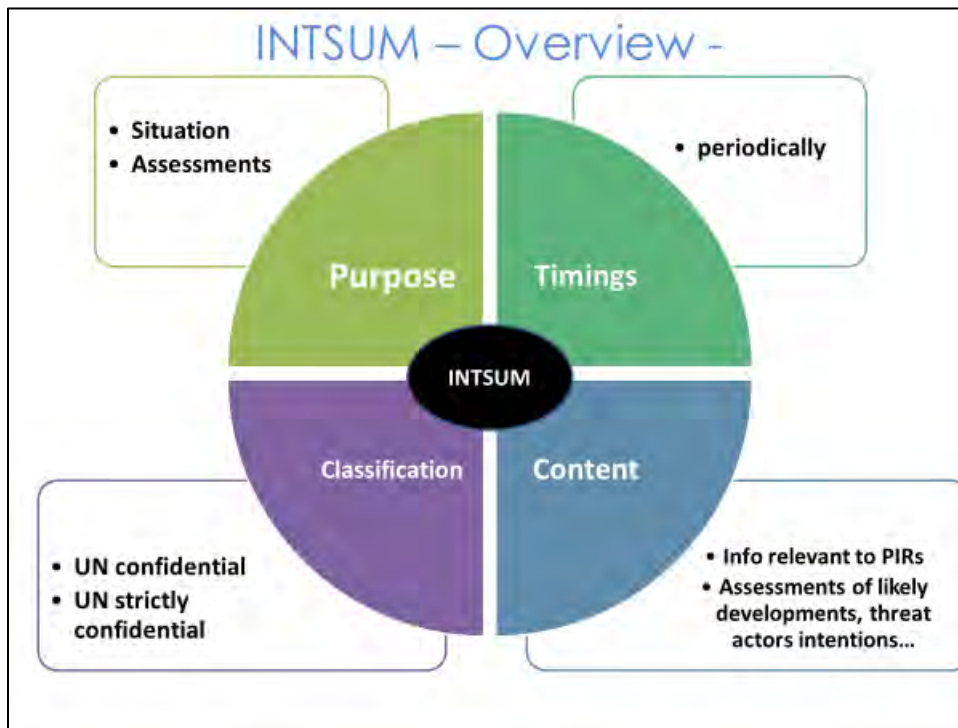
Key Message: The INTSUM is the main product of an intelligence staff section and the product that will maintain the common understanding of the situation at all command levels. This is very often the only product that will be read regularly by those with a need or interest in staying informed about the situation.

A peacekeeping intelligence summary, INTSUM for short, is a periodic summary of peacekeeping intelligence on the current situation within a commander's All. It is designed to update the current peace-keeping intelligence assessments and highlight important developments during the reporting period. The reporting period is usually 24 hrs, but there are also weekly and monthly INTSUMS. The longer the reporting period, the longer the outlook and assessment forecast should be.

The length of the forecasting period depends on several factors, such as the tactical situation, the accuracy with which it's possible to make a forecast, and the timescale of the operation. Its distribution should include all those whose responsibility and interest. Remember the Need to Share!

An INTSUM may be produced in several different formats, i.e. written or through graphical representation, or a combination of the two. In this lecture, we will focus on the written format, and specifically on the elements contained in the written format.

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

INTSUMs shall be classified based on content as either UN CONFIDENTIAL or UN STRICTLY CONFIDENTIAL.

Slide 5

INTSUM Format

Classification: UN CONFIDENTIAL		Precedence: IMMEDIATE.
SUB J	UN INTSUM 001/00 FROM 241200A DEC 17 TO 281200A DEC 17	
1	HIGHLIGHTS	
2	THREAT ACTORS	
3	FORCE PROTECTION	
4	OPPOSITION TO COHA	
5	MISCELLANEOUS	
6	POLITICAL	
7	UPCOMING EVENTS	
8	ASSESSMENT	
ORIGINATOR: U2/UN Mission XX. Releasing officer:		

Key message: An INTSUM must contain several elements. The elements are there for reasons of quality and consistency, and to provide traceability and accountability.

The INTSUM format, as exemplified in the MPKI Handbook, is shown in the slide, but there are several formats used by the respective missions. The INTSUM covers a period usually determined by the intelligence staff section in coordination with the chief of staff/commander. The core principles of writing an INTSUM are:

BLUF (Bottom Line Up Front) A short summary of the situation and a high-level assessment/outlook: This is an amalgamation of the information points given in the subsequent INTSUM paragraphs. It can be written as prose, displayed as graphics/maps, or both.

Information points with comments and assessments. This is where you put the information received during the reporting period, often derived from INTREPS or Incident Reports. The value-added should be:

- Putting the information in context (COMMENTS)
- Making assessments/forecasts based on the information (ASSESSMENTS)

The information can be organized in several ways:

- Topically (as shown in the format)

- Geographically (usually along unit/sector boundaries)
- By threat actor
- According to the IAP

The most important thing is that the information is organized in a way that is useful and accessible to the "customer" (Commanders and planners on all levels). The most common way to organize an INTSUM is, according to AORs (Battalion or Sector). This enables commanders at all levels to quickly extract intelligence from the INTSUM that is particularly interesting to relevant to them.

☞**Instructor note:** The template provides guidance. You can diverge from it, as required to meet the commander's requirements.

Slide 6

Key message: An INTSUM may come in many shapes and forms, but common to all INTSUMs is that they contain the core elements given in the format.

In this example, you will find all the elements from the INTSUM format as laid out in the legend on the right. You will find that the format, in this case, is chosen to support the commanders and planners at Sector and Force level.

The format used in a UN Mission should be determined by ISP or reporting SOP, at the Mission or Force level. The final product can be tailored by the needs of the Commanders and Planners.

Slide 7

Summary

Remember:

▪ An INTSUM is a periodic summary of peace keeping intelligence on the current situation within a commander's APIR

▪ In addition to the updated situation, a peacekeeping INTSUM shall contain updated assessments

Learning Activity

Slide 8

INTSUM- Learning Activity

- Assume the role of a U2-section at Sector HQ

- Using the four INTREPs from the previous lesson and template
- Each syndicate is to produce an INTSUM

- Focus on assuring all paragraphs in the fomat is covered in the product.

- Approx. Time: 40 minutes

Task:
Create an INTSUM based on the INTREPs received from instructors.

Resources:
A computer with a blank INTSUM format (.doc-file) will be required. The INTSUM may be produced in various forms if it contains all the elements found in the Intelligence Handbook.

Approx. Time:
40 minutes

Learning activity:
Assuming the role of a U2-section at a sector HQ, the syndicate should collate the four INTREPs produced earlier.

Learning activity:
Assuming the role of a U2-section at a sector HQ, the syndicate should collate the four INTREPs received earlier:

3 BATT INTREP 074/18
UNHCR Report
3 BATT SITREP 293/18
UNHCR Report
3 BATT SITREP 294/18
3 BATT INTREP 075/18
3 BATT SITREP 296/18

Expected outcome:
The students are to produce an INTSUM based on the INTREPS received.

Lesson
3.4d

Dissemination-PICINTSUM

The Lesson

Starting the Lesson

Slide 1

In this lesson, we will give you an overview of the PICINTSUM used for MPKI dissemination.
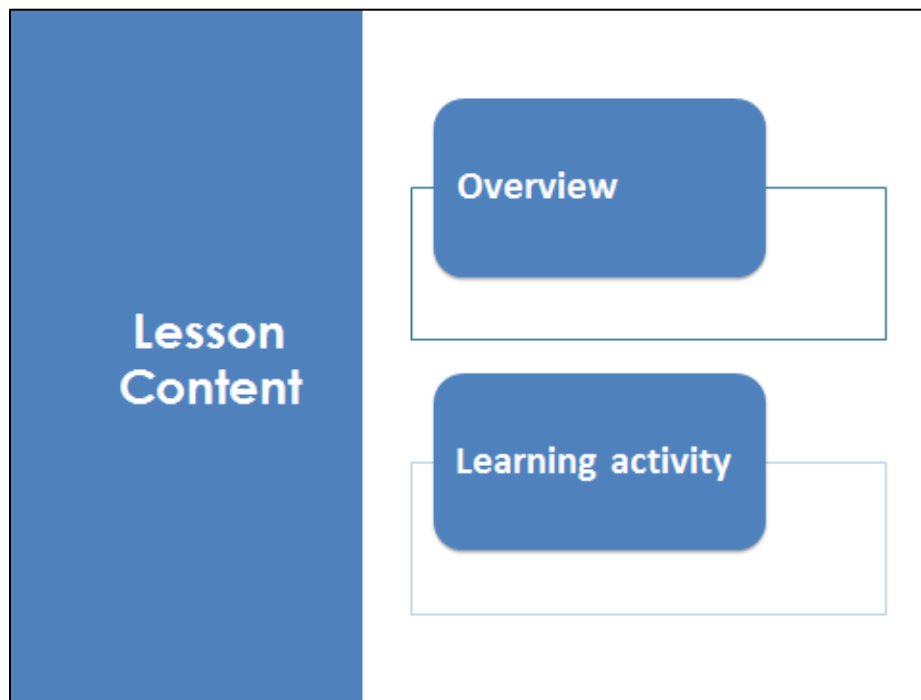
Slide 2

Here is the lesson content. The students will first be taken through an overview of creating a PICINTSUM and its components. They will then create a PICINTSUM as a learning activity.

Slide 3

Learning Objectives

- Explain why PICINTSUM is a graphic document driven by commander's PIRs

- Describe the PICINTSUM format

- Describe the content of a PICINTSUM and how it conveys information

Here are the learning objectives for this lesson. After this lesson, you should be able to do these objectives.

Slide 4
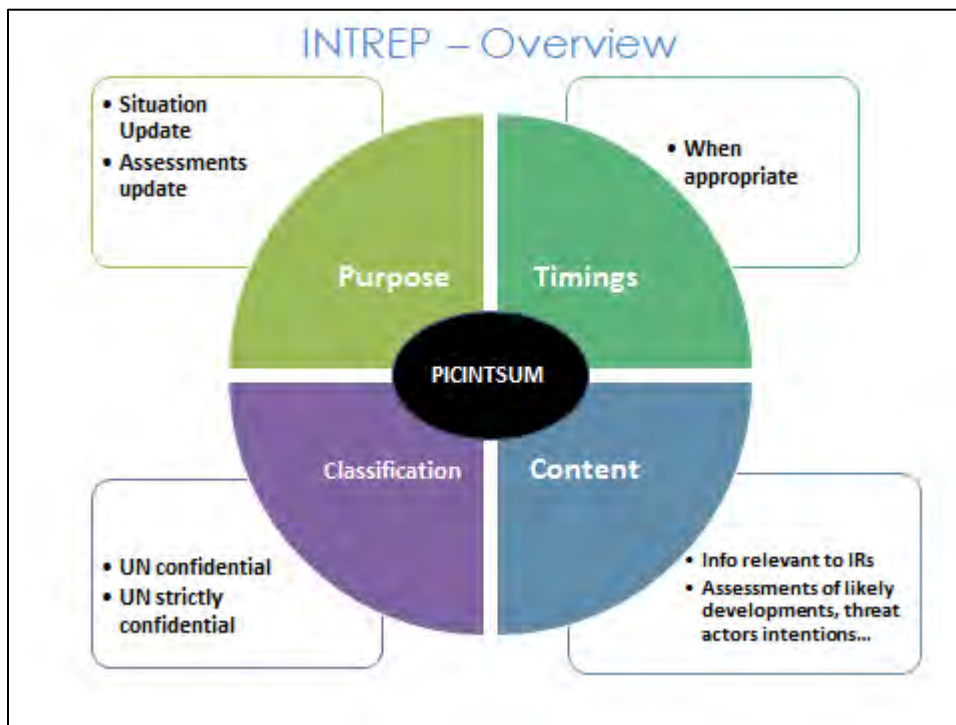
Key Message: It is a picture intelligence summary; PICINTSUM is a graphical representation of the written INTSUM.

As the information on the INTSUM, the PICINTSUM covers is a summary of peacekeeping intelligence on the current situation for a given period and within a commander's APIRs.

Its purpose is to – briefly - report essential elements of intelligence information. The PICINTSUM provides timely information regarding incidents/events that could influence current or pending operations.

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

A PICINTSUM is a presentation of incidents/events issued as soon as possible after their occurrence. It should include any information that may be relevant to the information/intelligence requirements of any commander to whom it is presented. It should include the issuing Intelligence staff's deduction of the significance of the information.

PICINTSUMs shall be classified based on content as either "UN CONFIDENTIAL" or "UN STRICTLY CONFIDENTIAL".

Slide 5

The PICINTSUM covers a period usually determined by the authority. It contains essentially three parts:

- A map that shows the area of responsibility as a whole or the area of the reported incidents or events.

- The significant peacekeeping intelligence should be reported on the map. In this regard, I encourage you to refer to the UN military symbols handbook to know how to depict incidents or activities on the map. If you're not familiar with the UN military symbols or there is no time to consult the handbook, use your common sense to create a legend. Blue is for water, red for the enemy, a plane for the airport.

- In the assessment part, put the summary of the analysis work with regards to impact on civilians, friendly ongoing or future operations/activities.

Slide 6
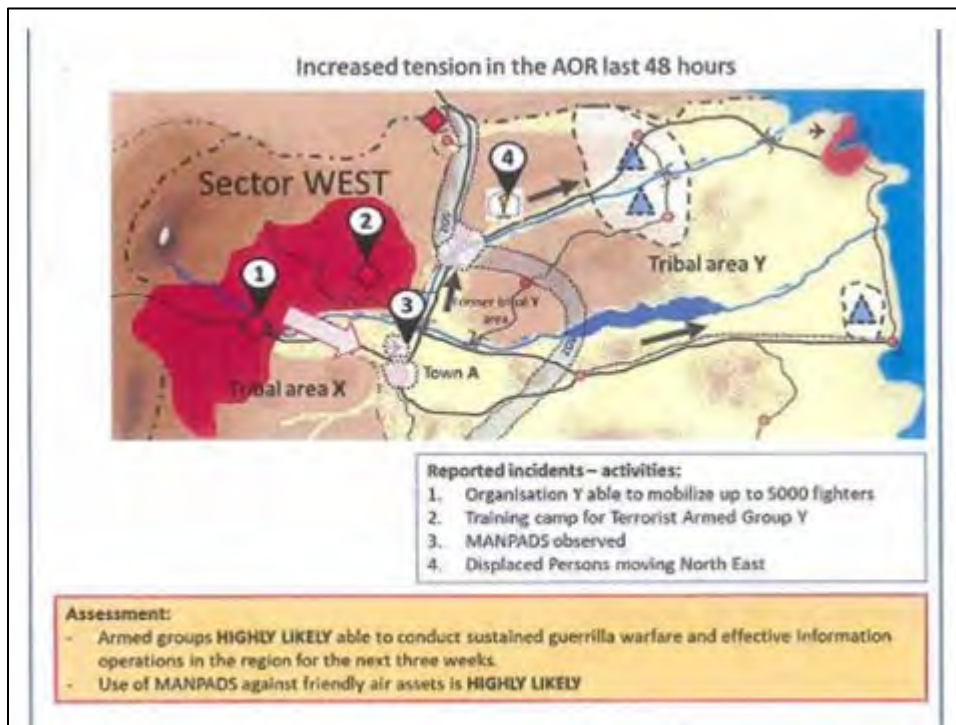
Here is an example of PICINTSUM. It contains the three parts we mentioned before:

- The map represents the area where the incidents or activities took place. You will notice that the reported incidents can be referred to by numbers, by conventional symbols or both.

- It is the case of incident number 4 (displaced persons) which is represented a number and the UN military symbol in the map. Specific details are put in the reported incidents box.

- the last box contains a summary of the assessment with regards to the impact of the reported incidents on civilians, friendly ongoing or future operations/activities, PoC

Use the uncertainty yardstick to avoid misinterpretation and misrepresentation. In this example, the first assessment is that armed groups are highly likely able to conduct sustained guerilla warfare and effective information operations in the region for the next three weeks.

Slide 7

> ## Take Away
>
> - PICINTSUM is a graphic summary of peace keeping intelligence on the current situation within a commander's APIR
>
> - Peace keeping PICINTSUM contains a map, reported incidents and activities and assessments

Summary

Remember that:

- PICINTSUM is a graphic summary of peace keeping intelligence on the current situation within a commander's APIR

- Peace keeping PICINTSUM contains a map, reported incidents and activities and assessments

Learning Activity

Slide 8

Task:
Create a PICINTSUM based on the INTREPS used to create the INTSUM in the previous lesson.

Approx. Time:
25 minutes

Learning activity:
Syndicate groups will go to their syndicate rooms and create one PICINTSUM per syndicate.

Expected outcome:
Each syndicate group will show their product on the main screen in the classroom. As this is to compare results, the students will not brief the product, but rather comment on each other's PICINTSUMs.

Lesson
3.5a

AOE- Introduction to Analysis of the Operating

Starting the Lesson

Introduction

AOE is a UN MPKI concept, which – even though it has many similarities with conventional military intelligence analysis concepts (example, IPB or IPOE, if mentioning this is relevant to the training audience) – is specifically designed to analyze the operating environment in UN military peacekeeping operations.

UN peacekeeping operations are affected by many factors – not only the physical terrain (often known as the "battlespace" in conventional military terms) and adversary/threat/enemy forces.

"Human Terrain" is probably the most important factor in the UN operating environment. Moreover, in today's hyper connected world, the information terrain governing how people communicate and how they are influenced is also important. These non-military factors must also be analyzed in order to conduct effective UN operations.

It is vitally important that the student considers these three factors in conjunction with each other, appreciating that they interact with and impact each other, rather than considering them as distinct entities.

Aim

The aim of this serial lesson is to provide you with the background for the lessons/serials in this table and give you an overview of the important parts of the course of instruction in this table. In other words, this lesson will "frame" the suite of analysis lessons

Slide 1
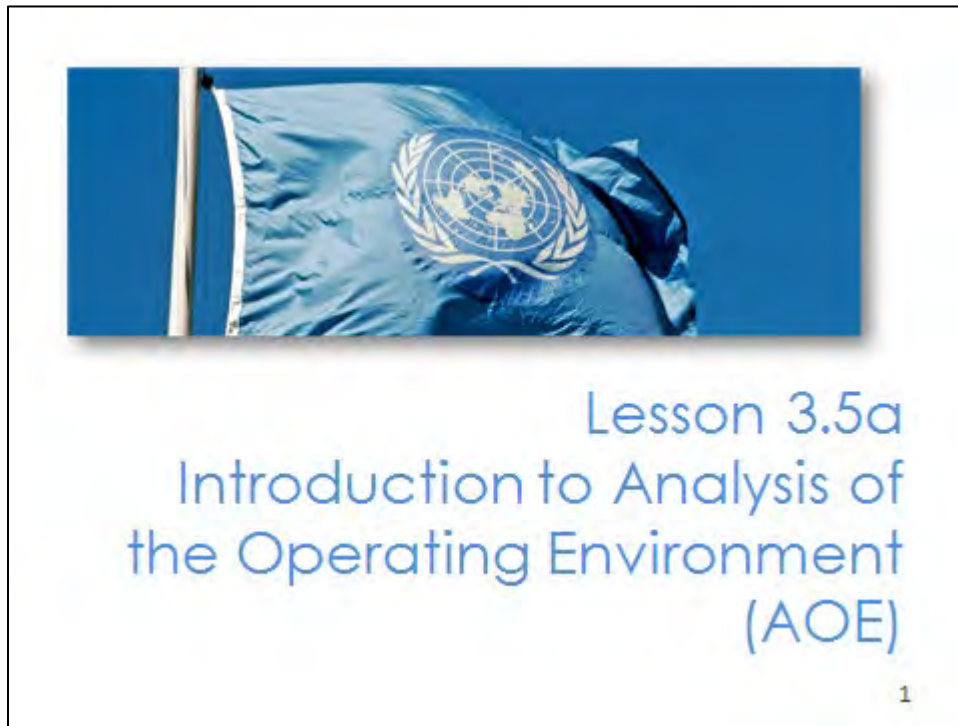
The following lessons aim to introduce students to the three phases of the AOE process, the products produced during each phase, and their subsequent use in support of the UN Military decision-making process, and planning information/intelligence collection.

AOE is where UN intelligence staff need to excel. AOE provides the basis for all operational activities – kinetic as well as non-kinetic. Therefore; it is essential that you fully understand the AOE process and can conduct it for the following reasons:

- Analysis of the Operating Environment (AOE) is the analysis used by UN MPKI staff to produce intelligence assessments, estimates and other intelligence products in support of the UN Commander's military decision-making process (MDMP)

- The AOE process helps you identify information/intelligence gaps and shortfalls, thus cueing additional acquisition through the intelligence acquisition plan and requests for information to higher and adjacent headquarters

- The AOE process provides a holistic view of the operating environment. The better you and the UN Forces understand the operating environment, the more effective operations will be in support of the mandate to protect civilians, and the more secure your Force will be from threats

Slide 2

Series of AOE Lessons

- Lesson 3.5a Introduction
- Lesson 3.5b Analysis of Physical Terrain (PT)
- Combining PT factors
- Lesson 3.5d Analysis of Human Terrain
- Lesson 3.5e Analysis of Information Terrain
- Lesson 3.5f ASCOPE – PMESII
- Lesson 3.5g Actor Evaluation
- Lesson 3.5h Situation Integration & COA Development
- Lesson 3.5i Short SPIE and situation paragraph
- Lesson 3.5j UN MPKI support to UN MDMP

2

Here is the content of all the AOE lesson series. In the first lesson 3.3a, we will introduce and explain the significance of AOE and why it is important to MPKIO and decision-makers

Next, we will present the analysis of the physical terrain as it is central to conventional Intelligence Preparation of the Battlefield (IPB).

To gain an appreciation of the operating environment, it is necessary to study the human terrain (the actors that live and operate in the physical terrain), and the information terrain (the way these actors communicate with each other). This gives a holistic 'systems' type evaluation of the operating environment.

It is necessary to consider these different types of terrain as a system. A systems approach means that you understand that a change to the physical terrain or weather will have an impact on the information and human terrain. Indeed, a change to any of these terrains will have an impact on the others.

For example, consider a change to the weather such as heavy rainfall. This will impact the physical terrain in that rivers could become less easy to cross, easy-going terrain could become impassable, and the health and sanitary conditions of the local population could also be affected.

As the MPKIO, it will be your role to recognize these first and second-order consequences of any change to any of the three different types of terrain. This takes time and practice.

We will also consider how the Human Terrain, particularly the actors that populate it, including armed and unarmed, interact with the physical, human, and information terrain. This Actor Evaluation process will not just focus on armed groups but also on all relevant actors, including political and socioeconomic.

Next, we will consider ASCOPE and PMESII. This is a system designed to make you think about the operating environment, and it will help you identify the variety of factors affecting and informing the evaluation of each of the three types of terrain, being particularly important to the Human Terrain.

We will also conduct an exhaustive Actor Evaluation. This phase will be recognizable to experienced intelligence officers as 'Threat Evaluation'. However, in a UN operating environment, the focus is on evaluating all relevant actors. Any actor, armed or unarmed that can have an impact, *positive or negative*, on the operating environment.

Finally, we will examine how the relevant actors interact with the three different types of terrain. This situation integration process, the second last lesson on the list, will help the MPKI cell to understand how these relevant actors are likely to behave; these are the Courses of Action that we will develop. Experienced intelligence analysts will recognize Situation Integration as conventional Threat Integration.

.

Slide 3

Content and Learning Outcomes

- Content: AOE Introduction, Analysis of the Operation Environment, AOE phases

- Describe the requisite tools and knowledge to analyze the operating environment

- Explain the application of AOE in support of the UN Military Decision-Making Process

As a good training practice, let's review the content and learning outcomes of this lesson: 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 this introduction to AOE.

Slide 4

Figure 13: The 3 Phases of AOE
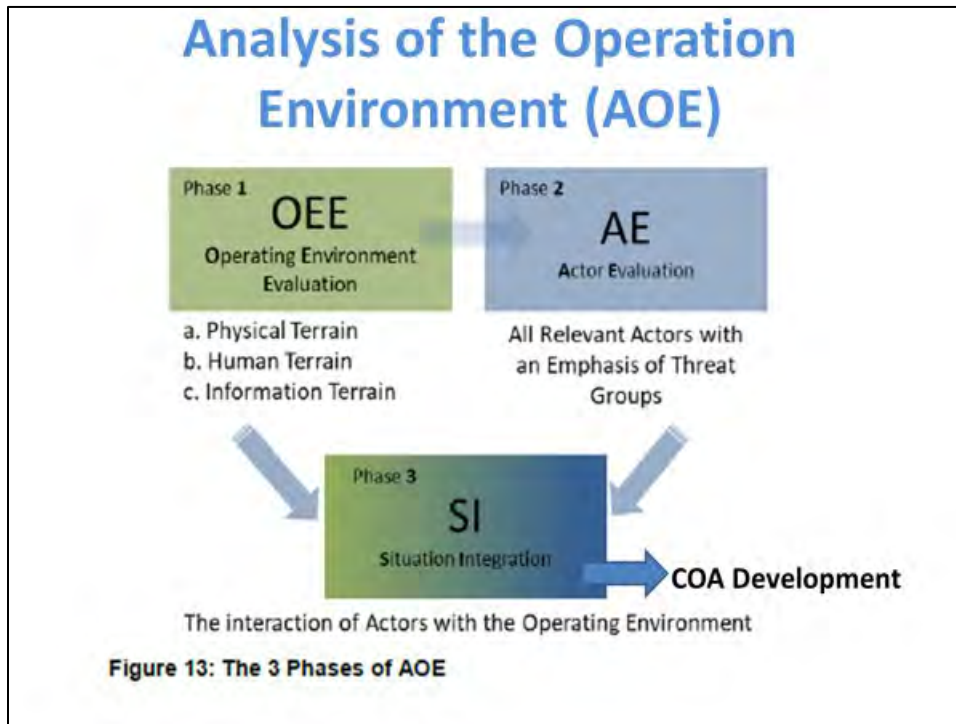
The AOE is a UN MPKI concept that is specifically designed to analyse the operating environment in UN military peacekeeping operations AOE consists of three phases:

- Operating Environment Evaluation, which analyses the three terrains: physical, human and information

- Actor Evaluation, which evaluates the intentions and capabilities of all relevant actors

- Situation Integration and course-of-action (COA) development designed to envisage how relevant actors will probably behave and react in the context of their operating environment

It is important to understand that AOE is a UN MPKI concept that is specifically designed to analyse the operating environment in UN military peacekeeping operations UN peacekeeping operations are affected by many factors – not only the physical terrain (often known as the "battlespace" in conventional military terms) and adversary/threat/enemy forces, which are the focus of conventional military intelligence.

Remember that the human terrain (people and groups) live in the physical terrain (the UN AO), and communicate and propagandize using the information terrain A change

to any of these types of terrain can cause a change or changes in the others, or the behaviour of actors.

This diagram is taken from the UN MPKI Handbook and shows the AOE process, which consists of the following three phases:

- Phase 1: Operating Environment Evaluation (OEE). The Operating Environment consists of three terrains (or dimensions): physical terrain, human terrain and information terrain. These terrains are interrelated, and they interact with each other.

- Phase 2: Actor Evaluation (AE)- In the AE phase of the AOE process, all relevant actors are evaluated with an emphasis on actors that can influence and threaten UN peacekeeping operations. It is important to note that the Actor does not operate in a vacuum. For example, a threat group lives within, can threaten, and often relies on the support of the human terrain. It must also adapt its capabilities to the physical terrain, and it communicates and interact using the information terrain to develop courses of action we must have a detailed understanding of both the terrain and the actor being evaluated

- Phase 3: Situation Integration (SI) - Based on the detailed results (products) of the evaluation of the OE (Phase 1) and the actors within the OE (Phase 2), the MPKI staff produce an informed, predictive assessment of how the actors can affect the achievement of the UN Force Commander's mission

This assessment is presented in the form of possible Actor Courses of Action (ACOAs), which then inform the UN Military Decision-Making Process These courses of action are determined based on how you assess the actor, based on its capabilities and intent, will interact with the Operating Environment

Interaction. Prompt a discussion of how a threat might affect a group of IDPs. How will the physical, information, and human terrain shape their likely courses of action in the face of a threat? Naturally, IDPs will flee from danger, along routes that are passable, attempting to maintain contact with loved ones and those that can protect them, ideally towards a sympathetic population. In this case, a knowledge of the operating environment can help the MPKI cell predict where these IDPs might reasonably be expected to go.

This is the critical part of the UN MPKI section's job It is here that you can shape your commander's decision-making process If you know the UN commander's intent, you can access how armed groups or other relevant actors are likely to react to various UN concept of operations designed to accomplish the mission.

Ideally, you will develop Courses of Action for both armed and unarmed groups These courses of action, when presented to operations personnel/your commander, will allow

them to mitigate the impact of adversary operations against UN forces or the potentially negative impact of UN forces on unarmed groups, or the local population

☞ *Note to Instructor:* *If some of your students have previous military intelligence training and experience, they may remark that AOE consists of three steps or phases, which are similar to the steps of the Intelligence Preparation of the Battlespace (IPB) or the Intelligence Preparation of the Operating Environment (IPOE) process, which is used in conventional military operations. However, do not use a comparison of AOE with IPB/IPOE to introduce this part of the lesson, as it may confuse students without a military intelligence background*

If the question of IPB/IPOE versus AOE should arise, you may explain the following:

- *The IPB/IPOE process is in several respects similar to the UN AOE process, as the IPB/IPOE process also consists of three steps or phases (IPB/IPOE consists of the following steps: 1 Battlefield area evaluation; 2 Threat evaluation; 3 Threat integration.*

- *Just as AOE supports the UN MDMP, IPB an analytical tool used by military intelligence to support the conventional Military Decision-Making Process However, in UN peacekeeping operations non-military ("civil") factors – especially human factors and factors impacting on human life and activities – are the focus when UN peacekeeping forces plan and conduct their operations.*

- *In conventional military operations, the focus is on the terrain and enemy forces, which are the primary military factors relevant to kinetic operations against identified adversaries/enemy forces There may be armed threats to UN Forces that have to be mitigated, but UN Forces do not conduct military operations to attack and destroy actors.*

☞ *Note to Instructor: Please note the use the term "Actor", the word "Enemy" is not used by the UN Peacekeeping; adversary, spoilers, or opposition forces/actors against the mandate are appropriate terms.*

Slide 5
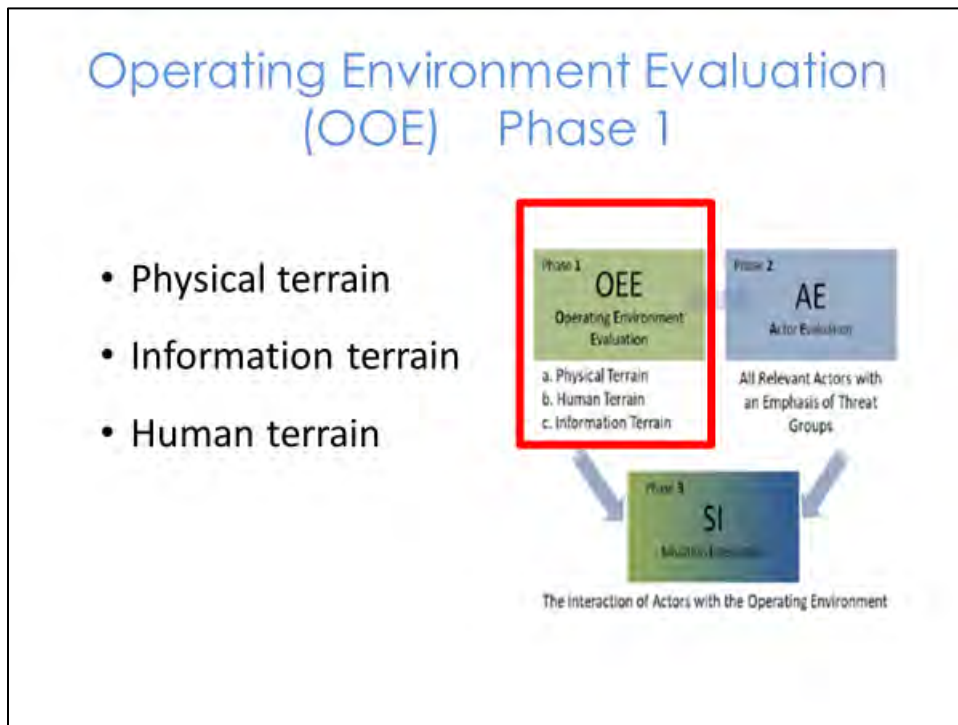
Phase 1 of the AOE is the Operating Environment Evaluation, which analyses three separate, but interlinked "terrains". The physical, the human, and the information terrain, each of which function as part of the UN operating environment's holistic ecosystem.

Perhaps a useful way to consider this is that although the process calls for us to analyse each type of terrain separately. Our overall evaluation must incorporate all three terrains. Again, it cannot be overstated how important it is to recognize that a significant change to one of the terrains will affect the other two

Interaction: Ask the students to consider the impact of a major terrain change on the human and information terrain. Suggest that a large area of what has previously been farmland has been flooded by heavy rains and that it has become a marsh. Ask them as a group how such a change will affect the physical, human, and information terrain.

Response: What we seek to know in this case is that the flood will undermine food production, could induce the local population to migrate and resettle, and could overload road systems and other lines of communication.

Physical Terrain:

The analysis of the physical terrain is based on mapping, satellite imagery etc. Engineers are qualified to assist in the analysis of the physical terrain, including the effects of weather conditions on the physical terrain, including mobility and use of critical physical infrastructure The analysis of the physical terrain includes identification of natural and humanmade obstacles that can disrupt, fix, turn or block the movement of a force based on the degree to which the terrain in various areas restrict the movement of UN Forces or actor groups, mobility corridors can be identified areas of cover, physical infrastructure, key terrain, vital ground, etc. are also identified as part of the analysis of the physical terrain

Human Terrain:

Human Terrain Analysis, uses human terrain mapping to produce overlays showing the areas inhabited by the various tribes, ethnic groups, religious groups, and political factions in the Area of Intelligence Interest. Other overlays used in Human Terrain analysis show the reach and influence of various leadership structures (political, military, religious, social, etc.), population density, income distribution, and the locations of IDP (internally displaced persons) and refugee camps. Separate overlays are produced showing positions of host nation military and law enforcement units and entities, as well as the positions and areas occupied by threat actors etc.

Human Terrain analysis employs link analysis to show the relationships between persons, events, organisations etc.

Through Human Terrain mapping and link analysis, key actors are identified, and an Items of High Importance List is produced. The Items of High Importance List includes individuals, equipment, infrastructure, etc. which are required by both threat actors and UN Forces to achieve their objectives.

Human Terrain analysis also encompasses gender analysis, which assesses the impact of the physical terrain, the information terrain and the various actors on the lives of women in the Area of Intelligence Interest.

Information Terrain:

The Information Terrain includes various means of communication and information exchange. These means of communication may be person-to-person communications or mass communications. Person-to-person communication means include:

- Voice communications such as telephones, two-way radios and voice messaging systems (such as Skype, Messenger, WhatsApp)
- Social media (such as Facebook)
- Email

Mass communication means include:

- Mass media (such as print media (newspapers and magazines), radio, television)
- Web-based media (online newspapers, journals, blogs etc.)
- Social media (Twitter, Instagram, Facebook)
- Video and audio sharing platforms (for example, YouTube)

Note that there are a close interrelationship and interaction between the "terrains". Each "terrain" impacts on the other "terrains". For example, the Information Terrain is shaped by the physical terrain (e.g. location of mobile/wireless telecommunication masts and internet coverage) and the Human Terrain (the producers and consumers of information with access to the communications infrastructure).

Note to the Instructor. The students must appreciate that simply identifying factors related to the physical, information, and human terrain, together with those related to relevant actors is not enough. This is simply stating known facts. The students must instead make deductions, which lead to specific outputs using the three-column format. This is a technique that will be taught later in this course.

Slide 6
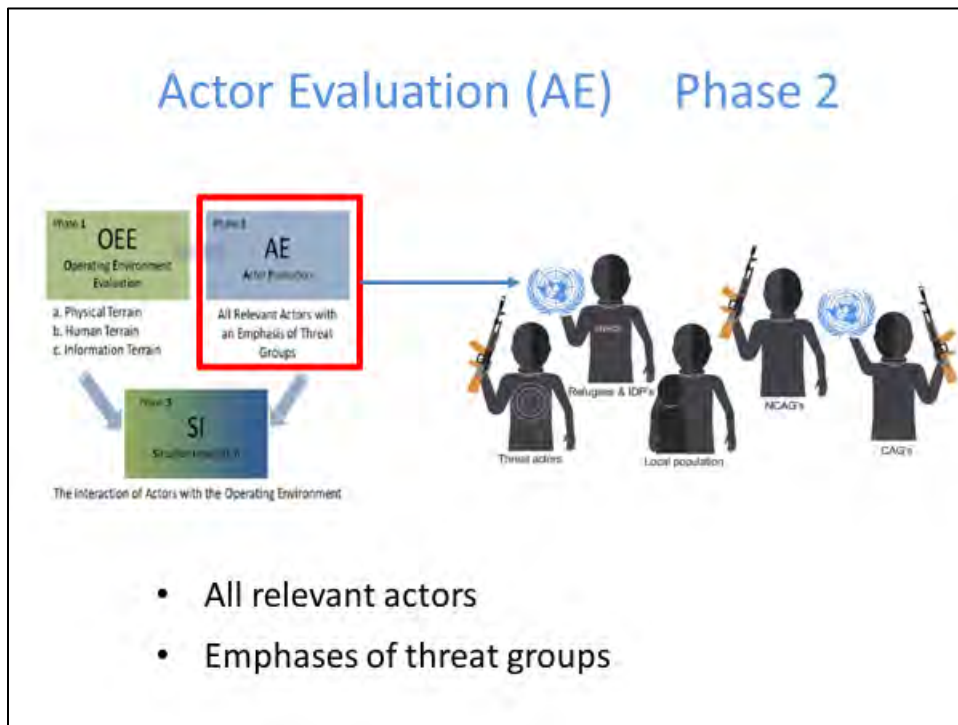
AE is the second phase of the AOE process. It analyses actors/groups that can have an impact on UN operations and the OE. The results of AE will be integrated with the results of the OEE in the third phase of the AOE process, which is Situation Integration.

Actors are individual humans or human collectives and structures (families, clans, tribes, ethnic groups, religious communities, organisations, interest groups, government authorities, security forces, armed groups, etc.) that are likely to influence (positively or negatively) or threaten - UN Forces and operations as well as influence/affect other aspects ("terrains") of the Operating Environment.

It is important to stress at this point that the UN approach differs from that of conventional military forces in that the UN does not just evaluate armed actors. Rather, it also evaluates and analyses all relevant actors that can influence the UN Force's operating environment.

These actors are identified in Phase 1 – primarily in the analysis of the Human Terrain. Often ASCOPE-PMESII also supports the identification of relevant actors.

AE has the following purposes:

- Analyse in further detail those actors/groups that are likely to have a significant impact on UN operations and on the OE

- Analyse the capabilities, including organisation, patterns of operation, tactics, techniques and procedures, and the actor's current situation

- Analyse intent, including desired end state, ideology, and motivation

- Evaluate an actor's strengths, weaknesses, opportunities and threats, and centre of gravity

- The product of which will be used in Phase 3, System Integration, to develop actor COAs

During Phase 2, further analysis is conducted of the actors identified in the HT analysis As part of the AE, the ways – broadly speaking – in which these actors could carry out activities in order achieve their assessed aims/desired end state is identified The AE includes the categorisation of each actor/group (for example, an armed terrorist group (TAG)) as well as its primary ethnicity, area of operations/responsibility, objective(s), assessed end state, the centre of gravity, critical requirements (i.e. critical to preserving its centre of gravity in order to achieve its end state), critical capabilities and critical vulnerabilities

It should be noted that threats can also be non-kinetic (for example, non-violent civil disobedience or epidemics). Actors can demonstrate a threatening intent – or have a friendly/neutral stance, which could provide opportunities for influencing them.

☞ **Note to Instructor.** Abbreviations

IDPs: Internally displaced persons

NCAGs: Non-compliant armed groups (groups not complying with UN resolutions and other agreements)

CAGs: Compliant armed groups

Slide 7
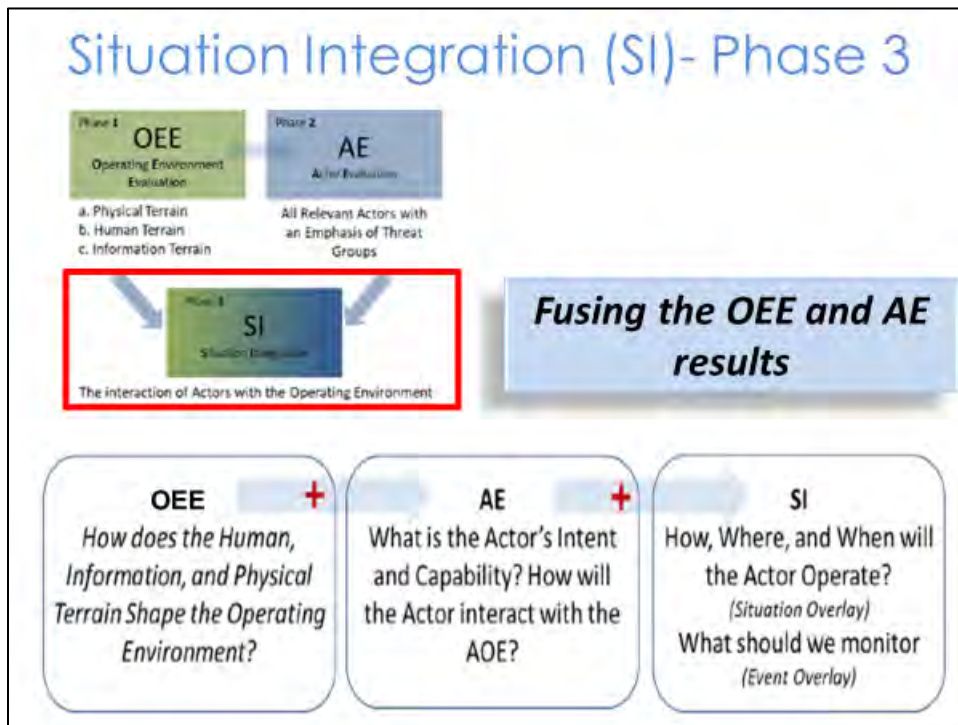
Slide 8
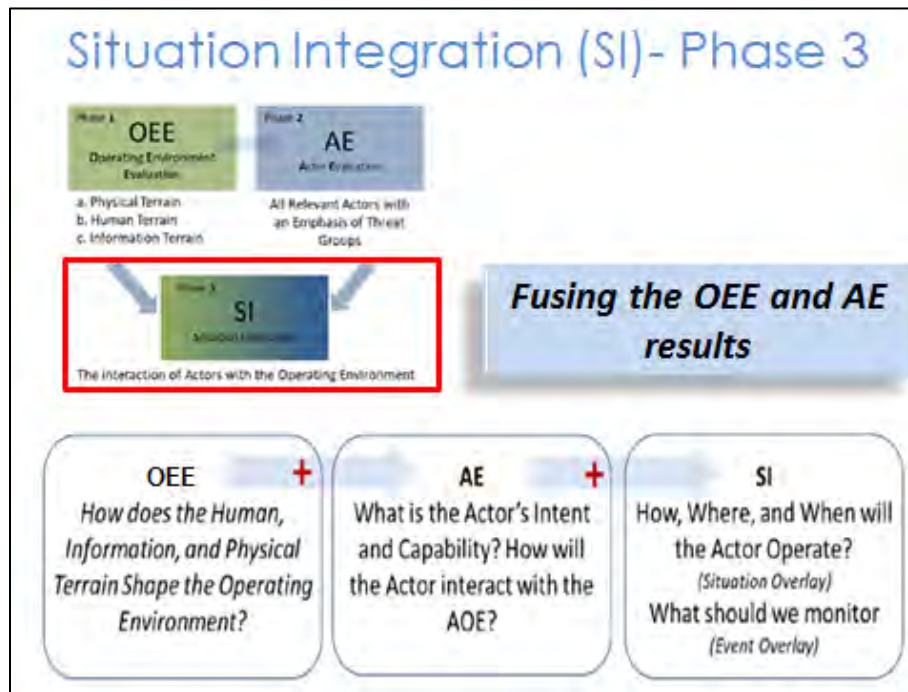
Situation Integration (SI), the third phase of the AOE process, fuses the results of Phase 1, the OEE, with the results of Phase 2, AE, in order to identify how actors, groups or threats can conduct operations and actions within the constraints and restraints of the Operating Environment as well as based on each actor/group/threat's capabilities and following its known doctrine (tactics, techniques and procedures).

SI is the third phase of the AOE process. This figure broadly illustrates the process in which the results of the OEE are fused with the results of the AE to provide the input to SI.

The results of Phase 1, the Operating Environment Evaluation, which answer how Physical Terrain, the Human Terrain and the Information Terrain shape the Operating Environment are combined with the results of Phase 2, which answer how the actor will interact within the restraints and constraints of the Operating Environment based on its intent and capabilities (means of achieving desired goals based on intent).

Combining the results of Phases 1 and 2 provide the basis for assessing how, when and where an actor can operate in each of several possible courses of action, shown in the form of a situation overlay for each Actor Course of Action (COA).

These assessments are also used to determine what and where we should monitor and acquire intelligence, as shown on an event overlay and included in the intelligence acquisition plan (IAP).

These are among the most important products that an MPKI cell will produce and will be used as the foundation to produce the short peacekeeping intelligence

estimate, the situation paragraph, and all other products used to support the UN MDMP.

Slide 9
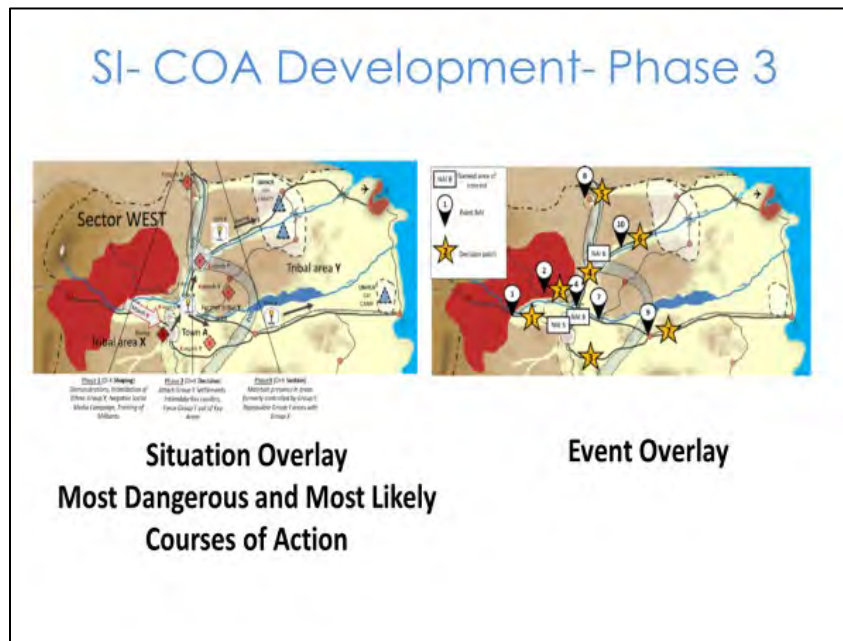
On this slide, we show how SI, the third phase of the AOE process, results in the identification of the Most Likely Actor COA (MLACOA) and the Most Dangerous Actor COA (MDACOA), each shown in the form of a Situation Overlay.

The situation overlays are combined with the results of the evaluation of the operating environment to identify Named Areas of Interest (NAIs) which are monitored as part of the information acquisition effort in order to determine an actor/group/threat's intent to pursue one or another COA and Target Areas of Interest (TAIs), where we, the UN Force, can take action to force or influence an actor to choose an ACOA that is favourable to us.

SI produces informed, predictive assessments of possible Actor Courses of Action (ACOAs) that will likely affect the UN mission and the Military Commander's operations and tasks

Actors may include tribal groups or factions within the population. For the planning and execution of every UN operation, whatever its size, the MPKI cell must, at a minimum, identify the ACOA most likely to be pursued by each actor/group/threat (MLCOA) and the most dangerous COA (MDCOA) that can be pursued by each hostile or potentially hostile actor (or threat).

Each ACOA is presented in the form of situation overlay showing how the actor would carry out its operation or activity, taking into consideration the restraints and constraints imposed by the Operating Environment. An example of a situation overlay is shown on the left of the slide.

The situation overlays are combined, to produce an Event Overlay, which shows Named Areas of Interest (NAIs) which are monitored as part of the information acquisition activities in order to confirm an actor/group/threat's intent to pursue one or another ACOA. The Event Overlay also shows Target Areas of Interest (TAIs), where we, the UN Force, can take action to force or influence an actor to choose an ACOA that is favourable to us.

In addition to the Situation Overlays, each ACOA is accompanied by an ACOA statement that states what action the actor will take when the action takes place, where it will take place, and how it will be carried out in the format of a Scheme of Manoeuvre or Concept of Operations – depending on the sophistication of the actor and the required level of detail. Each ACOA must be feasible (realistic), acceptable (regarding losses), complete (taking all operational considerations such as logistics into account), exclusive (essentially different from other ACOAs), and suitable (for achieving the actor's objectives).

These ACOAs support the Military Decision-Making Process by enabling the Commander and his/her staff to develop the most effective own COA to achieve the mission of the UN Force, and to mitigate any action that an adversary intends to take against UN Forces.

Situation Integration and ACOA Development will be covered in much greater detail in a five-hour lesson later in this Table.

Slide 10

It is important to understand the main points of this lesson. This is a recap of the main points of this presentation:

- AOE is essential to the UN Military Decision-Making Process because it provides intelligence products that are vital to effectively conducting the process

- AOE is specifically adapted to UN Peacekeeping Operations It focuses on the many aspects of the operating environment that can impact UN peacekeeping operations within an area of operations

AOE consists of three phases:

- Phase 1: OEE – Operating Environment Evaluation

- Phase 2: AE – Actor Evaluation

- Phase 3: SI – Situation Integration and course-of-action development

Learning Activity 33a

Slide

Learning Activity
Discussion of UN MPKI AOE process

Instructions:
- Explain the purpose of the AOE process.
- Explain why the UN has developed the AOE process.
- Name and briefly describe the three phases of the AOE process.
→ Prepare to present your answers verbally in class

Time: Approx. 10-15 minutes
Group work and Discussion in plenary

RESOURCES
Chalkboard, whiteboard or flipchart paper and markers.

TIME
Approximate-15 minutes

NOTE TO INSTRUCTORS
Break the class into two groups. Have the participants address the discussion points on the slide.

- Do the participants understand why the UN uses the term AOE?

- Can the participants name the three phases of the AOE process and briefly explain what each phase covers?

- If not, why? Try to identify possible causes and explain and briefly provide answers to the discussion points.

Possible discussion points:

- AOE is essential to the UN Military Decision-Making Process because it provides intelligence products that are vital to effectively conducting the process

- AOE is specifically adapted to UN Peacekeeping Operations It focuses on the many aspects of the operating environment that can impact UN peacekeeping operations within an area of operations

- AOE consists of three phases:

- Phase 1: OEE – Operating Environment Evaluation

- Phase 2: AE – Actor Evaluation

- Phase 3: SI – Situation Integration and Course-of-Action Development

Lesson
3.5b

AOE- Analysis of the Physical Terrain (PT)

The Lesson

Starting the Lesson

For an interactive start to this Lesson, have the participants explain the three phases of the AOE (the OEE, AE and SI, including ACOA development). As this is the first lesson of the OEE phase of the AOE, have the participants state the three terrains that are analyzed in the OEE phase (i.e. the Physical Terrain, which is the topic of this lesson, and the Human and Information terrains, which will be covered later).

Note to Instructor: You may want to emphasize that the Human Terrain and the Information Terrain exist within the Physical Terrain. The Physical Terrain is the real, physical (as opposed to the virtual) environment in which all actors live, move by various means of transportation, make a living on and off the land, plant IEDs, conduct ambushes, communicate, exchange and broadcast information, etc.

Slide 1

Slide 2
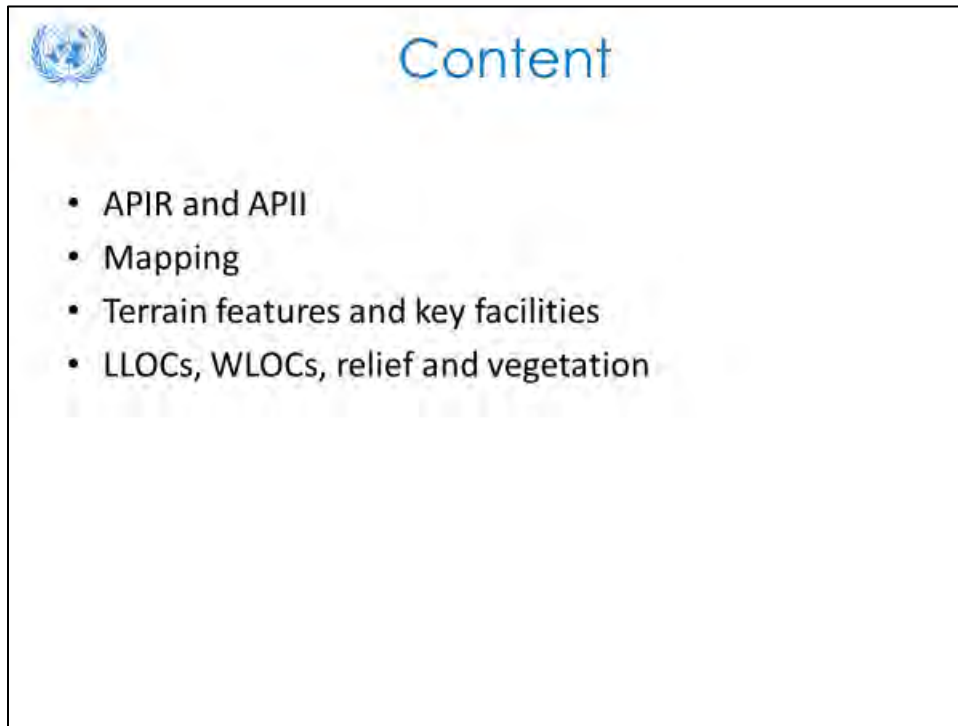
This lesson will cover the following topics:

- Definition and explanation of the Area of Peacekeeping Intelligence Responsibility (APIR) and the Area of Peacekeeping Intelligence Interest (APII)

- Mapping, which is the primary basis for analyzing the Physical Terrain

- Terrain features and key facilities

- Landlines of communication, water lines of communication, relief and vegetation

Slide 3

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

Slide 4

Key Message: The analysis of the Physical Terrain is crucial to the OEE as it forms the basis for the analysis of the Human and Information Terrains. Climate and weather are variables which affect the Physical Terrain and thus the two other terrains (or domains), the Human Terrain and the Information Terrain. The Physical Terrain thus determines the Courses of Action (COAs) open to UN Forces as well as other actors in the Area of Operations.

Within the Area of Operations, all movement of UN Forces and other actors, including groups hostile to the UN presence (i.e. threats), is constrained and restrained by the Physical Terrain as it is affected by climate and weather. Terrain determines which types of movement are possible, for example, whether is it possible for tracked or wheeled vehicles to operate in an area or along a particular route.

UN Peacekeeping Operations are, to a large extent, shaped by the Physical Terrain as it is affected by climate and weather. Weather and climate conditions (for example, heavy rains that cause flooding or snow in the winter) can change the physical characteristics of the terrain and impact the movement by vehicles and on flight conditions for UN aircraft.

The human and information domains exist within the Physical Terrain and are formed and influenced by it. Climate and weather also have a significant impact on the Human Terrain and the Information Terrain. Certain types of terrain (land) are favourable for human habitation – others are not. Different types of agriculture require favourable soil and climate conditions. Oranges cannot grow naturally in Northern

Norway but thrive in a Mediterranean climate. Radio communications are affected by terrain as well as weather conditions.

Analysis of the Physical Terrain and how it is affected by climate and weather are the means to determine which UN Courses of Action (COAs) can best exploit the opportunities the Physical Terrain provides and how the terrain affects the COAs available to the other actors in the Area of Operations including, actors that pose a threat to the UN Forces. Without a thorough analysis and understanding of the Physical Terrain, successful operational planning is not possible. Military history is full of examples of faulty appreciation of the terrain.

Slide 5

The Physical Terrain encompasses the land and ground environment – and if relevant, the maritime environment (oceans, seas, lakes, waterways, etc.) and airspace. It is the basis for the actions of all actors in the Area of Operations.

The physical terrain consists of open areas (routes, corridors) that provide good mobility; obstacles that impede mobility; areas that provide cover and concealment for own (e.g. UN) forces as well as other actors including hostile actors; infrastructure (typically humanmade structures); key terrain (that gives an advantage to UN Forces or other actors) and vital ground (the control of which is vital to the success of an actor's mission.)

There are many examples of how the Physical Terrain and weather/climate conditions have affected military operations:

- Napoleon's (or Hitler's) invasion of Russia hampered by "General Mud" (during the spring thaws and autumn rains) and "General Winter" (snow and ice with extremely cold temperatures)

- Monsoon season in Southeast Asia (Burma Campaign during World War 2, Vietnam War)

- The German Ardennes Offensive in December 1944 ("Battle of the Bulge"), where German Armor (tanks) attacked through the Ardennes Forest in Belgium, achieving surprise over the American forces of the 12th Army Group

and posing a potential threat to Allied logistics coming through the important harbour of Antwerp.

Slide 6
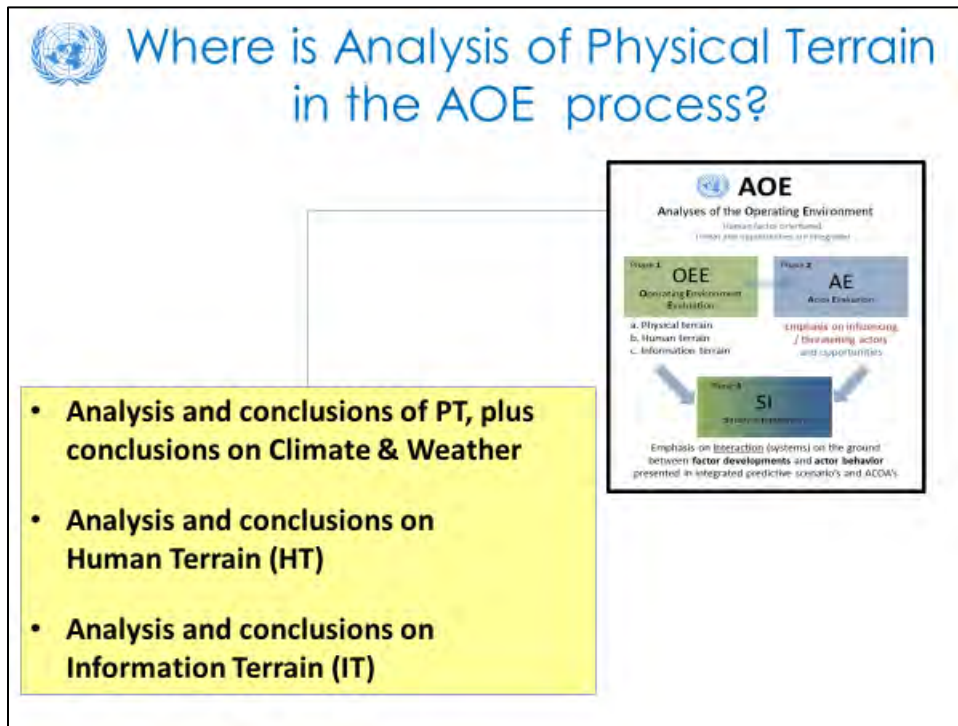
The analysis of the Physical Terrain is part of the Operational Environment Evaluation, which is the first phase of the AOE Process, together with the analysis of the Human Terrain and the Information Terrain.

Together with the next phase of the AOE process, Actor Evaluation, the OEE is essential to the conduct of the final phase of the AOE Process, Situation Integration and the development of Courses of Action (COAs).

Slide 7
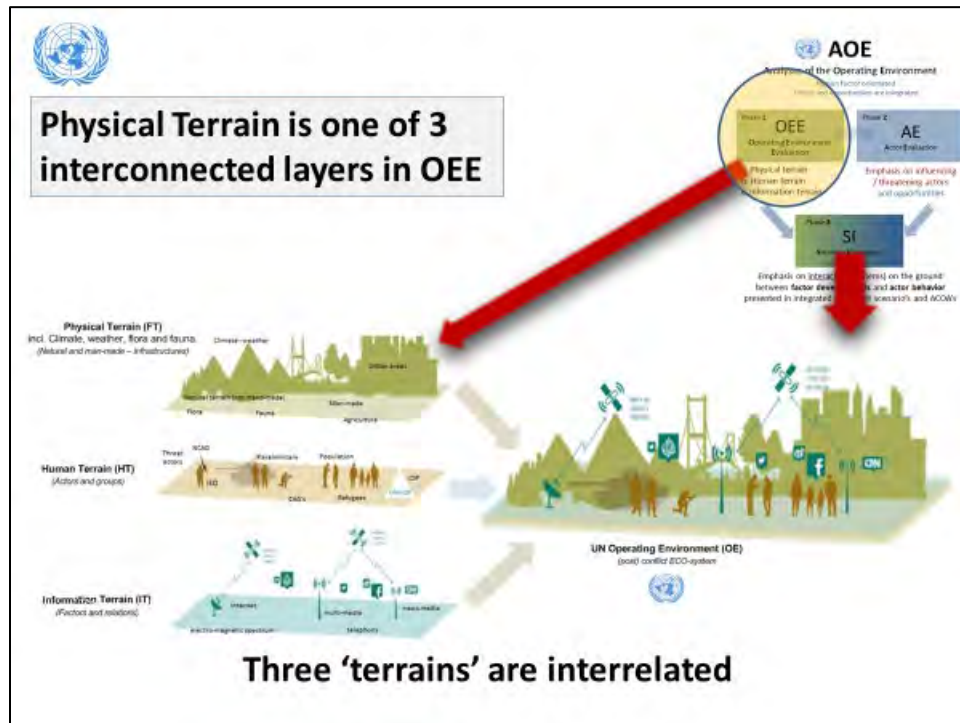
Key Message: The Physical, Human and Information Terrains are interrelated; they interact and "weave" among each other.

The Physical Terrain, or the" ground", is one of the interconnected terrains or layers that are analysed in the OEE.

As shown on the slide, these three terrains are interrelated; they interact and" flow" amongst each other.

The figure to the right illustrates how they meld together and form the Operating Environment. The drawing shows different types of terrain, such as urban terrain, which is humanmade, and humanmade infrastructure such as a bridge; as well as natural mountains. Vegetation (flora) and animal life (fauna) are also parts of the Physical Terrain.

The population as a whole" populates" the Physical Terrain. The physical terrain dictates where these population groups would operate.

The Human Terrain specifically consists of the various actors and groups in the Operating Environment. They can be threat groups (such as terrorist armed groups), non-compliant armed groups (armed groups that are not complying with UN Security

Council Resolutions or agreements between the parties to the conflict), compliant armed groups (that are complying with UN SC Resolutions and agreements between the factions); military and paramilitary forces, refugees and internally displaced persons (IDPs). The UN High Commissioner for Refugees as an organisation dealing with IDPs and refugees is also part of the Human Terrain. The Physical Terrain, as well as weather and climate conditions, affect the population in general and the various individual actors and groups in their activities and actions.

Interaction. Ask the class how they think the physical terrain would influence where a local population group would choose to live. The instructor should lead the debate. Responses would include close to a water source, in an accessible area, in an area not affected by flooding, close to arable land. The list goes on and on. This should last no more than 5 minutes.

The Information Terrain, of course, includes print media such as newspapers, magazines and books. Today the electromagnetic spectrum (EMS) is of greater importance as the carrier of TV and radio broadcasts as well as mobile telephony. The internet is the platform for social media (SOME) such as Facebook, Twitter, Instagram etc. which reaches wide audiences inside as well as outside the Area of Operations. Here the Physical Terrain, including weather conditions, affects connectivity. The distribution and circulation of information in physical (paper) form can be hampered by difficult terrain and unfavourable weather and climate conditions. Electronic communications can be affected by adverse weather and climate conditions as well as physical barriers to signals transmission such as mountains.

Interaction. Ask the class how they think the physical terrain affects how an actor communicates. The instructor should lead the debate. Responses would include mountains can undermine the EMS, such as mobile phone signal, internet penetration. This should last no more than 5 minutes.

Slide 8

Key Message: The Physical Terrain is analysed within the context of the Area of Peacekeeping-Intelligence Responsibility and the Area of Peacekeeping-Intelligence Interest because it is the habitat for all actors. Other factors relate negatively directly or indirectly to the Physical Terrain.

Human actors and groups must have a physical space (habitat) in which to live, work and function; therefore, it is important to understand the Physical Terrain in which they live and function. The Physical Terrain is the habitat ("living space") for all actors

- They live from and on it - shelter, housing, food etc.

- They are influenced by it, as it determines where and when they can live, move and work, and

- How they use it

When analysing the Physical Terrain, focus on the defined Area of Peacekeeping-Intelligence Responsibility (APIR) and the wider Area of Peacekeeping-Intelligence Interest (APII), as these areas have direct importance to the UN Force's planning and conduct of operations (APIR and APII will be explained in the next slide).

Note to Instructor- At this point, it is vital to stress that the key concept of 'so what' concerning physical terrain is how it informs the Courses of Action of individuals or groups of individuals.

Interaction. Ask the students how the physical terrain could shape a threat actor's course of action. Responses here could include that the physical terrain will force the threat actor to use certain Movement Corridors. Therefore, a good knowledge of the physical terrain will ensure that the MPKI cell can predict which Movement Corridors will be used.

Many factors like weather, unrest, famine, mobility, communications are often directly and indirectly affected by the Physical Terrain and the conditions on the Physical Terrain ("ground"). Weather and climate, as mentioned before, can change the nature of the Physical Terrain (rains cause flooding and winter close mountain pass, thus affecting mobility). Unrest can cause – and be caused by – famines. Infrastructure can be destroyed or built/repaired by actors in the Area of Operations, thus impeding or promoting mobility, or increasing or diminishing the reach of communications.

Slide 9
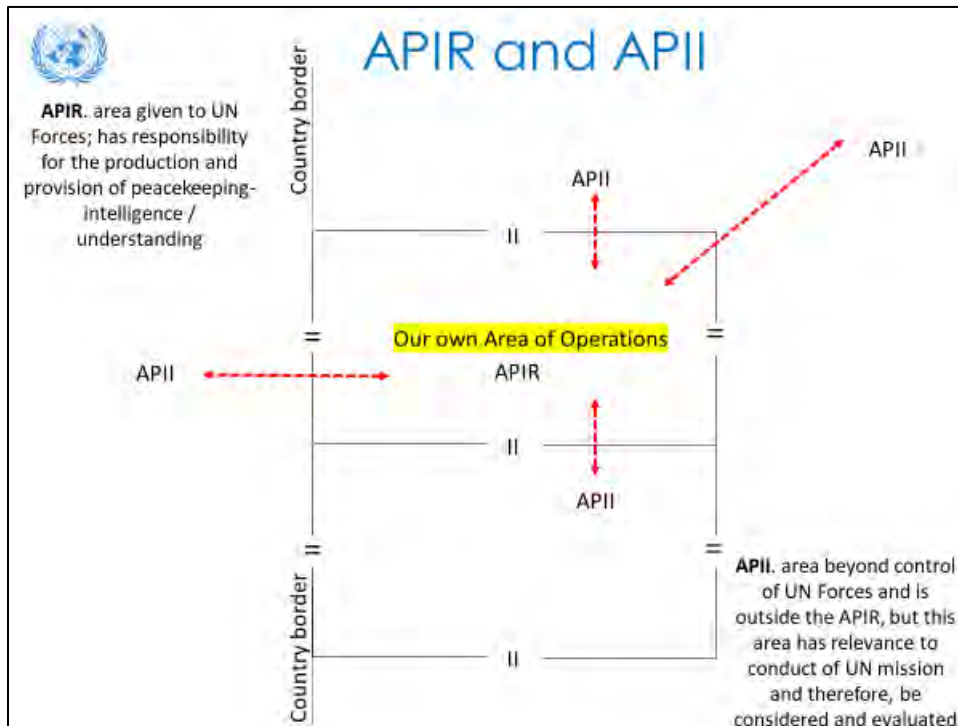
Key Message: A prerequisite for analysing the Physical Terrain is defining the APIR and the APII in order to focus the Analysis of Operating Environment.

Before conducting the analysis of the Physical Terrain, it is necessary to define the Area of Peacekeeping-Intelligence Responsibility (APIR) and the Area of Peacekeeping-Intelligence Interest. This enables us to focus our analysis of the Physical Terrain as well as the Human and Information Terrains to a defined, relevant area.

The APIR is defined as the area given to a UN Force for which it (i.e. the Commander) has the responsibility for the production and provision of peacekeeping-intelligence / understanding. In other words, the UN Force Commander is responsible for knowing everything about Operating Environment and the actors within the UN Force's APIR. It is, therefore, important that the UN Force has the necessary acquisition assets to adequately cover its entire APIR.

The APII is an area beyond the control of the UN Force (i.e. the Commander), and thus outside of the APIR, but the APII has relevance to the conduct of the UN Force's mission and must, therefore, be considered and evaluated. Events, actions and factors in the APII may affect the Operating Environment within the APIR and must, therefore, be taken into consideration. Information and intelligence about the APII will usually have to be collected by acquisition assets that are not controlled by the UN Force Commander.

This information and intelligence will usually have to be acquired through UN agencies or non-UN agencies.

Interaction.

A couple of examples are shown in the drawing: An armed actor is using country C as a haven and staging area for operations in country A, which is the UN Force's APIR. It is, important that the UN Force has adequate knowledge/understanding of what is happening in country C. Another example could be that violence in country A is causing people to flee to the neighbouring country B, which may affect the UN Force's operations in country A, its APIR. Therefore, countries B and C become the UN Force's APII.

As the Instructor, ask the students to define what their APIR and APII in a UN Area of Operations are.

For example, in Mali at the Sector level, the APIR would be the Sector AOR, but clearly, most Malian actors do not conform to the UN concept of an AOR. These actors will move freely between sector AOs, and some actors will even move between countries. Therefore, events in other sectors are clearly of interest to the MPKI cell.

Other Examples you can give:

- *MINUSMA: Actors use the border region between Mali and Niger to their advantage*

- *MONUSCO: Actors use the border region between DRC, Uganda and Rwanda to their advantage*

- *The LRA (Lord's Resistance Army) operates in the larger border area between CAR, SS, DRC, Uganda*

Slide 10

Learning Activity

How to analyze and evaluate the Physical Terrain (**PT**):

- **Situation:**
  - Use the scenario to identify APIR and APII

- **Task:**
  - Define the Area of Peacekeeping Intelligence Responsibility (APIR) and the Area of Peacekeeping Intelligence Interest (APII)

- **Time:** Approx. 10 min -group work and discussion

Key Message: Analysis of the Physical Terrain requires the definition of the APIR and the APII. Mapping is used to produce the" Golden Products" needed for MPKI understanding and for supporting the UN MDMP. Integrate the results of the analysis of the Physical Terrain. Remember that AOE is a continuous, cyclic process.

We use maps because they are depictions of the physical terrain and provide a common reference or base for the products (overlays) we will produce. Maps can be printed (on paper), or they can be electronic (computer-generated in Geographic Information Systems (GIS)) – depending on which type of Command Control Information System (C2IS) the UN Force HQ uses. Maps are low-tech but reliable. However, overlays and other map-based products must be reproduced in hard copy for distribution. C2IS require technical skills and may be subject to various problems (technical and human); however, products can easily be distributed throughout the UN Force – provided all headquarters and units are connected to the system.

In order to analyse and evaluate the Physical Terrain, we need to:
Define the Area of Peacekeeping-Intelligence Responsibility (APIR) and the Area of Peacekeeping-Intelligence Interest (APII), which was explained in the previous slide, as we need to determine which geographic area or areas we are to focus our analysis on. The group will be broken down into syndicates. Each

syndicate will represent a sector G2 branch and will have an officer in command (G2 Chief). Each Syndicate will have an instructor assigned to guide them through the process; each syndicate needs a sector map, a series of overlays, and semi-permanent markers of various colours (Blue, Brown, Black, Red, and one other colour at a minimum).

Slide 11

Key Message: Terrain features may be divided into natural terrain features and human-made terrain features.

There are two types of terrain features: naturally occurring terrain features and terrain features made/created/built by humans (i.e. "manmade").

This slide gives some examples of natural and human-made terrain features. Please have a quick look at each of the two categories and see if there are some natural or manmade features that are missing.

All such features must be identified, based on a combination of patrols and map recce.

Interaction. Ask the class what resources a UN MPKI cell has at its disposal to identify and confirm the physical terrain features, both natural and humanmade. Examples would include Map recce, use of aerial photos, GIS, use of ISR assets such as UAS to confirm, for example, the trafficability of roads/bridges, the deployment of patrols.

Slide 12

Key Message: Identification of the terrain features is an important part of the process. Integrate the results of the analysis of the Physical Terrain. Remember that AOE is a continuous, cyclic process.

AOE is a continuous, cyclic process! It doesn't stop; all products (overlays, etc.) must be continuously updated as new information/intelligence is made available.

Required minimum outputs, often referred to as the 'golden products' (due to their importance in support of peacekeeping intelligence understanding and informing decision-makers). To analyse and evaluate the Physical Terrain, we need to:

- Use mapping and other assets to identify natural and human-made terrain features

- Mark key features on the map, using overlays. Overlays must be of enough quality to allow all staff to deepen their understanding of the physical terrain environment

Working in syndicate groups have participants review the slide and then discuss. Have syndicate groups report back and brief the plenary. Each syndicate represents a sector G2 branch. What are essential and desirable for the overlay.

Note to Instructor-

We use maps because they are depictions of the physical terrain and provide a common reference or base for the products (overlays) we will produce. Maps can be printed (on paper), or they can be electronic (computer-generated in Geographic Information Systems (GIS)) – depending on which type of Command Control Information System (C2IS) the UN Force HQ uses. Maps are low-tech but reliable. However, overlays and other map-based products must be reproduced in hard copy for distribution. C2IS require technical skills and may be subject to various problems (technical and human); however, products can easily be distributed throughout the UN Force – provided all headquarters and units are connected to the system.

Slide 13
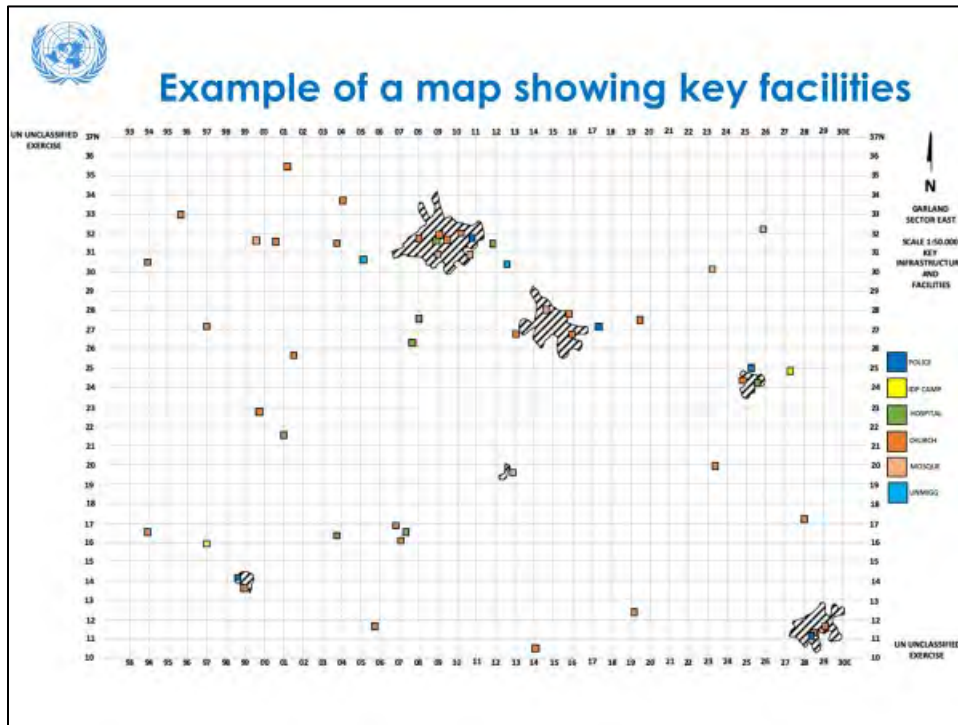
Key Message: Maps (or overlays) showing key facilities are one of the products of the analysis of the Physical Terrain.

Interaction. This example is taken from the main scenario and is a map showing key facilities. Ask the students which key facilities are shown on the map? Advise the students to move from east to west; and north to south. Having identified key facilities, the students would then clearly mark the map (the map becomes the 'key facilities overlay' and move these factors to the 3-column format for further evaluation. This is the process that is to be followed for each step of the physical terrain evaluation. Here are areas to be identified:

- *Religious areas (POC)*
- *Hospitals (POC)*
- *Schools (POC)*
- *Markets (POC)*
- *Tunnel*
- *Border crossing stations*
- *Roads*
- *Bridges*
- *Refugee and IDP camps*

- *Proposed oil pipeline*
- *Provincial and regional / provincial capitals*
- *An airfield in the provincial capital*
- *High-tension power line*
- *Provincial capital (EMBE)*
- *Dam with hydroelectric power plant*
- *Ferry across lake*
- *Zirconium mine*
- *UN bases, UN regional offices*
- *Facilities and areas designated by the SRSG*

Slide 14

This is an example of a key facility analysis.   Do not forget to identify areas that are linked to the protection of civilians and facilities designated by the SRSG.

Slide 15

Working in syndicate groups have participants review the slide and then discuss. Have syndicate groups report back brief the plenary.

Show students the process. It will not be conducted at each stage of this lecture set. Rather, at the end of the lecture, students will be asked to apply this process to all aspects of the physical terrain. It is, therefore, less important that the students finish this exercise and more important that they understand the process.

Ask them to use their sector information and mapping to identify key facilities. Mark all key facilities on the map. This is the key facilities overlay for the sector. Transfer the factors to the 3 Column format and make deductions. As an output, the instructor should ask students to identify RFIs that patrols or other sources of information can be tasked to confirm.

Note to Instructor *- Emphasize to students that they need to follow this process for every aspect of terrain outlined in these lessons. This will be confirmed at the end of the AOE lessons and the TTX, which is designed to ensure that each syndicate has already completed a full physical terrain analysis prior to the final exercise.*

Slide 16

Types of Terrain Analysis and Overlays to Complete
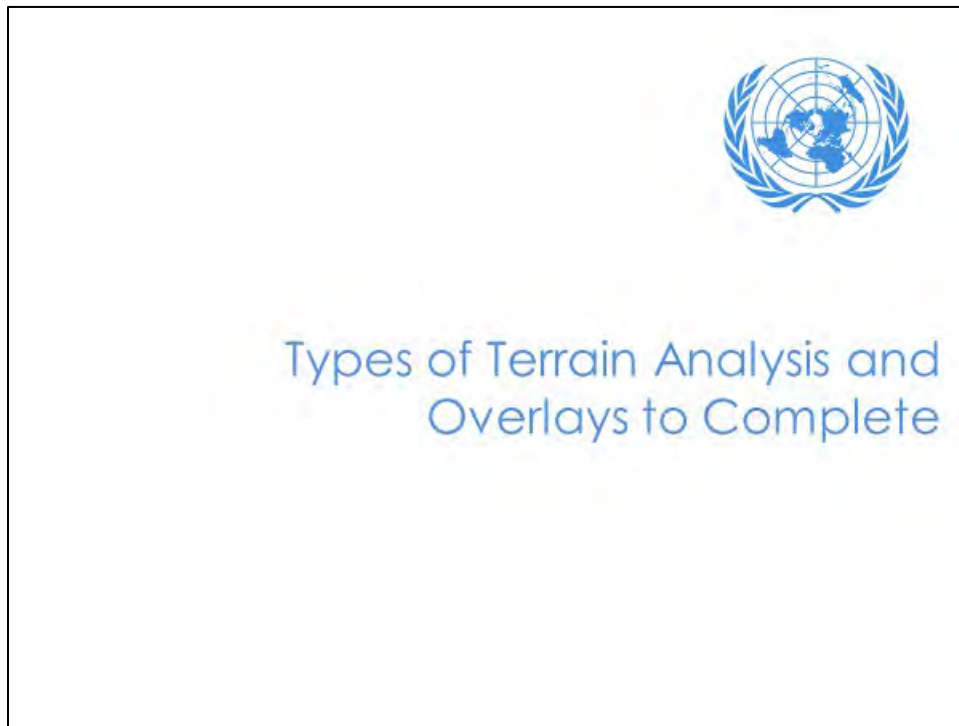
We are now going to look at some of our PT overlay products.

Slide 17

Key Message: It is essential to have accurate and up-to-date mapping. One overlay should be produced for each topic/factor to be analysed; avoid combining several topics/factors on one overlay. Details and clarity are important.

Always make sure that you have the best available mapping; it should be accurate and up to date. Old mapping can be misleading, since it may be based on outdated information and old topographical surveys – perhaps dating back to colonial times. Modern mapping is based on satellite imagery and telemetry and is therefore accurate and updated to the time the satellite imagery was produced.

Sometimes either digital mapping or analogy (printed) mapping may not be immediately available. In that case, MPKI staff, together with Operations and the Geographic Information Section, will need to acquire the necessary mapping in the required formats as quickly as possible.

Map scales should be 1:50,000 or 1:100,000 when evaluating the whole Operating Area. However, when conducting the AOE for a specific, small-unit operation, details and clarity are important. In such a case, detailed close-up imagery of the objective or target area may be necessary. Also, symbols must be clear and readable. If greater detail and clarity is required, use callout boxes to provide additional information, for example, as a text insert or even as an inserted photograph.

Overlays should be drawn separately according to the topic on clear sheets of plastic (or semi-transparent overlay paper (sometimes known as onion skin paper)) – and not directly on the printed map. Digital overlays should be produced on separate digital layers that can be added to and removed from the base map – and not drawn directly on the digital map.

Also, don't redraw map features on the overlay. Just highlight the objects and elements that are relevant to the topic of the overlay and that are necessary to make the necessary conclusions regarding that part of the analysis of the Physical Terrain.
A separate overlay should be produced for each specific topic/factor in order to focus on information and provide flexibility when different topical overlays need to be compared or combined.

Don't cover up the map! You must be able to see the map through the overlay.

Slide 18

Key Message: Always include a legend on overlays, so the reader/user is not in doubt as to what the symbols mean.

Always include a legend on overlays, so the reader/user is not in doubt as to what the symbols mean. Also, strive to have uniform symbology within the UN Force, thus avoiding that each staff section, unit etc. has its own overlay symbols that may even vary from task to task and from staff member to staff member.

Keep in mind that symbols should be readable/understandable whether an "analogy" (printed/drawn) overlay is reproduced/copied in colour or black and white.

Furthermore, include glossary or list of abbreviations used in the overlay – especially when abbreviations are not commonly used.

This slide shows some of the symbols used on physical terrain overlays during this course.

Note the symbology for the "going" of different types of terrain (restricted and severely restricted). Water bodies and watercourses are usually indicated in blue.

Slide 19

There are certain aspects of basic terrain evaluation that must be completed before analysis can take place. The basic evaluation layers are the following: key facilities; land and water lines of communication; elevation; and vegetation. We can then bring the results of these evaluation stages forward for deeper analysis.

Slide 20
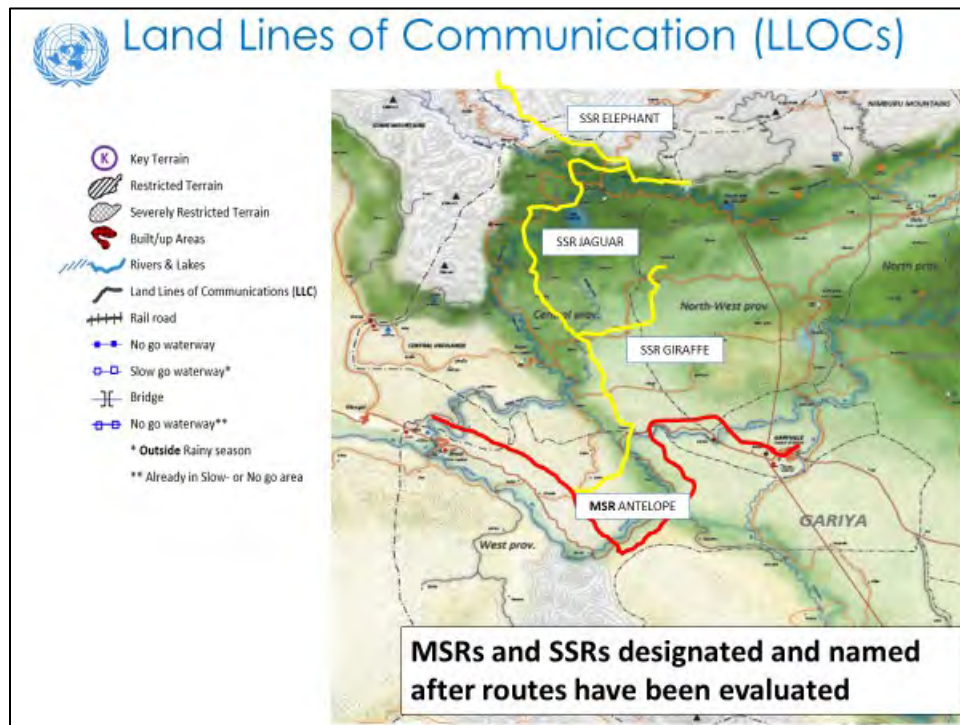
Key Message: The LLOC Overlay shows the land routes within the area of operations that may be used for vehicular and other traffic.

This slide shows an overlay of the Land Lines of Communication within Sector West and identifies all routes throughout the operating environment, including roads, tracks and likely transit routes that may be used by UN Forces and other actors.

Also evaluates all the routes for movement by different types of transportation such as motor vehicles (tracked as well as wheeled (two-wheel drive and all-wheel drive vehicles), pack animals and movement on foot.

Routes may permit only one type of movement (for example, on foot) or several types of movement (vehicles or pack animals). Weather conditions and seasonal climate conditions may also impact on the various routes. For example, the rainy season may turn unpaved roads into mud that cannot be used by motor vehicles.

Once more, MPKI cells are to mark the known LLOC factors on the map and to conduct a further evaluation using the three-column format.

Interaction. *Ask the students how LLOCs influence both an unarmed actor and a threat actor's course of action?*

Slide 21
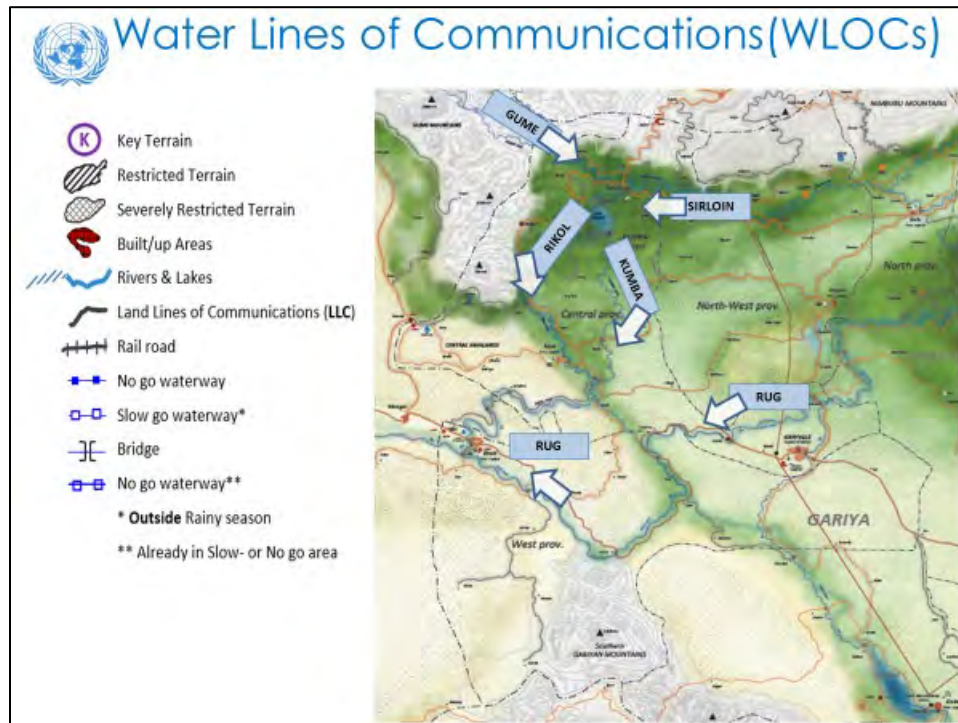
Key Message: The WLOC Overlay shows the water routes within the area of operations that may be used for waterborne traffic (different types of watercraft).

This second slide shows an overlay of Water Lines of Communication within Sector West. Identifying all waterways throughout the operating environment, including rivers, lakes, canals, channels etc. that may be used by UN Forces and other actors.

Evaluating all the waterways for movement by different types of relevant watercraft as well as places where these waterways may be crossed. Weather conditions and seasonal climate conditions may also impact on the possibility ("going") of the various waterways. For example, during the dry season rivers may dry out to such an extent that larger boats cannot navigate on them.

Note that the labels show the names of the waterways and the arrows indicate the direction of their flow. MPKI cells are to mark the known WLOC factors on the map and to conduct a further evaluation using the three-column format.

Interaction. Ask the students how WLOCs influences both an unarmed actor and a threat actor's course of action?

Slide 22
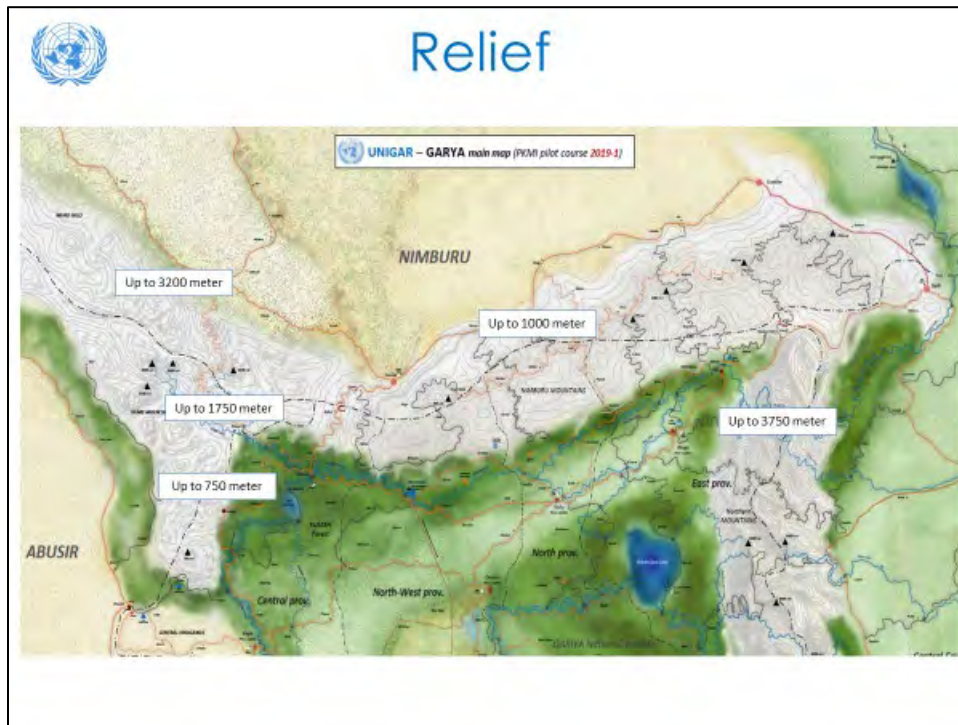
Key Message: This overlay shows the relief of the terrain.

This third slide shows an overlay of the terrain relief. The terrain relief is the physical shape, configuration or general unevenness of a part of the Earth's surface, considered with reference to variations of height and slope or to irregularities of the land surface.

It is determined by the elevation or difference in elevation, considered collectively, of a land surface. In plain terms, terrain relief is how "rugged", "bumpy", "rough" – or how "flat", "gentle" – the terrain is.

Relief determines to what degree the terrain restricts movement, what the terrain can be used for (agriculture or grazing, for example), and what other types of human activity that can take place in that terrain. Relief also determines points of observation as well as fields of observation and fire.

MPKI cells mark the known relief factors on the map, and to conduct a further evaluation using the three-column format

Interaction. Ask the students how relief influences both an unarmed actor and a threat actor's course of action?

Slide 23
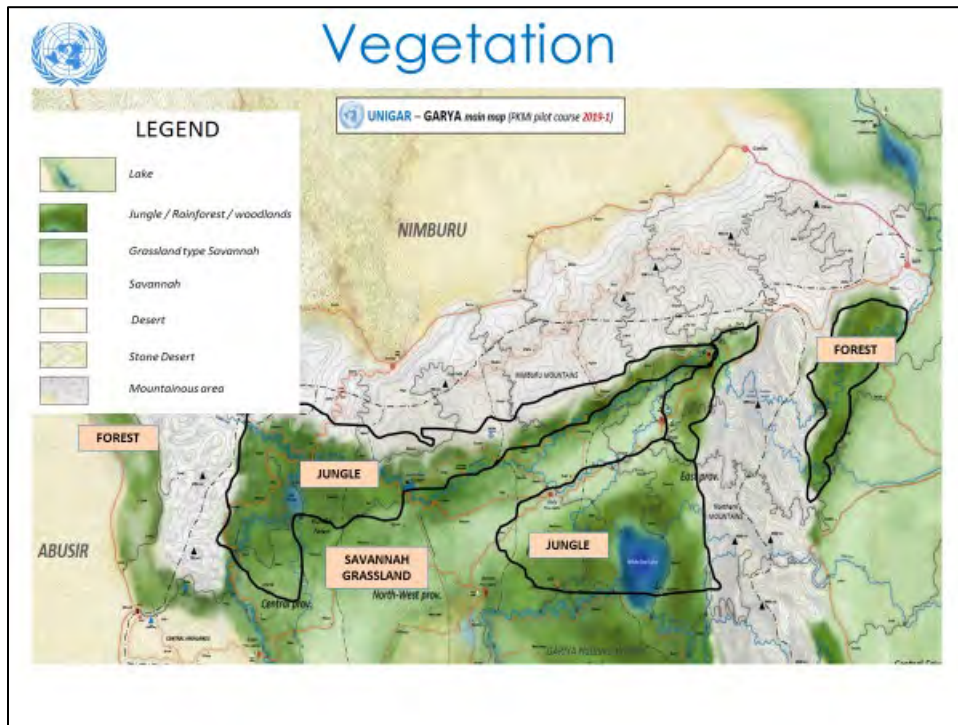
Key Message: This overlay shows the types of vegetation within an area.

This fourth slide shows an example of a vegetation overlay. Vegetation is the plant life found within a certain area. Vegetation impacts on movement. (Dense jungles, for example, severely restrict all types of movement, whereas there are usually few restrictions on movement in open grasslands.)

Vegetation can provide opportunities for an economic activity such as agriculture, including grazing, logging, and other types of human activity. Vegetation also impacts on points of observation as well as fields of observation and fire. Weather conditions and seasons also have an impact on vegetation. In the fall, trees may lose their leaves, making an observation in forests easier.

Once more, MPKI cells are to mark the known vegetation factors on the map and to conduct a further evaluation using the three-column format

Interaction. Ask the students how vegetation might influence both an unarmed actor and a threat actor's course of action?

Slide 24

Working in syndicate groups have participants review the slide and then discuss. Have syndicate groups report back brief the plenary. This is the basic terrain overlay for the sector. Ask them to use their sector information and mapping:

- *To identify WLOC, LLOC, Relief, and Vegetation*
- *Mark on the map*
- *Transfer the factors to the 3 Column format and make deductions*
- *To identify RFIs that patrols or other sources of information can be tasked to confirm*

Note to Instructor. *Emphasize to students that they need to follow this process for every aspect of terrain outlined in this lecture set. This will be confirmed at the end of the lectures with an exercise, which is designed to ensure that each syndicate has already completed a full physical terrain analysis prior to the final exercise.*

Slide 24

Summary

This lesson has provided some basic concepts and skills for Terrain Analysis. Here are the take-away key messages from this lesson.

Lesson
3.5c

AOE-Combined Physical Terrain Factors

The Lesson

Starting the Lesson

There may not be enough time for the students to produce a Combined Obstacle Overlay and a Mobility Corridor Overlay. Therefore, prepare "school solutions" of the overlays to be provided to the syndicates, thus refocusing the learning activities pertaining to the overlays so that the students analyse the prepared overlays (i.e. extract the "so what" from these overlays) and present their results in plenary.

Briefly review the content covered in the previous lesson on the analysis of the Physical Terrain – either by asking the students to explain the content of the previous lesson or by quickly highlighting the following:

- What is the Area of Peacekeeping Intelligence Responsibility (APIR)?

- What is the Area of Peacekeeping Intelligence Interest (APII)?

- What are some important terrain features?

- What are land lines of communication (LLOCs) and water lines of communication (WLOCs) and why they are important?

- What is relief (Give examples)

- What is vegetation? (Give examples.)

This sets the stage for combining the physical terrain factors in order to determine how the physical terrain and weather conditions affect the courses of action of the actors in the UN Force's area of responsibility/operations.

Slide 1

Lesson 3.5c
Combining Physical Terrain
(PT) Factors

Slide 2

Lesson 3.5c Content

- Military Aspects of the Terrain
  - Map Overlays
- Military Aspects of the Weather
  - Weather Effects Matrix

This lesson will cover the following topics:

- Terrain mobility, which is essentially the trafficability of the terrain by various means of transportation, for example by foot, beast of burden, different types of vehicles

- Cover and concealment, which is how the terrain can provide cover from the effects of different types of weapons, and concealment, which is how the terrain can hide personnel, weapons, facilities etc. from observation

- Key terrain and vital ground, which are important to the accomplishment of the UN Force's objectives as well as the objectives of various actors, especially hostile actors

- How to produce overlays

- The effects of weather and climate on the physical terrain

Slide 3

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

Of note, all these tools help us apply AOE products in support of the UN Military Decision-Making Process. Later, we will practice and apply these learning outcomes during the scenario-based exercise or table-top exercise (TTX) by using best-practice approaches in accordance with UN Military Peacekeeping Intelligence Doctrine.

Slide 4

Aspects of the terrain is an integral part of the intelligence. PT plays a key role in any peacekeeping operation. PT provides a base for all intelligence operations, tactical and tactical operations. This slide lists the aspects of the terrain. We will cover these in more detail.

Slide 5
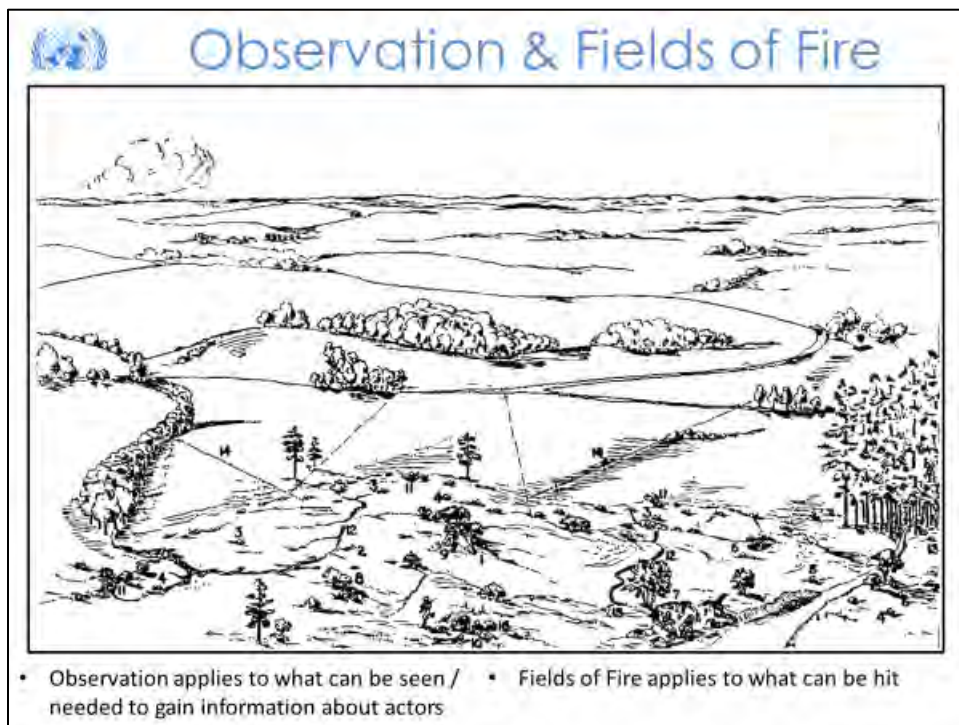
Observation is the ability to see over an area and is terrain dependent. More often, the best observation is gained from the highest terrain in an area. Fields of Fire is an area a weapon can effectively be used at its full potential from a given location.

Slide 6
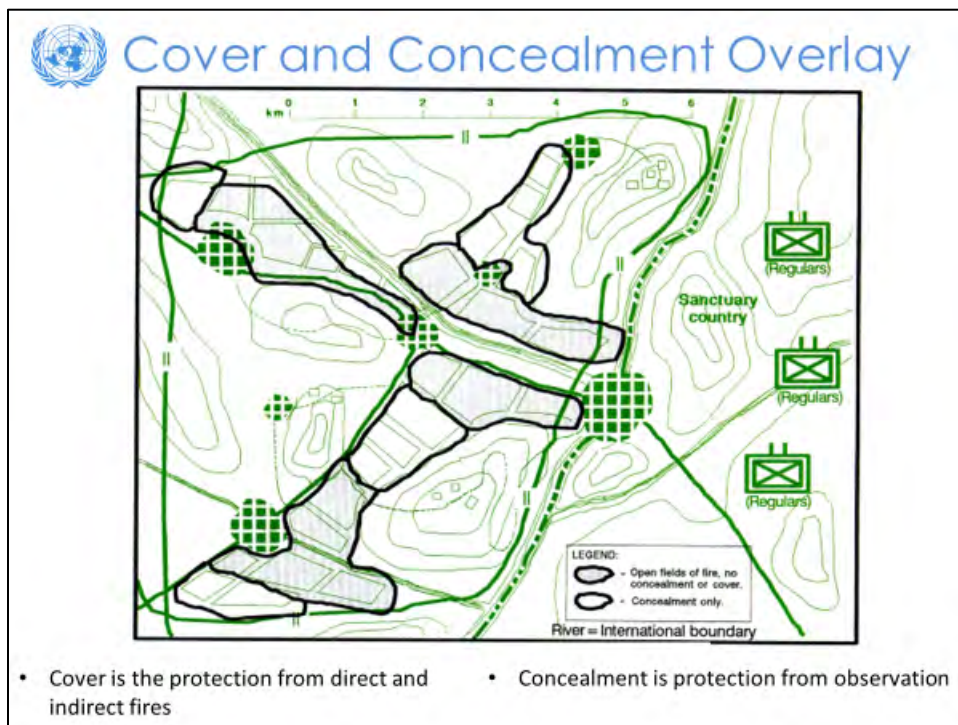
Key Message: The cover and concealment overlay identify areas where UN Forces and (threat) actors can use the terrain for protection from observation or surveillance and from the effects of fires.

The cover and concealment overlays are used to identify areas where UN Forces and (threat) actors can use the terrain to remain concealed and thus protected from observation or surveillance and/or areas where the terrain provides protection from the effects of direct-fire and indirect fire weapon systems.

This is particularly useful when identifying likely routes (avenues of approach/mobility corridors), locations for observation posts/reconnaissance positions, or likely firing positions – depending, of course, on the situation (the type of mission/task and the direction of movement) and the purpose of the likely operation.

Cover and concealment overlays are a critical part of establishing a new Forward Operating Base (FOB).

Interaction. Ask students why a cover and concealment overlay would be important to establishing a FOB? Responses should include the following: areas offering good cover could be used as Threat Actor fire positions, and areas offering good concealment could be used as form up areas or avenues of approach to a UN FOB.

Slide 7

Key Message: An obstacle is any natural or man-made obstruction to disrupt, fix, turn, canalize or block the movement of a group.

An obstacle is any natural or man-made obstruction to disrupt, fix, turn, canalize or block the movement of a UN Force or (opposing) group.

Therefore, the G3 (operations) and G5 (planning) staffs should be supported with information on obstacles within the OE that can impact on own operations and actions. All obstacles hinder movement and, as such, should be represented on a map.

Interaction. Ask the students to list obstacles to a movement that they can think of. Responses include mountains, cliffs, deep rivers and lakes, dense forests, urban areas etc.

Slide 8
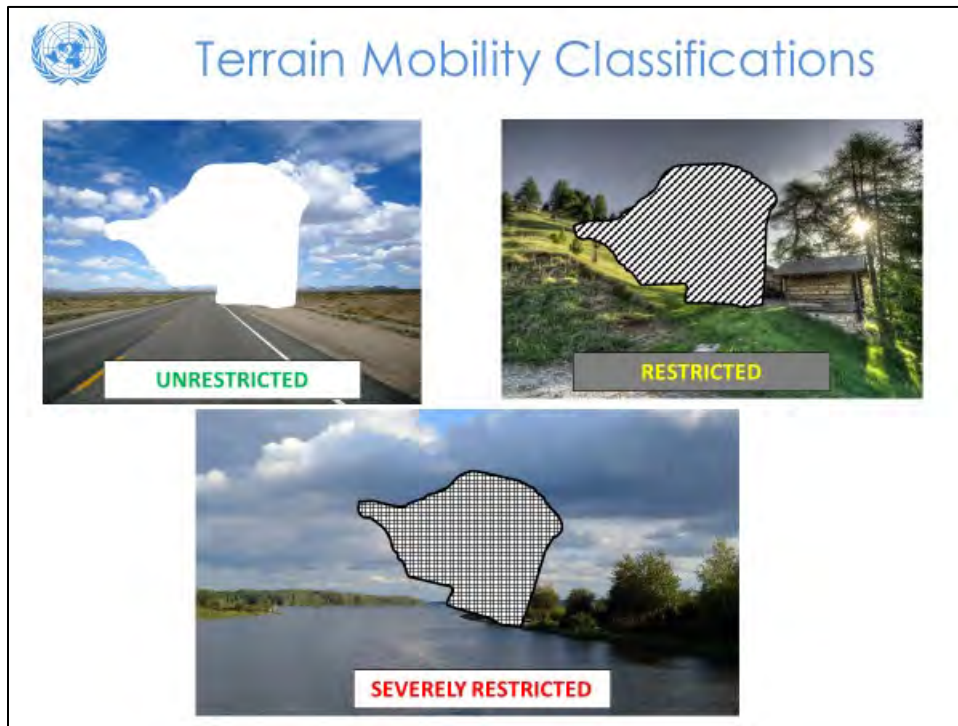
Key Message: Terrain may be classified according to the mobility it offers as having unrestricted, restricted or severely restricted mobility. This is often how obstacles to movement are depicted.

When analysing terrain factors and obstacles together, the mobility offered in terrain can be classified as:

UNRESTRICTED: Terrain over which movements of UN Forces or actor groups (like opposing armed groups or refugees) is not affected by the ground, vegetation, natural and man-made obstacles. Unrestricted terrain is not marked on overlays. – If it's clear on an obstacle overlay, then it's unrestricted terrain.

RESTRICTED: Terrain over which movements of UN Forces or actor groups is only possible at reduced speed, is canalized, or will be possible only with the assistance of additional non-organic assets like improvised bridges. E.g. steep ground, swamps / riverbeds etc. Hatching (without crossed lines) indicates restricted terrain on overlays.

SEVERELY RESTRICTED: Terrain over which movements of UN Forces or actor groups being assessed as impractical, for example, rivers that cannot be crossed/forded, known minefields. Cross-hatching is used to indicate severely restricted terrain on overlays.

Students should remember that the hatching shown will be blue for water obstacles. Remember that terrain that is restricted or severely restricted for motor vehicles may be unrestricted for personnel on foot (infantry).

Slide 9

Key Message: Key terrain is any locality, or area, that gives an advantage to either UN Forces or forces in opposition to or hostile to UN Forces.

In natural terrain characterized by terrain features that restrict mobility, the high ground can be key terrain because it provides good fields of observation (positioning of spotters and forward observers) and fields of fire and can be used to establish and maintain communications. The painting depicts the high ground at Little Round Top, which was key terrain during the Battle of Gettysburg in the American Civil War in 1863.

Key Terrain is denoted as a circled K on a map. In this case, we use the colour purple.

Interaction. Ask students what they think key terrain features are? Responses could include:

- *Hilltops could dominate avenues of approach with observation and fire*

- *In an open or arid environment, a draw – as shown in the photograph to the right – or a wadi can be key terrain because it offers good cover and concealment*

▪ *In urban environments, infrastructure (such as bridges, medical facilities, choke points, intersections, industrial complexes) can be considered key terrain*

Slide 10

Key Message: Vital Ground is terrain of such importance that it must be retained or controlled for the success of the mission.

The vital ground is a terrain feature of such importance that it must be occupied and held to ensure it is free of hostile occupation or use. Control of vital ground is essential to the success of the mission or operation.

The vital ground is denoted using a circled V, as shown. In this case, we use red to highlight it as a vital ground.

Interaction. Ask students what vital ground could be? Responses could include:

▪ *An area or piece of terrain illustrated by the painting from the Battle of Gettysburg. If the Confederate Army (the army of the Southern states) had captured/seized Little Round Top, the Union forces would almost surely have lost the battle*

▪ *An urbanized area or facility as shown by the soldier on patrol in a village*

▪ *In arid, hot environments, water sources and oases could even be considered as 'vital ground',*

Slide 11
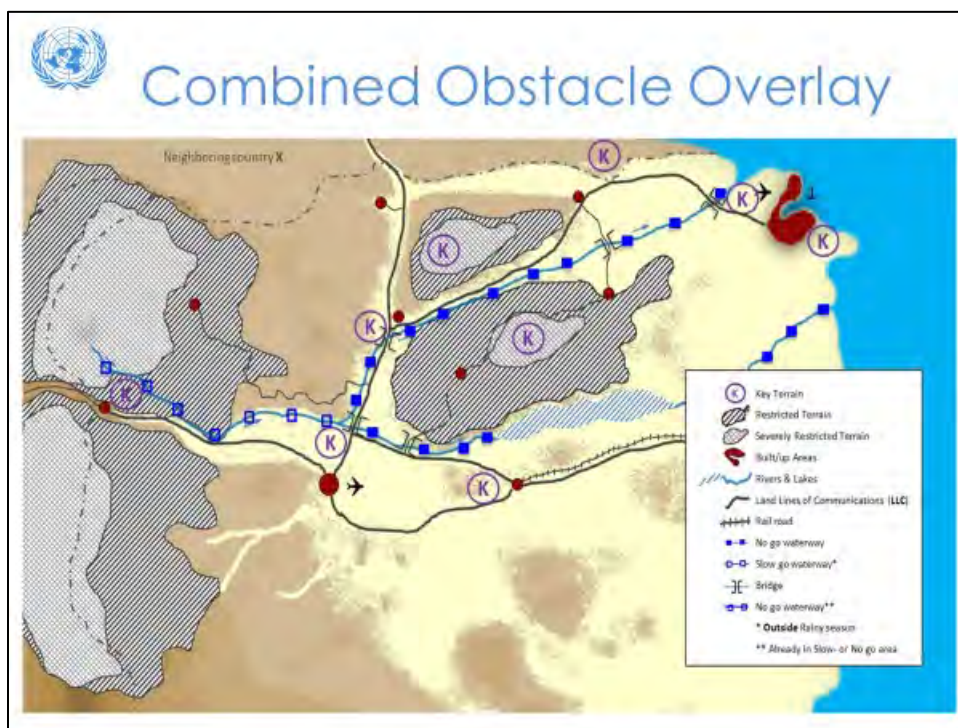
Key Message: The initial result of the terrain analysis is the Combined Obstacle Overlay, which amalgamates the Lines of Communication overlays, vegetation overlay, relief overlay, key terrain overlay, obstacle overlay etc.

The initial result of the terrain analysis is the Combined Obstacle Overlay, which integrates all impediments to mobility, such as built-up areas, slope, soils, vegetation, and hydrology into one overlay. This overlay also allows the UN staff to visualize impediments to mobility for both UN and hostile/threat forces. The overlay depicts areas that impede mobility (severely restricted and restricted areas) and areas where friendly and threat forces can move unimpeded (unrestricted areas).

The combined obstacle overlay provides a basis for identifying ground avenues of approach (AAs) and mobility corridors (MCs), which are shown on the Mobility Corridor Overlay.

The Combined Obstacle Overlay on the slide shows:

- Key facilities.

- Landlines of communication.

- Water lines of communication.

- Obstacles to movement, which incorporates relief, vegetation, and other natural and manmade obstacles. Terrain areas where mobility is restricted or severely restricted.

- Key terrain.

- Vital ground.

Cover and concealment maps are not generally used on such a large-scale map and are better suited to tactical operations in smaller, better-defined AORs, for example during FOB occupation of a defensive/offensive operation.

Slide 12
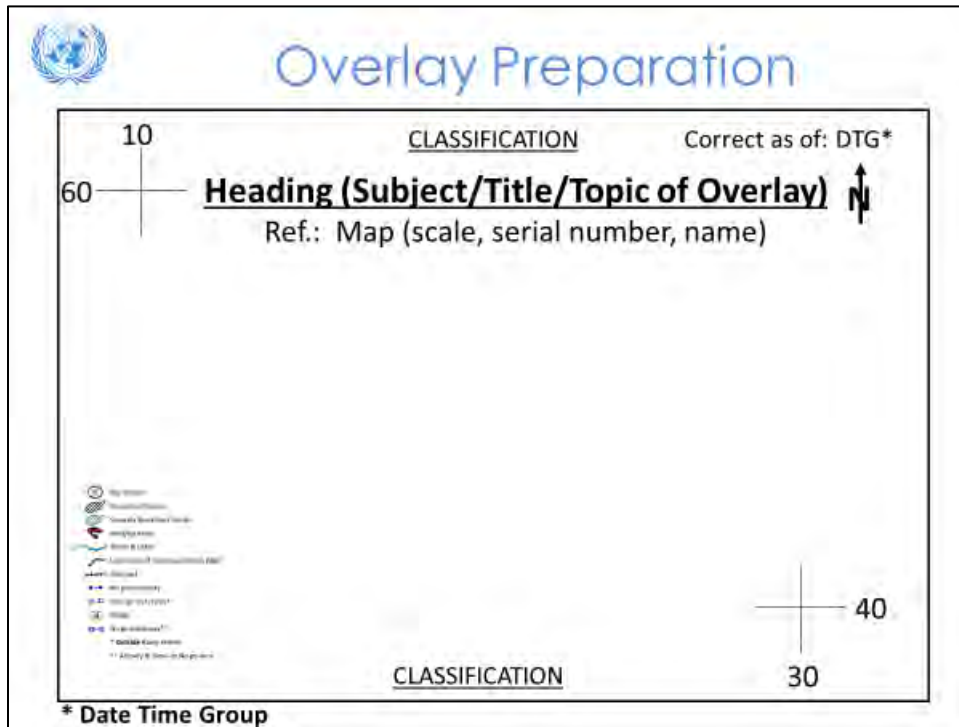
This slide is an example of an overlay and some key areas for preparation.

Slide 13

Learning Activity

- **Situation:**
  - Using the course scenario create a combined obstacle overlay in your AIR.
- **Task:**
  - Study the map and completed overlays and create:
    - Obstacle overlay
    - Key Terrain and Vital Ground overlay
  - Insert factors into the 3-column format (3CF) and make deductions
  - Draw up a list of Information Requirements
- **Time:** 30 minutes (group work and discussion)

FACTOR	DEDUCTION	OUTPUT
Border crossing at Point X is Key Terrain	Threat Actor A needs to be able to pass through BXP to reach consolidation area. UN needs to control/surveil BXP. Local population Traders will need BXP open to meet market expectations.	RFI. Who controls BXP X?

Working in syndicate groups have participants review the slide and then discuss. Have syndicate groups brief the results of their discussions in plenary. Have them use their sector information and mapping to identify obstacles, including key terrain and vital ground.

Create a combined obstacle overlay, paying attention to severely restricted, restricted and unrestricted terrain and mark key terrain and vital ground on an overlay.

On a different overlay, mark areas of cover and concealment on map. Transfer the factors to the 3-column format and make deductions.

Note to Instructor- The emphasis should be on creating the above products. Students may not have enough time to complete the next phase. As part of the output, the instructor should ask students to identify RFIs that patrols or other sources of information can be tasked to confirm.

Slide 14
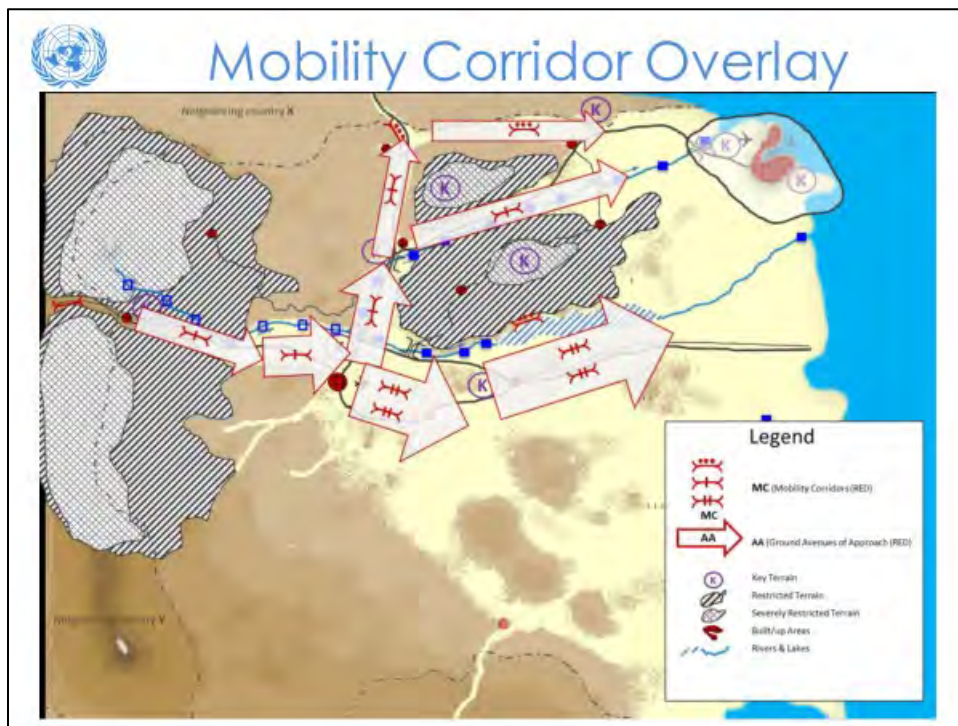
Key Message: The Mobility Corridor Overlay is produced after an analysis of the information contained in the Combined Obstacle Overlay. It is an AOE product used to depict the militarily significant aspects of the OE and identify mobility corridors

Mobility corridors are areas where a force will be canalized due to terrain restrictions. They allow military forces to exploit the principles of mass and speed and are therefore relatively free of obstacles.

The Mobility Corridor Overlay is an AOE product used to depict the militarily significant aspects of the operational environment, such as obstacles restricting military movement, key geography, and military objectives. The Mobility Corridor Overlay is tailored to the mission and is a collaborative effort involving input from the entire UN Force staff.

The staff uses its functional expertise to determine how the terrain will impact on that function. For example, the Communications Officer (S-6) provides input on how the terrain may affect line-of-sight communications for friendly and threat forces.

Specific aspects of the Mobility Corridor Overlay include but are not limited to avenues of approach, key terrain, mobility corridors, natural and man-made obstacles, and terrain mobility classifications. The Mobility Corridor Overlay depicts the terrain according to the mobility classifications, which are severely restricted, restricted, and unrestricted as previously explained. This makes it possible to identify mobility corridors and avenues of approach, as shown on this slide.

As you can see from the legend, in this case, we have created Movement Corridors of platoon, company and battalion size. The type and size of unit designations will depend on the threat actor. For example, if we are dealing with a terrorist actor, they may choose to infiltrate using non-conventional means. This is where the Actor Evaluation, taught later on this course will inform this part of the process.

Interaction. Ask students to point out where a full battalion can move according to this MC overlay and ask why they think this is the case. The response is the southern approach route as it the easiest terrain for a conventional force to move through.

Slide 15

> ### Learning Activity
>
> - **Situation:**
>   - You are still analyzing the terrain and are about to finalize and disseminate the products.
> - **Task:**
>   - Study the map and create the AAO and the MCOO
>   - Insert factors into the 3-column format (3CF) and make deductions
>   - Draw up a list of Information Requirements
> - **Time:** 30 minutes (group work and discussion)
>
> | FACTOR | DEDUCTION | OUTPUT |
> |--------|-----------|--------|
> | Good LLOC moving from east to west, surrounded by plains. | Threat Actor A requires cover and concealment to move and may choose a different AoA. Threat actor B needs to space to move armour and so will likely choose this AoA. | IR. What terrain areas will confirm or deny threat actor COA? |

Working in syndicate groups have participants review the slide and then discuss. Have syndicate groups brief in plenary. Have them use their sector information and mapping to create a Mobility Corridor Overlay. Advise students to use a separate overlay to the Combined Obstacle Overlay. If students, ask why this is the case it is because an MPKI cell will have to use an MC overlay for specific actors in their AO. For example, IDPs may not care about key terrain, vital ground, or covered approaches that are tactically sound, but an adversary would.

Transfer the factors to the 3-column format and make deductions. Have students identified RFIs that patrols or other sources of information can be tasked to confirm.

Note to Instructor- The emphasis should be on creating the above products. Students may not have enough time to complete the next phase. As an output, the instructor should coach the students to help them identify Named Areas of Interest which are terrain areas that should be monitored to confirm or deny a COA.

Slide 16

Key Message: Draw on expertise from engineers and from the GIS (geographic information systems) cells. Use the mnemonics ROBOT and OCOKA to ensure that the main physical terrain factors are covered in the analysis.

You are not alone! (Terrain Analysis is not solely a UN MPKI staff responsibility and effort.) Get support from:

- Engineer staff (G-3); They are experts on bridges, roads, terrain mobility etc.

- GIS cells (both military and civilian) can provide you with mapping (analogue (printed) and/or digital)

For the inventory of the terrain using the mnemonics:

- ROBOT (Routes, Obstacles, Boundaries, Timings)

- OCOKA (Observation and fields of fire, Cover and concealment, Obstacles (manmade and natural), Key terrain and Avenues of approach)

On completion of your overall terrain analysis, these mnemonics can be used to analyse the terrain for a specific mission. This should ensure that you have covered the most important factors in the physical terrain analysis for a specific mission. For example, if you are asked to locate an FOB at a place, consider the terrain in detail using OCOKA. This will ensure you cover the pertinent points for such an operation.

Slide 17
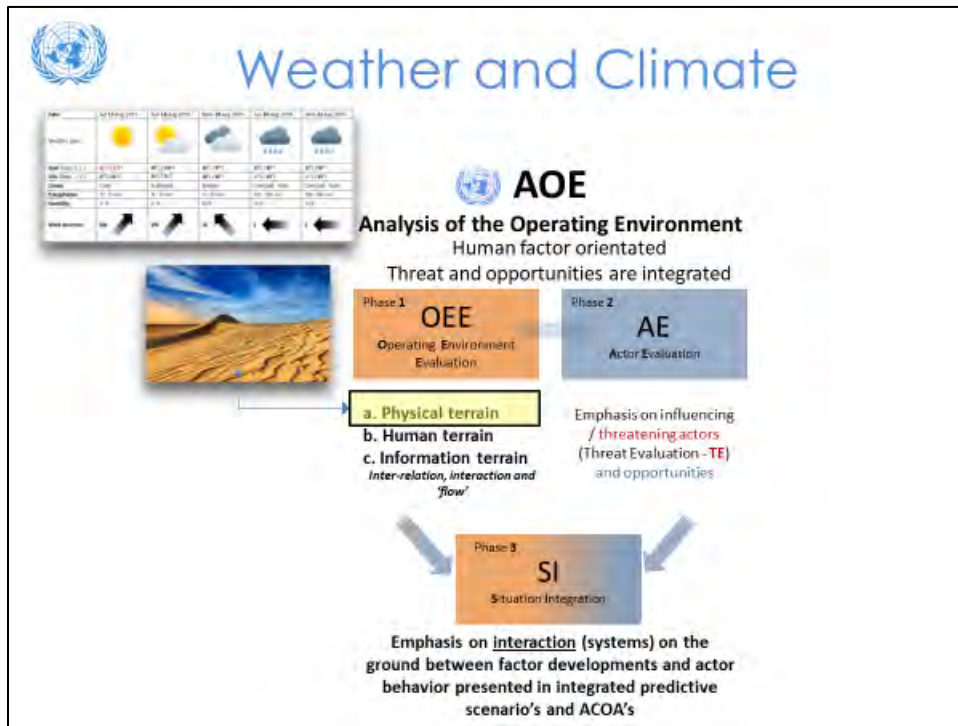
Key Message: Weather and climate affect the physical environment and must, therefore, be considered when evaluating the Operating Environment.
Slide Narrative:

Weather and climate affect the physical environment and must be considered when evaluating the Operating Environment. Therefore, no analysis of the Physical Terrain is complete without analyzing the effects of weather and climate on the various physical terrain factors.

The weather matrix is one of the "Golden Products" that must continuously be updated and assessed based on the most recent weather forecasts during the planning and conduct of UN operations.

Slide 18

Difference Weather and Climate

Weather:
- Short-term state of the atmosphere
- Can vary from time to time or location to location
- Always includes time and location

Climate:
- Long-term pattern of weather
- Long-term = 30 years or more
- Average weather over many years in one specific place

Key Message: The difference between weather and climate: Weather is short term; the climate is general with long term characteristics and short-term changes.

Ask the students what the difference between weather and climate? Responses are below:

- *Weather is the way the atmosphere is behaving, mainly with respect to its effects upon the actors and factors in the terrain*

- *Weather is about the short-term (minutes to weeks) changes in the atmosphere (temperature, humidity, precipitation, cloudiness, brightness (sunshine), visibility, wind, and atmospheric pressure (high- and low-pressure areas), etc.*

- *Climate is the average of weather over time and space, the long-term pattern of weather in a geographical area*

- *An easy way to remember the difference is that climate is what you expect, like a very hot summer, and the weather is what you get, like a hot day with pop-up (pulse) thunderstorms*

- *There are long-term climate changes due to the increase in carbon dioxide levels in the atmosphere, and short-term climate changes due to phenomena like El Niño, volcanic eruptions or other environmental changes in the physical Operating Environment within the Area of Operations or to the Earth's atmosphere, landmasses and oceans.*

- *Both climate and weather should be analysed by the MPKI section.*

- *El Niño is the warm phase of the El Niño – Southern Oscillation (ENSO), which is the cycle of warm and cold sea surface temperatures of the tropical central and eastern Pacific Ocean. It can result in intense storms in some places and droughts in other places.*

Slide 19

Key Message: Weather affects military operations in a number of areas: visibility, wind, precipitation, cloud cover/ceiling, temperature, humidity etc.

Visibility:
A major factor in evaluating visibility is the amount of available light based on weather conditions and illumination (time and amount of sunlight and moonlight).
Other factors affect visibility, too: clouds, temperature, precipitation, sandstorms. Negative effects of poor visibility are the reduced range of sight (both human and sensors) that also complicates command and control, reconnaissance, patrolling and acquisition of information by technical and human means. However, reduced visibility also provides UN Forces – as well as armed groups – with the opportunity of surprise.

Wind:
Wind of enough speed from any direction can reduce operational effectiveness Strong winds limit airborne, rotary-wing, medical evacuation (MEDEVAC) and other aviation activities including unmanned aerial system (UAS) flights. Strong wind can affect the movement or stability of materiel (arms, vehicles, equipment). Blowing sand, dust, rain, or snow can reduce the effectiveness or stability of radars, antennas, communications and other electronic devices.

Precipitation:
Precipitation is any moisture falling from a cloud in frozen or liquid form. Rain, snow, hail, drizzle, sleet, and freezing rain are common types of precipitation. Precipitation affects soil trafficability, visibility, and the functioning of many electro-optical systems. Heavy precipitation can have an effect on sustainment, communications, personnel, military operations, and many civilian activities. Long-lasting precipitation can lead to unwanted and uncontrollable flooding.

Cloud cover and fog:
Cloud cover affects ground operations by limiting illumination and could affect the thermal signature of targets. Heavy cloud cover can degrade many intelligence sensors and target acquisition systems and general aviation operations. Local visibility restrictions, such as fog can have an effect on observation for both UN Forces and other actors, including terrorist armed groups and hostile groups. It may limit or restrict safe aviation operations.

Temperature:
Temperature extremes can reduce the effectiveness of troops and equipment. It can affect the population's living conditions and even survival. Temperatures may affect the timing of operations. For example, extremely high temperatures in a desert environment may require dismounted troops to operate at night or restrict them to operate for a limited period. High temperatures can also affect the lift capability of medium rotary-wing aircraft in high altitudes and elevations. High temperatures also can increase fuel consumption in vehicles, cause overheating, and lower electrical output. Drought can cause famine and lack of drinking water, and thus threaten the survival of vulnerable civilian population groups.

Hot, dry weather might force friendly, population and opponent forces to consider water sources as key terrain. UN operations and mandated tasks (core business and support to Peacebuilding activities, support roles and cross-cutting thematic tasks) are highly influenced by weather and climate in positive or negative ways.

Slide 20

Key Message: The Weather Effects Matrix is one of the "Golden Products".

The Weather Effects Matrix is one of the "Golden Products", as the information contained in it has a direct impact on operations.

It is constructed by placing the date and weather forecast across the top. All pertinent detail should be included: rainfall, temperature, cloud cover, sunrise, sunset, moonrise, illumination at night, and humidity at a minimum.

The side is a close-up of the Weather Effects Matrix. Effects can be weighed against any factor. In this case, we have chosen personnel, material, unmanned aerial (or aircraft) systems (UAS), air transport (fixed and rotary wing), movement, communications etc.

The colour-coding used is:

- Grey = non-assessable or nothing special to report (NSTR)
- Green = favorable
- Yellow (amber) = marginal (some impact, which is described in the box)
- Red = unfavourable (adverse impact, which is described in the box)

Interactive. *Ask the class how the weather could impact a UAS, radio communications, movement. Then ask students how the effects of the weather might have a consequence for threat actor COA selection? Responses here include that the threat actor may choose to wait until 28 and 29 Nov to act, considering UN visibility will be degraded.*

Slide 21

Divide students into syndicate groups. Ask them to use the weather matrix supplied to define the impact on UN forces. Ensure students use the 3-column format to define so what from a threat actor perspective. Hand out a weather matric with varying weather for 5 days. If laptops are available, this can be given to them electronically.

Slide 22

Summary

It is important that you understand these take away messages in this lesson.

- PT analysis is crucial to OEE as it is the basis for analysis of the Human and Information Terrains

- Terrain analysis overlays are based on accurate mapping and it is essential to MPKI and the UN MDMP

- Climate and weather affect PT

- COAs for the UN and mandate spoilers are determined by PT

Lesson
3.5d

AOE- Human Terrain (HT) Analysis

The Lesson

Starting the Lesson

.

Slide 1
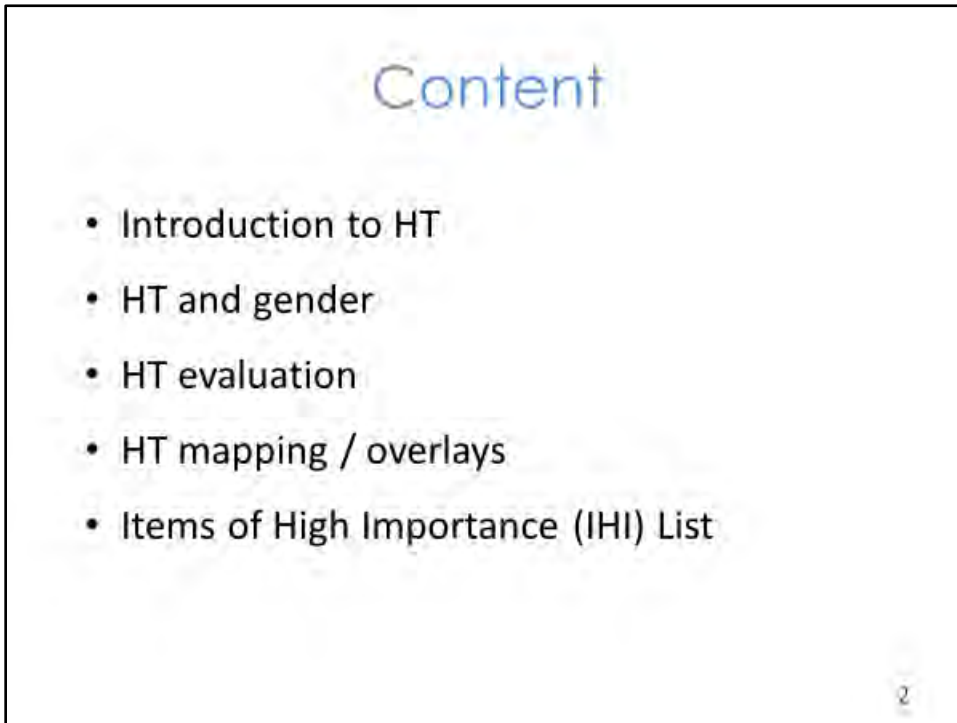
Lesson 3.5d
Human Terrain (HT)
Analysis

Human Terrain analysis is a vital component of the Analysis of the Operating Environment.

It is the point at which understanding is developed about the local population in the Area of Operations, and how the population interacts with and is affected by the characteristics of the physical and information terrain.

Slide 2

These are the topics we will cover during this lesson

Slide 3

Let's review the learning outcomes for the lesson. By the end of this lesson, you will be able to conduct these learning outcomes.

Slide 4
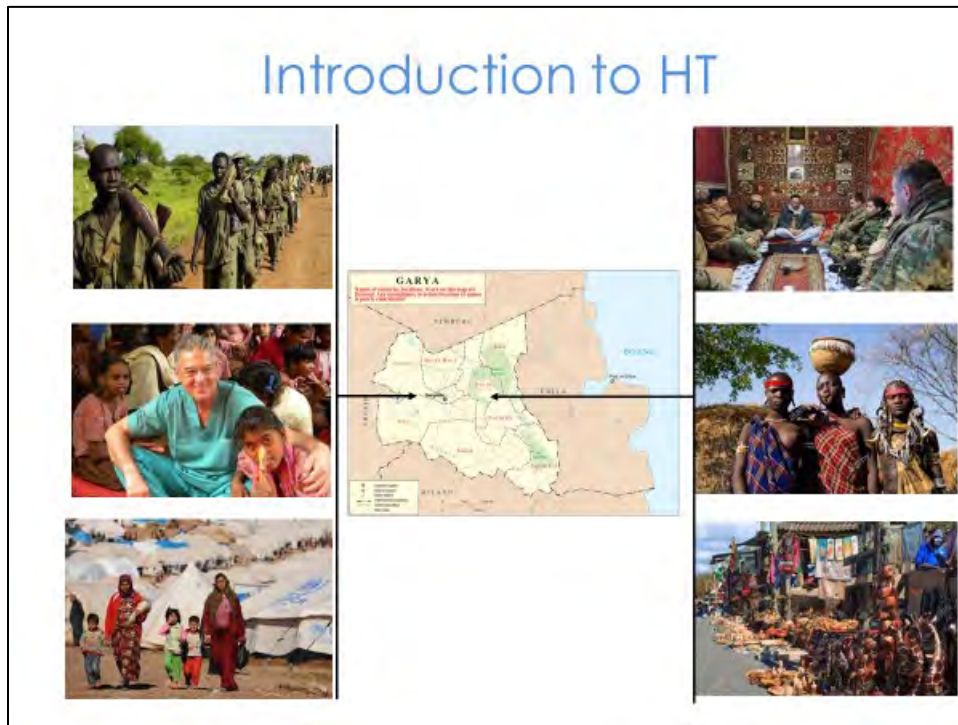
The Human Terrain encompasses all elements of the population living or operating in the Area of Peacekeeping Intelligence Responsibility. The Intelligence officer must understand the role and presence of different population groups within the APIR and how they may affect and be affected by UN operations.

Interaction. Ask the class to volunteer the various categories of human terrain that the Intelligence officer should consider. The types of responses that are sought are as follows:

- *Threat groups*

- *Local political groups*

- *Religious groups*

- *Vulnerable sections of the population such as women, children, disabled, ethnic minorities*

- *Refugees and IDPs*

- *Tribal groups*

- *Ethnic groups*

- *Sections of the population that are pro- or anti-UN*

- *Compliant armed groups*

- *Host nation security forces*
- *Non-compliant armed groups*
- *Key leaders or influencers (formal or informal) of all the above*

Slide 5

Key Message. The human terrain is central to UN mission mandates as humans represent both the causes of the conflict and the victims of the conflict.

The human terrain is always central to threat actor activity as it forms the membership of the threat actors, it offers the threat actor support or facilitates its actions, or it resists the presence of the threat actors. Similarly, sectors of the human terrain are often the target of threat actor activity.

Interaction. Ask the students for an example of an area where they have worked in the past or that they have studied where one section of the population have been supportive or members of a threat group, and another section of the population was targeted by that group. Potential examples you could offer are:

- *Serbian armed groups targeting Muslims, and vice versa, in Bosnia during the Balkan wars*

- *Selaka groups targeting non-Muslim groups in CAR*

- *Anti Belaka groups targeting Muslims in CAR*

- *Ethnically motivated violence in central Mali (Fulani versus Dogo)*

Slide 6
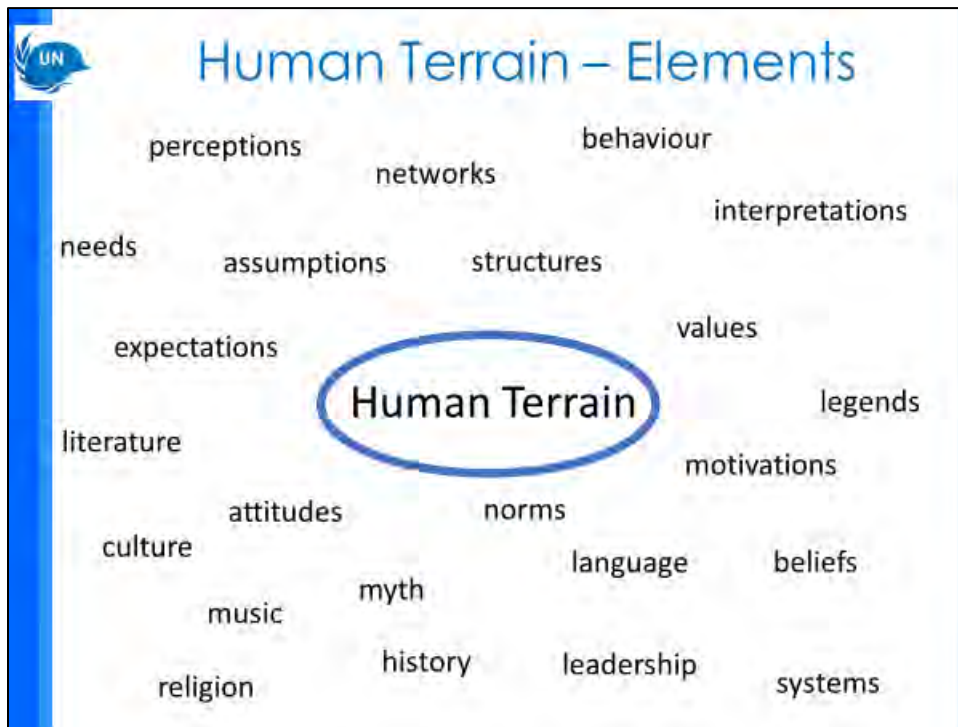
Key Message: Human Terrain is complex and involves many variables, both tangible and intangible, that contribute to our understanding of the Operating Environment.

Human Terrain is critical as a conflict is essentially a human endeavour. Understanding the human dimensions of conflict involves understanding the motivations, aspirations, grievances, perceptions and behaviours of the local population.

The slide shows some of the factors we should look at when analysing the Human Terrain. Some of these are visible, such as behaviours, but to make comprehensive and predictive assessments, we must look beyond the visible to understand factors such as the values and assumptions that drive visible behaviours.

Interaction. Ask the class whether these factors can be collected as part of the acquisition plan. What might be some sources of this data? Within the Mission / outside the Mission?

UN personnel are usually already at a disadvantage compared to hostile actors when it comes to an understanding of the Human Terrain, as these actors tend to come from and live within the local population. They may speak the same language or come from the same ethnic background, and therefore may be more effective in understanding local dynamics, communicating a message, and influencing the population.

In order to conduct Human Terrain analysis, MPKI staff must continue to examine their own biases about how the local society is structured – it may be very different from their own.

Interaction. Ask the class what kind of bias can affect assessments about local actors. Possible Answer to facilitate discussions:

- *Cultural bias, which involves a misunderstanding or lack of comprehension of why another culture conducts itself in the manner it does can be a factor. As a result, analysis in some fields can be hampered simply by a lack of relevant knowledge or experience. To overcome cultural bias, the analyst should try to develop an understanding or empathy with the cultural group being assessed.*

- *'Mirror-imaging' bias should also be considered as part of human terrain evaluation. This occurs where the analyst projects their assumptions and behaviours onto a local actor if the local actor responds to a situation in the same way the analyst would.?*

Slide 7
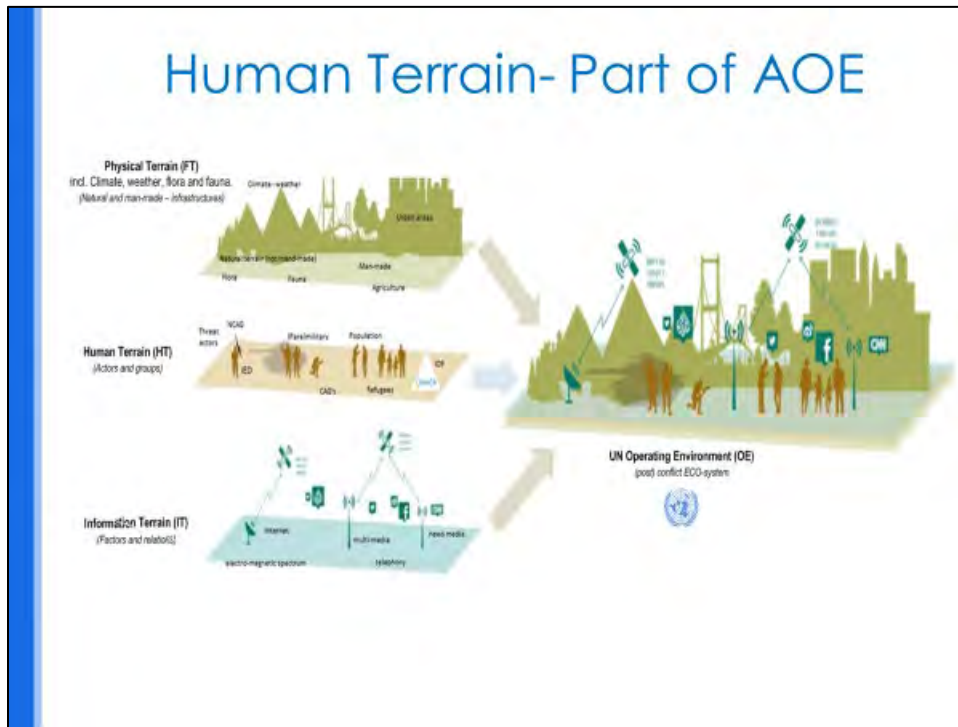
Human Terrain analysis is an essential component of the Operating Environment Evaluation (OEE). This is phase one of the Analysis of the Operating Environment (AOE).

It is important to consider the physical, human, information terrain, and the interaction of these elements with each other as part of a wider system.

If any part of this system changes, all other elements are also likely to be subject to change. It is the role of an intelligence officer to understand this and to be able to alter assessments accordingly.

For example, if we consider a refugee camp location, it interacts with the physical terrain in that it may be located close to an urban area, water source, or far from the axis of advance of an armed group.

The physical terrain area, therefore, informs where the refugee camp is located. This type of awareness can only be generated by combining our understanding of the physical and human terrain. Similarly, the weather also has significant impacts on the human terrain. In the first instance, adverse weather affects the physical terrain by, for example, raising the water level of rivers, which can make them less easy to cross for UN forces and for threat groups.

Slide 8
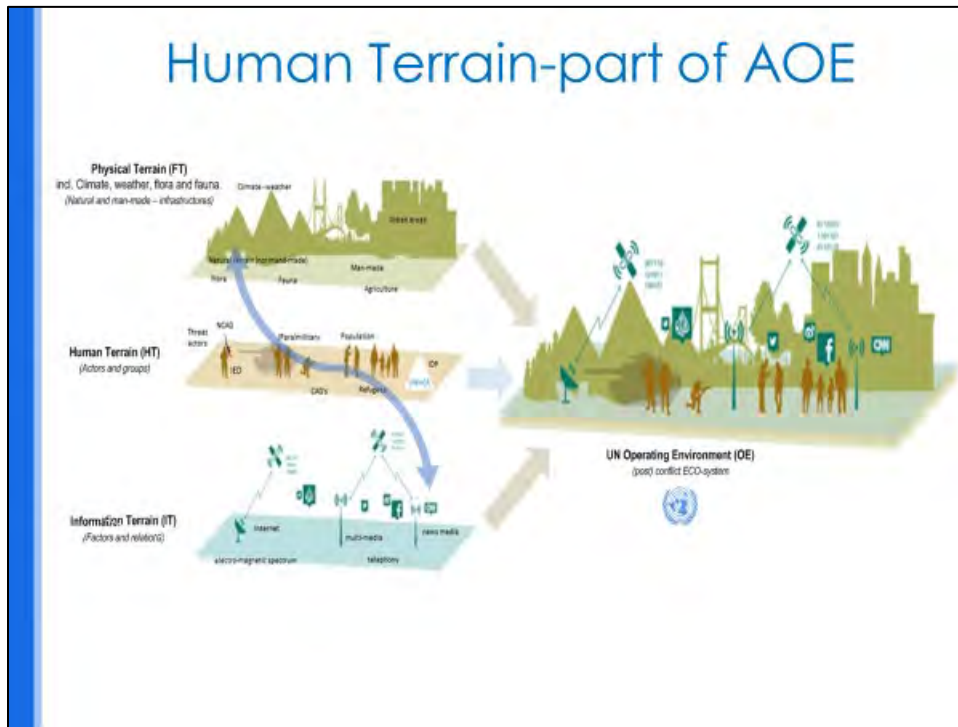
Key Message. Human terrain analysis is central to the evaluation of the operating environment.

This slide aims to capture the relationships between the three types of terrain. The Physical terrain influences where the human terrain lives and the information terrain influences how the human terrain communicates and interacts. Therefore, from a UN perspective, the human terrain is central to Step One of the Analysis of the Operating Environment. It is important that you understand that the human terrain is affected by every change to the physical and information terrain, and weather.

Interaction. Ask the class what physical and information terrain factors would influence where farmers would choose to locate, and what this means for the UN. The responses we are looking for include the following:
- *Close to arable land*
- *Away from obstacles to farming such as mountains, marshes, and very difficult physical terrain*
- *Close to water sources*
- *Close to lines of communication such as roads*
- *Areas with easy access to markets*
- *Close to urban centres*
- *The potential list is endless*

Slide 9
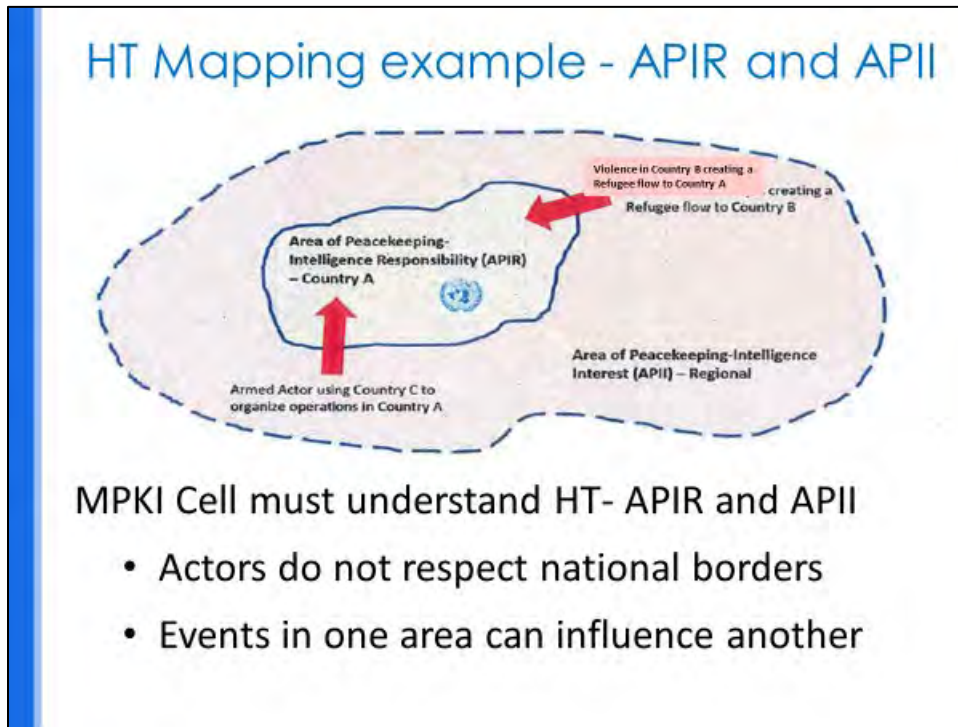
Key message: It is important that the Intelligence section is aware of the Human Terrain in its Area of Peacekeeping-Intelligence Interest as well as in its Area of Peacekeeping-Intelligence Responsibility. This will likely require significant liaison with other sectors, Battalions or with the Force Intelligence sections. If you ignore the human terrain in your APII, then you ignore key information that is relevant to your intelligence section.

This map demonstrates the impact that the human terrain in the APII can have on the human terrain in the APIR. For example, if there is violence against an ethnic group in the APII, it is likely that the civilian population will move towards areas where their ethnic group lives, far away from the violence. This could result in refugee or IDP flows to your AOR. It is therefore vitally important to understand the tribal, ethnic and religious breakdown of your APII. Such patterns of migration have been visible throughout history.

Another example would be the extent of support an armed actor enjoys in your APII. This could have an impact on its capabilities in your APIR. If your intelligence cell knows that armed group A has the support of the population in country C. This knowledge will enhance your understanding of armed group A's military capability. It may reorganize and consolidate in country C, and it may have its leadership there, it may raise money, recruit fighters and train there. Therefore, even though the area in which it operates in your APIR may not be supportive of the group, this may not matter if the group has support close at hand.

Slide 10

Key Message. Human Terrain Analysis is the most important component in the Evaluation of the Operating Environment.

It is important for the following reasons:

- Understanding the Human Terrain means understanding the risks and threats associated with it

- Sections of the Human Terrain are central to the activity of threat actors

- Sections of the Human Terrain form vulnerable communities for POC tasks. This is critical for UN mandate implementation

- Understanding the human terrain can lead to the identification of Items of High Importance. For example, we can identify key leaders and things (resources and assets) that are important to groups

- We can identify inter-ethnic/religious boundaries which can help identify potential violence hotspots

- It is critical for understanding the capability, intent, and opportunities of threat or other armed actors. For example, the human terrain will form the membership of threat actors, it will support the threat actor with resources (financial, logistics, human), and will often be the operational centres of gravity of such groups, supplying these threat actors with the moral and physical will to fight on. If the UN is to defeat or deter such groups from acting understanding the supportive human terrain is vital

The actor Evaluation methodology will be delivered later in the lecture series.

Slide 11

Key message: Gender factors are an important part of human terrain, and MPKI staff must understand the different roles that women and men, girls and boys play in the host nation society.

Interaction.

Start with the example below to get the students thinking about the different roles women play in conflict (not just victims but supporters, facilitators, perpetrators). How an analyst's biases may affect their assessments and how gender factors could have significant security outcomes (lack of screening, use of women to evade security).

Ask the class if anybody knows who the woman in the picture is. Can we make any initial judgments about her? The instructor may prompt that the picture is taken in Somalia, does that provide any additional information?

It is likely that the students will talk about women requiring protection, perhaps mentioning religious factors (attire), presence of young girls, or the fact that the women appear to be sight-impaired.

You should then explain that the woman was known as Basira Abdi Mohamed and that on 24 July 2019 she entered a meeting in Mogadishu and detonated a suicide IED, killing 8 people including the Mayor of Mogadishu. Her accomplice

was also a female, and they had evaded security as there was reportedly no female staff present to screen them at the compound.

Al-Shabaab claimed the attack and alleged that the target was the Special Representative of the Secretary-General (SRSG) of the UN Mission in Somalia (UNSOM), who had been at the compound several hours earlier for a meeting. What are the implications for the UN?

Show this article at some point to reinforce your learning objective.

https://www.voanews.com/africa/mogadishu-mayor-targeted-female-bomber

Slide 12

Key Message: Students understand the definition of gender, how it varies between cultures and contexts, and how it is a vital part of the Human Terrain.

In order to look at gender as a part of the Human Terrain, we must first understand what it is. The UN definition of "gender" refers to the social attributes, opportunities and relationships associated with being male or female. It defines power relations in society and determines what is expected, allowed and valued in a woman or a man in each context. Gender is socially-constructed and is learned – this means it can change based on different contexts and different times. What was standard in your area of operations five or ten years ago may no longer be valid.

Conflict itself can change how a country views gender – for example, as the conflict drags on armed groups may be more willing to recruit females into their ranks; or conflict can drastically increase the number of female-led households, which impacts on the local society and economy.

Slide 13

Conflict affects different parts of society in different ways. The conflict has different impacts on women and men.   For example, women more likely to be subjected to conflict-related sexual violence - But men and boys are also victims, as occurred in Libya where male rape was used as a tactic of domination and humiliation. More boys are recruited as child soldiers - but girls are also recruited (for example, in South Sudan); more males die or are injured by landmines; more girls become child brides.

References:
https://assets.publishing.service.gov.uk/media/59844e0c40f0b61e4b00005c/149
-the-impact-of-mines-and-explosive-remnants-of-war-on-gender-
groups__1_.pdf)

https://data.unicef.org/topic/child-protection/child-marriage

https://www.theguardian.com/world/2017/nov/03/revealed-male-used-
systematically-in-libya-as-instrument-of-war

Slide 14

The Santos Cruz report identified that one of the keys to preventing casualties was better tactical intelligence, gained through human sources. The female members of the population may have access to different kinds of information than the male population, so it is essential that the UN is leveraging that resource. In order to do so, the use of female peacekeepers and mixed-gender teams may be beneficial in reaching a larger proportion of the community.

Slide 15

HT: Gender – Early Warning

MPKI must be <u>predictive</u>; gender indicators provide early warning:

- Absence of women / children / men
- Girls not attending school
- Escalation of Conflict-Related Sexual Violence
  - Ill-discipline / lack of C2
  - Attempt to undermine social cohesion
  - Attempt to alter ethnic balance

Relies on understanding of HT / patterns

Key Message: We know that one of the requirements of MPKI is to be predictive, and we spoke about how important it is to define and monitor indicators to identify changes in the operational environment. Gender indicators can be a good source of information about changes happening in the local population. They can provide early warning to identify the presence of an armed group, identify vulnerable social groups and identify high-risk areas.

The absence of women and children in a town may be an indicator of a perceived threat to that population, or on the other hand, as has been seen in South Sudan, the absence of men can indicate a threat as they hide to avoid being killed or forcefully recruited.

An escalation of conflict-related sexual violence (CRSV) is another key indicator, particularly if perpetrated by members of a government security force or government-affiliated militia. This can be an indicator of ill-discipline or lack of C2 within these forces, be part of an attempt to undermine social cohesion within the local population or be aimed at subjugating certain ethnic groups or altering the ethnic balance. UN Women has published a set of CRSV Early Warning Indicators, which are published in the MPKI Handbook and are available in the student syndicate folders.

It is important to note that gender factors cannot be considered in isolation and must be informed by the broader analysis of the Human Terrain. The analyst must have a thorough understanding of the pattern of life, or what is normal behaviour for women and men, in the host community.

Slide 16

HT: Gender – Developing IRs

- Does ethnic group A support peace process
  - Do ethnic group A females support peace process
- Does Village X support Armed Group Y
  - Do Village X females support Armed Group Y
- Role women play in recruitment
- Role women play in facilitation
- Role women play in radicalization
- Women in leadership roles- Formal / informal
- Women have access to conflict-resolution mechanisms?
- Women have access to humanitarian assistance?

Key message: There are some key questions that can help ensure gender issues are captured as part of the Human Terrain analysis.

For every question, an intelligence analyst asks about the human terrain, ask a follow-up question on gender. If the broader question is: does ethnic group A supports the peace process, the follow-up question is "do the females of ethnic group A support the peace process? This method ensures the analyst is capturing the views and attitudes of different segments of society.

Similarly, the analyst should ask what role women play as part of armed groups. Do they play a role in recruitment, facilitation, radicalization or deradicalization? For example, one study showed that in an online social network of Islamic State supporters, not only were around 40% of participants women, but the women in the group were better connected.

Analysts should consider whether women perform leadership roles within the community, noting that their influence may be through formal or informal positions.

Analysts should also ask whether women have equal access to customary conflict-resolution mechanisms – critical in many UN environments to resolving issues over land, animal rustling, petty crime etc. – and whether women have access to humanitarian assistance or development opportunities. For example, if women don't have access to

the formal economy, then they may represent a particularly vulnerable segment of the population.

Another example is where women are required to walk long distances to collect water or firewood. If there are threat actors in the area, the Force may be involved in providing escort to the women. This is the case in the United Nations Mission in South Sudan, where military forces are involved in patrols to protect women from IDP camps who travel to collect firewood.

All these questions will allow the MPKI analyst to develop a better understanding of the Human Terrain – not just half of it.

☞ *Note to Instructor:*
You may wish to refer to an earlier lecture on Link Analysis during which connectedness within a group was discussed.
 [Reference: https://theconversation.com/womens-key-role-in-islamic-state-networks-explained-62090] women-key-role-in-Islamic-state-networks-explained-62090

Slide 17

There are several ways to ensure gender factors are considered as part of acquisition and analysis.

- The Gender Adviser or Gender Focal Point should be included in the MPKI support to operational planning

- Wherever possible the MPKI cell should encourage mixed-gender teams, and task engagement platoons if they exist in the Mission

- MPKI staff should ensure specific gender questions are included in the patrol briefing and debriefing formats, and that gender-disaggregated data is acquired

- You should be aware of what is 'normal' for gender relations in your operating environment – define indicators of change and report on them

- As much as possible, share information with gender advisers, JMACs, Human Rights, Women and Child Protection Advisers etc. These cells can all have valuable information about issues such as CRSV, forced recruitment, female community leaders etc.

Slide 18
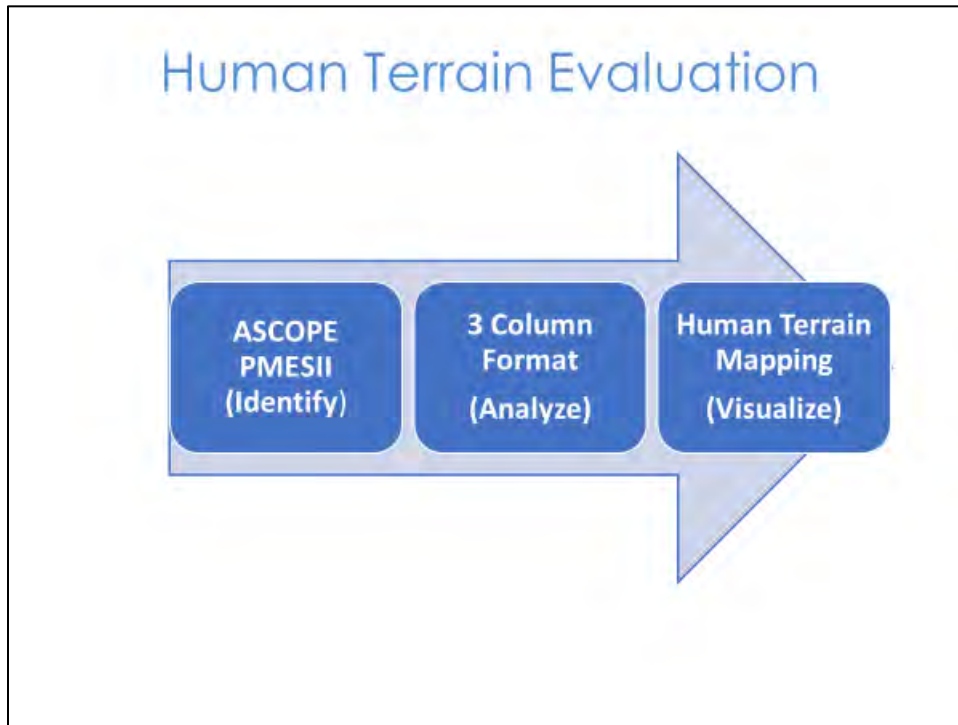
Key Message. These are the three methodologies we use to identify and analyse factors and actors. These three methodologies are ASCOPE-PMESII, the three-column format, and Human Terrain Mapping. We should understand that this is a process, not a menu from which to choose and that this is the structure and order they must associate with the process: ASCOPE-PMESI (identify); 3 column format (analyse); and mapping (visualize).

It is advisable to commence your evaluation of the Human Terrain with ASCOPE PMESII. This will ensure that you identify all known relevant factors and actors in the human terrain landscape. ASCOPE PMESII will also highlight what you do NOT know, thereby adding to your Information Acquisition Plan. ASCOPE PMESII was subject in a previous lecture [NOTE or future lecture].

Next, it is important to engage in the three-column format. This will allow you to make deductions for each identified factor and actor. This comprises the value-add or so-what.

Finally, it is important to recognize that the human brain does not deal well with pages and pages of information, no matter how well it is stored. It is much better to depict it visually on maps. We will do this using a series of overlays, taking what is known, combined with what is analyse d and situating it on a map.

We will move through these processes in the next few slides.

Slide 19

Key Message. ASCOPE-PMESII identifies the various known factors and actors. This process will also identify where the UN has information or intelligence gaps. This part of the process is the identification component, and the first step of the process.

Interaction. Ask students to demonstrate how the matrix comes together to identify a political area, a social area, and a military capability. Have them give examples of a military area, a social area, and a communications capability.
Ask what happens if we have too little information on an area. The response, in this case, is that it becomes an Information Condition. For example, if we do not know what Political personalities live in your area of intelligence responsibility, it is necessary to find out where key leaders live. The same is true for economic, military, and social key leaders.

We complete the ASCOPE PMESII table using the basic and current intelligence available to the intelligence section. Any gaps are identified and become information requirements. What is known become factors in the case of things and actors in the case of persons or groups? These factors and actors are listed and brought forward to the next step for analysis.

However, it is important to note that the ASCOPE PMESII process is ongoing and does not cease just because we have moved on to the analysis part of the process.

Ideally, your information requirements manager and acquisition manager will ensure that the ASCOPE PMESII table continues to grow and continues to inform the analytical process throughout the duration of the intelligence cell's deployment period.

Slide 20

Key Message. The factors and actors identified during the ASCOPE PMESII process are then evaluated using the three-column format.

Interaction. Ask students to confirm knowledge of the three-column analytical framework:

- *What is an actor? The response we are seeking is that any living person in the case of a key leader (political, economic, military etc.), or any group of persons bound by similar ideological, religious, political views, or tribal, ethnic affiliation in the case of a group. Relevant actors are also economic actors*

- *What is a factor? Any non-living thing that is closely related to the human terrain. There is spillover to the physical terrain in this case. Examples could include political, military, police HQs, marketplaces, areas of importance to the local population such as churches, graveyards etc.*

- *Should we just consider armed actors? The answer here is no. The UN Intel section needs to evaluate all elements of society, including those that are unarmed*

- *What is a deduction? The answer here that we are looking for is that it is the so-what? It is what makes the actor or factor relevant to the UN*

- *What is the output? The answer here is that outputs guide further action. An output could be an Information Requirement, a tasking, a risk, a constraint, a limitation, planning guidance, or Items of High Importance (this will be discussed in greater detail later in this lecture)*

Ask the student what action they would take in the event of creating an IR. The required response is that it would be added to the Acquisition Plan or sent to partners in the form of an RFI.

Taking each factor or actor commencing with the P of PMESII before moving on through the acronym, we list the key actors and factors. For each actor of factor listed, we must make as many relevant deductions as relating to the UN mission mandate.

For example, if we choose a political leader of political party A as an actor in the first column, we could make the following deductions: the area where the political actor lives may be an area supportive of political party A, though this will have to be confirmed and could become an Information Requirement in the output (third) column; if political party A is pro-government then the area could be permissive for UN operations. Again, this will have to be confirmed and could be another IR as an output.

Another example could be that tribal area B meets tribal area C in one area. A deduction here could be that this could be an inter-ethnic hotspot if there is a history of violence between the two tribes, or one area could be pro-UN, and anther could be anti-UN. An output could be risk mitigation measures are required in the anti-UN area.

Or for example, if group Z was in Area A, then a reasonable deduction could be that they have recruited, raised funds or they have supporters in that area. Outputs might include the following information requirements: How does group Z raise money? Does it own businesses in the area? What sections of the population area are supportive of it? Where does it recruit and train? Again, the list of information requirements arising could be very long.

When this process is complete, the intelligence section will have completed a short intelligence estimate as it relates to the human terrain. It is then important to record, collate and list everything listed in the second and third columns. These observations will inform further analysis, further information acquisition, planning guidance and, together with the operations section, the tasking of information acquisition assets.

Slide 21

Interaction. This in-class exercise is designed to reinforce student understanding of how to use the 3 Column Format to analyse factors/actors in the Human Terrain. Break the students into 4 groups and assign each of them a factor (left-hand column). Students should spend 10 minutes completing their deductions and outputs before briefing the class.

Slide 22

This slide is a partial 'instructor solution' to display while students brief their results, to trigger additional discussion and/or to assist where students haven't grasped the concept.

Slide 23

Our brains do not deal well with large volumes of information that is held on databases. If such information is not presented in a visual fashion, then some of its meaning will be lost. Therefore, it is necessary to map the human terrain in the same way as we map physical terrain, using overlays. This can be done digitally or by hand, but ideally, it will be done using both approaches.

Slide 24

Key Message. Our brains do not deal well with large volumes of information that is held on databases. If such information is not presented in a visual fashion, then some of its meaning will be lost. Therefore, it is necessary to map the human terrain in the same way as we map physical terrain, using overlays. This can be done digitally or by hand, but ideally, it will be done using both approaches.

Human terrain mapping is not complicated; however, the key is ensuring that relevant data is available. The steps involved are as follows:

- Take a map of our Area of Peacekeeping-Intelligence Responsibility

- Using the information on our three-column format process, and from the ASCOPE PMESII document and map it onto several different overlays

- The information should be shown with a clear legend, and different layers must stand out to ensure that it is intuitive

Interaction. Ask students / the class how they might represent an area inhabited by ethnic group A and ethnic group B, or religious group C and religious group D. The ideal response would be that these areas would be represented by different colours or different patterns.

We must remember that whatever we use to represent human groups, areas, or key leaders must be distinct and simple to recognize, or there is no point in taking the time.

The concept here is that the information jumps out at the intelligence officer and helps to bridge the cognitive gap between what you can read and what you can see.

There are many types of overlays, and the UN Intelligence section can use as many as are helpful and relevant to the intelligence process, including:

- Ethnic laydown
- Tribal laydown
- Areas in which armed groups predominate
- Areas that are permissive or non-permissive for UN operations
- Areas that are loyal to a political party and political affiliation
- Religious laydown
- Demographic laydown
- Rich areas and poor areas
- Pro-government and anti-government areas
- Host nation force lay down
- Areas of high and low employment
- Vulnerable population group areas such as refugee and IDP camps
- Schools and hospitals are key to POC; armed groups often target these areas for recruiting or leveraging medical care
- Areas of Mining (often illegal and criminal)

Patterns will be noted. For example, anti-government areas might coincide with areas that are not permissive to the UN, or areas where threat groups predominate. This is all useful for planning.

Slide 25

Overlays should be developed for maximum clarity. The detail should jump out at the observer for it to add any value. Overlays should use different colours to achieve clarity and distinction. For example, different ethnic groups should be represented using different colours. The only limit is your imagination and what works. However, every overlay must have:

- The name of the author so that observers can clarify detail with him/her, as required

- The DTG of when the overlay was drafted. This will allow observers to understand how current or up to date the overlay is

- At least 3 co-ord points. This will allow anyone to place the overlay over the map in the correct place

- The direction of North

- The overlay must be labelled to show what it is designed to show

- It must have a very simple and clear legend

- And it must NOT obscure map detail

Slide 26
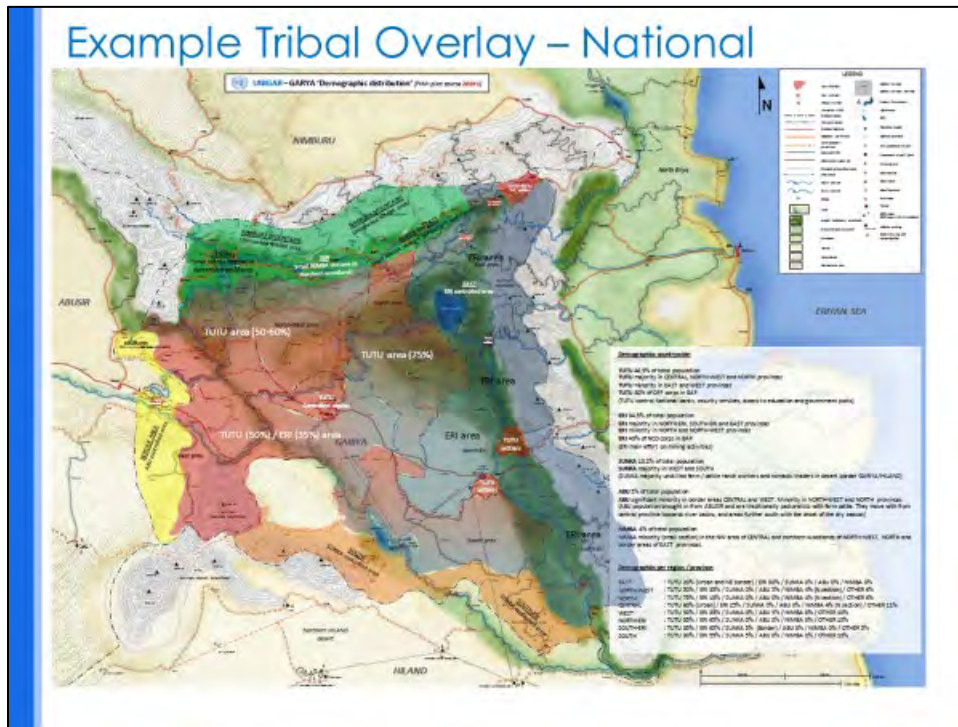
This is an example of a country-wide representation of tribal areas. It is important to note that at this scale, there will rarely be areas that are 100% populated by one specific ethnic group. It will be far more nuanced than this.

In this case, rather than labelling an area Ethnic group A and representing this with a red colour, one might assign different shades of red for areas with higher and lower concentrations of Ethnic group A.

Such an approach can be seen on the map where the colour red is assigned to the Tutu ethnic group. The areas of clearer red have a higher proportion of Tutus, and areas on its periphery are darker and are sometimes mixed with other colours.

This is not a science, particularly at this scale. However, at Sector level and lower, such things must be represented in a more granular fashion. Again, the key points here are that a tribal overlay or those like it are vital as it develops understanding.

Slide 27
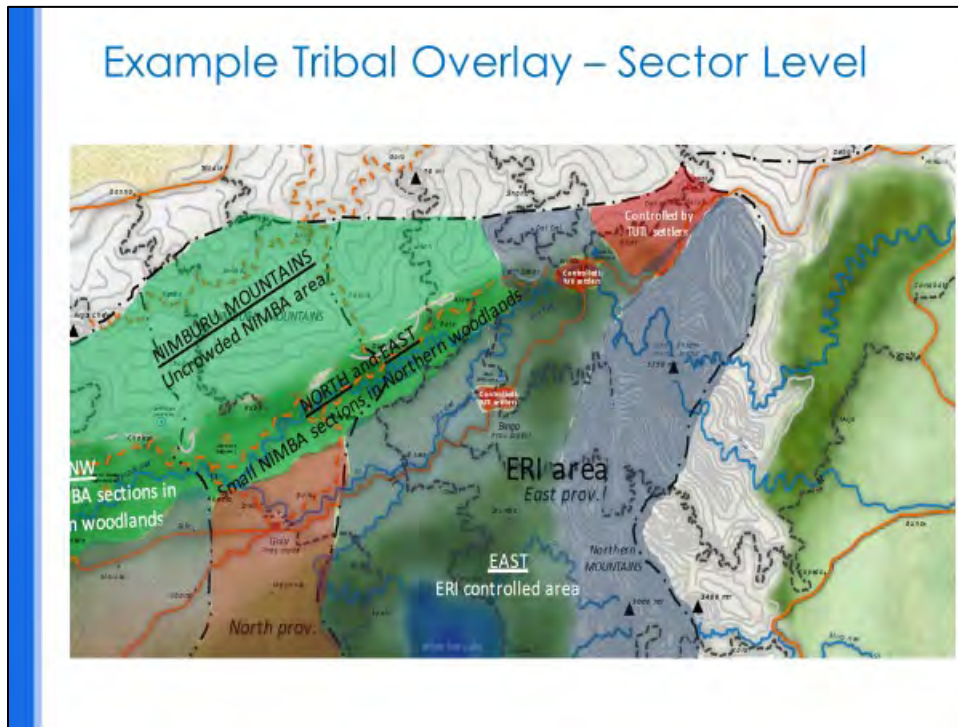
This is an example of a Sector-level overlay. This needs to be more detailed, and it can be used as an aid to military planning. For example, if it is known that the Nimba-inhabited area to the north (shown in green) is pro-UN then it may be permissive and lower risk than would be the case in red shaded areas, if it was known that Tutu areas were anti-UN. Again, this is just a quick visual representation on the information drawn from the ASCOPE-PMESII process.

Slide 28
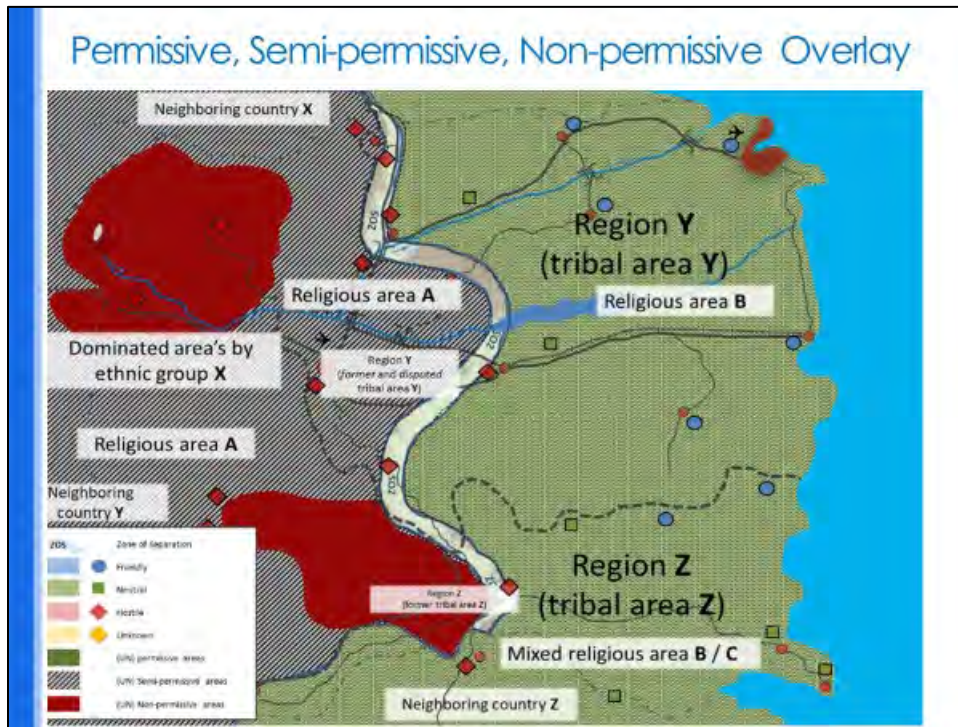
This is another map overlaid with permissive, semi-permissive, and neutral areas for the UN. At all times, the overlays must have a purpose. Areas of people that have more than 6 children could be shown on the map if the intelligence section had access to such data, but it would not be useful for operational planning.

Interaction. Ask the students how they would read this map. What are the areas that the UN is likely to be at the highest and lowest risk of attack? What would the students expect to see in areas shaded red? Is it likely that there is a government presence in these areas? Is tribe Z likely to be pro or anti-UN? Is ethnic group X likely to be pro or anti-UN?

Slide 29
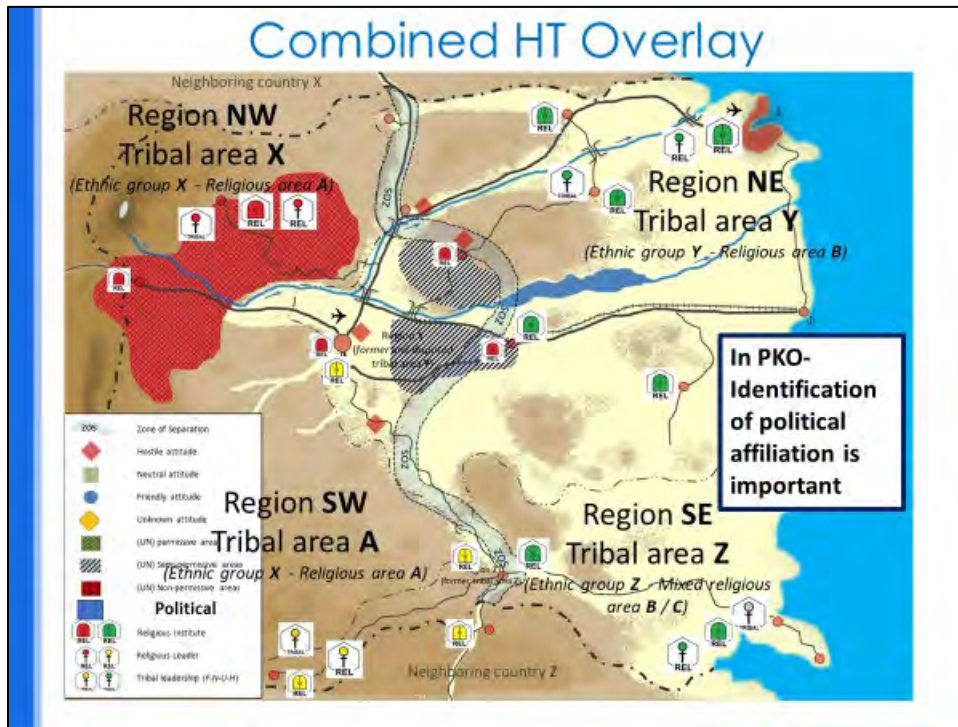
Human terrain cannot be evaluated separately to physical terrain as it is the space where the human terrain interacts with the environment. The human terrain overlays will always be laid across the physical terrain overlays. Combining overlays of different factors also allows the intelligence staff to see new relationships and draw new deductions. Remember that it is important in a PKO to identify the political component of HT.

This slide shows the physical terrain overlaid with another type of human terrain, this time semi and non-permissive areas for UN activity. This visual representation would be useful to intelligence staff involved in planning a UN resupply convoy in the area. It could highlight vulnerable areas. For example, the road through the red area could be an area where the UN convoy would be canalized and vulnerable to attack.

This slide also shows the locations of key structures such as religious institutes or structures, and where key leaders live.

The main point here is that the information must be represented in an easy to read manner that allows the key factors to be visualized by the intelligence staff, operations staff and commander.

Slide 30

Key message. An IHI is a generally a tangible physical item such as a key piece of hardware or location that is central to mission accomplishment for the UN or a threat actor, or to survival/normal life for other actors such as vulnerable population groups.

For a threat actor, an IHI might be anti-tank rockets or a border crossing it controls that give it financial strength. For the UN, an IHI might be an IDP or Refugee camp where it protects civilians. For a local town, an IHI might be a water source. IHIs are, therefore a matter of perspective. It is the role of the UN Intelligence section to prepare a list of such items.

Slide 31

HT: IHI List – So what?

- UN can target a threat actor's IHI
- UN can protect its own IHIs
- UN can protect civilian population's IHIs
  - Gain support
  - Ensure consent

Key Message: It is important to operationalize your IHI list. It must be useful, relevant, and must inform mission planning.

Their significance could be as follows. If the UN wishes to undermine a threat group, it could take control of a border crossing that group is operating, thereby denying it access to funds, or to a safe consolidation zone. However, if the UN takes such an action then because it is an IHI, it is almost certain to face resistance. This can inform planning as a tool for CPOC and can add exceptional value. For example, if denying armed actor access to funds is in line with the commander's intent, then the risk of conflict can be accepted. Still, if this is not the commander's intent, then the intelligence cell can advise the commander that the border crossing point is an IHI to an armed actor. The commander may then wish to avoid this risk, particularly if it is not in line with his/her original intent.

Similarly, for a UN deployment, an IHI is something that is an essential asset to mission implementation such as armoured vehicles, or something that is essential to mandate completion such as refugee or IDP camps.

An IHI does not have to be critically important to a mission. An IHI for a village might be the local market or water source. Again, the intelligence cell should highlight this to the commanding officer so that, for example, patrols are not planned in a village on market day, which could negatively affect the local economy, thereby potentially

undermining local support for the UN. On the other hand, market days are timings were an attack could result in lots of civilian casualties.

***Interaction.** Ask the class to list potential IHIs for:*

- *An armed group*
- *The UN*
- *The civilian population living in a town*

Explain to the class that it is not enough to identify an IHI. Ask the class how they could operationalise the list they have. Each student should be asked to outline with an item on their IHI, and what it means for the UN mission mandate.

.

Slide 32

Key Message: While it is tempting for inexperienced personnel to focus on mapping products, this is not the most important output from human terrain analysis. The key output is the meaning or significance of the identified factor and/or actor. This is the deduction or the 'so what?

Other outputs, all of which should be recorded and collated, include:

- Information Requirements are drawn from the information gaps highlighted throughout the process. These IRs must either be added to the Information Acquisition Plan (IAP), which is the central document for tasking acquisition assets or sent out as Requests for Information

- Other outputs such as planning guidance, constraints, limitations, risks identified, which should all be shared with operational planners; and items of the high importance list

- The Items of High Importance (IHI) list equates to what many of you, the students, may recognize as High-Value Targets. In conventional, non-UN environments there are often targeted to deny them to armed groups, or protected to maintain them for friendly forces, in a UN context they are known as IHIs

- An IHI is 'a compiled list of identified items (including individuals, equipment and infrastructure) which are assessed as being of significant importance to both

threat and non-threat actors and UN forces, which are required for the completion of their respective mission(s) within the context of the mandate

- An IHI can be identified throughout the human terrain analysis process, but are generally highlighted during the three-column analysis
- All outputs should be marked and recorded

Slide 33

Summary

At the end of this lesson you should be able to:

- Conduct a HT evaluation for a sector

- Understand ASCOPE PMESII and HT factors that are key to an analysis

- Understand that there are two IHIs analysis one for UN and one for Threat Actor as both are relevant to your analysis

- Be able to develop and complete HT map overlay

- Because most of the UN mandates include the POC it is important that HT evaluation is conducted and we better understand actors who are predators and vulnerable populations; this is an important tool in POC planning

Learning Activity

Learning Activity - Exercise

- **Task**: Commence Human Terrain Evaluation for your Sector

- **Process and Outputs**:
  Complete 'People' row of ASCOPE PMESII
  - List Factors
  - List Information Requirements
  Use 3 Column Format to Evaluate Factors
  - List Deductions
  - List Information Requirements / Tasks
  Complete map overlays
  - Ethnic groups
  - Locations of key leaders

TASK: Complete a Human Terrain analysis

RESOURCES: Each Syndicate will have an instructor assigned to guide them through the process, a sector map, a series of overlays, and semi-permanent markers of various colours (Blue, Brown, Black, Red, and one other colour at a minimum), a whiteboard and flip chart.

APPROX. TIME: 2 hours

NOTE TO INSTRUCTORS:

- The group will be broken down into syndicates of no more than 5.

- Each syndicate will have an officer in command.

- Each syndicate will have to conduct a full human terrain evaluation for their sector area.

- The process they will follow will be ASCOPE PMESII; 3-column format for analysis; and human terrain mapping (visual representation).

KEY OUTPUTS:

- ASCOPE PMESII for the sector
- Information gaps identified and listed as Information Requirements
- Short human terrain-focused intelligence estimate using the 3-column format
- List of deductions and additional Information Requirements
- Human terrain overlays for ethnic areas, areas of armed groups, and non-permissive and permissive areas for the UN

Lesson
3.5e

AOE-Analysis of Information Terrain

The Lesson

Starting the Lesson

The aim of this lesson is to introduce military peacekeeping-intelligence officers to the practices and processes of analysing the information terrain in UN peacekeeping operations.
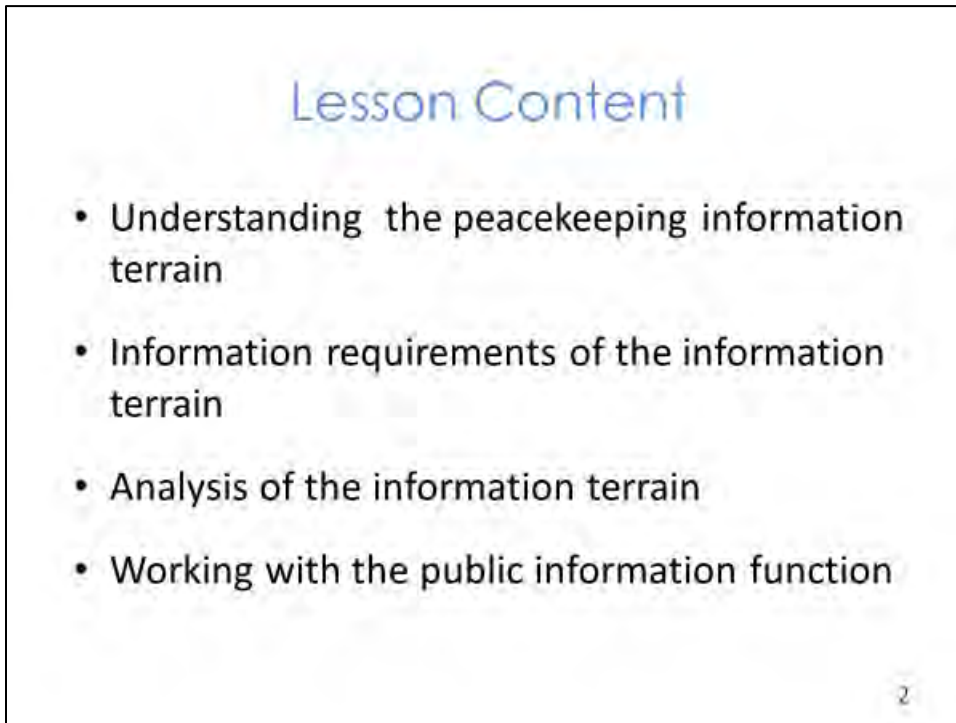
Slide 1

Information is a vital resource. Peacekeeping operations depend on information and information systems for many simultaneous and integrated activities. For peacekeeping operations to succeed, it is necessary for peacekeeping missions to gain and maintain information superiority. The first and foremost is to understand the information environment within which peacekeeping operations are conducted.

The aim of this lesson is to introduce military peacekeeping-intelligence officers to the practices and processes of analyzing the information terrain in UN peacekeeping operations.

Slide 2

Here are the subject areas we will be covering.

The information environment (henceforth referred to as the Information Terrain) is an important aspect of the peacekeeping operating environment. For a comprehensive understanding of the peacekeeping information terrain, deliberate analysis of the information environment is required. This is often overlooked by some UN Forces, but it should be given the same time as an analysis of the physical terrain.

Frequently, the results of the MPKI section's analysis of the information terrain will inform the wider mission of public information or communications strategy.

Slide 3

Intelligence staff officers must understand both the peacekeeping information terrain and what the commander needs to know about it. They must also understand the analytical tools used to evaluate it and understand how to apply this knowledge in support of communication operations.

Let's review the Learning Outcomes for this lesson. At the end of the lesson you are expected to:

- Explain the peacekeeping information terrain

- Describe information requirements for the information terrain

- Apply techniques to analyse the information terrain

Slide 4

The information terrain is the space in which humans communicate. The information terrain governs how such communication occurs, and the systems that are used.

The transmission of information informs how people think and, in turn, how they act and react. Clearly, a comprehensive understanding of this is central to the understanding of the overall operating environment and to operational decision making, as this will have an impact on chosen actor Courses of Action.

The key elements of the information terrain include actors (leaders, decision-makers, individuals and organisations), resources (the materials and systems employed to collect, analyse, apply, or disseminate information) and the employment of resources by actors to influence others.

Interaction.

Actors. Ask the students which actors could influence the local population? Responses here include politicians, armed groups, community leaders, tribal leaders etc.

Resources. Ask the students what resources a key leader would need in this case? The response here is, among others, GSM towers, Internet access, and physical space and freedom to hold a meeting.

Employment of resources to influence others. Ask the students how these resources could be used to influence the local population, and what this could mean for the UN? Responses here include pro or anti-UN propaganda.

Interaction. Ask the students what it could mean if a local radio station was transmitting anti-UN propaganda in a part of the UN AO. How could this impact UN Operations? Would this help or hinder it? How could this influence the course of action that a group could take when meeting with a UN patrol?

Slide 5
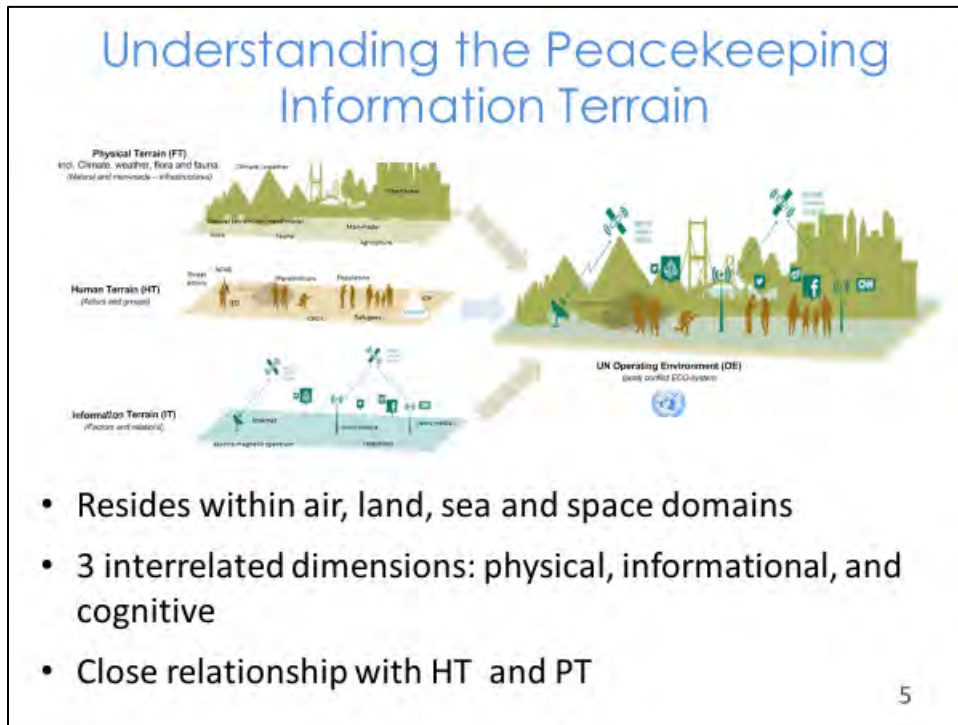
Even though the information terrain is distinct from air, land, sea and space domains, it resides within each of them.

The information terrain is made up of three interrelated dimensions: physical, informational, and cognitive. We will expand on this as we move through this lecture.

As such, it is closely related to the human terrain (those who employ information) and the physical terrain (which provides the conditions for the employment of information).

Interactive. Ask the students to discuss the links between the information terrain, the physical terrain, and the human terrain.

Slide 6
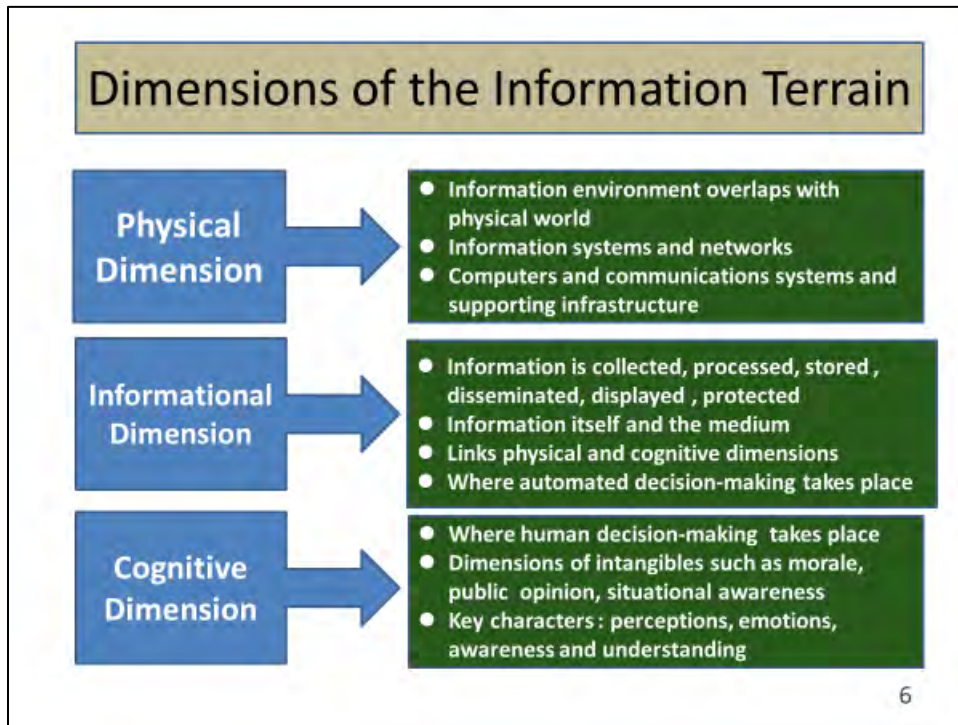
The physical dimension is composed of the command and control (C2) systems and supporting infrastructures that enable individuals and organisations to communicate. It is also the dimension where physical platforms and the communications networks that connect them reside. This includes the means of transmission, infrastructure, technologies, groups, and populations.

Interactive. Ask the students to identify the relevant infrastructure that supports the passage of information in their AOs. Responses include radio masts, GSM towers, internet coverage, TV masts, electricity lines. The list is endless.

It is important that we identify what is known and what is unknown. The unknowns are added to the Information Acquisition Plan (IAP).

The informational dimension is where information is collected, processed, stored, disseminated, displayed, and protected.

The protection of UN information is governed by UN information security policy and executed by IT services, but the MPKI section must ascertain the following:

- Threat actor capabilities. For example, does a threat or otherwise, hostile actor have the capability to obtain UN information, or to prevent the UN form transmitting information?

- Threat actor vulnerabilities. Where does a threat actor have difficulty communicating and why? How does a threat actor communicate, and how could this be undermined?

- It is also a role of the UN MPKI section to find out where the physical terrain could prevent UN communications. These areas are known as communications blackspots

Slide 7

The information terrain of peacekeeping operations is not as simple as it might initially seem. The global information environment and its associated technologies are potentially available to everyone and can change rapidly.

As a result, actors now possess growing information capabilities. For example, regardless of their size, actors, including terrorist groups, can counter UN efforts through propaganda campaigns. They now have the capability to pass information, coordinate, exchange ideas, and synchronize their actions instantaneously.

☞ *Note to Instructor- Point out to the students that before 2007, social media had not penetrated most UN operating environments, but social media is now a significant factor influencing the information environment. The implication here is that the MPKI cell must constantly revisit the information terrain evaluation.*

Slide 8

> ## Learning Activity # 1
>
> **Case 1:**
> In 1994, a radio station, Radio Mille Collines, played a crucial role in launching, inciting and directing the Rwandan genocide and triggered conflict throughout the Great Lakes region
>
> **Instructions:**
> Discuss how the information terrain of UN peacekeeping operations can impact mandate implementation. You will receive a detailed Handout for use in this case.
>
> **Time:** Approx. 20 minutes (group discussion)

Key message: An actor's employment of information resources to influence others may impact a UN peacekeeping mission's mandate implementation, and the effective employment of information resources by a UN peacekeeping mission may also contribute to mandate implementation.

Interactive. Print out the narratives of the Radio Mille Collines case and hand out to the participants. Divide the class into groups and give them the necessary time to read the narrative. Attach at least one instructor to each group. Ask the participants to evaluate the study using the factor, deduction, output process. Ask the students to discuss the implications for the UN as they existed at that time from an information terrain perspective. Provide the students with the Handout in the Learning Activity folder Annex.

Instructor Note: See Annex B for Learning Activity #1Handout- Radio Mille Collines transcript.

Slide 9

Key Message. This slide is designed to make students think about the different components of the information terrain to develop a list of knowns, which become factors for further evaluation and unknowns, which will then become Information Requirements.

Collectively, the physical, informational, and cognitive properties of the information environment comprise step one of this process. These headings provide a start point for structured thinking. The Physical Properties of the information environment include people, places, things, and capabilities of information infrastructure and adversary information capabilities.

Interactive. Ask the class what should the MPKI section know about the physical environment in terms of place, structures, and information capabilities. Ensure the class notes what it does not know and stores these as IRs.

Examples should include The location of GSM, radio and TV masts, the penetration of such means, and the access of various actors to these means. The location of key information actors, locations where meetings are held etc.

Informational properties of the information environment include those systems and networks where information is created, processed, manipulated, transmitted, and

shared. It includes those properties relevant to the electronic collection, transmission, processing, storage, and display of information.

Interactive. Ask the class what the MPKI section should know about the information systems? Examples should include the area of mobile, radio, and Internet penetration. Access to information processing technology and hardware. Print media coverage.

Cognitive properties of the information environment are the psychological, cultural, behavioural, and other human attributes that influence decision making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organisation.

Interactive Ask the class what the MPKI section should know in this case? Examples would include: is it customary for a societal group to be influenced by means of communications? Are there psychological or historical factors that make this group particularly open or vulnerable to propaganda. The potential list is endless.

Note to Instructor- It is important that the students list both the knowns and the unknowns generated by the evaluation of the physical, informational, and cognitive dimensions. Ensure that the students are aware that knowns will be brought forward for further analysis, while the unknowns will be transferred to the IAP.

Slide 10

This slide commences step two of the structured process to iterate what is known and to develop information requirements. The actors in the peacekeeping information environment include the local population, the host nation-state actors such as the security forces and the non-state actors such as rebel factions or armed groups.

All these factors have access to information resources and have the potential to employ the information resources available to them to influence one another or the UN peacekeeping mission. Therefore, it is imperative for the UN mission to know each of these actors, the information resources available to each of them and how each of them may employ the resources to influence one another and the UN peacekeeping mission.

The information requirements concerning the local population may include but are not limited to:

- How do the local nationals communicate?

- How do they influence/advertise?

- Is there any media bias linked to demographics or religion?

Interactive Ask the class to think of other questions that the MPKI section should know as they pertain to the local population. If we do not know the

answer to any of these questions, then they become information requirements. Ensure that the students are aware that knowns will be brought forward for further analysis, while the unknowns will be transferred to the IAP.

Slide 11

Information Requirements of the Information Terrain

Host Nation

- How do host nation security forces communicate

- Is this secure

- Do the host nation security forces conduct information operations / influence media or social media

11

The information requirements concerning the host nation may include but are not limited to: How do the host nation security forces communicate? Is this secure; do the host nation security forces conduct information operations/influence via media or social media?

Interactive *Ask the class to think of other questions that the MPKI section should know as they pertain to the host nation. If we do not know the answer to any of these questions, then they become an information requirement. Ensure that the students are aware that knowns will be brought forward for further analysis, while the unknowns will be transferred to the IAP.*

Slide 12

Information Requirements of the Information Terrain

Threat Actors

- How does threat actor communicate?

- Is this secure

- How does threat actor communicate with local nationals

- Does threat actor conduct information operations / influence media or social media

12

Some actors in the host nation may employ information resources for their activities that may post a potential threat to the UN peacekeeping mission or the local civilians that the mission is mandated to protect. The intelligence staff must be able to identify potential threat actors and acquire necessary information concerning the threat actors.

Information requirements concerning threat actors may include but are not limited to:

- How does the threat actor communicate? Is this secure?

- How does the threat actor communicate with local nationals?

- Does the threat actor conduct information operations/influence via media or social media?

Interactive Ask the class to think of other questions that the MPKI section should know as they pertain to a threat actor. If we do not know the answer to any of these questions, then they become an information requirement. Ensure that the students are aware that knowns will be brought forward for further analysis, while the unknowns will be transferred to the IAP.

Slide 13

In addition to the information requirements about the local population and the host nation, the intelligence staff should also identify the essential elements of friendly information concerning the information environment for the planning and execution of UN information activities.

Essential elements of friendly information concerning the information environment include but are not limited to:

- Can we use host nation information infrastructure? Is it secure?
- Can we collect information from the opponent media?
- Are there exploitation opportunities?
- Can we communicate with local nationals via host nation media or social media?
- Can we conduct information operations/influence via media or social media?

Interactive *Ask the class to think of other questions that the MPKI section should know as they pertain to the UN. If we do not know the answer to any of these questions, then they become an information requirement. Ensure that the*

students are aware that knowns will be brought forward for further analysis, while the unknowns will be transferred to the IAP.

Planning for public information should be part of the peacekeeping strategy from its outset. A public information strategy allows the UN mission to ensure that the public can receive objective information about the peace process. In addition, public information can assist a peacekeeping mission in executing its mandate by establishing a favourable image of the mission, communicating clearly its role and objectives and winning acceptance and support for the mission's activity and ultimately the peace process itself. The MPKI section must always be prepared to support the PI section, just as it supports the operational sections and the UN MDMP.

Slide 14

> **Learning Activity # 2**
>
> **Arguments for and against using social media for UNMMIG**
>
> **1. Situation**
>
> Use social media to support the mission by promoting the mission, enhancing communications and sharing information.
>
> **2. Instruction**
>
> Conduct a short discussion about the Pro's and Con's regarding using social media by UNMMIG in Garland.
>
> **3. Approx. Time: 20 minutes** Group work and discussion

Interaction. Working in syndicate groups, have participants review the slide and then discuss the UNMMIG plan on the use of social media to share information with the local population. Ask them about the factors that they should consider before making a recommendation; ask to come up with pros and cons, and report back their findings to the entire class.

Help facilitate, and coach- what we are looking for in this case are some of the following considerations:

- *What is the UNMMIG target audience?*
- *Does it use social media?*
- *What social media platforms does it use?*
- *Is there Internet coverage in the area?*
- *What languages does the local population speak?*
- *What kind of messages will be effective?*
- *Is the target population literate?*

- *Will social media reach all the target audience; for example, do the elderly use social media?*

☞*Note to Instructor- Additional information about social media:*

Social media are web-based communication tools that enable people to interact with each other by both sharing and consuming information.

Social media include digital media tools that enable users to easily create, modify, link, share, and post content collaboratively through computers, mobile phones or tablets. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking and wikis are among the different types of social media.

One of the features of social media is that they usually give users the flexibility to manage the information they see in their news feeds and even give feedback on what they want or don't want to see.

Slide 15

While we are approaching the development of information requirements for the Information terrain in a slightly different fashion, the ASCOPE-PMESII tool is also useful for highlighting what is known about the information terrain, and what is not.

Once again, by showing how the ASCOPE-PMESII tool can be applied to the generation of factors and information requirements, we create a structure for the MPKI section to work with, thereby assuring our evaluation is comprehensive. We have seen in earlier physical and human terrain lectures; we use the ASCOPE-PMESII framework to structure our thought processes.

In the case of information terrain, we focus on the information part of the PMESII acronym and match it with Areas, Structures, Capabilities, Organisations, People, and Events. This will offer a relatively comprehensive overview of what we know and what we do not know.

Slide 16

Key Message. The 3 Column Format tool will be used as a framework for analysis. The first part of this lecture involves the key knowns form our initial review of basic and current intelligence as it pertains to information terrain.

The knowns have been identified using the frameworks we have just used: the physical, informational, and cognitive dimensions; and using ASCOPE-PMESII. The following process should be adhered to:

- List what the key factors pertaining to the physical dimension of information terrain: places, structures, key leaders, organisations such as threat groups and their known capabilities.

- List the key factors pertaining to the information dimension, such as information systems and penetration.

- List the key factors pertaining to the cognitive dimension such as important historical, cultural and social factors.

- List the key factors pertaining to the local population, to the host nations, to threat actors, and to UN Forces.

These are all the key knowns about the information environment.

Slide 17

The 3-column format can be applied in evaluating the effects of the information terrain. Here is an example.

Slide 18

Moving to the second column, make deductions based on what is known. As we have been previously shown, deductions or the 'so what' populate the second column of the three-factor process. This is where the MPKI section really earns its money.

Consider each factor as follows:

- So what for civilian population (tribal/religious/ethnic groups);
- So what for UN Forces
- So what for threat actors

Interactive Ask the students what the implication of the following factor: 'NO Internet connectivity in area X'. What are the implications or so what for each of those 3 groups? Responses could include such things as Tribal group A cannot be influenced by social media or other internet-based media; UN personnel will not be able to communicate using internet-based devices; Threat Actors can only communicate using GSM or radio-based capabilities. The students must record the deductions as they form a basis for further evaluation and will inform the MDMP.

Slide 19

The third column will constitute a series of outputs or tasks as they relate to the information environment. These outputs can be additional information requirements, planning guidance or tasks for assets. Outputs for the MPKI section come in the form of Information Requirements, tasks for ISR assets, and/or planning guidance.

Interactive. Ask students to derive tasks from their previous deductions. For example, an information requirement relating to the threat actor could be 'is there GSM coverage in area X? Or consider bringing BGAN or another portable Internet system for UN Forces.

Slide 20

> ## Learning Activity # 3
>
> What do you know about your sector (factors)?
>
> What are your unknowns (IR)?
>
> Consider:
>
> > Physical (areas, structures, people, organizations), informational (systems, penetration), cognitive dimensions (how people are influenced)
>
> **Approx. Time: 15 min**

Interactive *Ask the class to break into their syndicate groups with each group focusing on their specific sector; Ask the students to list what they know and what questions they have about the information terrain in their sector; Guide the students to focus on: areas, structures and actors; resources available to actors; how information influences behaviour in their Area. Students should evaluate what they should know about information: areas in a UN AO; structures in a UN AO; capabilities in a UN AO; and organisations in a UN AO. Each group should focus on one topic only. Each group should produce a list of knowns and questions as to its output.*

Slide 21

Mapping can help the commander and the staffs visualize and better understand the information terrain. It is intuitive, and humans tend to process information better in visual form. The list of overlays the MPKI section is extensive, but the most important are listed above. It is important to remember that there is always a reason why an overlay is created. Intelligence staff should consider producing different overlays and combine them into one, noting that the normal map marking considerations should be adhered to, including:

- Three reference points to enable the correct positioning of the overlay on the map
- The DTG of the map so that the user knows if it is up to date
- A clear legend
- Clear colours to mark different themes
- The map detail should not be obscured
- The direction of North
- The signature of the creator
- Classification

For this course, students should include communications infrastructure; communications blackspots; pro and anti-UN media coverage.

Slide 22
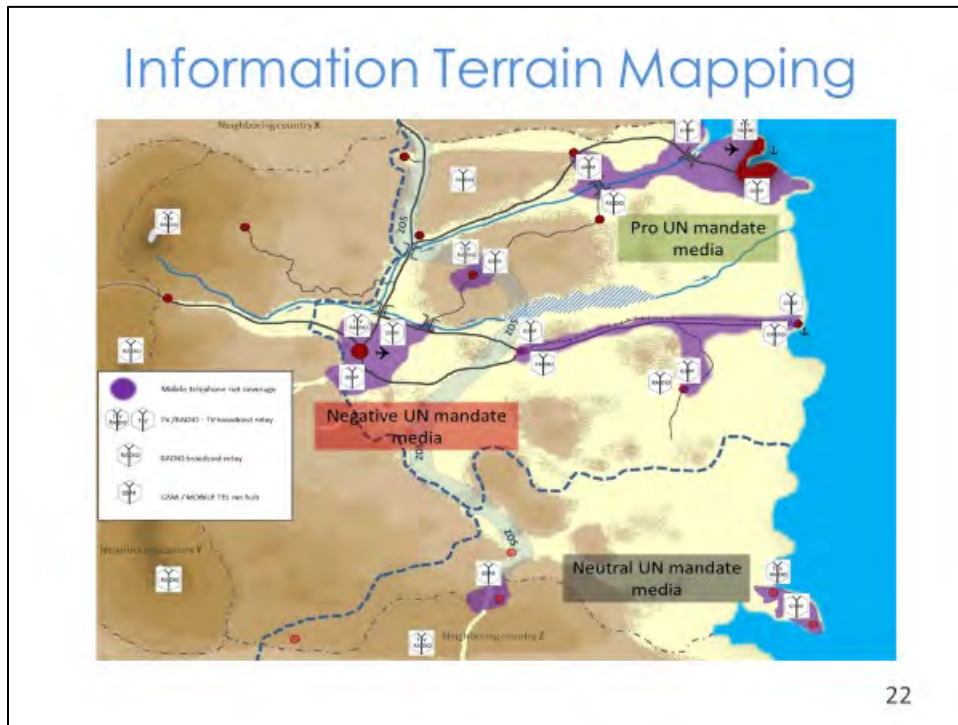
Here is an example of combined information terrain mapping.

Interactive. Ask the students what this overlay tells them. Based on our guidelines, ask the students what is missing here?

Slide 23

Key Message. While an effective public information strategy is a political and operational necessity, it is not the central role of the MPKI section. Rather, the MPKI section should be ready to support the UN Public Information Officer (PIO) or the strategic communications section.

Peacekeeping operations require the understanding and cooperation of all parties in the mission area, the general population, as well as the political and material support of the international community, to fulfil their mandates and ensure the security of United Nations personnel.

Depending on the level of literacy, communications infrastructure, media environment and level of civil society activity in the mission area, the public information program may include public relations activities aimed at community groups. Such activities may include briefings, "town hall" meetings, concerts, and theatrical performances.

The UN MPKI role in this regard is to support the Public Information Officer, or strategic communications section by providing them with the results of the analysis of the information terrain.

Interactive. Tell the students that the UN PIO plans to launch a messaging campaign in support of an UN-supervised ceasefire. The campaign will target a

specific tribal group. How could the UN MPKI section assist? Ask the students to approach this issue methodically using the three dimensions: the physical; the informational; and the cognitive. Responses here would be briefing the UN PIO on the following:

physical information dimension *– how best to transmit the message. For example, there is no point in transmitting the information via TV programs if there are no TV masts in the tribal group's area. The MPKI section should explain how the physical terrain would help or hinder the passage of the UN message;*

Information dimension: *can negative actors block the transmission? If so, how can the UN prevent this from happening? How can the message best be transmitted? For example, if the tribal group is largely illiterate, then there is no point in printing pamphlets. The MPKI section should advise on protections needed, and the best means to reach the tribal group.*

Cognitive dimension. *How can the tribal group be influenced to act or react? How is the tribal group likely to react based on what is known about the group. Once again, this highlights the link between the information terrain and what we know about the human terrain.*

Ensure the students understand that they will not operate in a PIO function, but that they should actively support the PIO nonetheless

Slide 24

Learning Activity # 4

Tasks: - Identify Knowns

- Identify IRs

- Analyze using 3-column format

Outputs: List of IRs; record of relevant deductions; Terrain overlay.

Tip: Have one-member recording IRs, and another recording deductions; put two students preparing the overlay based on knowns and deductions

Time: 1.5 hours

Interactive. Break the class into syndicate groups with each group focusing on their specific sector; Ask the students to work out what they know and what questions they have about the information terrain in their sector. Guide the students to focus on: areas, structures and actors; resources available to actors; how information influences behaviour in their AO;

Students should evaluate what they should know about information: areas in a UN AO; structures in a UN AO; capabilities in a UN AO; and organisations in a UN AO. Each group should focus on one topic only. Each group should produce a list of knowns and questions as to its output.

Slide 25

Take Away

- The success of peacekeeping operations depends on information and information systems

- An effective information strategy is an operational necessity

- Analysis of the information terrain is key to understanding the peacekeeping information environment and decision-making

- Intelligence staff must work closely with the public information function for planning and executing operations

25

Summary

- The success of peacekeeping operations depends on information and information systems.

- An effective information strategy is an operational necessity.

- Analysis of the information terrain is key to understanding the peacekeeping information environment and decision-making.

- Intelligence staff must work closely with the public information function for planning and executing operations.

L e s s o n
3.5f

AOE-ASCOPE_PMESII

The Lesson

Starting the Lesson

The ASCOPE-PMESII tool was briefly presented / shown during Lesson the AOE introduction lesson. During this Lesson the students will be taught how to use ASCOPE-PMESII in the further analysis of AOE – especially the Human Terrain – and to identify information/intelligence gaps that need to be filled.

ASCOPE-PMESII is a tool developed to focus intelligence collection and analysis on all relevant factors that can impact on operations – and not just the military factors.

Before starting the lesson prepare the following materials to be handed out to the students - preferably in soft copy:

- A generic ASCOPE-PMESII matrix explaining the general content of the individual boxes as shown in slide 5 for reference

- A blank ASCOPE-PMESII matrix to be filled out during the learning activity at the end of the lesson

- 3-column format form

Slide 1

ASCOPE and PMESII are analytical tools that are well-suited to the Operating Environment Evaluation in UN Peacekeeping Operations. The topic of this lesson is ASCOPE – PMESII. The acronyms stand for: Area – Structures – Capabilities – Organisations – People – Events (ASCOPE) and Political-Military – Economic – Social – Information – Infrastructure. This is one such tool in our toolbox to help us. It looks complex, yet it is not. It is very similar to an index in a book.

Slide 2

Here is the content we will cover in this lesson. The ASCOPE societal factors or dimensions (Area – Structures – Capabilities – Organisations – People – Events), and the PMESII systems/sub-systems (Political-Military – Economic – Social – Information – Infrastructure) The ASCOPE – PMESII Matrix, which is a tool used to systematically identify factors relating to the Human Terrain, and to highlight information gaps. The lesson will conclude with a scenario-based classroom exercise using the ASCOPE – PMESII Matrix.

Slide 3

Let's review the Learning Outcomes for this lesson. When this lesson has been completed, you are expected to be able to explain the ASCOPE - PMESII headings, how the ASCOPE-PMESII matrix can assist us in identifying factors for further evaluation of the operating environment, and how it can drive the formation of the Information Acquisition Plan (IAP).

Throughout this lesson, students will be expected to demonstrate the understanding of ASCOPE – PMESII by completing an exercise in which you populate one or more intersecting boxes in the ASCOPE – PMESII Matrix based on the information provided in the exercise scenario.

Slide 4

Key Message: ASCOPE – PMESII is a very useful tool which enables the MPKI cell to systematically break down all the factors associated with the operating environment. However, it has a particularly strong relationship with the Human Terrain.

When using the matrix, we should consider populating it from three perspectives: the local civilian population and the organisations therein; friendly or allied forces; and threat actors. From the factors on the screen, you can see that we are not just looking at tangible 'things'. Rather, we consider all aspects, including beliefs.

Slide 5

Key Message: The purpose of this slide is to refresh the students' memory regarding the ASCOPE-PMESII matrix, last seen during the introduction to the Analysis of the Operating Environment. It shows the intersecting societal factors (ASCOPE) together with the operational variables or systems (PMESII), thus making it possible to guide the analysis of the Human Terrain.

This is the ASCOPE-PMESII matrix. You must first understand how to read it. Move across the societal factors on the horizontal axis and match it with the variables on the vertical axis. The example on the slide matches the Social with the social system's structures.

Interaction. Ask the students what they would expect to see in this box. Ask the students to consider it from a threat actor, friendly forces, and local population perspective. The factors that the students identify are moved to the 3-column format for further analysis. Quickly become apparent that the students lack some information on social structures. These information gaps should be recorded and sent forward as Requests for Information or should enter the Information Acquisition Plan (IAP).

Ask students to consider their own countries and to offer up what areas they may want to focus on, e.g. what areas of your economy you would focus on?

Slide 6

The ASCOPE elements are the societal factors in which the PMESII systems and sub-systems operate. Generally, ASCOPE-PMESII covers what the MPKI section should know about their operating environment. Here is what the letters in ASCOPE stand for: Area – Structures – Capabilities – Organisations – People – Events. Each of these dimensions has a series of sub-systems, which is why we cross-reference each dimension with PMESII.

Slide 7

A is for Area is the first ASCOPE factor and is the physical locations and terrain that affect all relevant actors. Areas are localities or physical terrains that have a direct impact on all actors.

The photograph illustrates an international border (between Germany and Poland).

Area factors may affect choices among relevant actors, such as the routes various relevant actors choose to travel, the places where relevant actors choose to settle, and the people with whom relevant actors choose to interact for various reasons. Area factors also impact the UN Force Commander's decisions during the planning and execution of operations.

Interaction. Ask the students for examples of this factor/sub-system before listing them. Examples include tribal regions, police districts, political boundaries, religious boundaries, territorial boundaries, military boundaries, polling stations, and government centres.

Slide 8
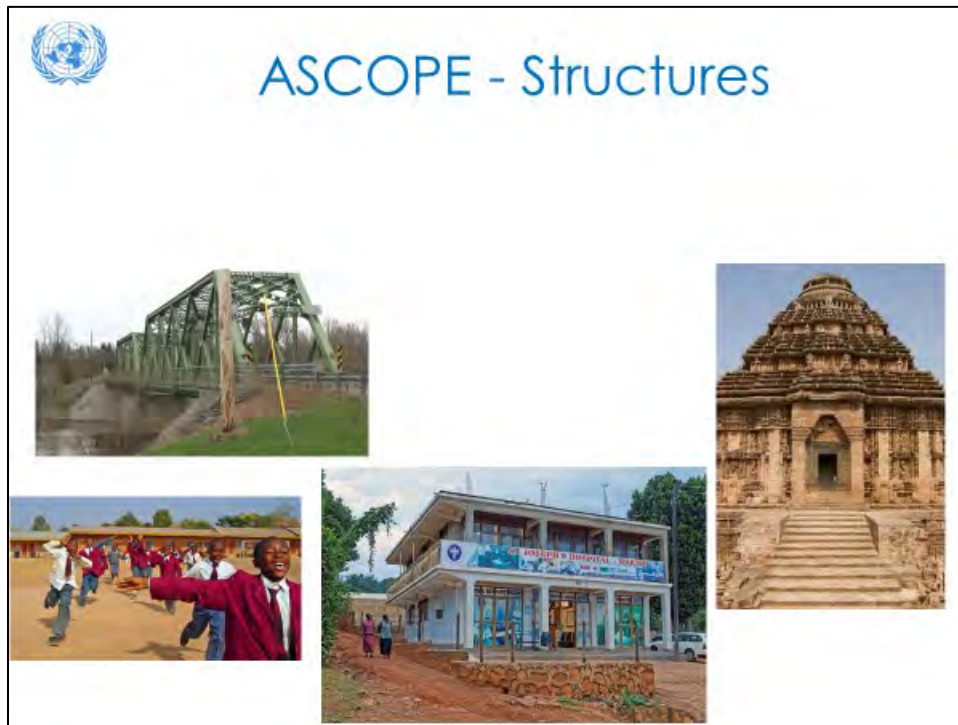
S is for Structures is the second ASCOPE societal factor and includes significant infrastructure such as bridges, religious sites, hospitals and schools. Structures are existing infrastructure. Examples include hospitals, bridges, communications towers, power plants, dams, jails, warehouses, schools, television stations, radio stations, and print plants.

In the context of Peacekeeping Operations, some cultural structures maybe even more important, such as churches, mosques, national libraries, and museums. The photographs show (clockwise): a girder bridge, a Hindu temple, a hospital and a school. In a PKO environment, we cannot overemphasise the potential for problems and sensitivities when the UN operates near and around such structures.

Analysis of the relevant structures includes determining why they are important with respect to their location, functions, capabilities, and application. It is even more important to understand which structures matter, what their significance is to political and military strategy, and how they influence the decision-making and actions of relevant actors.

Slide 9

C for Capabilities is the third ASCOPE societal factor and includes such key functions as administration, food/water supplies, healthcare, social services. Relevant capabilities may include but are not limited to, administration, safety, emergency services, food distribution, agricultural systems, public works and utilities, health, public transportation, electricity, economics, and commerce. Sewage, water, electrical, academic, trash, medical, and security infrastructure are some of the essential services that may be relevant.

Capabilities often affect the security and quality of life of relevant aspects of the population and can sometimes influence decisions among the populace about whether to behave in a manner that assists a government or insurgency.

It is important to understand the interdependence each of these capabilities has upon one another, as well as upon other ASCOPE factors. Electricity affects the ability to bring in information and freshwater; water affects the ability to maintain sewage, prevent disease, and maintain quality of life for the population. These factors are all interdependent upon one another, and the impact of any action affecting one capability must consider the impact this action will have on other capabilities or factors.

Interaction. Ask the students for examples of this factor/sub-system before listing them.

Slide 10

O for Organisations is the fourth ASCOPE societal factor. Organisations can be political, religious, social, criminal, media, patriotic, and community watch groups, as well as other international organisations (e.g. the African Union), NGOs, merchants, squatters, and other groups. The photographs show the logos of the major political parties of France, a shura (meeting of a council of tribal elders) in Afghanistan, and the logo of an Afghan NGO.

Insurgents, counterinsurgents, and the population are not the only relevant actors within the Operating Environment, and it is important to understand how various organisations (or groupings) impact on the OE.

Interaction. Ask the students for examples of this factor/sub-system before listing them.

Slide 11

P for People is the fifth ASCOPE societal factor. Historical, cultural, ethnic, political, economic, and humanitarian factors should be considered when examining the people within the OE. The map shows the distribution of ethnic groups in Afghanistan, and some of the main political leaders in Afghanistan are shown in the photograph. Understanding who is where within the OE will almost always be a relevant factor in the decision cycles of each relevant actor.

For example, areas where people and terrorist armed groups transit, retreat, evade, or hide may have relevance. Knowing where squatters, the homeless, refugees, displaced persons, and outcast groups are and why they are there may also be relevant. The information environment has increased the ability of diaspora populations living abroad to have a direct effect on the attitude, finances, behaviour, and support of the population within the OE. The attitude and beliefs of this external (to the OE) population and how they affect internal behaviour should also be considered.

Interaction. Ask the students for examples of this factor/sub-system before listing them.

Slide 12

E for Events is the sixth ASCOPE societal factor and includes harvest seasons, dates for markets, public and religious holidays. Events are routine, cyclical, planned, or spontaneous activities that affect the OE.

Some examples are planting and harvest seasons, elections, changes in government, key leader succession, economic reforms, political reforms, holidays, observances, anniversaries of key historical events, riots, and trials.

The photographs show Afghan farmers harvesting grain; people celebrating Now Ruz, the Persian New Year, at the shrine of Hazrat Ali in Mazar-i-Sharif in Afghanistan; and a local market in Afghanistan.

Events may spur an increase or decrease in armed attacks. For example, terrorist armed groups may escalate violence to prevent an election, or terrorist activity may decrease during a harvest season as they assist the population. The analysis helps determine which events are relevant and how events help shape the behaviour of relevant actors. Some factors to consider may be the political, economic, psychological, environmental, and/or legal implications of each event.

Slide 13
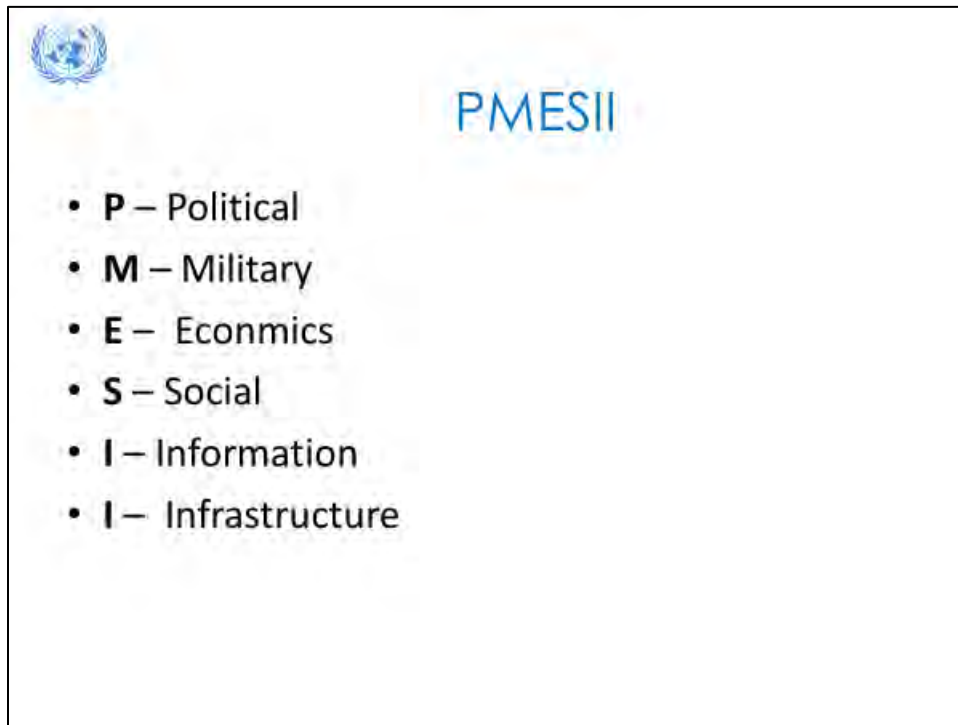
The acronym PMESII covers the systems listed on the slide. The PMESII components comprise the systems and subsystems that operate within the OE. Combined with ASCOPE, PMESII becomes a useful analytical tool in support of the OEE phase. (This will become apparent when the ASCOPE – PMESII Matrix is presented and explained.)

The development of a systems perspective should be founded on the identification and analysis of all mission-relevant characteristics of the various actors' PMESII systems. Because the relevance of PMESII factors and characteristics will depend upon the specific situation associated with each mission, there can be no definitive listing of all characteristics appropriate under all circumstances.

For example, some of the characteristics that may be considered significant during a sustained humanitarian relief operation may receive slightly less emphasis during operations to protect civilians against terrorist armed groups. The analysis of relevant actors' PMESII systems could provide significant indications regarding the circumstances (ideals, goals, territory) that may cause that actor or actors to resort to the use of force or to exercise other political options.

Slide 14

P in PMESII stands for" Political" and includes the political system and systems at the national, regional and local levels. The political system is comprised of the central and local governments as illustrated on the slide by photographs showing Afghan President Ashraf Ghani receiving US Secretary of State Mike Pompeo, the first woman district governor in Afghanistan, and an Afghan village elder.

The political system also comprises political organisations (including political parties and interest groups), and regional/international actors who receive and process political system demands. Political considerations may also include international relations; foreign alliances; unofficial power centres (gangs, cartels, multinational organisations, and militias); and political or ethnic grievances and affiliations.

Interaction. Ask the students for examples of this factor/sub-system before listing them.

Slide 15

The **" M" in PMESII stands for" Military"** and comprises friendly forces, threat actors, and host nation security forces, including the police. Military as illustrated on this slide by photographs of Afghan National Army (ANA) troops on patrol, two female Afghan police officers, and Taliban fighters.

Interaction. Ask the students for examples of this factor/sub-system before listing them.

Slide 16

The "E" in PMESII stands for" Economic", which includes agriculture, industry, and business; and is illustrated by these photos from Afghanistan of a field being harvested, a marble processing plant and a businesswoman whose company sells dried fruits, nuts, fruit juices etc.

An analysis of the economic system takes into consideration the sum total of production, distribution, and consumption of all goods and services in a country. This may be seen as the combination of the formal and informal economies.

Factors to be analysed could include:

- Type of economic model (capitalism, socialism, other)
- Major industries that drive the economy (manufacturing textile/apparel, vehicle, or machine tools)
- Agricultural base (i.e. food production)
- Economic relationship with other countries and with international trade (imports, exports, and the balance of payments)
- The health of domestic markets (i.e. the economic situation: growth, stagnation or decline)
- Opportunities for people to borrow money or own businesses.

- Relationship of the country to foreign investors and the international community for foreign aid and debt relief
- Labour force—skills and employment levels
- Factors regarding the informal economy (terrorist financing, narcotics trade, trafficking in humans, unregulated labour, and smuggling).
- Impact of corruption, accountability (or lack thereof), and transparency (or lack thereof) on the economic system.
- Sources of economic tension (e.g. between socio-economic classes and/or ethnic/religious groups in the population).

Slide 17

The" Social" in PMESII includes communities as represented by the photo of an Afghan village, religious (and ethnic) groups such as the Afghan Shia Hazaras in the second photo, and social classes. Bill Gates, as one of the richest men in the world, belongs in a socio-economic class of his own – together with nine other people. It is important to know the social system's framework in order to evaluate and dissect social interactions. Considerations for analysis could include:

- The cohesion of socio-religious groups
- Causes of societal pressures and discontent
- Impact of immigration and emigration
- The health of the population, including the availability of food and medical supplies
- Educational and economic opportunities
- Role of Intergovernmental Organisations (IGOs) and NGOs
- Types and extent of crime
- Presence and impact of separatist and terrorist armed groups
- Cultural differences among population
- Tolerance for religious freedom

Interaction. Ask the students for examples of this factor.

Slide 18

The first" I" in PMESII, which stands for Information, may be illustrated by print media such as the Afghan newspaper Islah Daily, the first women-only TV station in Afghanistan, and an Afghan using mobile phone communications.

The information system – or systems – in the OE are examined regarding national objectives, communication capabilities, and operations in support of a focus area. Primary subsystems include global information, national information, and defence information networks. Factors for analysis could include:

- Capabilities (reach and capacity (e.g. bandwidth)) of national communications systems (and the communications systems of non-state actors).

- Location of critical communications facilities.

- Foreign technical support to the construction and maintenance of internal telecommunications systems.

- Assessment of IT infrastructure.

- Censorship of the media and the internet.

Interaction. Ask the students for examples of this factor.

Slide 19

 The second **"I" in PMESII stands for "Infrastructure**", and is illustrated by these photos from Afghanistan showing a train on the railroad from Mazar-i-Sharif (in Afghanistan) to Uzbekistan; Highway 1, the main highway in the country; and the Kajaki Dam and hydroelectric plant.

Interaction. Ask the students for examples of this factor/sub-system before listing them.

An infrastructure system includes utilities, transportation, industry, and public facilities. Considerations for analysis could include:

- The ability of the utility network to support industry and the population.

- Sufficiency of water and wastewater facilities.

- Adequacy of the transportation network.

- Adequacy of public facilities in meeting the needs of the population.

Slide 20

This slide shows the "intersection" of societal factors (including examples for each ASCOPE characteristic) with the operational variables (PMESII). this makes it possible to systematically identify known factors and actors to be brought forward for further analysis in the 3-column format (Note to Instructor. The students can and should use this matrix before engaging in their evaluation of the operating environment as it will focus it, particularly as it relates to the human terrain. This helps the MPKIO Identify unknowns or information gaps, which will drive the formulation of the Information Acquisition Plan.

Here is an example of possible content – which by no means are exhaustive – of the ASCOPE – PMESII Matrix in which the ASCOPE societal factors "intersect" with the operational variables (PMESII) in the Matrix. The items listed in each" intersecting" ASCOPE – PMESII" box" are by no means complete but should give a general idea of the information/intelligence contained in or derived from the Matrix.

Using the ASCOPE – PMESII Matrix, it is possible to guide the analysis of the Human Terrain, systematically identifying factors for evaluation and unknowns.

In this example, we cross-reference people with political. This informs the MPKI cell that it should know who the local key political leaders are at all levels.   The MPKI cell will make deductions based on their knowledge of this individual. If the answer is now known, then it becomes an RFI or enters the IAP as a general question. For example, who is the local political leadership in each town in the Sector AO?

As the matrix is filled, it can be 'colour-coded' using red, amber, green to highlight the level / confidence of knowledge and understanding. Green would mean the MPKI cell was confident of its understanding, and red would mean the section has extremely limited information on an area. Note the colours on the slide, what is this section confident in its knowledge, and what does it have significant information deficits?

Interaction. Have the students take a moment to study the matrix; focusing on People. Ask them to develop additional RFIs.

Slide 21

Key Message: Factors identified from the ASCOPE-PMESII matrix as having an impact on the Operating Environment are analysed using the Three-Column Format (3CF). This includes factors for which there are information/intelligence gaps that must be filled.

When factors impacting on the Operating Environment are identified, we use the 3CF to analyse, deduce and determine the necessary output to address the factor in question.

The example on this slide is based on the intersection of people with political. Here we know that John Snow is the local leader of village X but know little else about him. It is important that we find out. Therefore, our unknowns drive further information acquisition.

Similarly, what we must list what we do not know. In this case, we do not know who the leaders of villages A, B, and C are. This becomes another RFI.

Slide 22

ASCOPE-PMESII is simply a tool to facilitate a structured, systematic evaluation of what we know, and a means of recognizing and recording what we do not know.

There are other useful tools that can be used in conjunction with ASCOPE - PMESII:

- STEMPLES (Social, Technological, Environmental, Military, Political, Legal, Economic, Security)

- PEST (Political, Economic, Social, Technological)

- PMESII-PT (Political, Military, Economic, Social, Information, Infrastructure, Physical environment, Time), which are add-on variables to PMESII

- DIME (Diplomatic, Information, Military, Economic), which are the instruments of power available primarily to actors

These tools, just like ASCOPE-PMESII, simply put structure on our approach to ascertaining a deeper understanding of what we already know and identifying what we do not know.

Slide 23

Summary

- ASCOPE PMESII is a tool that puts structure on the identification of knowns (for further analysis) and unknowns (for RFIs/IAP)

- The ASCOPE societal factors are the dimensions in which the PMESII operational variables (systems and sub-systems) operate.

- ASCOPE – PMESII is central to Human Terrain Evaluation.

- ASCOPE – PMESII can be colour coded to denote levels of confidence.

- ASCOPE-PMESII is best completed and stored in soft copy.

Learning Activity

Learning Activity

Instructions:

- Produce an ASCOPE – PMESII Matrix for your Sector
- Focus on the Human Terrain.
- Provide **at least one example of a known** and **at least one unknown** for each intersecting area
- Analyze 2 knowns using the three column format
- Create two questons for the IAP on the basis of the unknowns

Approx. Time: 60 minutes

RESOURCES

- An ASCOPE PMESII chart
- A three-column format chart
- Whiteboard or a flip chart and markers
- If possible, the ASCOPE PMESII chart and the 3CF should be given to students in soft copy and worked on a laptop

TIME
Approx. 60 -90 minutes

PREPARATION
Break into syndicates, try to assign one instructor per syndicate. Syndicates work on their sectors based on information from their sector information pack.

NOTE TO INSTRUCTORS:
Reinforce the learning outcomes and access the knowledge of the group and individuals

Lesson
3.5g

AOE- Actor Evaluation

The Lesson

Starting the Lesson

Slide 1

Slide 2

Content

- Actor evaluation and analysis overview
- Threat analysis
- Threat actor templates- COWARD & 3 column
- PIN and SWOT analysis
- Center of gravity (COG) analysis

Here is the content we will cover in this lesson

Slide 3

Learning Outcomes

- Develop and develop a basic threat actor template

- Explain assess capability and intent

- Describe opportunity and inhibiting factors

- Apply the COG analysis

- Explain the links between actor evaluations and COA development

Let's review the Learning Outcomes for this lesson.

Slide 4

Key message: Evaluating all relevant actors present in a UN Area of Operations is critically important as it will allow you to develop an understanding of how these actors can positively or negatively affect the UN Mission and/or mandated tasks.

It is imperative that the MPKI cell actively acquires information on all relevant actors in its Area of Intelligence Responsibility (AIR) and in its Area of Intelligence Interest (AII). Note that a relevant actor is any important political, economic, humanitarian, or military figure or group that can have an impact on your operating environment.

Using data sheets, which will be outlined in this lecture set, to list all knowns about relevant actors can help you more readily identify what you do not know. This can help you identify information requirements for patrols or other sources.

Throughout this lecture set, we will demonstrate how Actor Evaluation can help identify: the doctrine or Tactics, Techniques, and Procedures of a relevant actor (Note to Instructor: this could show how an NGO or an Armed Group functions); the relevant actor's capability to conduct operations (which could be positive or negative in a UN AO); the approaches that an armed actor could use in operations against the UN, its mission or its mandate; likely adversary objectives; and how an adversary may seek to operate.

Slide 5

Topics such A Course of Action board (essential for operational decision making) for an adversary or other relevant actor cannot be completed without using the tools taught on this lecture. Indeed, every heading that you see here can be completed by combining the results of the Actor Evaluation process, with the results of your analysis of the Operating Environment.

Senior leadership's focus will be on adversarial actors, considering the threat they pose to safety and security/POC-related tasks, and the MPKI cell should apply these tools to all relevant actors. However, on initial deployment or for high-risk missions, it is important to focus on armed or adversarial actors as these will have the most impact on mandate implementation. Explain that therefore the course will generally use an armed actor for most examples.

For example, understanding the relevant actor's intent and overall objectives will help your MPKI cell will help you assess how the actor is likely to react, positively or negatively, to a UN Operation;

Similarly, understanding the relevant actor's capabilities (both organisational and operational) will ensure that you can accurately list them in the Functions column. This will also help your section to populate the Items of High Importance (IHI) list;

Slide 6

Key Message. Actor Evaluation should be completed for all relevant actors, not just those that are armed.

Interaction. Ask the students to suggest which groups are relevant actors are in a UN Operating Environment. Answers could include any person or group which through its interactions with the information, human, or physical terrain could affect the situation in a positive or negative way. Encourage the class to discuss what is and what is not a relevant actor.

Ask the students to give an example of a positive impact a relevant actor could have, and the negative impact a relevant actor could have. Offer the following example if assistance is needed: an NGO operating at a POC site can be a positive, stabilizing influence, but if that NGO was to cease operations, it would have a negative impact.

The example photos on the slide are just a few of the many available options. We are looking for: NGOs; local political or tribal leaders; women and children; different tribal or ethnic groups; religious leaders; non-state armed groups; state armed groups; terrorist groups. The potential list is long.

There is a tendency to focus on conventional threats to UN safety and security and to POC-related tasks. This is natural – even necessary – on initial deployment, but this slide is intended to demonstrate that all actors can influence your operating environment. If you can identify a wide variety of relevant actors; you will better understand a given operating environment.

Slide 7

Interaction. Before showing the slide, explain the concept of the Pyramid (given below) and then draw the conflict pyramid on a whiteboard or flipchart and ask the students for ideas to populate the chart. The students should be asked to justify why an actor is at Level 1, 2, or 3.

Key Message. The UN is generally deployed to conflict or post-conflict environment, where there is an existent threat to the local population. The conflict pyramid tool offers a framework for students to help them identify all relevant, influencing actors. Understanding the conflict pyramid is an effective framework to identify relevant actors and understands how to implement it.

The conflict pyramid offers a framework that acts as an aide to identifying relevant actors. The pyramid suggests that there are actors that have a strategic impact on a conflict. These are Level one actors. Typically, these actors are strong military actors or leaders, well known political leaders, government representatives, leaders of ethnic or tribal groups and/or international organisations. These actors have the capacity to influence the national-level situation or the situation within an entire UN Mission AO. It goes without saying that the MPKI cell needs to understand these personalities and conduct an actor evaluation on them;

Level two actors are generally found at the sub-national level. They may be actors, for example, that only impact a specific UN sector. These level two actors have a less obvious national impact, but are generally linked to level one actors and, as such, can be influenced by them. Examples include regional tribal, religious or ethnic group leaders; the heads of NGOs; regional armed groups; terrorist groups; regional military formations and leaders; regional political organisations. Level two relevant actors have often linked to both level one and three actors but can generally only influence at the regional level.

Level three actors are found at the local level. They have generally linked to level two actors, and less often to level one actors. They can impact the local operating environment. Examples of such actors are local leaders (IDP camp, a POC site, a local wise man), influential people such as local religious leaders, doctors, tribal chiefs, and/or policemen.

Slide 8

Learning Activity

Time:
Approx. 10 minutes

Task:
- Identify the relevant actors (people / groups)
- Assign actors a location / position on the conflict pyramid

Hint:
Use ASCOPE PMESII tool

Interaction. This mini exercise should take place in class. Based on the Sector-level information that has been provided to the class in reading material, ask the students to identify the relevant actors in their respective AOs, and where these actors sit in the conflict pyramid. Have them report back to the class

Approx. Time. 10-15 minutes

Slide 9

This slide will help us go through the analysis process. We will go step by step.

Interaction. Give the students a template to highlight what is known about the actors they have identified. Ask the student to:

- *Collate and store the data on a PC in order to maintain corporate knowledge*

- *To structure what they know about actors, and to highlight what is not known*

- *Complete these templates from information that is stored on current and basic intelligence*

- *Take that known data and analyse it using the Positions, interests, needs, SWOT, and Centre of Gravity Analysis tools*

- *Identify what they do not know, or information gaps*

Slide 10
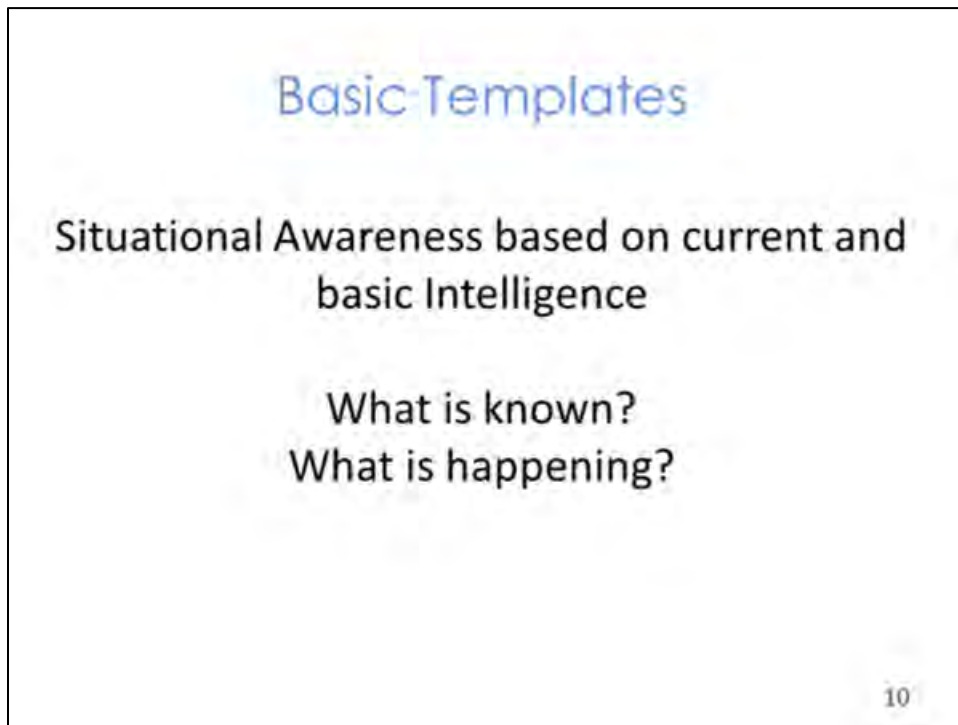
The information that populates these basic templates will be taken from what is already known. This information exists in basic and current intelligence databases.

Slide 11

This format is the UN method for systematically evaluating a threat actor in an Area of Operations. The acronym COWARD should be used and applied to the three-column assessment format. All threat actors in the UN AO should be examined/evaluated in this way. If you follow this process using the three-factor format, you will benefit from multiple insights (deductions) into the threat actor, which will all serve to enhance understanding.

The factors are the COWARD headings, that the deductions are the 'so what' for the UN, and the outputs are the actions to be taken. These can include, but are not limited to: identifying Items of High Importance (IHI), unknowns, threats to the UN, threats to civilians, threats to mandate etc.

Interaction. Asked the students what they consider capabilities to be. List these on a whiteboard. Capabilities can include armoured vehicles, artillery or indirect fire; anti- armoured vehicles; strength; communications; logistics; intelligence; operational security; the level of training; recruitment capabilities; propaganda. The list is endless.

Ask them to make some deductions on what they have listed. For example, if a threat actor has a high indirect fire capability then it can engage in stand-off

attacks, spotters may have to be located close to a UN base, the UN is vulnerable from a certain distance away.

An example of outputs, in this case, may include the following: sentries may be tasked with looking for spotters, the FOB will likely need bunker protection if the type of indirect fire asset that the threat actor has is unknown then that could become an information requirement (IR). The IR might be as follows 'what type of indirect fire assets does threat Actor A have?'.

Let's look at COWARD in more detail.

Organisation. The factors could be as follows: hierarchical like a conventional military force; it is important to examine such a force's Order of Battle to ascertain what kinds of units it uses (Brigade, Battalion, Company, platoon, section etc.), and how these units interact; look at how a conventional or unconventional force would organize for various types of operations; a cell-type structure or a network in the case of an unconventional threat actor. As an example, the types of deductions and outputs made in this case could be as follows: Factor – threat actor is organized in platoon-sized structures; deduction – this force needs to move through platoon-sized movement corridors; output – Information Requirements such as 'where is out FOB vulnerable to approach of a platoon-sized unit', this could become a Named Area of Interest (NAI).

Weapons. It is useful to list weapons such as HMG, MMG, LMG, sniper rifles, anti-armour, mines, indirect fire weapons, and small arms here. There will be some crossover with capability. Again, ask students to name one weapons system and progress through the three-column format. For example, if a threat actor has an anti-armour capability, it means that our convoys are vulnerable to attack, and Information requirement could, therefore, be to identify where the UN is vulnerable to such attacks on a particular patrol route, guidance to the commander or Operations cell might be to only use armoured vehicles while patrolling in areas there the threat group is known to operate.

Asymmetric Capabilities. We should look at what kind of unconventional approaches the threat group uses. Such things could include roadside bomb; IED capability (command wire or self-detonated); suicide bombers; VBIED; SVBIED; ambush etc.

Reinforcement Capability. Also, look at how quickly can the group reinforce while on operations and if the group can regain strength after operations or losses.

Doctrine. There will be some overlap with capabilities here, but it is more important that it is complete. You should look at how does the threat actor organize itself for defence, attack, or other forms of operations. Also, it is important to see how the threat actor organizes itself for asymmetric attacks. This should lead to a series of Information Requirements and tasks. For example, if the intelligence cell decides that a group tends to target the UN with IEDs before attacking with small arms, then an output could be 'where is the UN most vulnerable location to be attacked when patrolling', and the lead vehicle could be tasked with looking for IED ground sign, or covered areas from which threat group personnel could hide to launch a small-arms attack.

Slide 12

Now let us do a mini-Learning activity that will help reinforce your understanding of the COWARD framework, and how it is applied in the three-column format

Interaction. Divide students into groups arranged according to the sector they are assigned. Ask each group to go through factor, deduction, output process with one part of the COWARD headings. Example, group one takes Capability, group two takes Organisation, group three takes Weapons, etc.

Using a flip chart with factor, deduction, and output headings; you, the instructor, should be allocated to assist each group, particularly when it comes to listing deductions and outputs. After their group work has them report back to the class with their findings. It is important that each group also offers a deduction or a 'so what?'. Students should identify Items of High Importance to the threat group and identify some information requirements;

Total Approx. Time: 20-30 min

Slide 13

Key Message. The relevant actor template is used to store information on all relevant actors in the UN Area of Operations. It is important as it is a single form and can be handed over to subsequent deploying forces, thereby maintaining corporate knowledge. All MPKI Cells must maintain one.

This is a tool that helps maintain corporate knowledge, and that it is a living document. That is to say, that should be constantly updated as new information about the relevant actor is discovered. As you fill the template out, some detail may be missing. This missing information becomes an Information Requirement. Sentences highlighted in red are the product of more analytical approaches that will be taught later.

Naturally, there will be some detail that will overlap with the threat actor evaluation COWARD method. Look at the template and fill in what they know, and list what they do not know. The points that they do not know should be converted to IRs and sent to acquisition units or added to the IAP. You should maintain one template for a threat actor, and one for any other relevant actor, such as a political party or personality.

Slide 14

You should now realize that with a basic (using basic and current intelligence) knowledge of the relevant actors using the COWARD and relevant actor template, we can now move on to apply this knowledge to analytical tools to create greater understanding. This will help you to forecast threats; assess Courses of Action (COAs), and create a greater understanding of how the relevant actor will interact with the operating environment.

Slide 15
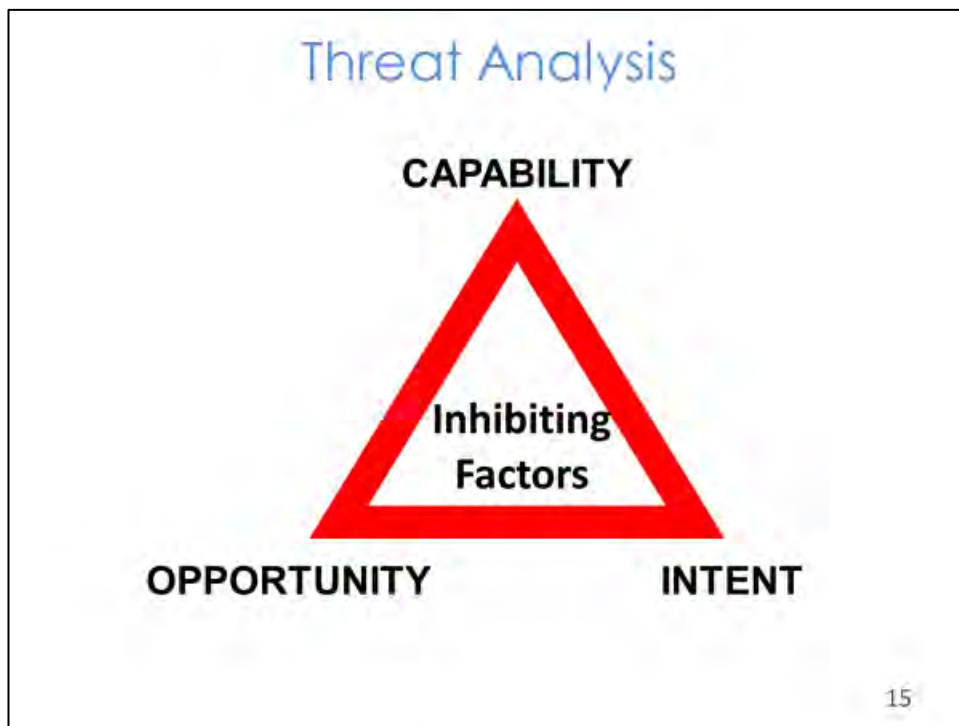
Here are a simple model and method to display the threat analysis.

Slide 16

Interaction. *Using a whiteboard or paper chart ask the students to comprise a capability, intent and opportunity list. Interactive as possible, ensuring all students participate. Encourage students to consider capability using the COWARD format.*

If need be, remind students of the following:

Capabilities include any factor that allows the threat group to act and includes: weapons, logistics capability, lines of resupply, finances, recruitment, training, support of other state or non-state actors, disposition, composition, reinforcement capability, asymmetric capabilities, and any other factors that allow the actor to take action.

Intent. Is what makes the actor do what it does (why it takes a certain action. What motivates it, what are its objectives, both military and political. The intent is towards the UN. Also, look at 'how does the UN harm or hinder the threat actor from carrying out its intent.

For example, in some post-conflict states, the UN acts as a stabilizing factor. For some threat actors, this is not considered a positive development. Therefore

they may seek to deter the UN from operating in the AO using their various capabilities.

The intent should be considered under the following headings: threat actor ideology (religious, ethnic, nationalist etc.); threat actor objectives, which can be financial (organized crime or terrorist groups), territorial (secession, control of certain areas etc.); threat actor supporters – what its constituents expect of it; threat actor narrative or strategic messaging – what does it say it wants or will do. The list goes on.

Opportunity. This is straightforward. The threat actor cannot act, even if it wants to, against the UN unless the UN operates within its area of operations, or in an area where the threat actor has the capability to act through its network.

An inhibiting factor. This is something which may cause the threat actor not to act, even though it has the capability, intent and opportunity to do so. An example of this could be that the material cost of acting against the UN may be too high, or that the UN is popular amongst the local population or is doing good and to act against it would cost the threat actor support. Another example is where an extremist actor chooses not to act against the UN as it would prompt an external intervention. This was the case in southern Syria where UNDOF operated. In that case, an extremist actor had the capability, the overall intent, and the opportunity to act against the UN, but chose not to as it feared the intervention of external actors, which would have destroyed it.

The next slide will show how this process can lead us to a mathematical evaluation of the level of threat that a threat actor poses.

Slide 17

Key Message. Commanders do not like evaluations that have no basis in fact. They prefer quantifiable data. MPKI personnel must understand that for their evaluations to have added weight. They must have an audit trail.

Using the factors for capability and intent, we must assign a number from 1-6, with 1 being low and 6 being very high for both. This is a very subjective process, but in most cases, evaluations should not vary too much.

An example let us use a UN mission deployed into an area controlled by the Islamic State to demonstrate to how the process works.

Threat equals capability multiplied by intent. For example, if a capability is 5 and intent is 5, then the Islamic State poses a threat of 25. This is high, and so the MPKI cell can state that the threat posed by the Islamic State to the UN is high. The MPKI cell also knows that the Islamic State can attack the UN because the UN is operating it's an area under its control.

However, now we must ask ourselves about inhibiting factors. Are there any reasons that the Islamic State might not attack the UN, considering the high threat it poses?

In any case, the threat is high, one cannot rely on inhibiting factors to mitigate it, and the threat must be mitigated, or at least presented to the commander so that he/she can make an informed operational decision. The commander can choose to accept, reject, avoid, or mitigate the risk.

The last item that should be considered is a likelihood. This is expressed using the language of likelihood shown on the screen. Again, this is highly subjective, but this is where opportunity and inhibiting factors can inform the assessment process. For example, while the threat posed by a threat actor may be high, a lack of opportunity or inhibiting factors may combine to make an attack 'unlikely'. Conversely, if the threat actor presents a high threat, if the threat actor can attack the UN, and if there are few or no inhibiting factors then the threat is high, and the likelihood of an attack could be very high.

The next slide shows how the threat analysis fits into mission planning.

Slide 18
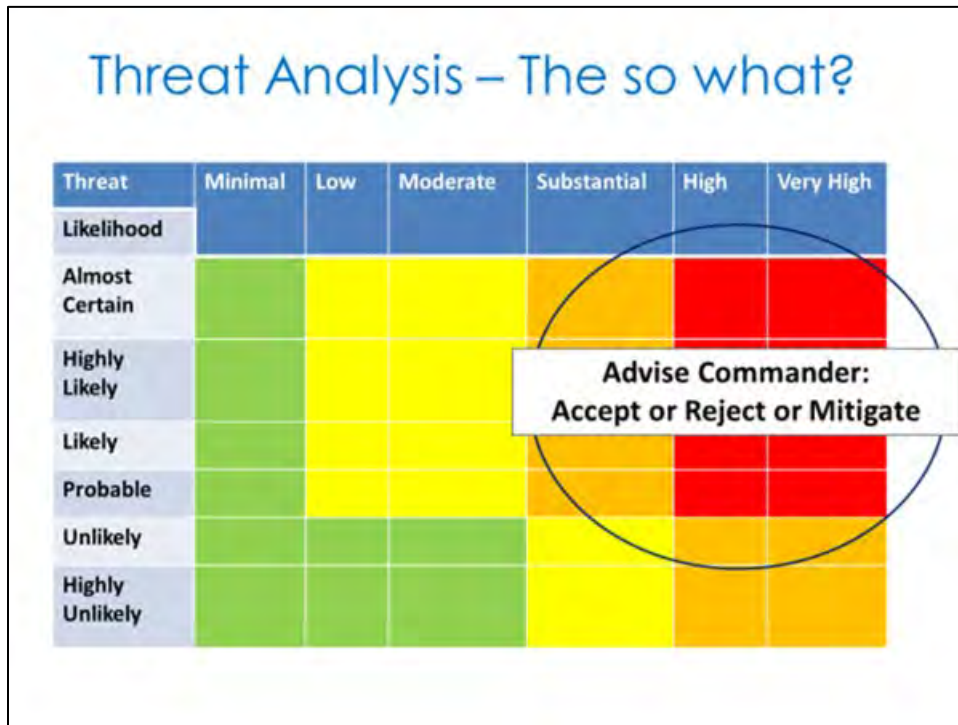
Any threat that is SUBSTANTIAL or GREATER, with a likelihood higher than 'probable' must be mitigated. It is important that we inform Operational planners that a threat group presents a SUBSTANTIAL or above threat to the UN or to the civilian population.

The threat score combined with the likelihood of attack s an overall risk rating. This slide shows a graph as a traditional X/Y scale with Likelihood shown on the X-axis and threat shown on the Y-axis. If the threat is Moderate and the likelihood is probable, then the overall score falls into the yellow area. Operations personnel should be informed of this.

Similarly, is the threat being Substantial, and the likelihood of an attack is almost certain, the overall risk falls into the red zone. Operations personnel should be warned.

Slide 19

If we understand how to accurately assess threat using an auditable process. We can better understand how to assess the likelihood of a threat and can express this to a commander.

Interaction. Divided students into syndicate groups by their sectors. Ask the students to:

- *Use the threat evaluation tool*
- *Considering intent and capability to assess the threat*
- *List the threat actors that present a threat to the UN*
- *Assess the likelihood of this group attacking the UN*
- *Justify this*
- *Chart where the threat actor is on the threat / likelihood (Risk) matrix*
- *Explain their next action would be- example, the requirement on how we might mitigate the threat*
- *Using a whiteboard or paper chart*

Approx. Time: 15-20 min.

Slide 20

Analytical Tools and
Approaches

We will now move on to use more advanced analytical tools for actor evaluation. The students should be reminded that the SWOT, PIN, and COG analysis will provide answers which will help to populate their Course of Action (COA) boards, and considerations.

Slide 21

Positions, Interests, Needs Analysis

- **Positions-** stance taken by a conflict party, articulated in media or from official communications
- **Interests-** of a conflict party are what they need to meet their needs
- **Needs-** goals pursued by an individual or group to survive (Objective and Subjective)
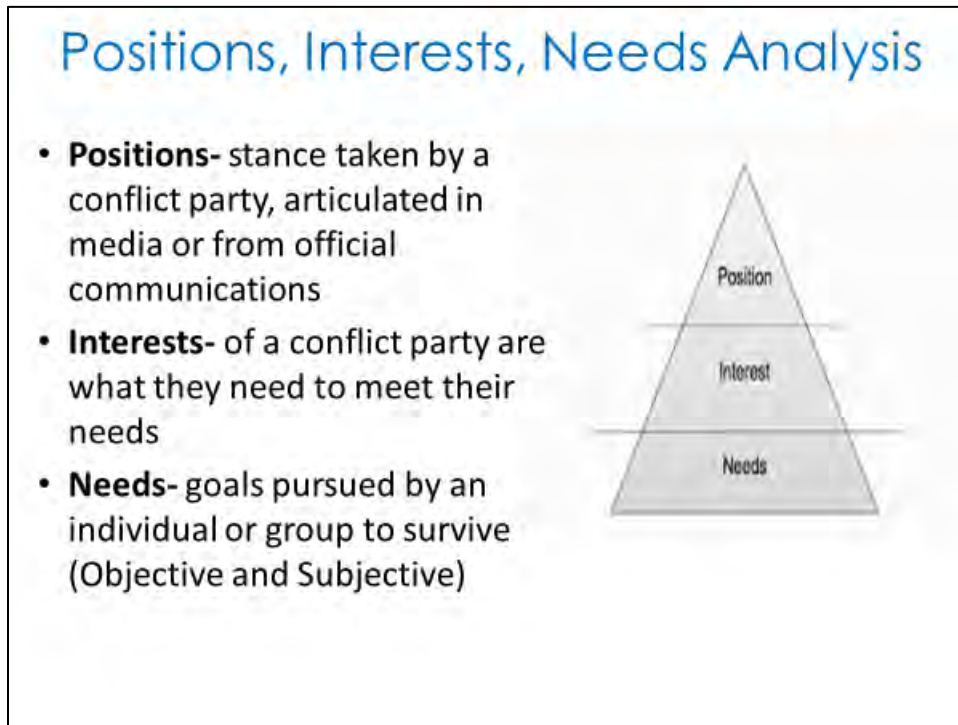
Key message: Working out the position, interests, and needs (PIN) of an actor deepens understanding. It will also help inform deliberations about how any relevant actor will react to a UN presence, operation, or change to the operating environment. A thorough (PIN) analysis can help the analyst understand how a UN operation or presence can help or hinder the relevant actor.

It is important to understand why a relevant actor adopts a certain position, what the relevant actor needs, and what its interests are. This will allow us to identify how the UN may have a positive or negative impact on the relevant actor and how the relevant actor may react.

This will help us decide on the course of action that a relevant actor may choose when faced with a UN operation, deployment, or any other change to the operational environment.

This can have serious operational repercussions. For example, if the UN deploys to a border post, it may undermine an actor's ability to raise funds by collecting taxes at illegal checkpoints, or it may prevent the actor from engaging in smuggling activity. This may adversely affect their 'need' for money and could lead to a violent course of action being taken against the UN.

Position, this is the public stance taken by the relevant actor. Generally, this is the relevant actor's stated mission. The relevant actor, in this case, could be an NGO with a mission of 'inoculating all children under the age of 5 against Ebola'. Similarly, it could be the Islamic State stating that it wants to 'create an Islamic Caliphate and to unite the Ummah'.

Interest. This is what the relevant actor are the things an actor needs to have in order to meet their objective and subjective needs. In the examples above, it is in the interests of the NGO to have safe and secure access to areas where children live, to have access to enough quantities of drugs, and to have a positive PR campaign about its operations. There are many more examples of what is in this NGO's interests. In the example of the Islamic State, it is in its interests to have, inter alia: a land to govern; people who can govern; finances to run a state; the ability to extract resources; an army; a police force etc.

Needs. This is what the relevant actor cannot live without. Generally, such things are food, water, shelter. These are objective needs and are things that everyone needs. However, there are also subjective needs. These are things that the relevant actor believes it cannot live without. In the example of the Islamic State, objective needs would be food, water, shelter, and subjective needs might be religious legitimacy; sharia law etc.

The key point is that every relevant actor has a position, has interests, and has needs.

A useful way to conduct a successful PIN analysis is to start with the relevant actor's mission statement. Sometimes this will be unclear and needs to be assessed on the basis of what its leaders say, and the group's strategic messaging.

This will allow the MPKI cell to work out the relevant actor's position - generally, this can be found in open sources. It is then useful to move straight to working out the relevant actor's objective and subjective needs.

Work out what interests it will have that will enable them to bridge the resource gap to guarantee their needs. For example, in order to assure food for its people, the Islamic State needs land on which to grow food. This means it is its interests to control land; to control water sources to grow crops; to have access to people to farm; to have roads; to have markets; to have access to a monetary system etc. The Islamic State also needs shelter; therefore, it is in its interests to have builders; town planners; raw materials etc. The list quickly becomes very long.

The 'so what' in this case is that if you can identify the interests and needs of a relevant actor, then you can identify how a UN presence can help or harm that actor. This will go a long way to creating a deeper understanding as to how these actors will react to a UN presence. This should inform mission planning and relevant actor course of action development.

For example, if an NGO requires access to a local population in an insecure part of the world, then an armed UN presence as an escort is in their interests. It helps the NGO. The NGO is, therefore, likely to have a positive perception of the UN.

Conversely, if a threat actor needs illegal mining revenues as a source of income, and the UN builds a FOB close by, then this is likely to adversely impact the group's financial interest. Naturally then, this group is likely to have an unfavourable perception of the UN.

Slide 22
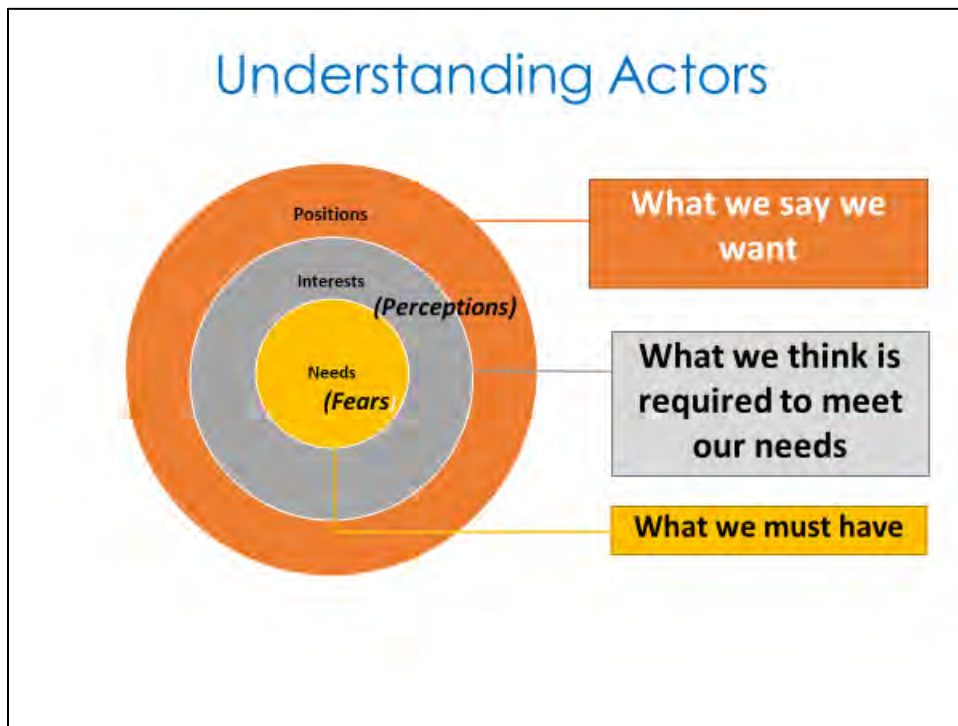
This slide further simplifies the PIN concept.

Slide 23

PIN Analysis

Exercise: Carry out a PIN Analysis of the Islamic State.

Step 1 (List primary Factors)

    What is the threat actor's position?
    What are the threat actor's interests?
    What are the threat actor's needs?

Step 2 – Apply the 3 Column analytical framework (so what?).

Step 3 - Outputs:

    How will these factors affect how the group will react to a UN presence?
    How will these factors affect Threat Group objectives (End state)?
    How will these factors affect how it will choose to operate (Method)?

Interaction. Ask the class the following questions and facilitate discussion:

- *What is the public position of the Islamic State is; the response should generally align*

- *What does the Islamic State need to be viable: responses should include objective needs: food, shelter, water, security, and subjective needs: money, Islamic faith, people, soldiers, etc.*

- *What are the interests of the Islamic State; interests should include: having religious legitimacy, controlling borders, sources of revenue, effective narratives and recruitment strategy*

- *Use the knowledge gleaned from this PIN analysis to develop the selection of factors for the three-column analytical format. (This will give them a series of deductions or so-what's?)*

Facilitate the process. Guide / Coach to make deductions as they pertain to the UN, to the actor under consideration, and to the local population. This will enhance understanding.

For example, if the factor is the Islamic State needs an effective recruitment strategy, deductions could include: the Islamic State needs access to media channels; the Islamic State needs access to the internet; the Islamic State is vulnerable to a counter-narrative etc.

Ultimately, this process should enhance the students' understanding of any threat actor and how these factors could inform its chosen course of action.

Approx. The time allowed: 15-20 minutes

Slide 24
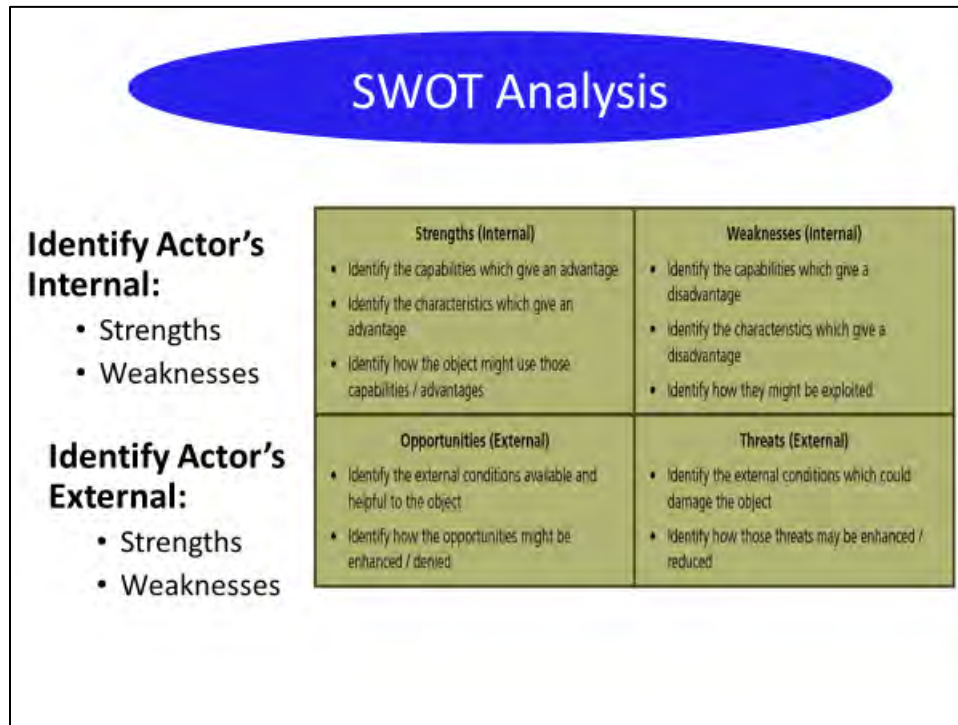
Key Message. This analytical tool is also designed to gain a deeper understanding of a relevant actor. It should be used to identify how the UN can help, in the case of a positive actor, or hinder, in the case of a threat or otherwise negative actor.

It is important to note that as SWOT factors are listed, they are analysed d using the three-column format. This is to ensure that students move through the process in a systematic manner, always asking themselves what a SWOT factor means for the relevant actor, its COA selection, and for the UN.

☞ *Note to Instructor. As each term is explained, the instructor should stand at a whiteboard or flip chart and ask for examples of each term as they might apply to a threat actor and to a non-threat actor. This is important as the student must become accustomed to assessing all actors in the operating environment.*

Strength: A strength is internal to the relevant actor. This is a capability of characteristic that gives a relevant actor strength. Strengths can be, among other things, diplomatic, political, military and security, economic, and social. It is important that students do not consider strengths only through the lens of security.

In the case of a non-threat actor such as an NGO, a strength may be a capable workforce, a good relationship with the community, steady funding, corporate knowledge etc. In the case of a threat actor, it may be a compelling anti-government

narrative, finances, asymmetric capability, a strong recruitment base, internal lines of supply, access to weapons. Students should focus on these strengths and should assess how the relevant actor uses them to its advantage.

A key point here is that a relevant actor is unlikely to act in a manner that does not align with its strengths. For example, an NGO that does not have strong skills in disease prevention is unlikely to engage in an anti-Ebola vaccination program. Similarly, a threat actor that has high asymmetric capabilities is unlikely to engage in a conventional all-arms attack on a UN FOB. This is the critical link between analyzing a relevant actor's strengths and its COA selection process.

The second key point is that if the UN threatens a relevant actor's strength through its operations, then that actor may choose to act against the UN. This is the second link to understanding a COA that this actor may choose to take.

Identifying a strength can also inform UN planning. For example, the UN could deliberately take action to undermine the strengths of a threat actor, or it could plan its operations so that the UN does not make itself vulnerable by allowing the threat actor to use its greatest strengths. For example, if a threat actor has a high-level of asymmetric capability, the UN may choose to use Unmanned Aerial Systems (UAS) to surveil a route to ensure that a complex attack is not being prepared on the planned convoy route.

Weakness: A weakness is also internal to the relevant actor. This is a lack of a capability or characteristic that disadvantages the relevant actor. Weaknesses can be, among other things, diplomatic, political, military and security, economic, and social. It is important that students do not consider weaknesses only through the lens of security.

In the case of a non-threat actor such as an NGO, this could be not having employees that speak the local language, not having access to all-terrain vehicles, not having internet connectivity to conduct its business, having a poor understanding of the local environment. In the case of a threat actor, it could be not having the support of the local population, of not being able to raise funds, or of not having an IED manufacturing capacity.

Once again, the link to COA development is twofold: if the relevant actor does not have a capability, then it is unlikely to act in such a way that it would rely on that missing capability. A threat actor without an IED manufacturing capability is unlikely to choose to attack a UN convoy using this approach; moreover, if the UN acts in such a way as to exploit a weakness, then an actor might choose to act against the UN.

Identifying a weakness can also inform UN planning. If the actor is a positive influence, then the UN could decide to help the actor overcome its weaknesses through, for example, a CIMIC project. Similarly, if a threat actor has a weakness, the UN may wish to exploit this weakness through its operations.

Opportunity: Opportunities are external factors or conditions that are favourable to a relevant actor. Opportunities can be, among other things, diplomatic, political, military and security, economic, and social. It is important that students do not consider opportunities only through the lens of security.

Examples of opportunities to a non-threat actor such as a political leader could be a change regional/international security or political environment leading to support for a new policy, stability in a neighbouring country that allows for greater trade, a growing economy. For a threat, actor opportunity could include a deteriorating economic environment an unpopular government policy which could facilitate recruitment or radicalization, or the possibility of an alliance with other groups.

The MPKI cell should examine the opportunities available to relevant actors as an indicator as to how they could influence the actor to act in a certain way. Once again, it is important to stress that opportunities will affect COA selection of all actors.

The MPKI cell should also consider how opportunities available to relevant actors can inform UN decision making and planning. The MPKI cell should consider how a UN plan would undermine a relevant actor's ability to exploit an opportunity. If, for example, the UN denies a threat actor an opportunity the threat actor could choose to act against the UN. The UN may also decide that it wants to actively undermine a threat actor's opportunities, and it is therefore important that it understands what these are. For example, if security breaks down in a neighbouring country, then the UN may identify the resulting porous borders to be an opportunity for a threat actor. The UN may decide that it will reinforce its positions or enhance patrolling in these areas as a result.

Threats: Threats are external factors or conditions that are unfavourable to a relevant actor. Threats can be, among other things, diplomatic, political, military and security, economic, and social. It is important that students do not consider threats only through the lens of security.

Examples of threats to a non-threat actor such as a political leader could be an unfavourable change regional/international security or political environment leading to reduced support for a new policy, instability in a neighbouring country that reduces trade, or a contracting economy. For a threat actor threats could include a UN deployment in its area of operations, new security policies, a national government or army that is increasing in strength or popularity.

The MPKI cell should examine the threats to relevant actors as an indicator as to how they could influence the actor to act in a certain way. Once again, it is important to stress that threats will affect COA selection of all actors.

The MPKI cell should also consider how threats to relevant actors can inform UN decision making and planning. The MPKI cell should consider how a UN plan would exacerbate the threats to a threat actor. Similarly, the UN may consider protecting a positive, relevant actor from an external threat.

Slide 25

SWOT Analysis

Exercise:
Conduct a SWOT Analysis of the primary threat actor in your Sector.

Step 1 (List primary Factors)
   What are its strengths (internal)?
   What are its weaknesses (internal)?
   What are threats to the NGO (external)?
   What are the opportunities (external)?

Step 2 – Apply the 3 Column analytical framework (so what?).

Step 3 - Outputs:
   How will these factors affect how the group reacts to the UN?
   How will these factors affect Threat Group objectives (End state)?
   How will these factors affect how it will choose to operate (Method)?

Key Message. The SWOT analysis is to be applied to the three-column format. This allows the students to not only identify the SWOT factors, but also to draw a 'so what' for both UN operations and planning, and relevant actor COA selection.

Interaction.

- *Break the students into their syndicate groups.*

- *Ask the students to list the SWOT of the main threat actor in their Sector. When all SWOTs are listed, they become factors in the three-column analytical framework*

- *Ask the students after listing the factor is make a deduction*

- *Remind the students that deductions should be made based on what the factor means for the UN, for the actor under consideration, and for the local population*

- *Ask students to evaluate how this threat actor is likely to react to a UN convoy operating in its AOR*

- *Ask students to develop a list of unknowns or IRs*

- *Remind the students that their deductions lead to outputs and can be included in Information Requirements, planning guidance or considerations for UN COA selection. It is important that these observations are given to the U/G 3 section or reach the commander for consideration*

Resources: Whiteboard or flipchart, pens. One instructor per group to guide the process.

The time allowed is about 30 minutes, with 10 minutes to brief/discuss.

Slide 26

Centre of Gravity Analysis

What is a Center of Gravity?
Gives an actor its moral, physical strength, will to act, freedom of action

Levels of Center of Gravity

Strategic- Diplomatic support, Alliances

Operational- a specific assets, military, economic etc

So what:
- Break down an Actor's characteristics to undermine or strengthen
- How an actor behaves to maintain CC, to gain CRs, to mitigate CVs
  → Link to COA development

	Entity's aim/ objectives	
Centre of Gravity		Critical Capabilities
Critical Vulnerabilities		Critical Requirements
	Conclusions	

Key Message. A centre of gravity (COG) analysis is an important part of evaluating what is important to a relevant actor. A relevant actor's COG, what that COG allows the actor to do, what the actor must do to maintain it, and how it is vulnerable is vitally important in evaluating how that actor will act (COA) or react in theatre. An actor must act to defend its COG, or it cannot achieve its mission or objectives.

The COG is not always a tangible thing. For example, a strategic COG could easily be the political support of an alliance or bloc. A COG does not have to be linked to resources or capabilities.

A COG can just as easily be something that gives an actor the moral strength, will, and freedom to act. The support of the UNSC could be a COG for an actor, depending on the circumstances of your evaluation. Similarly, a compelling narrative or strategic message could be the COG of a threat group. Using the example of the Islamic State, one could posit that its COG was a perception of religious legitimacy among its adherents.

A COG can also be something tangible, which gives a relevant actor the physical strength to act. However, this is most seen at the operational level and is often linked to specific assets. For example, if country A was beset by sanctions and could not finance its war effort or import arms, having a country that was willing to help country A undermine the sanctions regime could be an operational level COG.

Understanding the COG is key to determining what is most important to a relevant actor. Once more, this can inform UN mission planning. The UN can act to help or undermine a relevant actor's COG.

Moreover, if UN operations threaten the COG of a relevant actor, it is almost certain that it will act against the UN. This will help our assessment of a relevant actor's COA.

MPKIO should be able to use the tool shown on the slide and plot the COG.

Slide 27

A COG cannot be evaluated in isolation, or as the first step in actor evaluation. Moreover, it is impossible for someone with no information or knowledge of a relevant actor, and its operating environment to work out its strategic and/or operational COG. This is why the COG is one of the final steps in actor evaluation and is only conducted after the human, information and physical terrain have been evaluated in the analysis of the operating environment, and after COWARD, PIN, and SWOT tools have been used in actor evaluation.

Critical vulnerability – how is the COG vulnerable? This is important as it could allow the UN to identify how to undermine a threat actor. It is also something that the UN could avoid doing if the actor is a positive influence on the operating environment. For example, if a local political leader facilitates a calm environment in his area, the UN should identify his COG and should attempt to avoid operations that would exacerbate his/her COG's critical vulnerabilities.

Critical requirements – what does the actor need to maintain its COG? What resources, freedoms or conditions does it need to maintain? It is important for the UN to understand this as a threat actor will seek to act to protect these critical requirements if UN operations or any other actor threatens them. For example, if an actor requires control of an artisanal mine to maintain its COG, it is likely to fight to protect it. Once again, this will inform its COA decision making process.

Slide 28

COG Excercise

Exercise: COG Analysis of the main threat actor in your Sector AO.

What is its Operational Center of Gravity?

What are the:

Critical Capability - Method/COA choice)

Critical Requirements - Objectives / Mission / End state

Critical Vulnerability (Method)

Apply the 3-column analytical framework?

Interaction. The main learning outcome here is for students to develop a full COG evaluation and explain its links to System Integration and COA development. Break the students into their syndicate groups. Have the groups do the following:

- *Considers one threat actor in its AO*

- *Based on what is known about the operating environment, go through the COG evaluation process as outlined in the previous slide*

- *Brainstorm ideas for the COG and label*

- *The time allowed for COG Analysis: 30 minutes, 10 minutes to brief/discuss*

- *List operational and strategic COG*

- *Select an operational-level COG*

- *Decide what COG allows the threat actor to do – critical capabilities*

- *Explain what makes that COG vulnerable – critical vulnerabilities*

- *Describe the actor needs to ensure that the COG remains viable – critical requirements*

- *Place relevant information into the factor column of the three-column format*

- *Make deductions as to what these factors mean for the UN, for the threat actor, and for the civilian population*

- *Describe how these factors influence how or why the threat actor could choose to act against the UN*

Slide 29
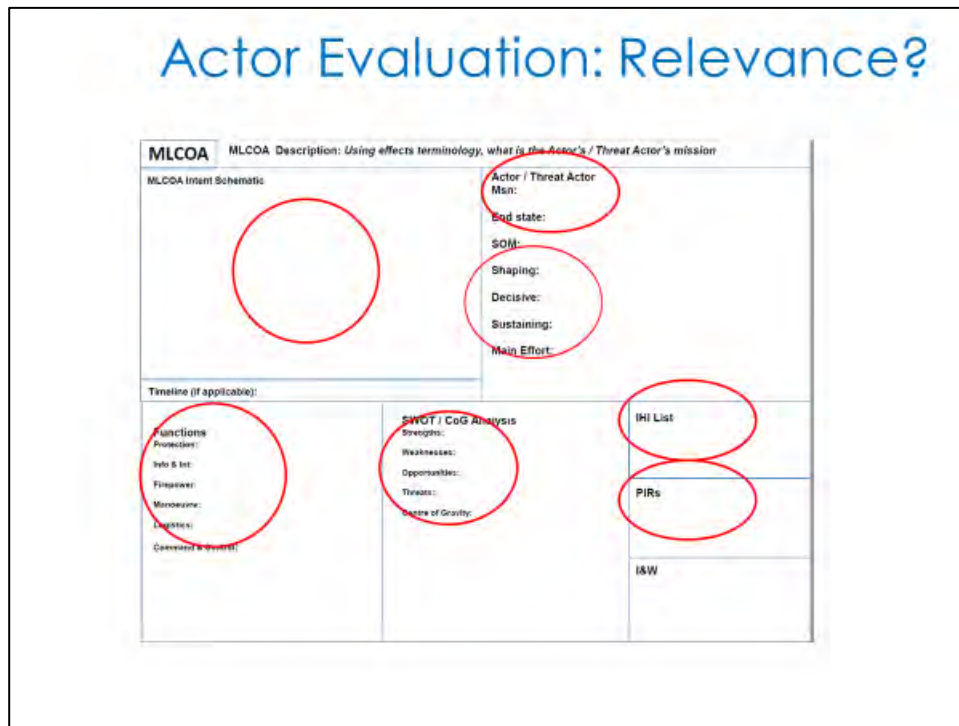
This slide shows actor relevance.

- Items of High Importance. These come from the COWARD evaluation and the critical requirements of COA evaluation

- PIRs. These are drawn from every analytical process

- Mission and end state. These are drawn from the intent evaluation. What the actor wants to achieve. This can also be drawn from the PIN analysis. What is in the actor's interest, and what does the actor need

- SWOT and COG evaluation. These are drawn from the COG and SWOT analytical tools

- Combat functions or functions for a non-threat actor. These are drawn from the actor's Order of Battle, from its asymmetric capabilities in the COWARD format. Information can also come from the critical capabilities from the COG evaluation, and from the strengths evaluated in the SWOT analysis

- The Most Likely and Most Dangerous COA schematic comes from combining the MPKI cell's knowledge of the relevant actor, and how the actor is likely to interact with the physical, human and information terrain. In short, this schematic is a reduced System Integration or threat integration PICINTSUM

Slide 30

Take Away

- There are several tools and templates to help you conduct actor analysis

- COWARD / 3 column format are useful tools

- Understanding actor's capability, intent, opportunities and inhibiting factors will assist the analysist

- COG analysis is a useful tool in better understanding of actors

Summary

Here are the key messages of this lesson. Everything that we have done in this lesson informs the MPKI cell's understanding of a relevant actors most likely/most dangerous COA.

Lesson
3.5h

AOE-Situation Integration and COA Development

The Lesson

Starting the Lesson

The Situation Integration phase is the culmination of the AOE process in which the results of the Operational Environment Evaluation and the Actor Evaluation are integrated to develop probable Actor Courses of Action (ACOAs) and to identify areas and activities (Named Areas of Interest)that can confirm or deny an actor's intent to pursue one or other ACOA. Situation Integration also identifies areas and activities (Target Areas of Interest) where it may be possible for the UN Force to achieve a desired outcome or effect and the Decision Points – in time and space – at which the UN Commander must decide to act in order to achieve the desired outcome.

The products of the Situation Integration phase – especially the Actor Courses of Action (ACOAs) feed directly into the UN Military Decision-Making Process (MDMP). Therefore, it is important that the students fully understand this phase of the AOE process and are able to identify the Most Likely ACOA (MLACOA) for each relevant actor in the UN Force's Area of Operations (AO) and the Most Dangerous ACOA (MDACOA) for each hostile (threat) actor in its AO. If it is not possible due to lack of time for the students to produce all the products resulting from Situation Integration during this class, the following adaptations may be made:

- Interactive activities may be omitted. The instructor presents the answers that should have been given by the students as examples to reinforce the slide message.
- The students should be allowed whatever time is available during the lesson to begin development of each product – i.e. to produce a quick, rough and incomplete draft or sketch – to ensure that they understand the process and the contents of the product.
- Further development and refinement of these products may – if possible – be assigned as "homework"
- Time and instructor support should be allocated for review and further development of these Situation Integration products during the TTX

Slide 1

The key point of this lesson is to demonstrate the logical links between the Analysis of the Operating Environment and Actor Evaluation with the development of courses of action.

Slide 2
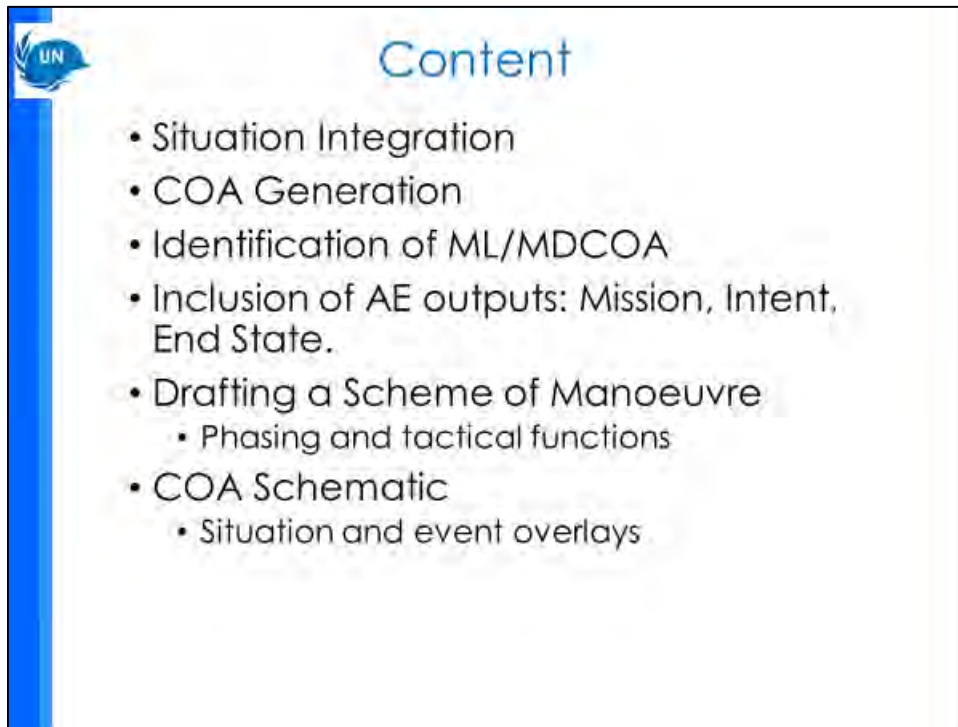
We will cover the following topics during this lesson:

- COA generation – how we generate multiple, mission-specific COAs, and use the FACES (Feasible, acceptable, complete, exclusive, suitable) criteria to identify true COAs

- How we select COAs using the COA scoring tool to identify ML and MDCOA

- How we develop the COAs to provide a mission-specific assessment of Actor's Intent and End state

- How we 'tell the story' of the Actor's COA through drafting a scheme of manoeuvre. How this is enhanced through deeper analysis and relating Actor's TTPs and capabilities to the physical terrain

- How we brief that analysis – all the outcomes from Situation Integration and the graphical representation in order to provide a simple briefing tool

- Highlight the two outputs required for the COA schematic

Slide 3

Let's review the Learning Outcomes for this lesson. At the end of this lesson, you should be able to perform the following actions:

- Explain the linkage between the Terrains (physical, human and information), Actor Evaluation and the development of COAs
- Explain how the FACES criteria are used to assess COAs and identify ML and MD
- Explain the difference between NAI and TAI and how they facilitate the confirmation of an actor COA
- Explain what is depicted on a COA board

Slide 4

Phase 3 - Situation Integration

- Fuses results from AOE and Actor Evaluation (Phase 1 and 2)
- Identification how the operating environment shapes actor capabilities and TTPs
- Relates capabilities, intentions, and TTPs to the ground enabling the assessment of Actor Courses of Action (ACOA)
- Most Likely and Most Dangerous ACOA
- Mission specific

Key Message. Situation Integration is the final phase of analysis. It fuses phases 1 and 2 to identify actor courses of action that will affect our mission.

Situation integration fuses all the analysis from phases one and two. It enables the intelligence staff to assess how the actor will operate – a predictive assessment through the identification of most likely and most dangerous courses of action for relevant actors. Reinforce the lesson that situation integration has to be mission-specific.

Slide 5
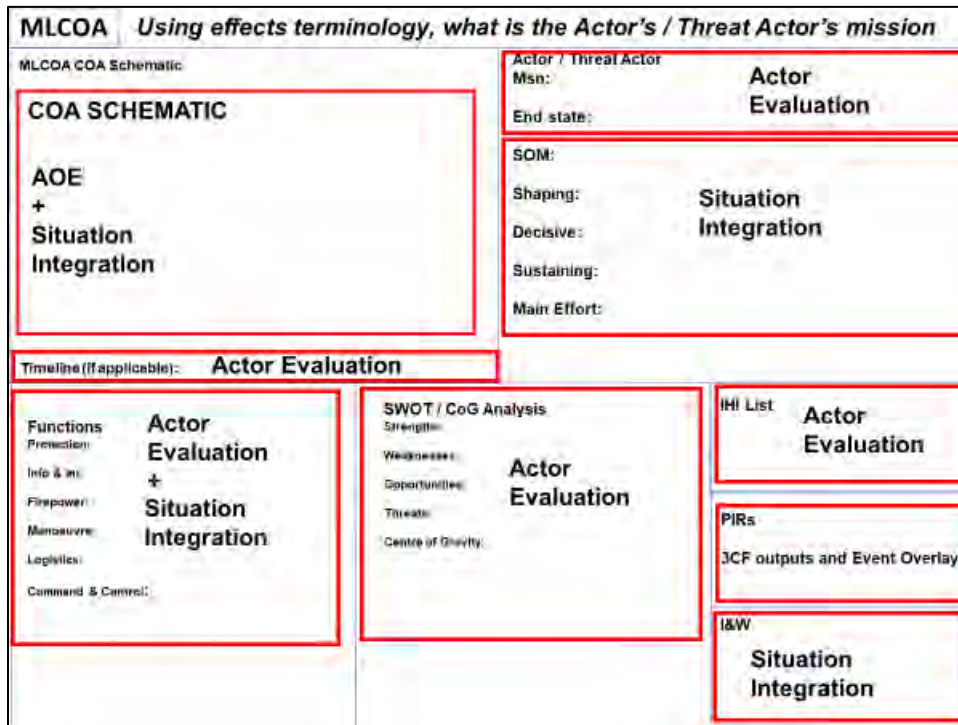
This slide is indicative of the current COA board (used in briefing the situation integration element of the Phase One Brief. These must be created for both Most Likely and Most Dangerous COAs.

Interaction. Ask the students what they can already complete on this board, based on the work they have done to date? Responses include all Actor Evaluation detail. The situation integration is the combination of the Actor Evaluation and the Analysis of the Operating Environment.

Slide 6

Situation Integration: Context

- Nothing in this presentation relates to the scenario you have been given.
- The UN mission as the basis for this Situation Integration is the **UN force has been tasked to establish a TOB south of a WALESI.**
- Situation Integration is always mission specific.
- Remember that your are learning an analytical process that can be used at all levels. It is scalable from Strategic to Tactical level planning.
- This process is about the fusion of all the analysis and situating it in time and space.

The mission for this AOE is UN force being tasked to establish a TOB south of WALESI. This should situate their subsequent analysis. The tools and processes they are being taught are scalable, i.e. and can be used at the strategic, operation and tactical levels. This process is about situating the analysis within time and space.

Slide 7
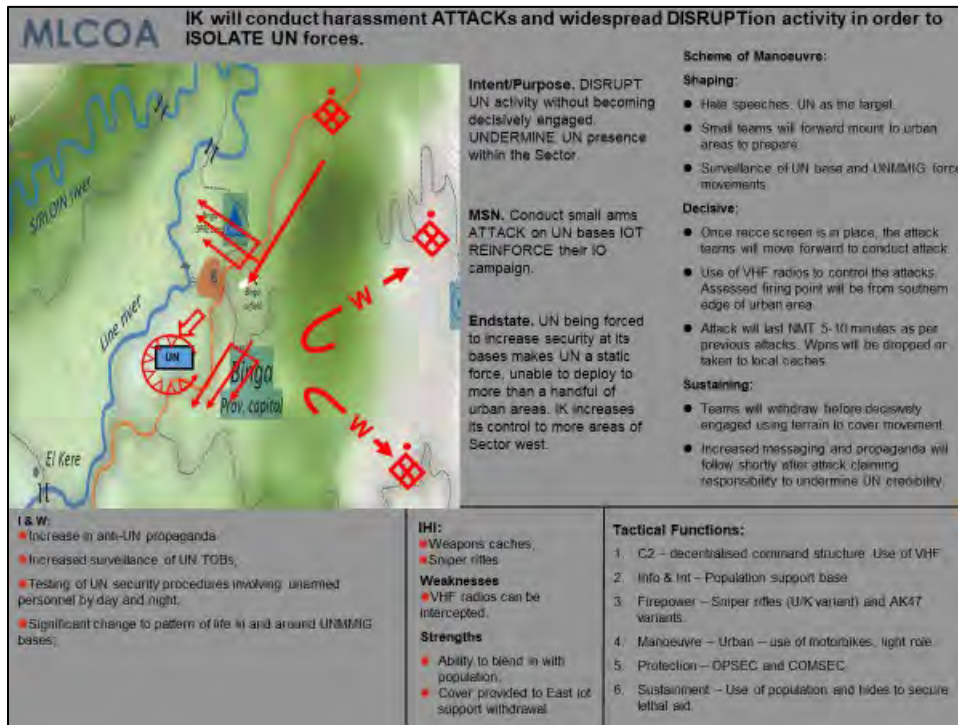
this slide is an example of a completed COA board. This is what your product should look like to achieve at the end of the lesson.

Slide 8
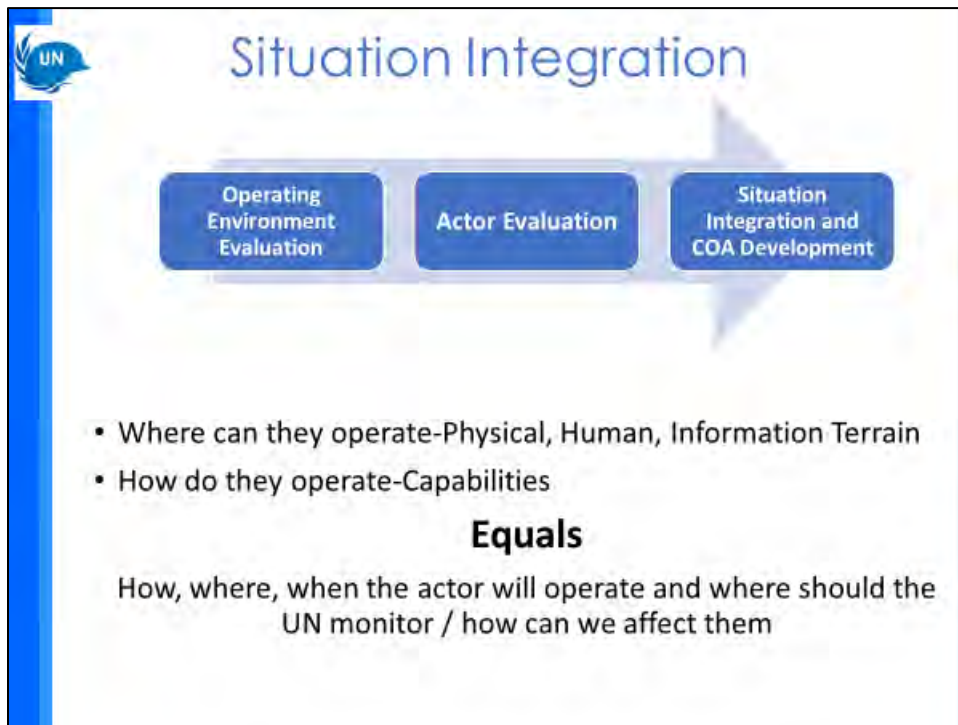
This slide highlights the 'flow' of the processes in order to get to situation integration.

Slide 9

The key outputs from situation integration are:

- An assessed actor intent and end state – developed from Actor Evaluation to be more mission-specific.

- An assess actor scheme of manoeuvre. How will the Actor seek to enact their intent and achieve their mission-specific end state?

- The production of two COA schematics and two COA boards.

- Remember that there are some golden thread products that will assist in a briefing later – MPKI support to MDMP.

It will allow the MPKI staff to identify IRs and remind the students to update their IAPs.

Slide 10

Interaction. Why do we need Actor Courses of Action? Responses here may include: by predicting the way an actor will behave in a given set of conditions (the operational environment), in a particular set of circumstances (the UN mission), within that actor's capability set, we can better prepare our personnel to plan a response.

Why do we focus on all relevant actors rather than just threat actors? In an in-extremis situation, we should prioritize threat actors as they can have a profound impact on the mission mandate. However, the COAs of many other actors are also important. For example, a political or tribal leader can influence the local population to behave or interact with the UN. This can lead to positive or negative outcomes for the UN. With advance warning, the UN MPKI cell hopes to avoid negative outcomes.

How can we help the Commander and his/her staff with Actor COAs? They assure that the identified threat can be mitigated. They inform operational planning for mission mandated tasks. They can identify problems before they occur. They help the commander priorities limited UN resources. For example, if the MPKI cell identifies that a population group is at risk from a threat actor, he/she can deploy protective forces to the area, ensuring that patrols are not sent to low-risk areas instead.

What kind of information should a COA contain? At a minimum, the actor mission, intent, scheme of manoeuvre and desired end-state.

Slide 11

ACOA generation is the key output from AOE. In briefing the commander, through the P1B in the MDMP process, the MPKI staff can provide the commander with a detailed understanding of how the relevant actors will affect their mission and mandate.

In doing so, it will enable the commander to prioritize scarce resources and assets.

It will enable the commander in their planning. If they plan to mitigate the threats and risks posed by the ML and MD COAs, then it will provide an initial steer for mission planning and contingency planning.

Slide 12

More than two COAs exist. Through COA development, the MPKI staff should identify many potential COAs. Those that do not meet the FACES criteria should be discounted. The remaining COAs should then be assessed using the impact and capability criteria to identify the ML and MDCOAs. The ML and MDCOAs should then be developed in greater detail.

Slide 13
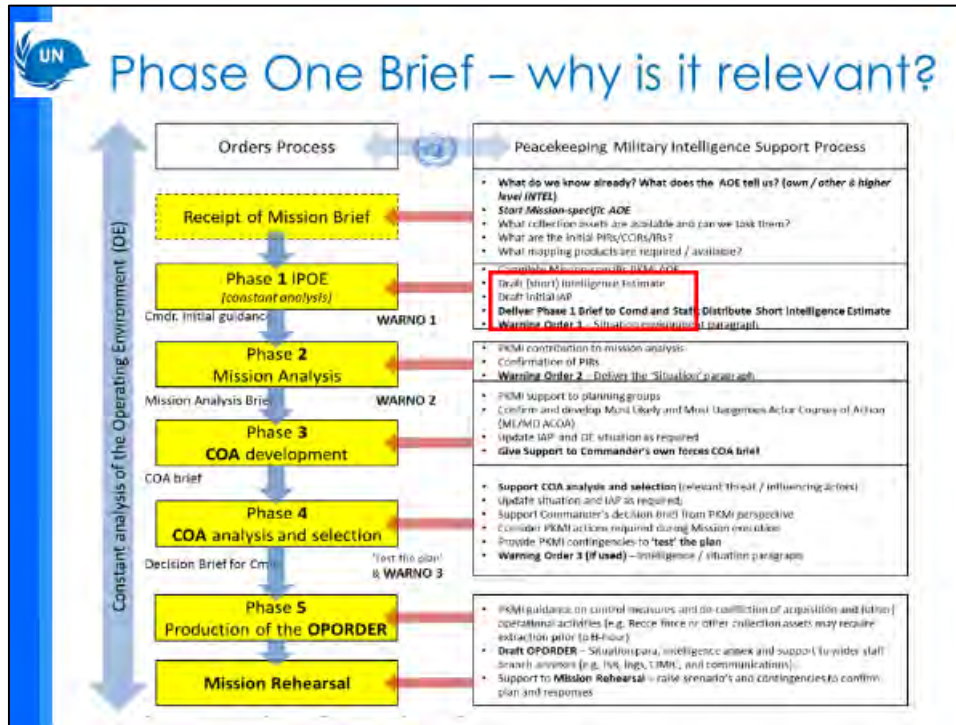
This slide highlights the relevance of the Phase One Brief (P1B). In conducting detailed analysis and briefing it to the commander, you can situate the planning staff to the operating environment and the relevant actors. In addition, you will provide an assessment of how those actors will look to affect the UN mission and therefore greatly assist the UN staff throughout the remainder of the planning process.

Slide 14

During the COA identification process, several potential COAs will be identified.

Analysts can use several tools in order to assist in the identification of potential COAs. Tools that could be used are listed on the slide. Students should be reminded that more tools exist (e.g. cone of plausibility) and can be applied when the MPKI staff have time.

The identified COAs are then subjected to the FACES criteria with those COAs that don't meet all the criteria being discounted.

The scoring of COAs is subjective. Students should be reminded that they should rely on their intuition and experience and apply 'common sense'. However, the COAs must be supported by the current intelligence – MPKI staff can't simply create COAs without a supporting intelligence base.

Slide 15

Here are FACES criteria. Take a minute to look at each one in turn and let us discuss.

Slide 16

The ML COA is that COA which is most likely to achieve the Actor's assessed intent and end state. It must be supported by the current intelligence picture and should have a history of achieving success.

Slide 17

The MDCOA is the actor's COA that has the greatest impact on the UN's mission. It still must meet all the FACES criteria and be supported by the understanding of the Actor's TTPs and capabilities; it is not fantasy. However, we must give consideration that this COA will require the actor to commit greater resource, accept greater risk and may involve an increased level of planning.

Slide 18

Key Message. The FACES criteria (Feasible, Acceptable, Complete, Exclusive and Suitable) are used to score all the identified COAs. In scoring them and annotating the results in a table as that shown, the MPKI cell can provide detailed analysis to the Command element how they came up with the ML and MD COAs and which COAs were assessed but dismissed.

The table shows that each column is scored out of 5 based on the assessment of the MPKI Cell. Other scoring methodologies can be used but, in practice, this simple and effective method is time saving and helpful.

A table is constructed in line with what appears on the screen. There are 4 columns: the first is a COA; the second is the likelihood that COA will achieve the actor's desired end state; the third is that impact that COA will have on the UN mission mandate, and the fourth verifies that it aligns with all FACES criteria.

The MPKI Cell should score each column out of 5. This allows for the quick identification of ML and MD COAs. Whilst this may seem an inaccurate method, the MPKI Cell must apply its detailed understanding of the actor. This will enhance as the operation develops, and the MPKI cell should look to revise their assessment accordingly.

Finally, the FACES criteria are applied to each COA:

- Feasible. Based on the current understanding of the actor's TTPs and capabilities, is the COA feasible for them to conduct

- Acceptable. Does the COA come with an acceptable level of risk

- Complete. Does the COA fully complete all the criteria expected of it? Does it have a start and an end with coherent and complete activity

- Exclusive. Is it distinct or does it copy other COAs

- Suitable. Does it match the actor's purpose or situation? Is this something the actor would do based on their beliefs, intent and history

Interaction. Based on the table shown on the slide, which is the most likely and most dangerous COA? Ask the students how they came up with their responses? Response: COA2 is the most likely as it best suits the actor. COA 5 is the most dangerous, as it has the highest impact on the UN mission.

Slide 19

This is the answer to the previous question set at the bottom of slide 18, the previous slide.

Slide 20

Now let's shift to COA development. After we have identified the ML and MD COAs, the MPKI staff should look to develop them in greater detail. To do so, the MPKI staff should look to apply several developmental stages to the COA in order to draw out the critical analysis. The first step in this process is to define a mission-specific assessed actor intent, end state and main effort.

Slide 21

The intent is a concise statement of what the actor intends to do and why. Often military personnel use military effects terminology to ensure brevity and accurate use of language. However, this terminology may not always be applicable when talking about a civilian (non-Armed or non-threat) actor.

The end state is what the actor is trying to achieve. What does mission success for the actor look like? Where does the actor want to be at the end of their mission?

The main effort is one activity that needs to be achieved in order to ensure mission success.

Remember that this is mission-specific and scaled to the level you are working at. For example, the actor's strategic intent and end state will not be applicable at the tactical level.

Slide 22

There are several elements to the intent

Indeed, MPKI staff must be aware that an actor can have several intents There may be an over-arching intent where they seek to achieve a strategic aim, or where they seek to achieve something at the tactical level, For example, to counter UN activity in a specific location

However, Phase One briefs must be mission-specific If the MPKI cell is operating at the Force level, then the assessment of each actor's intent will likely be over-arching, whereas a tactical-level commander will seek to identify the intent of the adversary commander within his AO

A fully efficient MPKI cell must understand both levels of operations in order to understand how a strategic intent will drive tactical activity. The intent is a concise and precise statement of what the actor intends to do and why

Where applicable, effects-based terms such as task verbs are to be used Effects-based terms and task verbs have a clear definition and are widely understood by military personnel Using terms such as 'take out' instead of 'DESTROY' adds confusion and lacks the clarity of language Everyone the MPKI cell briefs must understand what is meant

In drafting the intent statement, MPKI staff must be clear in their language. The narrative must also be chronological in terms of activity

The intent leads to the end state. Therefore, we use the term 'in order to' i.e. an actor must do this in order to achieve their end state The end state is the result What does 'mission accomplished' look like for the actor? If the intent does not lead to the end state, then the intent is incorrect

Once we have identified the intent and end state, we can assess the main effort is that one activity the actor MUST achieve in order to be successful It is helpful if this is expressed as an effects-based or task verb to add additional clarity of language The main effort is annotated in the intent narrative; if not, then the intent narrative needs to be re-drafted

Slide 23
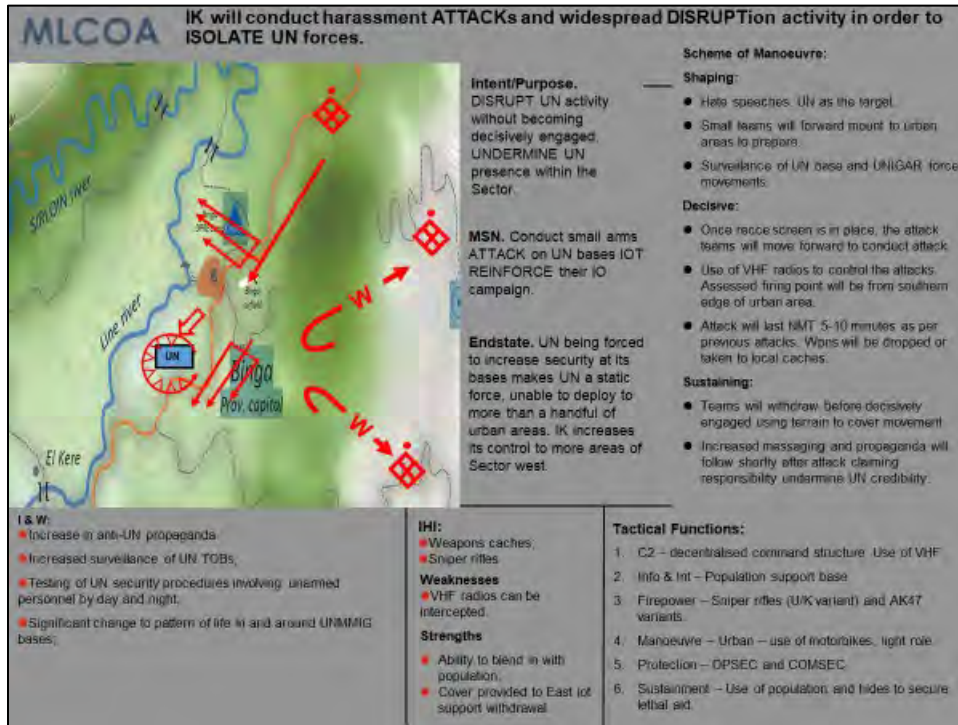
This slide is used as a reminder to illustrate the importance and relevance of this analysis. Where does it fit in the P1B and how it is briefed?

Slide 24

Exercise
Defining Intent, End State and Main Effort

Task: Each syndicate is to draft an intent, end state and main effort for one threat actor within their Sector

Approx. Time: 40 minutes.

- **Intent:** A concise and precise statement of what the Actor / Threat Actor intends to do and why; expressed as the effects they intend to achieve.

In Order To

- **End State**: The aim to be attained at the end of an operation, which indicates that the objective has been achieved. It is, in short, 'where the Actor / Threat Actor wants to be, mission accomplished.'

- **Main Effort**: What the Actor / Threat Actor considers to be the activity which is crucial to the success of the mission

This exercise is to confirm understanding. A detailed understanding of the scenario for each sector is required. The syndicates must have read and understood the relevant detail. Activity conducted during Terrain Analysis and Actor Evaluation will have been the key foundation work to facilitate this analysis. this exercise seeks to identify the operational intent, end state and main effort due to the current level of detail in the scenario. A more detailed scenario, with a specific UN mission upfront, will allow for the generation of greater understanding during this phase.

Interaction. Have the students break out into their syndicates, reflecting their assigned sectors as outlined in the central scenario, and ask them to identify one relevant actor's intent, end state and main effort.

Ideally, the focus should be on the threat actor that syndicates have chosen to work on throughout the course. Students should be made aware that they will be asked to back brief their drafts with justification.

Allow approximately 30 minutes for this task, and 10 minutes for one group to present. Ensure the students are aware that one group will be asked to present the results.

When the results are presented, allow for constructive debate between the groups. Ask each group if the presenting group has provided a clear and

concise description. At all times, ask the students to provide the analysis behind their findings.

Slide 25
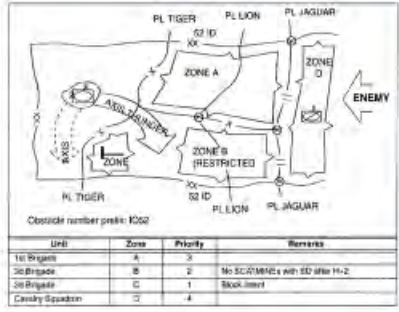
The next stage of COA development is drafting a Scheme of Maneuver.

Slide 26

The SOM is effectively a story describing how the actor will act. It effectively provides an understanding of where, when and how the actor will achieve their purpose.

Each COA will have an overlay depicting actor activity in effects graphics.   The MPKI cell should situate this activity through the identification of routes, objectives boundaries and timings as a minimum.

Other headings can be used such as OCOKA (should the actor be conducting defensive activity); the acronym stands for Observation and Fields of Fire, Cover and Concealment, Obstacles, Key Terrain and Avenues of Approach.

The systematic analysis, using useful headings, will enable the MPKI staff to break down the activity into coherent actor activity.

Analysis of the terrains and actor during Phases 1 and 2 will provide the foundation details. A Scheme of Maneuver (SoM) will likely have three phases; Shaping, Decisive and Sustaining. These will be covered in turn.

Slide 27

The shaping phase will provide the clearest indicators and warnings (I&W) that a certain activity is going to take place. Therefore, detailed analysis at this stage will identify critical I&W – more on this will follow later. The shaping phase will contain all the required activity an actor needs to conduct to set the conditions for the decisive phase. Examples of shaping activity are highlighted on the screen.

Remember that this activity must be pertinent to the actor and be the feasible activity for the actor to conduct, for example, if they have no IED capability, or the current intelligence picture and understanding of the actor's TTPs and capabilities does not include an IED capability then it is not realistic to expect this to be a shaping activity.

Interaction. Ask the students to list the shaping activity required for a threat actor to attack a UN FOB? Responses should include reconnaissance, testing of UN TTPs, procurement of arms and ammunition, securing safe houses, test firing of weapons etc.

Note to Instructor. The instructor should look to draw out obvious examples of shaping activity such as reconnaissance, influence and facilitation activity. The slide contains a list of examples but is not exhaustive.

Slide 28

SOM – Decisive Phase

- **Action** that leads to successful completion of the mission
- Task that makes the plan unique
- May include these verbs for a threat actor:
  - Destroy
  - Neutralise
  - Secure
  - Seize
  - Clear
  - Disrupt

The decisive phase is where the action that achieves mission success takes place. For threat actors, this will include the decisive action and may include such effects verbs as those listed. The decisive phase will contain all the required activity an actor needs to conduct the activity that leads to mission success. Remember that this activity must be pertinent to the actor and be the feasible activity for the actor to conduct.

Slide 29

Key Message. Sustaining activity is that activity which enables the actor to reconstitute, reorganize, consolidate, and reinforce mission success.

Interaction. Ask the students how they think success is reinforced or sustained. Responses could include resupply, redeployment to key terrain or vital ground.

This is more than just logistical considerations. Examples of sustaining phase activity are listed on the slide. Sustaining activity allows the actor to reorganize, consolidate and reinforce success This can be illustrated using task verbs and effects terms where applicable (such as withdraw, establish caches, intimidate, resupply) and should be situated in time and space The sustaining phase will contain all the required activity an actor needs to reinforce mission success

Remember that this activity must be pertinent to the actor and be the feasible activity for the actor to conduct, e.g. if they have no history of demanding a ransom, then this is not a feasible activity. If they do not have the capability to propagandize, then this is not a feasible activity etc.

Slide 30

This exercise is to confirm the understanding of how to create a viable and credible scheme of manoeuvre for a threat actor. A detailed understanding of the scenario for each sector is required. The syndicates must have read and understood the relevant detail. Activity conducted during Terrain Analysis and Actor Evaluation will have been the key foundation work to facilitate this analysis.

Interaction.
Output / Task. A FACES Scheme of Manoeuvre, with shaping, decisive, and sustaining phases situated in space (on the map) and time (chronologically).

Have the students break out into their syndicates, reflecting their assigned sectors as outlined in the central scenario. Having already identified one relevant actor's intent, end state and main effort, the syndicates should draft an SoM for that actor. Emphasize that this is how the actor will accomplish its end state through its main and supporting efforts.

The instructor should provide a handout to each syndicate stating the activity.

The instructor should remind the students of the current stage. That the TOB has been established south of WALESI and that they are to build on the actor's mission-specific intent and end state through the development of the SOM.

The instructor should look to emphasise that the SOM is a story of how the actor will conduct their mission in order to achieve their intent and end state. That the SOM is based in our current analysis of the actor's TTPs and capabilities, drawn out from AE.

That the SOM should be complete, it should have a beginning, during, end. I.e. what does the actor need to achieve before, during and after the mission?

Time allocated: 45 minutes, 35 minutes for analysis and 10 minutes for a back brief.

Mentors/facilitators need to be present in order to ensure that students understand the requirement and are making relevant and logical deductions.

The syndicates may need to be reminded that they are building on this previous analysis. Remembering this is mission-specific, the syndicates are to be reminded of the UN mission. Students should be made aware that they will be asked to brief their drafts with justification.

Allow approximately 20-30 minutes for this task, and 10-15 minutes for one group to present. Ensure the students are aware that one group will be asked to present the results. When the results are presented, allow for constructive debate between the groups. Ask each group if the presenting group has provided a clear and concise description. At all times, ask the students to provide the analysis behind their findings.

Resources: Students will need to be in their syndicate rooms with a sector map. The students should also use the intent, main effort and end state that they have previously drawn up.

Slide 31

The next stage of COA development is understanding the Tactical Functions. Here is where we are in the process.

Slide 32

Key Message. The Tactical Functions are a helpful checklist to identify how an actor will conduct a certain activity. It uses the knowledge of the actor's equipment and capability to assess how it will be employed during its scheme of manoeuvre.

A detailed understanding of weapons and equipment is crucial in making feasible assessments, e.g. the effective weapon ranges. Actor Evaluation will have identified most of the actor's capabilities, but more detailed analysis is required. In identifying an intent, end state and main effort, annotating this in an SoM, we can now analyse how a group will use its equipment to operate during each phase. When analysing the group's equipment and capabilities, and situating it to the ground, the MPKI cell will then ascertain if the actor SoM and overall COA is achievable

These are mainly applicable to a threat actor but may also be useful when looking at all armed groups. These are applied to the SOM in each phase. How will the actor look to achieve or implement these factors to best effect in order to achieve the desired outcomes at each stage of the SOM?

The headings to be evaluated are Command and control, information and intelligence, firepower, manoeuvre, protection, and sustainment. Each of these headings will be related to the actor SoM, during each of the three phases.

For example, if threat actor intent is assessed to be an attack on a UN FOB, then the following might be an MPKI assessment:

- During the shaping phase, the adversary will conduct command and control via encrypted mobile phone message apps It will gather information from reconnaissance on the FOB using civilians and through observing UN SOPs

- It will test its weapons systems and store them close by for use It will move in small groups using civilian cars to avoid detection The adversary will assure its Operations Security (OPSEC) by using small groups of fighters that operate in closed networks It will also operate in civilian clothes and without arms to ensure it is not targeted It will sustain itself by using local services

Slide 33

Based on your detailed evaluation of the actor's command and control capabilities, the MPKI cell must list these capabilities and assess how each will be used during the shaping, decisive and sustaining phases of the operation. Each time a C2 capability is listed, the MPKI cell should make deductions, and create new IRs.

This stage looks to identify how the actor will exert command and control throughout the conduct of the mission. By taking the analysis from AE and applying it to the ground relevant to this mission, the MPKI staff can make a detailed assessment of how the mission will be commanded and controlled. E.g. if the group uses cell phones to communicate, but the AO has no GSM coverage, then the MPKI staff must assess how the actor will conduct C2.

We must draw out the critical analysis by asking - What would be seeing a specific capability be indicative of? Where are the MPKI staff likely to see that capability employed? i.e. where should it be employed in order to achieve maximum efficiency? This will give the MPKI staff an initial steer for NAIs/TAIs. In addition, what would be the impact in the actor should that capability be denied to them?

Slide 34

Based on your detailed evaluation of the actor's information and intelligence gathering capabilities, the MPKI cell must list these capabilities and assess how each will be used during the shaping, decisive and sustaining phases of the operation. Each time a piece of information and intelligence capability are listed; the MPKI cell should make deductions, and create IRs and CCIRs if there are unknowns.

How will the actor look to gather information / intelligence to support the planning and conduct of their mission? What capabilities could they employ? What considerations should MPKI staff look to implement in order to protect our own forces?

In addition to the points raised in the previous slide, the MPKI staff should look to make an assessment of where they are likely to see this activity being conducted and what the impact on denying/disrupting that activity would have on the actor.

Slide 35

Based on your detailed evaluation of the actor's firepower capabilities, the MPKI cell must list these capabilities and assess how each will be used.

Firepower can achieve several effects and is not always employed within the decisive phase. MPKI staff must give consideration of how firepower can be used during all stages of the actor's mission. The MPKI staff should also be aware of what Actor's firepower represents a threat to UN forces.

MPKI staff should also assess the feasibility of employing firepower. What are the effective ranges? What are the optimum employment conditions for that firepower asset? In understanding this, the MPKI staff can identify where and how the firepower capability will be employed during the SOM.

The MPKI staff can then assess where they should look to focus acquisition assets to identify that capability and what stages of the actor's mission.
The MPKI staff should assess how the actor will be affected should that capability be disrupted or denied to them.

Slide 36

Based on the already completed actor evaluation, the MPKI cell should already know how the actor can move, within its capabilities; for example, by foot, motorbike, vehicle, armoured vehicle, air, or boat. Now the cell must assess how the actor is likely to move, based on its chosen Scheme of Maneuver and the terrain.

The MPKI staff should look to assess how the actor is going to move during the conduct of their mission. What assets do they have available to them, and how are these affected by the physical terrain? Think about all stages of the SOM, how will the actor seek to use the physical and human terrains to their advantage? Where should the MPKI staff look to prioritize acquisition assets in order to identify that manoeuvre?

.

Slide 37

The MPKI cell should develop an understanding of how an actor protects its assets, its personnel, and its communications. This will allow the cell to understand how these protection measures will be or are likely to be employed during a specific COA.

The MPKI should look to assess how the actor will protect itself during operations? Just as UN forces would do, the actor will look to mitigate the threats and risks that they are likely to face. Will the actor look to decrease its communication activity (COMSEC)? Will the actor look to have a screening force to provide early warning of UN activity? If so, where will the actor look to situate this? The MPKI staff should look to identify opportunities to mitigate or negate the actor's protection measures.

Slide 38

The MPKI cell should develop an understanding of how an actor sustains itself (food, water, ammunition, medical, etc.). Does the actor have a resupply or medical plan?

How will the actor sustain a COA? What does the actor need in order to conduct this COA? This is more than just logistical considerations. What should the MPKI staff look for, and where, in order to affect the actor's sustaining activity?

Slide 39

This exercise is to confirm understanding of the tactical functions and how they relate to each phase of the Scheme of Maneuver. Your understanding of the scenario for each sector is required. You must have read and understood the relevant detail. Activity conducted during Terrain Analysis and Actor Evaluation will have been the key foundation work to facilitate your analysis.

Interaction.

Have the students break out into their syndicates, reflecting their assigned sectors as outlined in the central scenario, and ask them to use the previously assessed threat actor's SoM and to assess how the adversary will employ its tactical functions during each phase (shaping, decisive, sustaining). Ask the students to back brief their drafts with justification.

Ensure the students are aware that one group will be asked to present the results. During the presentations, allow for constructive debate between the groups. At all times, ask the students to provide the analysis behind their findings. In doing the SoM, they should have highlighted I&W, Items of High Importance and possible NAIs.
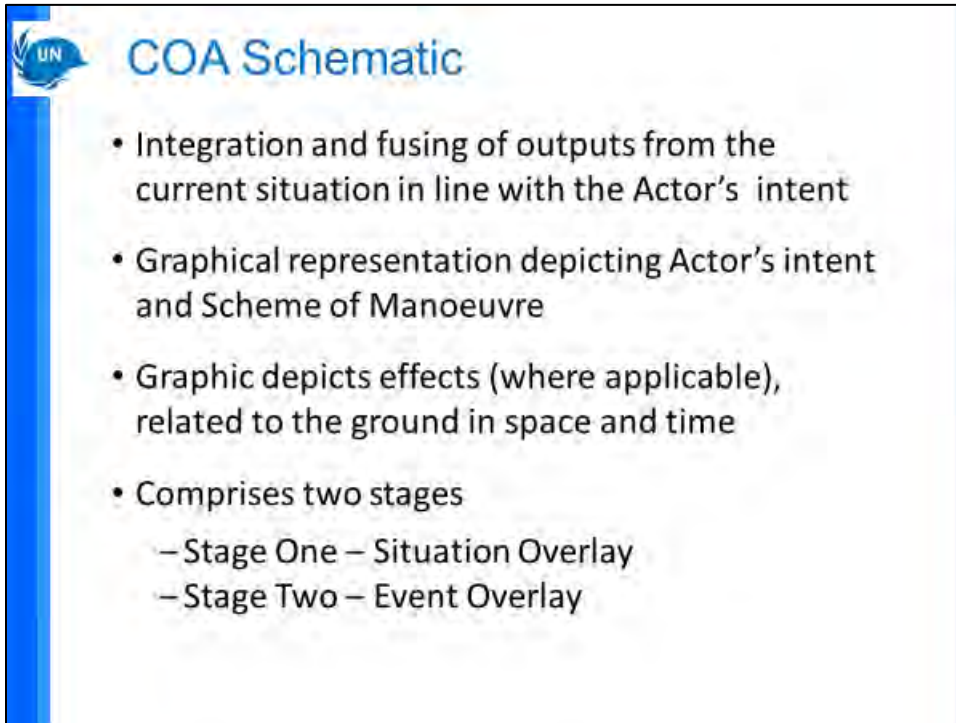
The students are one step further in the development of the identified actor's COA; they should look to deepen the assessment of the COA by applying the

tactical functions for each stage. In doing so, this will enable the MPKI staff to deepen 'the story' and situate activity within time and space?

The instructor should provide a handout to the student about what is required from the exercise. The exercise will last 30 minutes, 20 minutes for analysis and 10 minutes for back brief.

Slide 40

The next stage of COA development is understanding the identification of indicators and warnings. The identification of indicators and warnings is crucial to the identification of NAIs and TAIs (more to follow in later lessons).

Interaction.

Ask the students why indicators and warnings are important.

If COAs are exclusive, indicators can quite accurately point to a particular COA. For example, an ambush on a convoy and a complex attack on a convoy are very similar adversary COAs. As such, the indicators for both will be similar. These should not be two distinct COAs. Conversely, the indicators for an attack on a UN FOB or an ambush on a UN convoy will be very different. In that case, the indicators will be a useful way to achieve early warning.

Slide 41

Indicators and warnings (I&W) are those factors that are observed during the shaping phase of the SOM. They should assist the MPKI staff in the confirming or denying of the actor's chosen COA. Some I&W will apply to more than one COA, so it is imperative that MPKI staff identify those

Slide 42

Interaction. The exercise should confirm that the students understand what constitutes and an indicator and warning. Have the students break out into syndicates, reflecting their assigned sectors as outlined in the central scenario, and ask them to identify I&W during the shaping phase based on the SoM they have previously drafted.

Allow approx. 10-15 minutes for this task, and 5-10 minutes for one group to present. Ensure the students are aware that one group will be asked to present the results. When the results are presented, allow for constructive debate between the groups.

The instructor should give the students a handout stating the requirements of the exercise. This process should be relatively quick. The students are to look at the shaping phase of the SOM and look for the critical I&W for that phase.

Slide 43

The next stage of COA development is identifying the Items of High Importance. Once the COA has been developed, the MPKI staff should look to analyse the COA and identify the critical capabilities the actor requires in order to carry out the SOM successfully. These are known as Items of High Importance.

Slide 44

Key Message. The Items of High Importance will be familiar to those who understand doctrinal example of High Payoff Targets etc. IHIs are those assets which, should they be denied or lost, would significantly damage the actor's capability to achieve their intent.

The identification of IHIs is critical in assessing where UN forces can have a significant effect on an actor's intent. Identifying critical equipment or individuals throughout analysis of the actor, their TTPs and SoM, the MPKI cell can advise the Commander about which IHIs should be prioritized. IHIs have already been identified during previous processes, for example, during the Actor Evaluation phase and during the identification of tactical functions.

Examples of IHIs are listed on the slide. In addition to identifying the actor's IHIs, the MPKI staff should look at the UN forces and identify UN IHIs that will need to be protected.

Slide 45

This exercise is to confirm understanding. A detailed understanding of the scenario for each sector is required. The syndicates must have read and understood the relevant detail. Activity conducted during the SoM drafting will be crucial.

Interaction. Have the students break out into their syndicates, reflecting their assigned sectors as outlined in the central scenario, and ask them to identify one relevant actor's critical IHIs required for their SoM. Students should be made aware that they will be asked to back brief their drafts with justification. The instructor needs to provide a handout stipulating the requirements of the exercise. Time allocated: 10 minutes to include a 2-minute back brief to the instructor.

Allow Approx. 10-15 minutes for this task, and 5-10 minutes for one group to present. Ensure the students are aware that one group will be asked to present the results. When the results are presented, allow for constructive debate between the groups. At all times, ask the students to provide the analysis behind their findings.

Slide 46

The next stage of COA development is drawing COA Schematics. The COA schematics are one of the 'golden thread' products. Once the actor's assessed mission / COA has been fully developed, we must capture this fused analysis in a coherent and concise product. The method that will be used during this course is the COA schematic.

Slide 47

Key Message. The COA schematics are a 'golden thread' product and summarize in pictorial form, the analysis of the Phases. MPKI cells should prepare a schematic indicating what effects an actor seeks to achieve – situated geographically and overlaid on a map.

A Situation Overlay is a graphical representation of an Actor's available COAs. An Event Overlay is a graphical representation of where critical events are likely to occur (situated in time and space) and where IHIs are likely to be situated. An Event Overlay will result in NAIs and assist in the monitoring of I&Ws.

If the SOM is a 'story', then the COA schematic is a 'painting' that illustrates that story. Effects graphics should be used to aid in the simplification of the drawing and to situate effects in time and space.

In producing the COA schematic, the MPKI staff will produce a situation overlay and an event overlay. These will be explained in more detail in the following slides.

Slide 48

The situation is a graphical representation of the SOM. How will the actor conduct the assessed COA using the physical terrain? The Situation Overlay is the actor's TTPs and capabilities situated to the ground and should be a visual representation of the SoM. An SoM that is not feasible and based upon known actor TTPs is incorrect.

The actor's COA should be situated to the ground in time and space. This requires a detailed assessment of the actor's doctrine and capabilities and understanding of the terrains. This enables the MPKI to geographically overlay the COA on a map of the operating environment and assess likely locations for a pertinent activity to take place during each phase of the SoM.

Slide 49
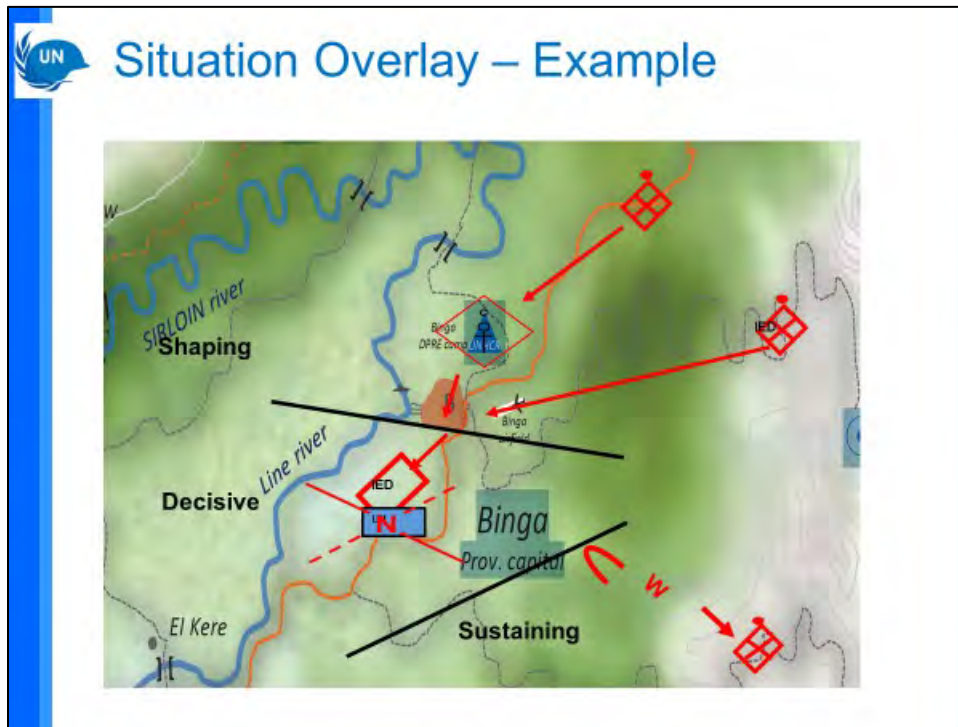
This is a simple example of highlighting a situation overlay. The instructor should look to highlight how effects symbols have been used to depict where the specific activity will take place in time and space. By showing the phase lines, this enables those observing the product to situate the activity further. For non-threat actor COAs, the MPKI staff should look to use coherent images and symbols in order to illustrate the COA.

Slide 50

Interaction. Have the students break out into syndicates, reflecting their assigned sectors as outlined in the central scenario, and ask them to produce a situation overlay for their respective actor's COA.

The students will require overlay materials (map and acetate) and permanent marker pens, and provide a handout stating the aim of the exercise. The students will have 45 minutes to produce a situation overlay for the COA that they have produced.

When the results are presented, allow for constructive debate between the groups. Ask the non-presenting groups to comment on whether the overlay depicts the COA concisely.

Remind the students that this is a pictorial / graphical representation of the SOM and must situate the activity to the terrain. Also, students must add all key physical terrain features to the overlay in order to clearly define where the activity takes place in relation to the ground.

Slide 51

The Event Overlay outlines where UN assets should focus in order to confirm actor activity. This allows the Staff to prioritize acquisition assets.

The event overlay is a separate overlay the MPKI staff produce in order to identify NAIs and TAIs. In other nations, this is often described as a decision support overlay. This overlay allows the commander to prioritise assets in order to monitor/look for activity.

NAIs and TAIs are not just boxes on a map. They can be specific points, or lines (along routes) where an acquisition asset could be tasked to monitor.

The identification of key timings and NAIs / TAIs will enable the MPKI cell to confirm/deny an actor's COA and enable the commander to look to affect that COA if applicable.

Slide 52
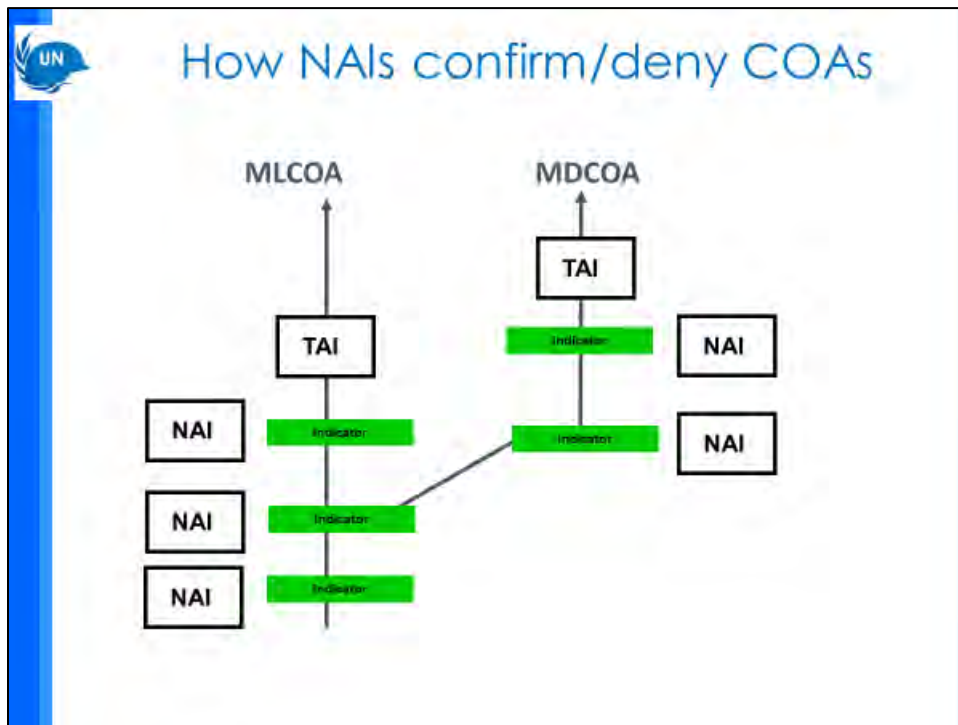
This slide is a very simple example of how a series of observed indicators can confirm or deny an actor' chosen COA. The instructor should look to explain the diagram.
If we look at the left side of the slide, we can see the initial indicators, in the shaping phase, that the MPKI staff have identified as unique/distinct and indicative of the actor's MLCOA.

The NAI boxes indicate that these indicators have been observed. However, after the second indicator on the left, the black line over to the right, state that a new indicator has been observed, which is indicative of the MDCOA. Following the right-hand side flow, the instructor should point out that the second observed indicator then confirms that the actor has adopted the MDCOA. That is how NAIs can confirm or deny an actor's chosen COA.

TAIs are therefore placed in order to provide an option to the commander in order to affect that actor's chosen COA. This effect does not have to be a kinetic response, and UN personnel must be mindful that kinetic responses are largely the least applicable solution.

Slide 53
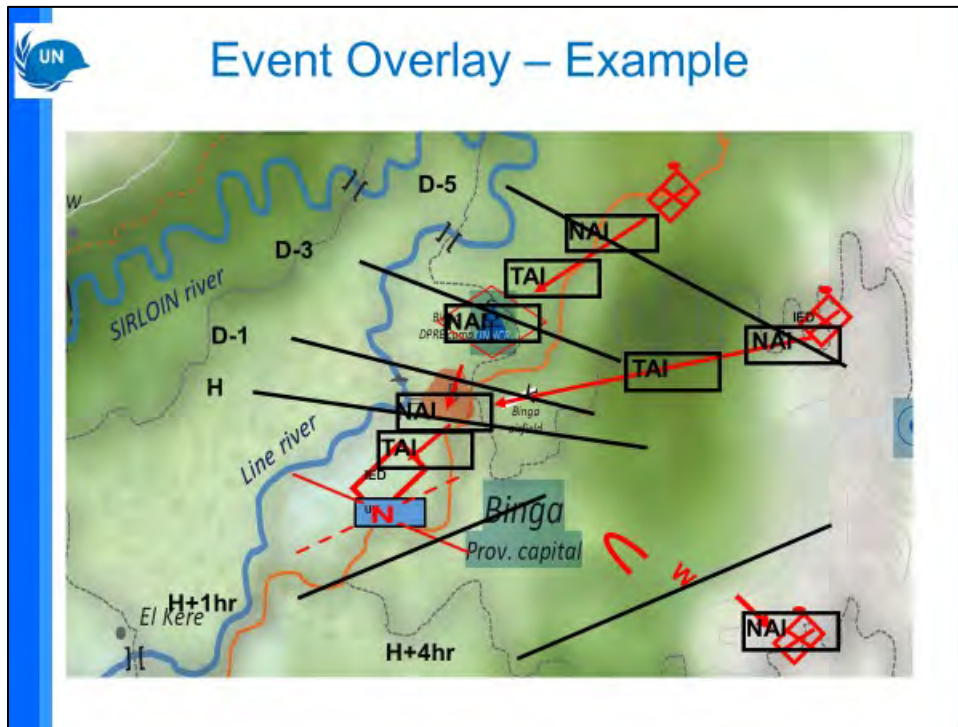
This is how the Event overlay would look on the COA board/map. Situation the NAIs and TAIs in space and time.

.

Slide 54

It is important to confirm the understanding of what NAIs and TAIs are, using clear definitions. This slide confirms the key definitions of NAIs and TAIs. Note that TAIs are not target specific and can be applied to information and other non-lethal effects; NAIs confirm/deny actor activity. Take a minute to read the definitions and if there are questions; let us ensure everyone understands these concepts before we move on to the lesson.

Slide 55

Syndicate Exercise – Event Overlay

Task:

Each Syndicate creates a Event Overlay for their respective Threat Actor within their Sector.

Approx. Time: 10 mins.

Include: Graphical representation of where likely events are to occur – Identification of NAIs, TAIs.

Interaction.

Using the Situation Overlay already produced, ask the students to produce an event timeline and overlay – on a separate overlay – to situate NAIs and TAIs. You will need to provide overlay materials and permanent markers. Provide the students with a handout to state the requirements of the exercise. Have the students break out into syndicates, reflecting their assigned sectors as outlined in the central scenario, and ask them to identify the relevant actors in their respective sector-level AOs.

Allow approx—10-15 minutes for this task.

When the results are presented, allow for constructive debate between the groups. From the timeline has been drawn, the syndicate should be asked how they analysed the timings depicted. Time: 10 minutes to include a two-minute back brief.

Slide 56

The final stage of situation integration is the completion of the COA boards for the ML and MD COAs that have been developed.

Slide 57
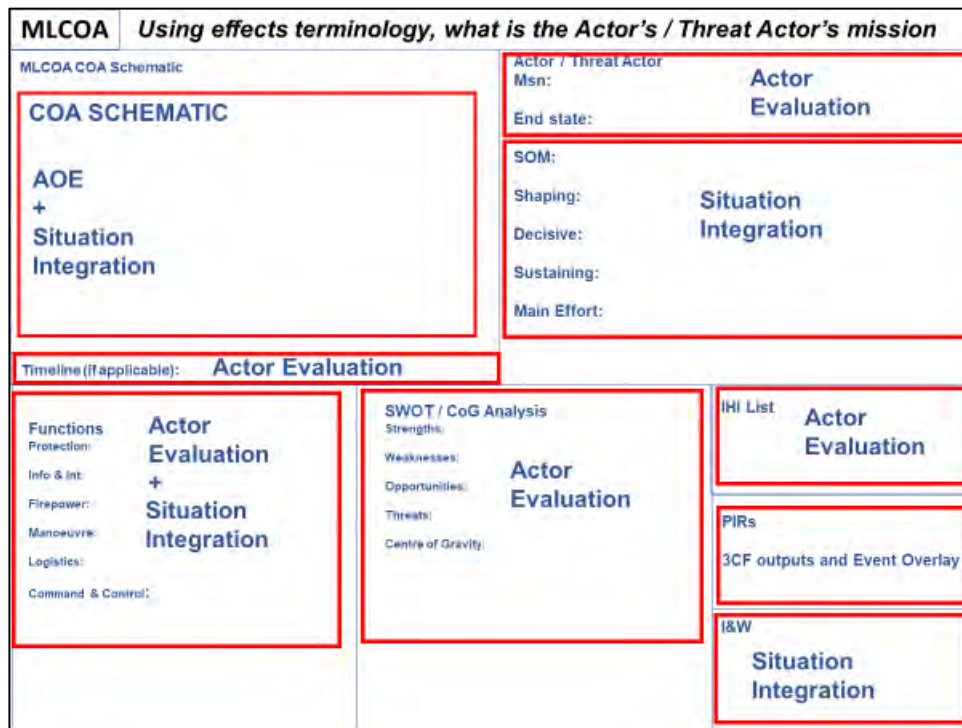
Key Message. COA Boards are the briefing aid used to present the Situation Integration analysis to the commander and their staff during the Phase One Brief. It is a 'golden thread' product and depicts all the analysis conducted by the MPKI Cell in a concise and clear format.

The COA board is the final stage of Situation Integration. It is a concise product depicting the analysis from Phases 1, 2 and 3, and it informs the Commander and their Staff regarding the ML and MD COAs during the Phase One Brief. This is, perhaps, the most important supporting product.

The slide depicts where each element of the COA board is drawn from this slide represents how all the analysis is fused into a briefing product.

We use a single COA board as a template and use an overlay (clean piece of acetate) for filling in the schematics and other required information for each ACOA. Remember to label each overlay appropriately.

As MPKI cells become more efficient, they will understand how important the 'golden thread' products are; therefore, time spent drafting presentable products depicting analysis will save time when producing briefing aids.

Slide 58
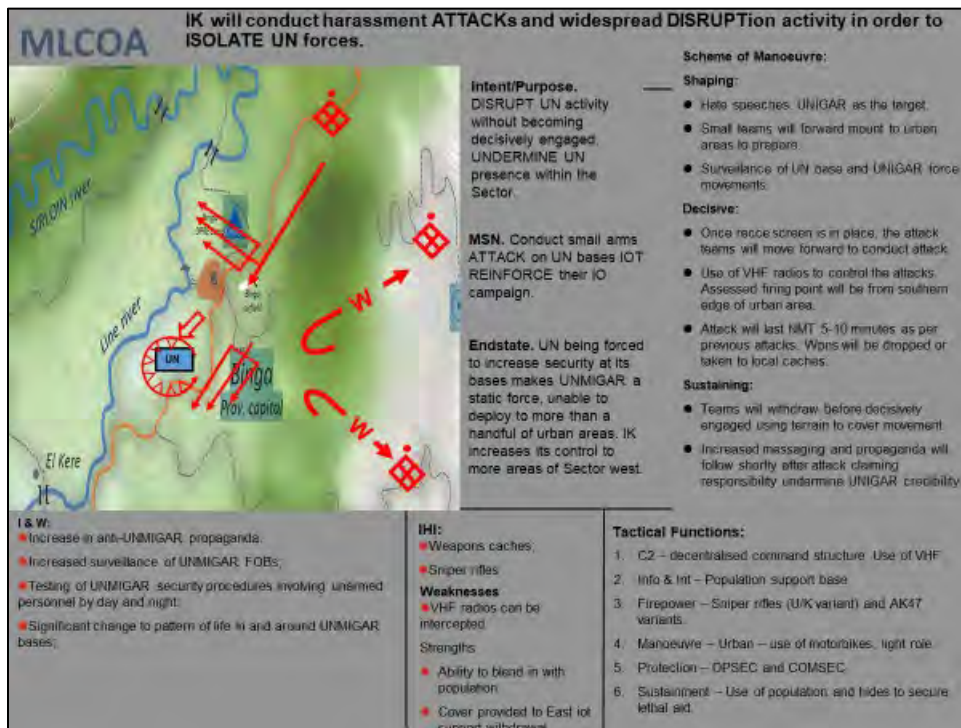
Here is an example of MLCOA Board.

COA Description. Using task verbs and effects terminology, describe the actor's mission in the form of a concise statement that is then illustrated in the COA schematic.

COA Schematic. A graphical representation of the SoM depicted on the map. The physical terrain should be drawn within this box.

Intent. Annotating the actor's intent.

End state. A concise statement of what the actor is trying to achieve.

SoM. Tell the story. What activity will the actor conduct during each stage – this MUST be depicted in the COA schematic.

I&W. State which I&W is pertinent to this COA.

IHI. State the critical IHI pertinent to this COA.

SWOT / COG analysis. State the key deductions relevant to the actor for this COA.

Tactical Functions. Explain how the actor is going to use its capabilities to conduct this COA, and during which phase.

Each COA board MUST be a standalone product that is clear, concise and contains all the relevant information. It is particularly important that the COA Schematic is clear and is supported by the analysis in the other boxes.

Slide 59
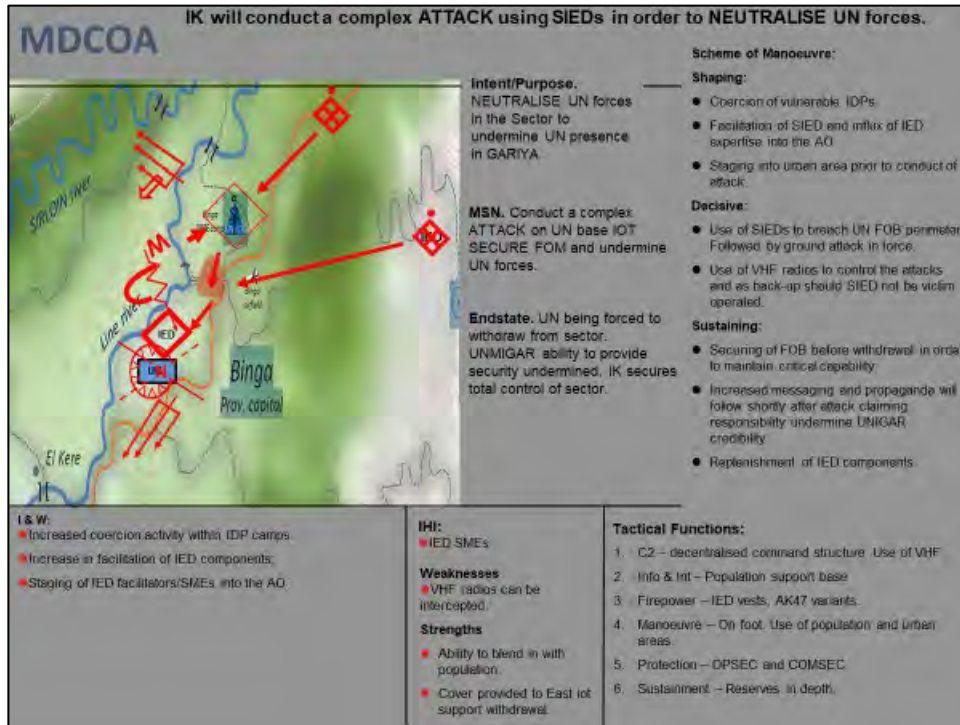
This is a very basic example of a completed MD COA board. COA Boards must be distinct; for example, the intent, end state, schematic, I&W, SWOT/COG, SoM for each the ML and MD COAs must be distinct. It is not good enough simply to copy the details from one COA to the other.

Slide 60
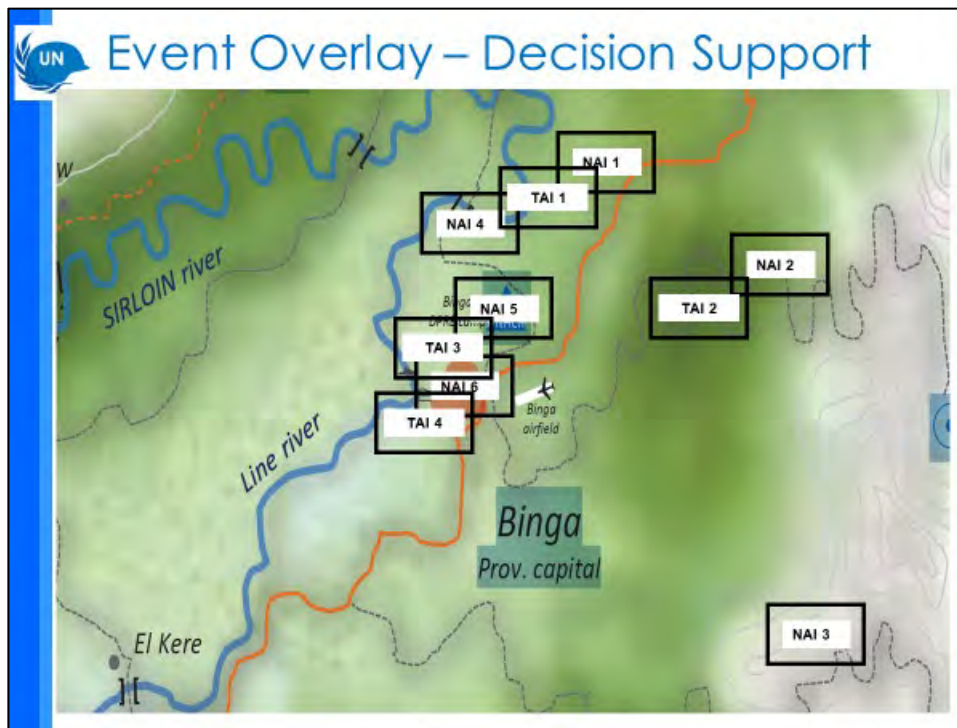
This is a very basic example of a completed Event Overlay.

Slide 61

Take Away
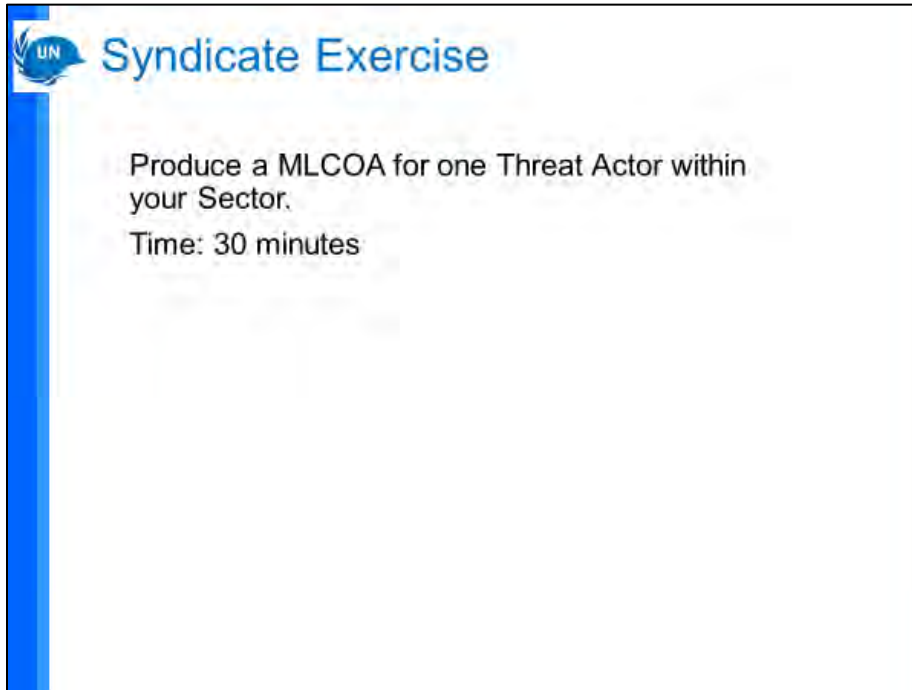
- There is an important analysis link between AOE, Actor Evaluation and development of COAs
- The physical, human and information terrains and Actor Evaluation are building blocks to COA development
- FACES criteria is an important tool to assess COAs
- Scoring of COAs and feasibility within the current intelligence picture, actor's TTPs and capabilities are key to developing situation and event overlays
- NAI and TAI and how they facilitate the confirmation of a COA
- The COA Board, situation and event overlays are important MIO tools

Summary

These are the key takeaways from the lesson. In real terms, the MPKI staff have developed a story, based on the assessment of the actor's TTP and capabilities related to the ground, of how the actor will operate against the UN mission in order to achieve their assessed intent and end state. The COA board paints a picture of that SOM and provides a succinct briefing tool to enhance the understanding of the staff.

Learning Activity

NOTE TO INSTRUCTORS:
This exercise will reinforce the understanding of all the elements of the phases. Students should be aware that they will brief Commands using these COA boards and that it must be of an acceptable standard.

Break out the students into their respective syndicate rooms. The syndicates will develop an MLCOA for one threat actor in their sector. One (ML) COA board needs to be produced to confirm understanding. Ensure that the students are aware that one group will be asked to present the results.

Highlight that if the syndicates have completed previous analytical work in enough detail, this should be a simple exercise of transposing the details onto the COA Board. Remind the students that these boards will be used to brief the course and should be of an acceptable standard.

Approx. TIME:
Thirty minutes and 10-15 minutes for discussion.

3.5i

Short Peacekeeping-Intelligence Estimate (SPIE) and Situation

The Lesson

Starting **the** Lesson

Slide 1

Now we are going to cover the Short Peacekeeping Intelligence Estimate, (SPIE), and the situation paragraph format.

Interaction. Which part of the MPKI management cycle do these products fall under and contribute? Answer: Direction

Slide 2
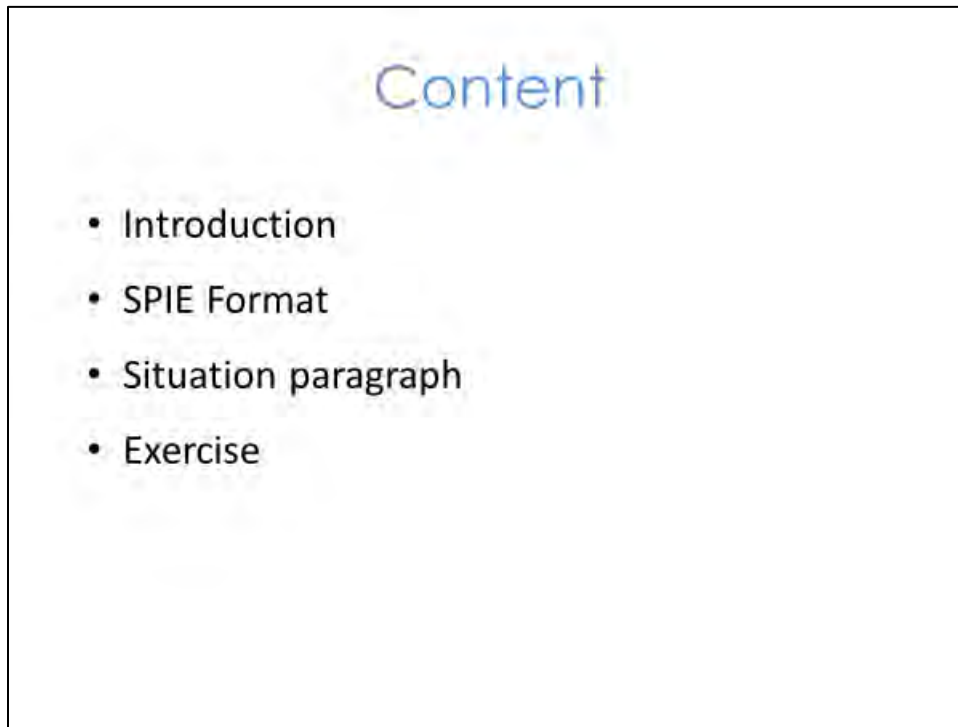
Here is the content we will cover in this lesson.

Slide 3

By the end of this lesson, you will have your analysis consolidated and be able to produce a completed Short Peacekeeping-Intelligence Estimate (SPIE) and a situation paragraph for inclusion in the Warning Order.

Slide 4
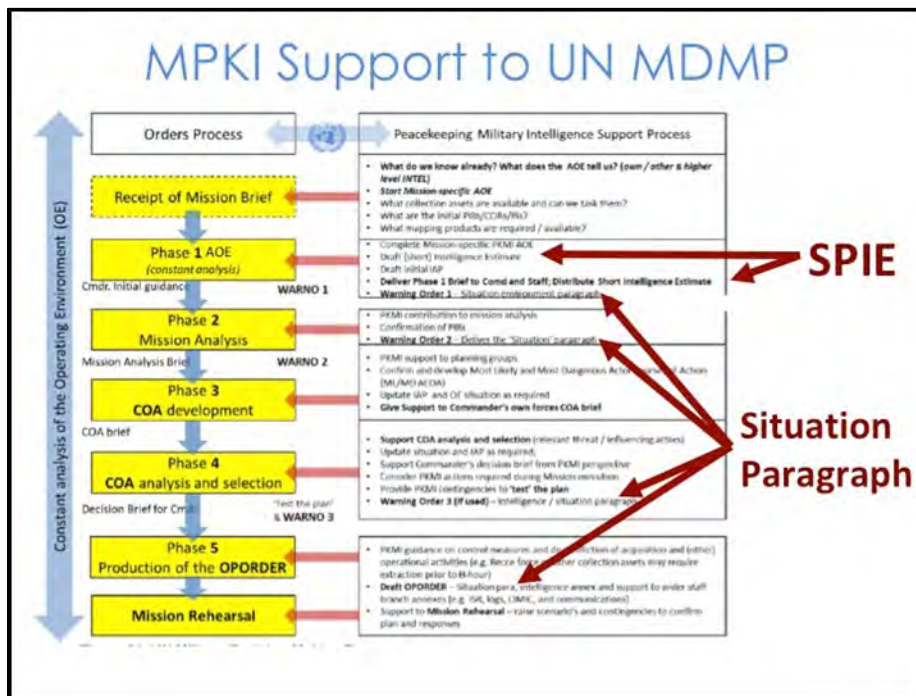
Key Message. The SPIE and a situation paragraph are products of intelligence integration with the Military Decision-Making Process.

MPKI supports decision-making with specific products during the planning process. The SPIE draft starts during the IPOE phase, where the AOE is conducted. The SPIE is a product of the AOE.

The situation paragraph will be produced by intelligence staff. It will be part of the Warning Orders, as the students can see in the slide of phases 1, 2 and 4, and the final product will constitute the OPORDER/Task Order, including the intelligence annex, when required.

You do not have time to produce an SPIE to support the receipt of the mission, but you will have time to deliver an SPIE product to support Phase 1 of the IPOE and include in the first warning order (WO). The situation paragraph is based on SPIE and is included in the WO 3 and OPORDER.

Interaction. What do you do if the situation changes between WO 3 and the production of the OPORDER? Answer: Update the SPIE, and the Situation paragraph as they are living documents.

Slide 5
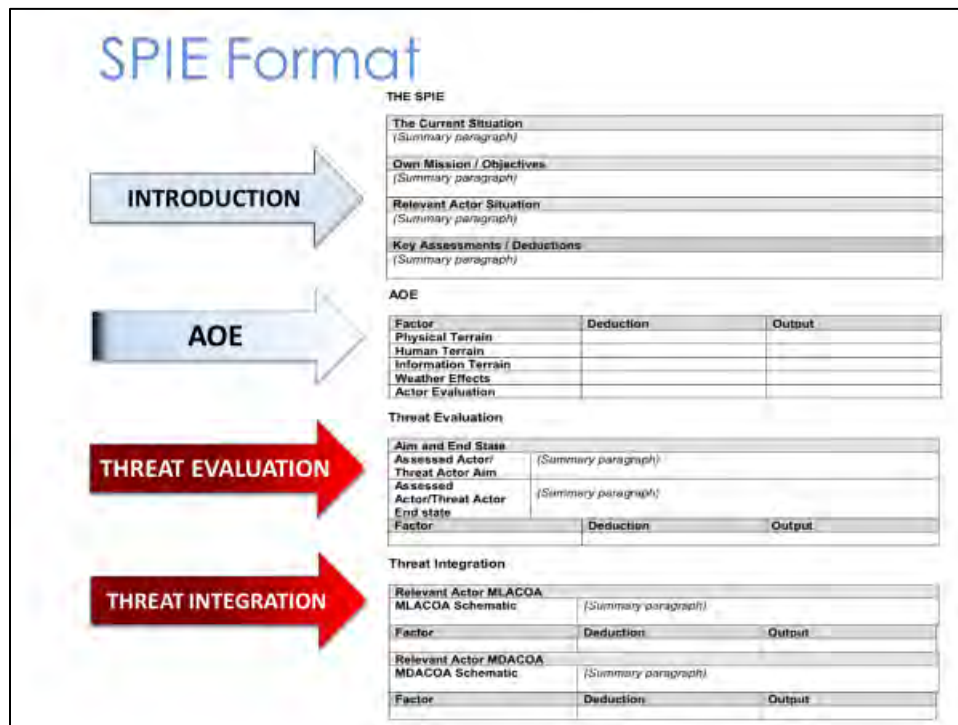
Key Message: The 3 Column Format products that have been developed during the AOE process need to be refined and consolidated into an SPIE format to provide a clear understanding of analysis to date and provide a base for further analysis.

The SPIE format is used to consolidate our three-column analysis produced during the AOE. In the process of constructing the SPIE, we also have an opportunity to consider and further refine our factors, deductions and outputs, creating a more succinct product, focused on the commander's priorities.

During the analysis, it is usual for different factors to lead to the same deductions and outputs, so, as we consolidate our analysis into the SPIE, we should remove or consolidate any repeated deductions and outputs.

The SPIE format is broken into four parts:

- Introduction
- AOE, not the complete AOE, only key elements
- Threat Evaluation
- Threat Integration

Slide 6

Key Message: The introduction provides a reader with basic information to read into the situation and a summary of key assessments and deductions.

What do you think should have been included in the current situation paragraph? The Current Situation is an indication of events within the area of interest that have led to the SPIE. It may include a brief description of political events, national relations, diplomatic relations, regional situation and third state and non-state actors.

Why do we include our Mission and objectives? Because it provides the UN mission and any key UN objectives or stakeholder objectives that help to focus analysis (by understanding mission and objectives, we can check that our factors are relevant to the mission and objectives, and therefore, refine our analysis).

Who might be the relevant actors in our AO?   These can include civilians, humanitarians, NGOs, political, criminals, other UN agencies, economic, foreign, IDPs, refugees, etc. Under the Relevant Actor Situation, provide a brief description of the current threat actor and other non-threat actors that may impact the mission. Include any assessed mission, objectives and intent.

How do you decide what key assessments and deductions to include? List the most important deductions and assessments that you want the reader to be aware of. While Key Assessments/Deductions are placed in the first part of the SPIE, it is best to fill this in last, after you have completed the rest of the SPIE and consolidated all of your

assessments and deductions and know which ones are the key ones. Don't forget to go back and complete it!

Slide 7

Key Message: In this part of the SPIE, simply transfer your factors, deductions and outputs from the relevant AOE products, then read through and refine them.

The AOE section of the SPIE is where you simply transfer your factors, deductions and outputs from the relevant three-column format AOE products that you have already produced. In the process of transferring factors, deductions and outputs:

- Consider and further refine your factors, deductions and outputs, creating a more succinct product

- Identify and remove or consolidate any repeated deductions and outputs

- The key is to make it clear enough for commanders and other interested parties to understand

Slide 8

Key Message: Under Threat Evaluation, for each assessed actor or threat actor, provide a summary of their aim and intended end state, and any key factors, deductions and outputs from your analysis.

Of note, in the top portion of the slide, you will see SPIE format, more specifically "Threat Actor" summary required. We should also include relevant actors that have a positive or negative impact on the operation.
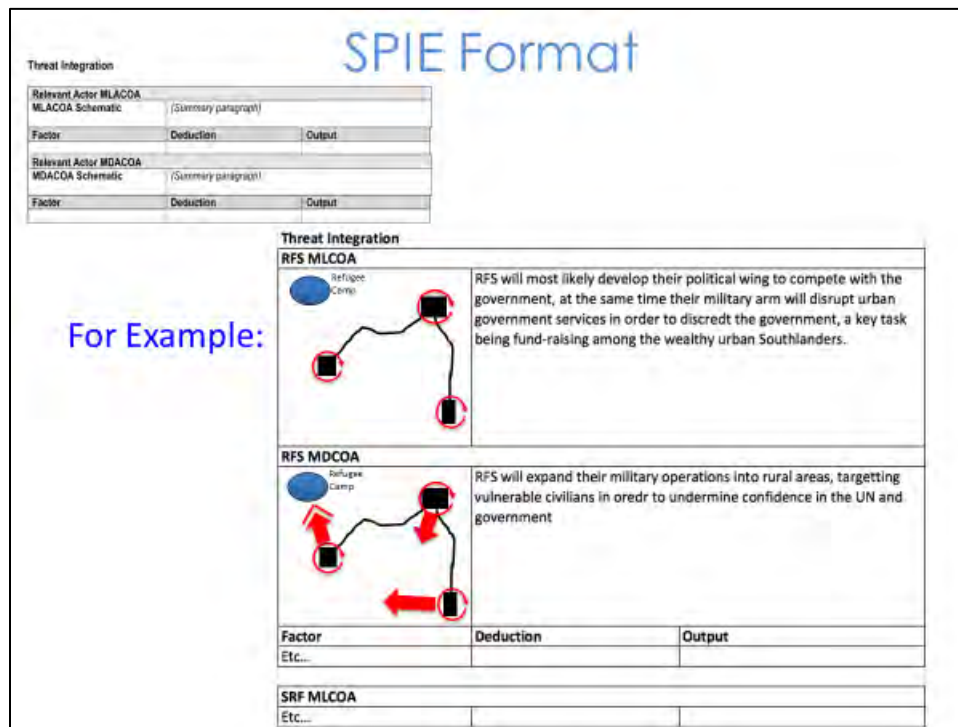
The Threat Evaluation section of the SPIE includes summary paragraphs of the assessed actor or threat actor's aim and intended end state. These paragraphs may also include additional key information that helps a reader to understand the relevant actors and threat actors better.

Transfer the factors, deductions and outputs from your three-column analysis conducted during your evaluation of actors and threat actors.

In the process of transferring factors, deductions and outputs:

- Consider and further refine your factors, deductions and outputs, creating a more succinct product
- Identify and remove or consolidate any repeated deductions and outputs
- Repeat this process for each assessed actor/threat actor

Slide 9

Key Message: Under Threat Integration, for each actor and threat actor, provide MLACOA and MDACOA overviews and key factors, deductions and outputs.

The Threat Integration section of the SPIE includes a simple schematic and summary paragraph of the assessed actor or threat actor's MLACOA and MDACOA drawn directly from your MLACOA and MDACOA products. What should be in your schematic? The answer is whatever graphically communicates the actor's COA. Also, try to get as much relevant information without being confusing.

The summary paragraph should include:

- A broad statement describing the overall intent of the COA

- An explanation of any significant aspect of the COA that is not obvious from the schematic (i.e. don't waste time/space by describing anything in words that are obvious from the schematic), e.g. threat intent

- The reason why the COA is most likely or most dangerous

- Transfer the factors, deductions and outputs from your three-column analysis conducted during your development of the MLACOA and MDACOA

In the process of transferring factors, deductions and outputs:

- Consider and further refine your factors, deductions and outputs, creating a more succinct product.

- Identify and remove or consolidate any repeated deductions and outputs. Repeat this process for each assessed actor/threat actor.

Slide 10

Key Message: Analysts use the SPIE to produce the Situation Paragraph for the Warning Order.

MPKI Staff provides the Situation Paragraph for the Warning Order.

The Situation Paragraph is derived mostly from the SPIE – you have done most of the thinking already so this is the process of simplifying your analysis even further so that decision-makers can quickly absorb the most important things to know about the situation.

So how do you decide? It should be brief but contain enough detail on the situation for subordinate units to initiate their planning processes. If units require more detail, they will raise an RFI for MPKI Staff to answer.

Slide 11

Key Message: The format for the Situation Paragraph of the Warning Order is a guide, the critical thing being to include any important information that the analyst believes will help decision-makers better to understand the current situation in support of their planning.

The basis of the Situation Paragraph is an overview of the situation and the key deductions from:

- Physical terrain analysis
- Human terrain analysis
- Information terrain analysis
- ASCOPE PMESII – only put the major assessments that are not found in the other products
- Actor evaluation
- Other important information for planning

Slide 12

> ## Take Away
>
> - The SPIE is a consolidation and refinement of the 3 Column Format analysis conducted during the AOE process
>
> - Repeated deductions and/or outputs should be consolidated or eliminated
>
> - The Situation Paragraph of the Warning Order is derived from the SPIE
>
> - The Situation Paragraph should help decision makers to plan

Summary

The SPIE brings all of the analysis to date together in an abbreviated format that is easy to follow and becomes the basis for the Situation Paragraph of the Warning Order in support of the UN MDMP.

Learning Activity

SPIE AND SITUATION PARAGRAPH EXERCISE

RESOURCES
- Class notes
- MPKI HB
- Pen and paper
- Exercise Instructions (see instructions into the folder materials)
- AOE 3 Column Format products

TIME

Approx. 2 hours (all times below are approximate based on skill sets)

PREPARATION

Break into syndicates, try to assign one instructor per syndicate. Syndicates work on their sectors based on information from their sector information pack.

NOTE TO INSTRUCTORS:

- Manage the time for the students, ensuring that they complete their SPIE as best they can after 50 minutes and begin the 10-minute discussion around the updated situation

- Have the students write the Situation paragraph after the 10 minutes discussion and stop them after 50 minutes

- If students complete their Situation Paragraph before 50 minutes, they may continue to work on their SPIE

- After the 50 minutes for the Situation, Paragraph begins the review.

TASK 1: Produce an SPIE (50 minutes)

Ensure that the students have the Exercise Instructions and their 3 Column Format products they produced during the Learning Activities in support of the AOE lessons (if some students have not been able to produce useful 3 Column Format products, you may allow students to use each other's products or provide an adjusted set of products). A suggested time allocation:

- 15 minutes to write the introduction.

– 5 minutes to transfer key factors, deductions and outputs to the AOE section.

– 5 minutes to transfer key factors, deductions and outputs to the Threat Evaluation section.

– 15 minutes to write the summary paragraphs and transfer schematics, key factors, deductions and outputs to the Threat Integration section.

– 10 minutes to review the SPIE and remove redundancy.

Look for students who are not writing and coach them. Check on the content of SPIE and resolve problems and coach students throughout the time.

TASK 2: Discussion and Produce a Situation Paragraph for a Warning Order (60 Minutes total for both. Discussion (10-15 minutes): Lead a discussion around any new insights gained as students reviewed their AOE products and consolidated analysis in the SPIE.

Ask students:

- What key deductions did your analysis reveal in the area of Physical Terrain?

- Why do key decision-makers need to understand this?

- What key deductions did your analysis reveal in the area of Human Terrain?

- Why do key decision-makers need to understand this?

- What key deductions did your analysis reveal in the area of Information Terrain?

- Why do key decision-makers need to understand this?

- What key deductions did your analysis reveal from your ASCOPE PMESII analysis?

- Why do key decision-makers need to understand this?

- What key deductions did your analysis reveal in the area of Actor Evaluation?

- Why do key decision-makers need to understand this?

Remind students that they may include any important information that they believe will assist decision-makers to better understand the current situation in a way that helps them to plan.

TASK 3: Produce the Situation Paragraph (50 minutes). Ensure that the students have their completed SPIE (if some students have not been able to complete an

SPIE, you may allow students to use each other's SPIE or provide an adjusted SPIE). Look for students who are not writing and coach them to get them writing.

A suggested time allocation could be:
- 20 minutes to write a brief overview/introduction.
- 20 minutes to transfer key deductions from the AOE section of the SPIE.
- 10 minutes to review the paragraph and remove redundant deductions and/or outputs.

TASK 4: Review the Exercise (10 minutes): Ask students what they found difficult – problem solve.

Lesson
3.5j

UN MPKI support to UN MDMP

The Lesson

Starting the Lesson

Interaction. Ask the students how they usually integrate intelligence with the planning of operations in their armed forces and to provide some lessons learned in that regard (what works – and what does not work).

Ask the students why we have a planning cycle and planning tools? Here are a few points to facilitate the discussion:

- *Decision makers at all levels required detailed understanding of the operating area in order to inform their planning*

- *MPKI staff can provide predictive, forward looking assessment enabling informed decision making*

- *MPKI staff can support the other stages of the planning process in order to test the plan and enable contingency planning*

Slide 1

Lesson 3.5j
AOE-UN MPKI support to UN
MDMP

This lesson will clearly outline how the UN MPKI cell supports the UN Military Decision Making Process. For the purposes of this course, this includes the Phase one brief, which will be detailed in this lesson, and Short Peacekeeping Intelligence Estimate, which will be shown in another lecture.

Slide 2

Here is the content we will cover in this lesson.

Slide 3

Let's review the Learning Outcomes for this lesson.

Slide 4
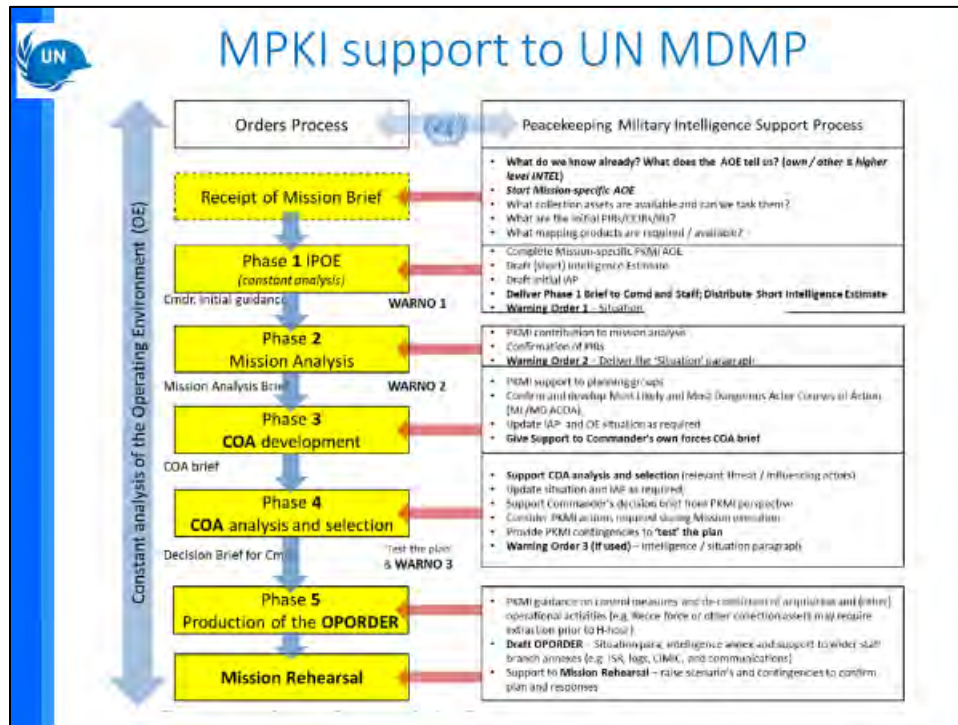
Key Message. The importance of the integration between the intelligence and operation branches is critical for success. The peacekeeping intelligence support for the MDMP provides inputs that should be integrated during all phases of the planning process, as shown in the slide (right column).

Here is the Military Decision-Making Process as annotated on the slide. It shows the MPKI staff input. Keep in mind that intelligence is a continuous process and does not stop with the conduct of the Phase One Brief.

This is the endorsed UN Military Decision Making Process (MDMP). This has been authorised by the Under-Secretary-General for the Department of Peace Operations and now forms the basis for the UN Office of Military Affairs planning.

MPKI staff must ensure they own and control the MPKI processes – ensure that common assessment exist at all levels. Proactivity and personal relationships are key to ensuring effective intelligence flows between the intelligence community of interest.

The Chief of Staff (or empowered staff officer) will stipulate the planning timelines. Ensure that you, as MPKI staff, meet the stipulated timelines.

Concurrent activity. Once MPKI staff become more experienced and familiar with the MDMP processes, they will be able to identify areas where concurrent activity can take place.

Use clear and simple products. MPKI products should stand-alone and be understood by those with limited knowledge. Identify how a Commander likes the analysis to be presented and to produce appropriate products.

The input of the MPKI staff does not stop with the delivery of the Phase One Brief. AOE does not stop. MPKI staff need to engage at all levels to provide expert input to inform and test the planning.

Slide 5
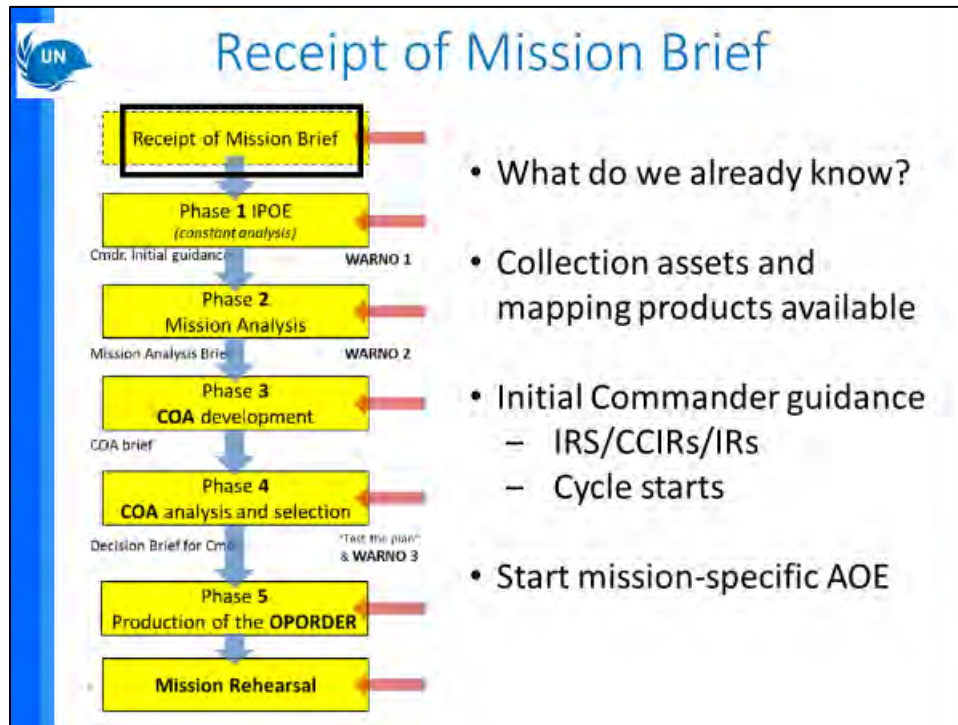
The Receipt of the Mission Brief is conducted at the start of the MDMP and should not last more than 30 minutes.

It is unlikely that the MPKI branch will have all the information or a detailed analysis at hand, but they should brief the following key/critical information in general terms. In other words, tell what we already know about:

- The physical and human terrains
- Threat actors
- Acquisition assets and mapping that is currently available to the staff for planning (with assistance from GEO)

This is the first opportunity for the MPKI staff to start the peacekeeping-intelligence dialogue with the Commander. At this stage, it is important to identify initial requirements, prioritize acquisition, focus analysis confirm reporting procedures. The drafting of initial PIRs, CCIRs and IRs will follow, and the intelligence cycle will begin to function. You may want to refer to the lesson on Direction in the block of instruction on the MPKI cycle.

This phase will initiate the mission-specific AOE.

Slide 6
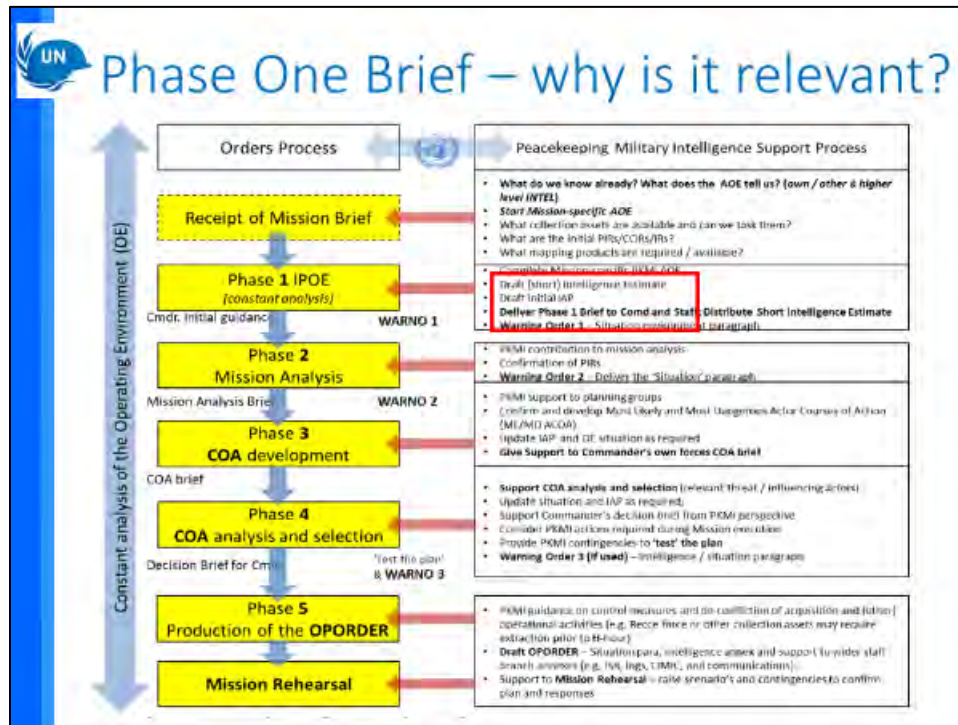
Key Message. The Phase One brief is the MPKI cell's moment to present the intelligence picture to the commander and staff and inform them of any intelligence issues prior to the conduct of planning.

The Military Decision-Making Process is shown and annotated on the slide. It specifies which MPKI staff input is required. It should be emphasized that intelligence is a continuous process and does not stop with the completion of the Phase One Brief.

Phase one of the MDMP is the Analysis of the Operating Environment – this is MISSION SPECIFIC. What has the commander been asked to do? The MPKI staff should look to provide a detailed AOE – which is delivered in the P1B, the Short Peacekeeping Intelligence Estimate.
The MPKI staff should seek the Commander's direction through the intelligence dialogue in order to frame the MPKI products.
In addition, the MPKI staff should look to write the initial situation paragraph to warning order one.

Slide 7

The Phase One brief comprises of the work done during terrain and actor evaluations, overlaid with the situation integration and Actor COA development, as it pertains to a specific UN mission or task.

It will be covered in more details in future slides, and you will be provided with a rough example to illustrate the key elements.

The P1B situates the commander and the staff before they develop UN COAs to meet the mission requirement.

The AOE foundation will ensure the creation of 'golden thread' products – those products that assist in the P1B such as physical, human and information terrain overlays, key actor capabilities including POC considerations etc.

Slide 8

Key Message. The Phase One Brief (P1B) has a specific structure. This can be amended when looking at conventional or asymmetric environments, i.e. with a human-centric focus. What must be expressed is the importance of the Situation Integration element of the P1B.

Here is the P1B template in the handbook. This is a guide but provides a structure that the MPKI staff can follow to ensure that all relevant factors are included in the P1B. The red star highlights that situation integration is the most important element of the P1B and should have 50% of the time allocated to it. For example, if the P1B is 45 minutes in length, then 20 minutes should be allocated to the briefing of the situation integration.

The instructor should identify that other staff branches can assist in the production of the P1B, e.g. Physical terrain analysis can be assisted by the inclusion of engineering input, the human terrain can be assisted by POC or CIMIC expertise inclusion.

Slide 9

Phase One Brief – Summary

- Mission specific
- Not telling the Commander all you know
- No more than 45 minutes
- Focus on situation integration and not the ground
- Know audience
- Keep it simple
- Remember the 'Golden Thread' products

The P1B must be mission-specific – the AOE must be focused on the mission area.

A P1B should last no longer than 45 minutes – the focus of the P1B is the situation integration should have at least 20 minutes allocated to the briefing of the ML and MD COAs. The MPKI staff should be mindful of the audience being briefed. How does the Commander like the information to be briefed? Keep the brief simple. Ensure that relevant analysis is briefed coherently and simply.

Slide 10

Example of a Phase One Brief

The following example of a phase one brief is not consistent with the current scenario we provide.

Slide 11

Mission

- UNMMIG deploys in three conflict affected areas (sectors west, east, and north) of GARLAND, 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; and, where possible, to ASSIST the government in the re-establishment of State authority.

Sector East mission is to establish a TOB south west of BINGA to DISRUPT IK freedom of movement, REASSURE local population and IDPs iot to establish SECURE environment and ASSIST Government of GARLAND.

For the purposes of the P1B example, the AOE is on Sector East. BINGA is a made-up town. In conducting initial mission analysis, the MPKI staff can look to draw out the critical elements to focus on during the conduct of the AOE. In this example, the threat posed by IK, the human terrain considerations relating to the population in the vicinity of BINGA and the IDP/POC considerations.

Slide 12

Scope – Part One

- Vital Intelligence
- Key Assumptions and outputs (if applicable)
- Analysis of the Operating Environment
  Ground in General
  Ground in Detail
- Information Terrain
  GSM/Radio coverage
  Local media – TV and Radio – are they supportive of UN?
  Use of social media
  Local communication systems/meetings.
- Human Terrain Analysis
  Tribal/Ethnic Laydown – if important
  Key actors: NGOs, Key Leaders, Refugees etc.
  Pattern of life – If applicable
  HN Armed Forces

The scope of the P1B is as follows. During the conduct of their P1B, we should look to draw out the key analysis for each heading, i.e. how the factors analysed during each heading effect the Commander's missions and tasks.

Slide 13

We should look to draw out the key analysis for each heading, i.e. how the factors analysed during each heading effect the Commander's missions and tasks. The key learning outcome for this slide is that you should understand the situation integration and the briefing of the COA boards.

Slide 14

Vital intelligence:

At this stage of the P1B, the commander should be made aware of any vital intelligence that could affect the Commander's mission. The MPKI staff should look to assess what vital intelligence means in order to give a consolidated brief.

Slide 15

Analysis of the Operating
Environment (AOE)

Slide 16
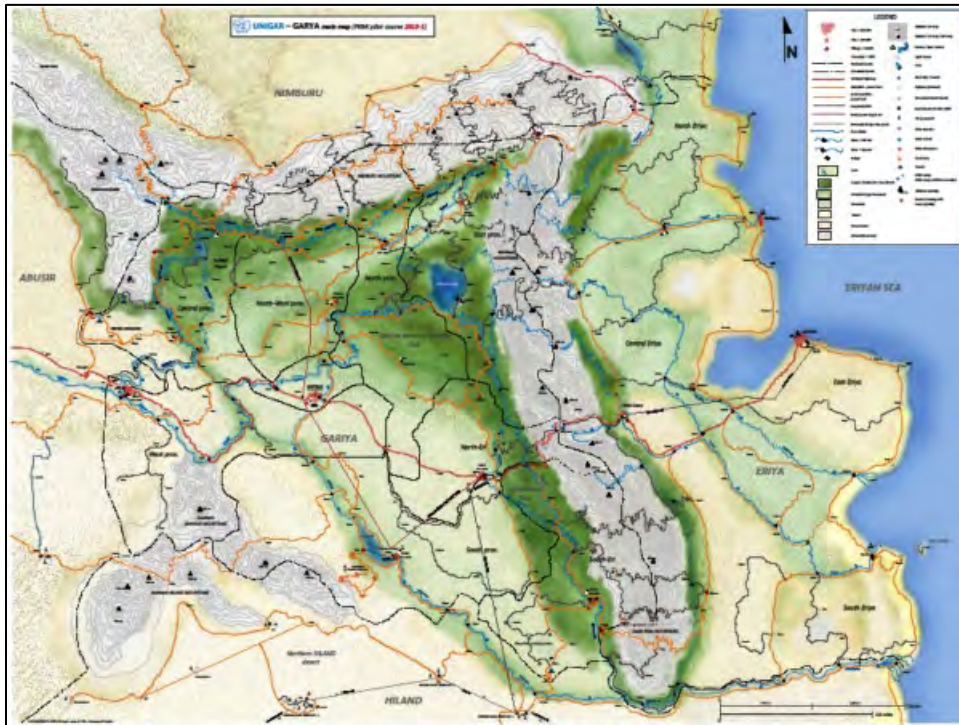
This slide is to illustrate that the MPKI staff are not to brief the entire Area of Operations but to focus on the analysis to the area of terrain that is pertinent to the mission.

Slide 17
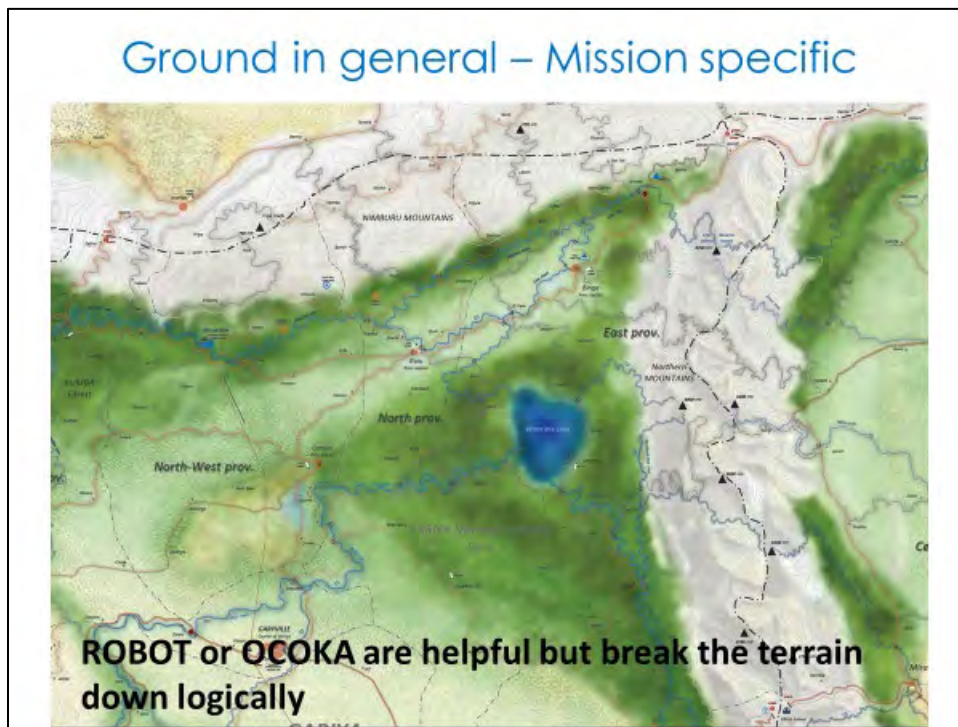
The ground in general. The briefer (as it could be GIS or engineer staff that briefs the ground) should look to provide key analysis of the ground in a structured manner; this could be from north to south, east to west; or by using acronyms such as ROBOT and OCOKA. In any case, the briefer should only brief that ground, in general, that is important to the conduct of the mission.

Slide 18
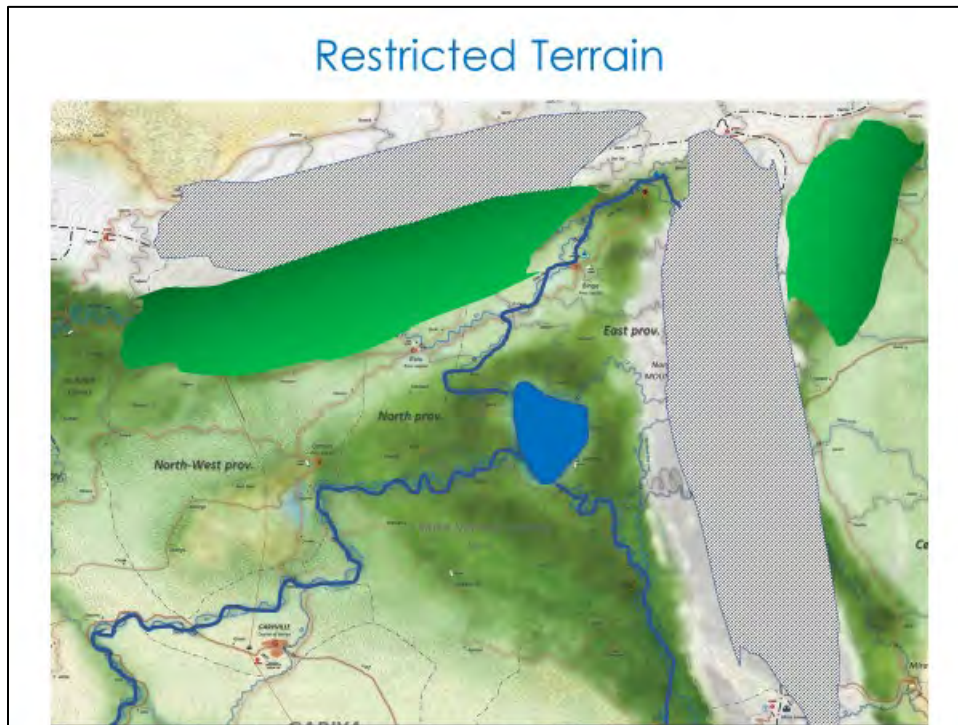
We should highlight the Combined Obstacle Overlay. This representation shows any areas of key or restricted terrain. This should be identified from the point of view of the (threat) actor and our (UN) capabilities. This diagram informs the commander how relevant actors can manoeuvre through the mission area, including our forces.

Slide 19
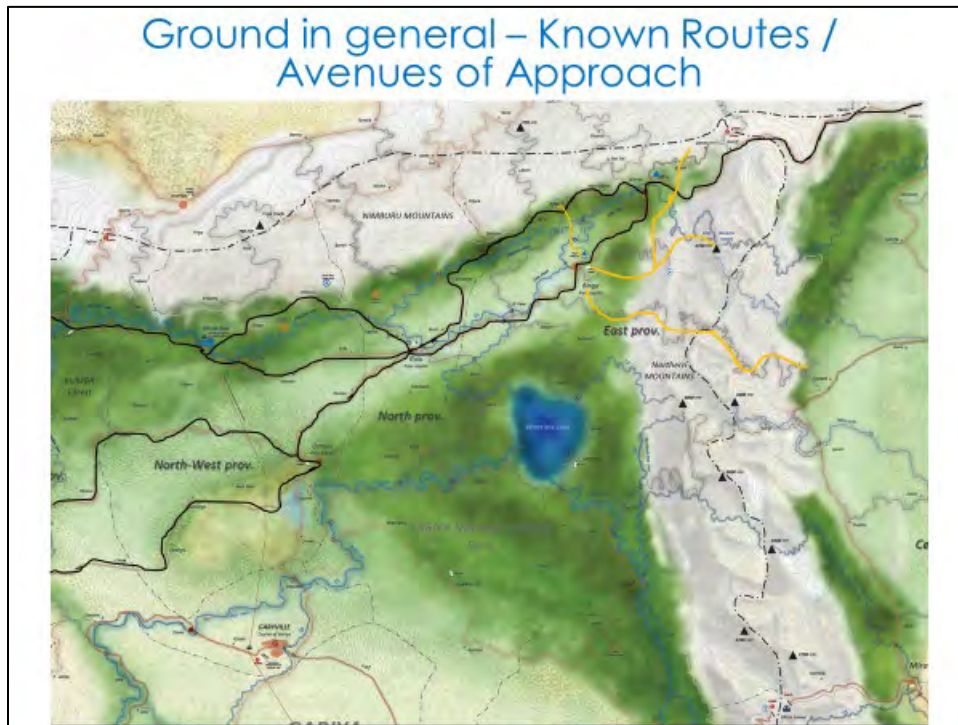
The MPKIO briefer should draw out the pertinent analysis such as assessment on route capabilities and whether knowledge gaps exist that require additional staff consideration (e.g. engineer recce to provide route assurance). The briefer should look to highlight any known timings to transit main and secondary routes in order to inform the staff about transit timelines.

Slide 20

The ground in detail.

This is where the MPKIO briefer should look to focus on the relevant mission area in more detail. In this example, the briefer should draw out the key analysis relating to the physical terrain required for the specific missions and tasks.

Slide 21

This is a continuation of the previous slide.

Slide 22

Information Terrain

Slide 23
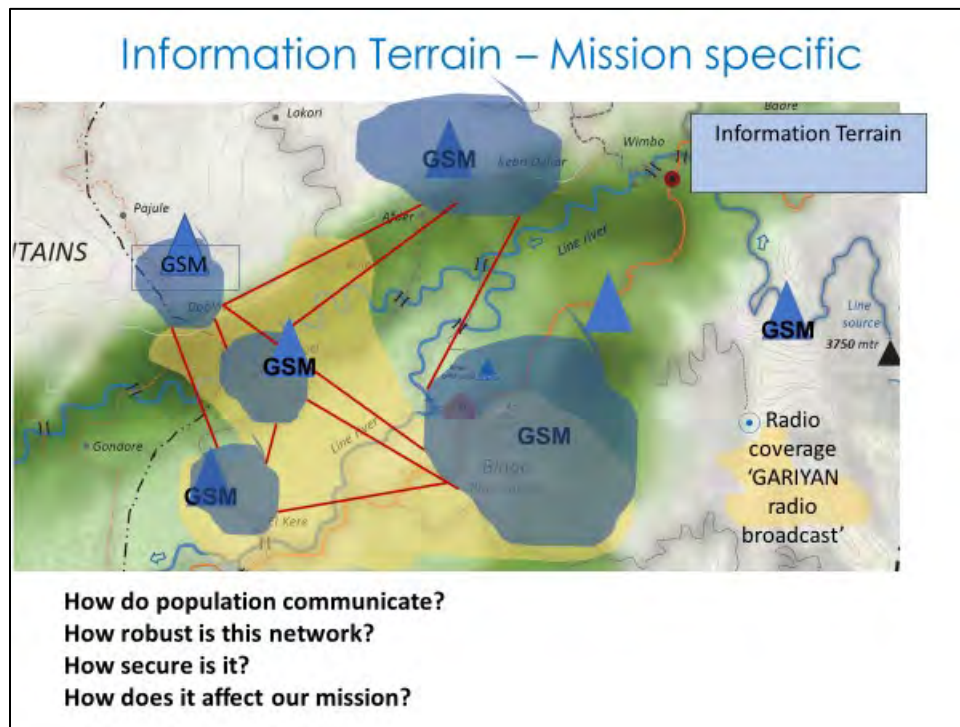
The MPKIO briefer should explain what key analytical deductions are required. They are highlighted on the slide.

Slide 24
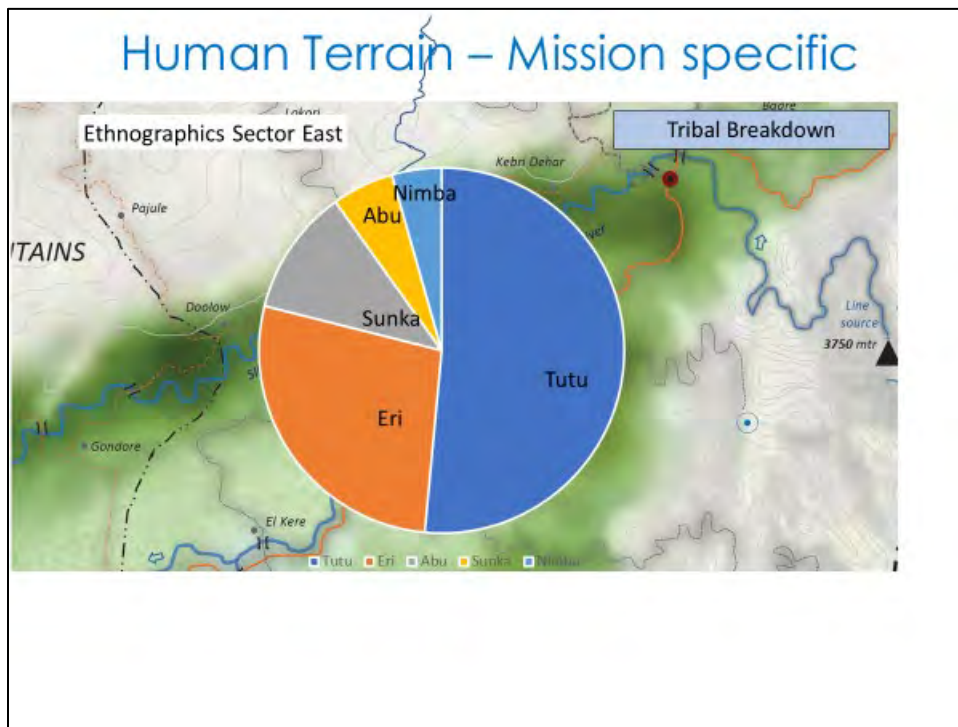
Slide 25

Within the human terrain analysis, the briefer should draw out the key ethnic and tribal groups that live within the mission area.

Slide 26
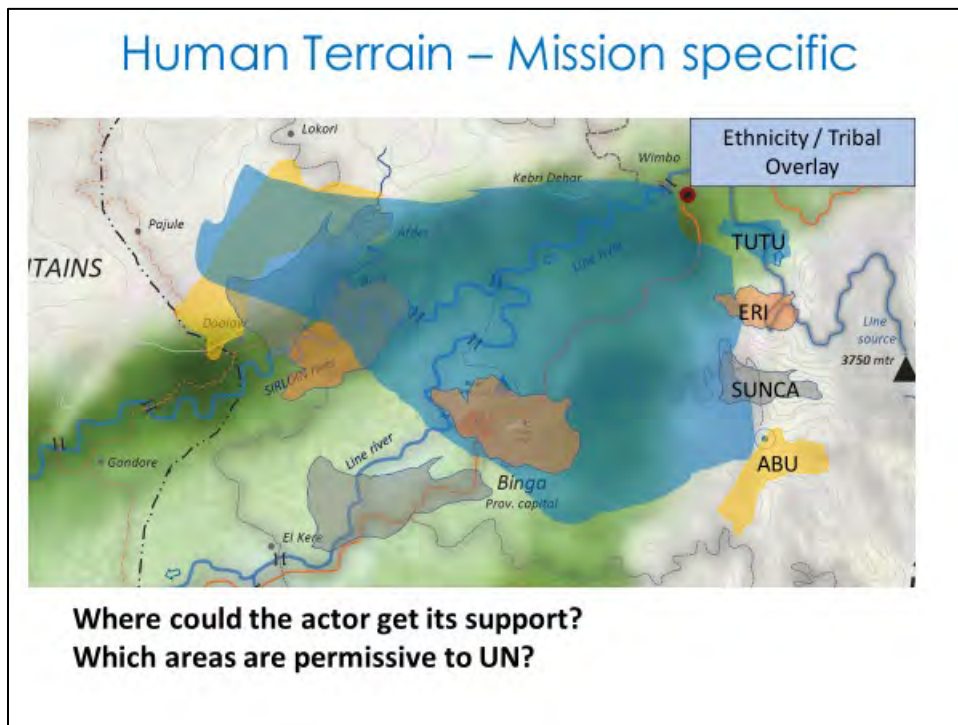
A tribal overlay enables the commander to understand the tribal and ethnic lay down within the AO. Within this mission context, the commander should be made aware of all the possible drivers for friction. This should include all the IDP camp considerations and understanding.

Slide 27
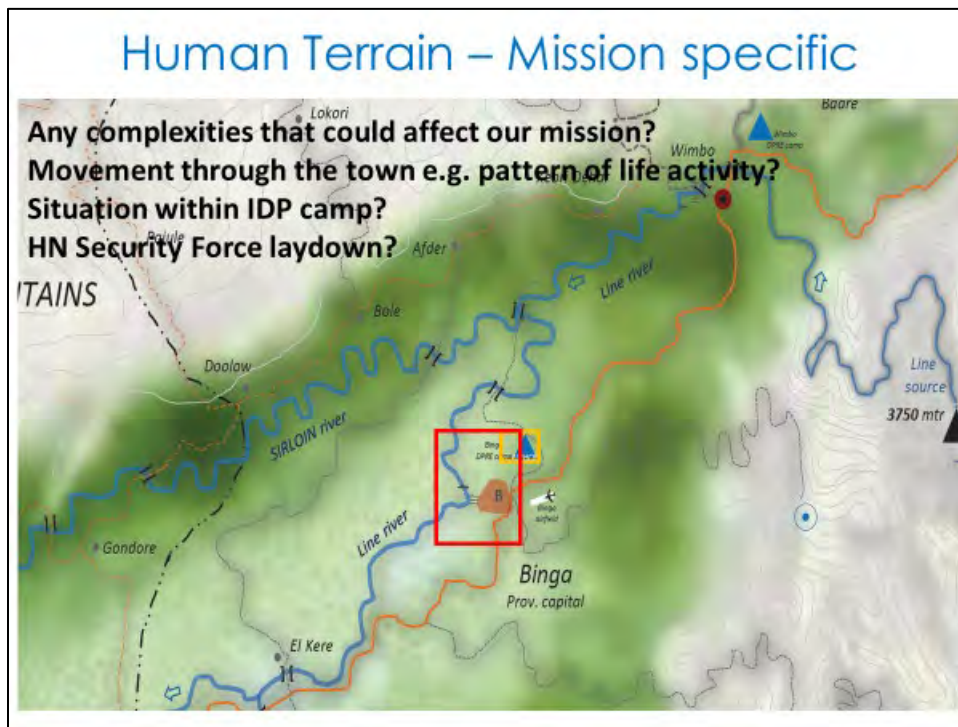
Ask these questions when it comes to human terrain:

▪ Any complexities that could affect our mission?

▪ Movement through the town, e.g. pattern of life activity? The situation within IDP camp?

▪ HN Security Force laydown? What does this mean to the commander?

▪ How will the human terrain situation affect their plan?

Slide 28

How does it affect the mission?
What pertinent detail is included here?

The briefer needs to explain the impact of the weather during the mission period—for example, any effect on acquisition assets and manoeuvre. The briefer should draw out the critical analysis that would inform the commander of the specific freedoms and constraints provided by the weather.

Slide 29
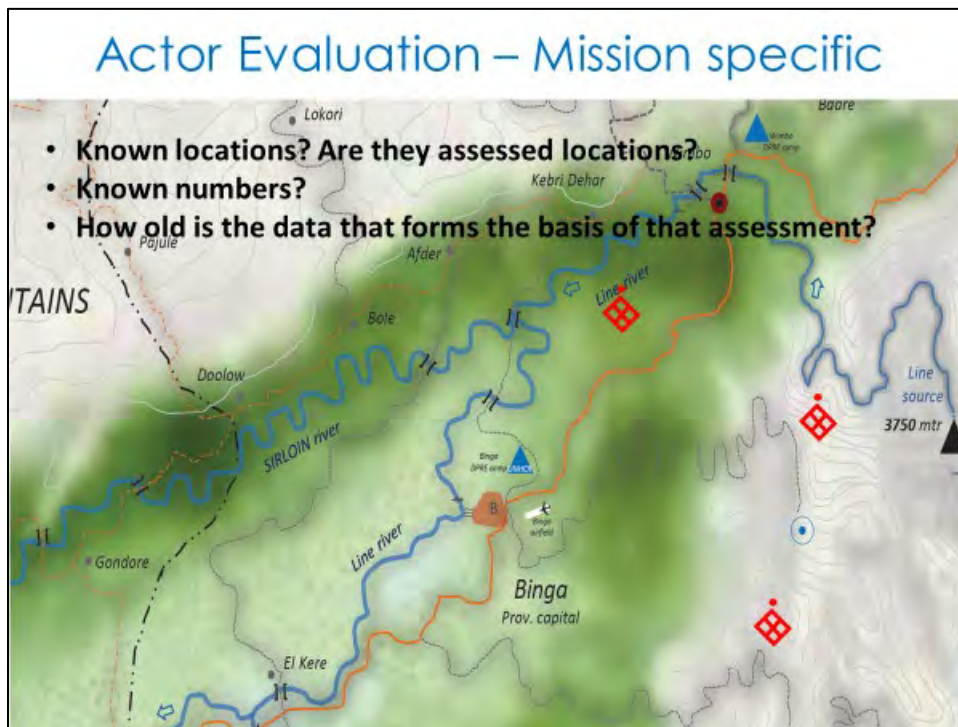
Here are some questions the MPKIO should answer when briefing:

- Known locations? Have they assessed locations?

- Known numbers?

- How old is the data that forms the basis of that assessment?

Ensure a Mission specific actor evaluation and outlining the detail above for all known relevant actors.

Slide 30
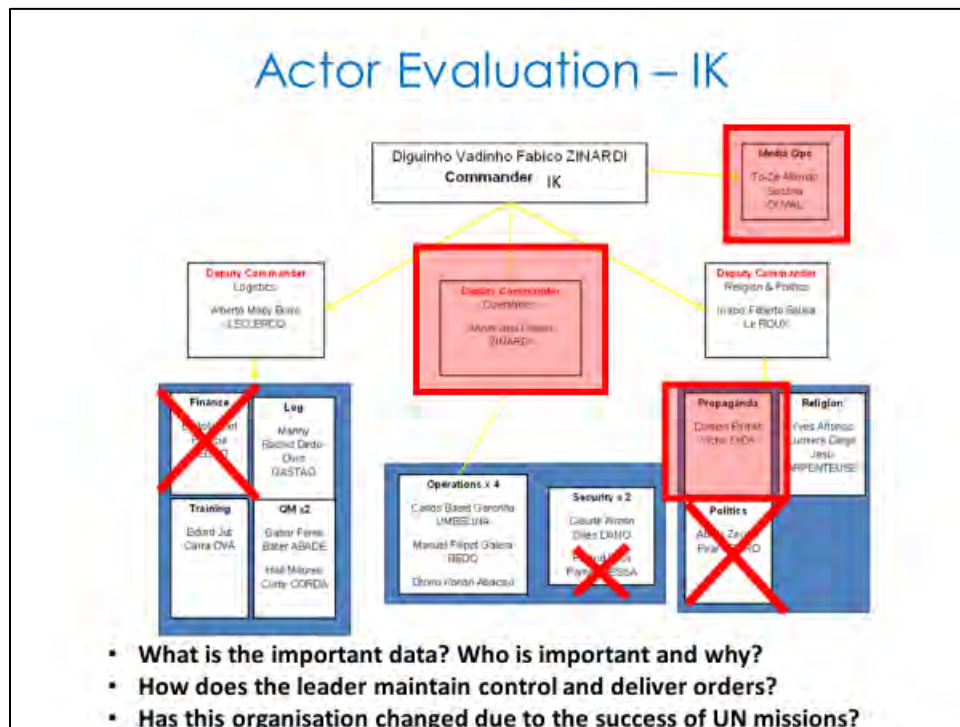
The hierarchy of the group. Draw out key conclusions about the efficiency of the group…. What is currently known and unknown and how the group is likely to arrange itself. Key actors, whom the UN should look to affect.

Slide 31

Here we ask the questions:

- What are the key capabilities that the group have?

- How are they likely to be employed?

Answers are key to the briefing.

Slide 32
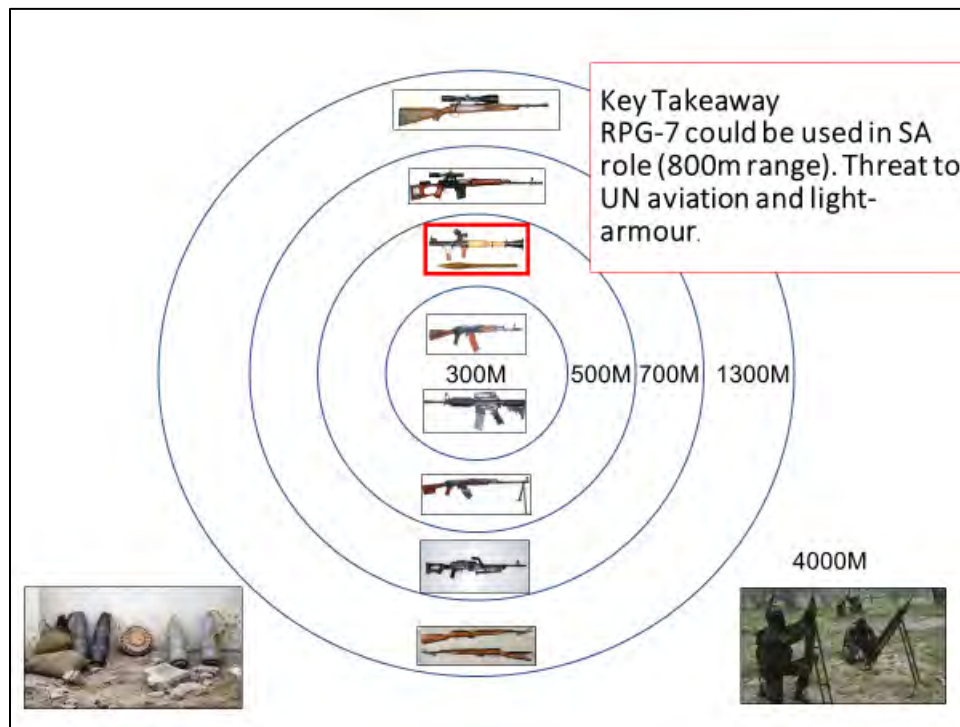
Here note the RPG 7 variants are a threat to UN aviation and vehicles which lack the defensive aide suites and armour to counter the HEAT variants. Effective weapon ranges. How is the threat actor likely to use its capabilities on the UN?

Slide 33

Strengths:

The decentralised leadership model means that networks reconstitute quickly, even after key leaders have been eliminated. Moreover, even if one Katibat is critically weakened due to intel-led Security Force operations, others remain untouched and can assume the weakened Katibat's operational responsibilities.

COMSEC and OPSEC. This means it is difficult to use modern surveillance methods against the group.

Combat Experience on the 6th Continent. The group has access to combat-hardened fighters making them more effective fighters than the GAF and Abusir Forces; their tactical-level engagements are generally successful.

Ideology. The group's hard-line religious ideology makes them effective fighters. It also facilitates recruitment and the deployment of suicide bombers.

Access to sophisticated weaponry. The group's links to extremists operating on the 6th Continent and its control of desert trafficking routes means that it has access to increasingly modern firearms and ammunition.

Reputation/Propaganda. Fear of the group means that host nation (GAF and Abusir) security forces do not project force at night, and rarely stand and fight if a retreat is possible. This allows the group significant freedom of movement and action.

Ethnic make-up. The group's ethnic make-up allows it to use the local population as cover. This assists reconnaissance operation, and its ability to raise funds in urban areas through legitimate businesses.

Weaknesses:

The requirement for religious justification acts as an operational constraint. The group needs to justify its operations and target set to its base, let them lose popular support. The group is, therefore, vulnerable to effective counter-narratives.

Physical Terrain. Considering its Area of Operations comprises of the desert, there is little natural foliage to cover the large-scale movement. This is exacerbated during the wet season when the group is forced to use metaled roads. This makes the group vulnerable to aerial surveillance and attacks, undermining its ability to scale its operations.

Human Terrain. Support for IK is far from universal among the Abu. Indeed, most Abu resent the group for making them a pariah ethnic group in Garya. This has the potential to erode IK OPSEC as both UNMIGAR, and the GAF are likely (if security in outlying areas improves) to find sections of the population willing to act as informers, thereby reducing its FOM.

Composition. The fact that some personnel have fought in and been radicalised by the war on the 6th Continent makes the group less ideologically coherent than has been the case in the past. Evidence of this comes in the content of sermons of religious leaders associated with those that have fought on the 6th continent and those that have not. It is assessed that tensions between these groups make fictionalisation an increasingly realistic possibility. UNMIGAR/GAF strategic messaging could focus on this to weaken the group by encouraging in-fighting.

Limited access to modern armour defeating weapons systems. This affords UNMIGAR an advantage when moving in IK-dominate areas.

Lack of encrypted real-time communications systems. While this does improve COMSEC, it reduces the group's capability to react to surprise friendly force operations.

Opportunities:

Weak host nation security presence in the border and other inaccessible areas means the group has the potential to expand its presence.

Expanding links with the AWF. The group has the potential to widen its AO to Sector North and to conduct operations that will put additional pressure on the GAF.

Lack of formal economic opportunities available to the local population (Abu, Eri, and Nimba) means that the group can at least maintain and probably increase its recruitment. It is a realistic possibility that IK could widen its recruit and support base to non-traditional support groups.

Structural causes of the conflict (political and socioeconomic isolation of non-Tutu groups) remain unchanged across the country. This makes future alliances (ENLF, EIMF, Linohas, etc.) of convenience a realistic possibility.

Threats:

Deployment of UNMIGAR (and its mandate to professionalise the GAF) will reduce IK freedom of movement/action.

As Garya stabilises, economists expect Foreign Direct Investment in extractive industries to increase. This will increase employment opportunities for minority groups in the country. In time, this is likely to lead to the increasing integration of minority groups into the formal economy. Typically, this reduces the appeal of extremist groups.

Agreement of Abusir and Garyan Security Forces to work together on cross border operations. This reduces space for IK reorganisation and consolidation.

Ongoing International CT efforts which have now moved towards eastern Abusir. Drone attacks are expected to erode existing C2 structures at a rate that is faster than the group's ability to reconstitute – the group's decentralised structures notwithstanding.

Centre of Gravity:

COG – support of the population.

CCs. Recruitment contributes to OPSEC, to its ability to raise finances through front businesses, FOM and Action, legitimacy.

CRs. Sufficient revenues to pay recruits, maintaining the support of religious leaders to justify operations, maintaining a narrative of success, maintain the freedom to proselytise, capacity to deliver underlying security and some services to the population under its control.

CV – vulnerability to sophisticated counter-narratives/strategic messaging, expansion of state security, economic development, expansion of government services, fringe group operations, criminal activity of some members/exploitation of the local population.

So what? A sophisticated CT strategy is required to target the group's CRs.

UNMIGAR, X-border (international) CT kinetic operations and the professionalisation of the GAF should create the operational space necessary for economic development, the expansion of government services to minorities, and an end to impunity for

criminal/terrorist activity. This should reduce the group's appeal to its base, thereby undermining recruitment and its ability to raise funds.

Sophisticated counter-narratives can undermine the group's religious reason to deter and reduce the group's coherence.

Slide 34

Situation Integration

Slide 35

MDCOA.

IK will conduct an aggressive campaign of sophisticated attacks on UNMIGAR FOBs throughout Sector West. These sophisticated attacks will involve IDF, SVBIEDs, PBIEDs, and ground troops to assure maximum casualties, denying UNMIGAR access to most urban areas.

Intent/Purpose. To deny UNMIGAR access to all rural and most urban areas of Sector West, and to disrupt TCC political willingness to sustain UNMIGAR.

End state. Being forced to increase security at its bases makes UNMIGAR a static force, unable to deploy to more than a handful of urban areas. IK increases its control to more areas of Sector west.

SOM:

Shaping. Online hate speech targeting UNMIGAR increases. UNMIGAR becomes the target of radical preachers. The local population is warned not to cooperate with UNMIGAR, and those that do are targets for reprisal. IK moves weapons caches and a large number of fighters into key urban areas and increases IED/SVBIED/PBIED construction. Several safe houses are occupied. Reconnaissance and surveillance of UNMIGAR FOBs are conducted. IDF launch sites are prepared, and target registration begins from multiple launch sites.

Decisive. A series of attacks on UNMIGAR FOBs occur.

Sustainment. IK increases its control throughout the sector west, including in urban areas. Messaging/propaganda campaign to undermine UNMIGARs standing as a credible security provider in the eyes of the local population is maintained and increased.

Tactical Functions:

Protection. The group has no access to armour, but its structure, disposition, and ethnic composition provide a high level of OPSEC. The group also has good COMSEC.

Information and Intel. Can move within the local population—benefits from a local, albeit relatively small, support base which offers information on UNMIGAR movement.

Firepower. Small arms and IEDs (PBIEDs and SVBIEDs). Effective against UNMIGAR convoys.

Manoeuvre. IK is highly mobile. 4x4 vehicles offer an off-road capability, which reduces in the wet season. IK can also operate on foot over long distances and in urban areas.

Logs. Fighters can self-sustain for short periods. Use of local population/services possible due to support network and strong financial position.

C2. The group is widely dispersed, and its decentralised command structures offer operational freedom to individual groups.

Identifying Indicators & Warnings

Increase in anti-UNMIGAR propaganda (online, graffiti, religious sermons);

Reports of increased movement of IK cadres into urban areas, including the presence of extremists;

Reports of IK taking over safe houses in the area;

Increased surveillance of UNMIGAR FOBs;

Testing of UNMIGAR security procedures involving unarmed personnel by day and night;

Reports of movement of arms/explosives into urban areas;

Reports of large-scale attack rehearsals taking place;

IDF attacks from multiple launch sites indicative of ranging and target acquisition ongoing;

A significant change to the pattern of life in and around UNMIGAR bases;

Large gatherings of military-aged males in and around UNMIGAR bases;

Vehicles are moving at speed towards UNMIGAR gates.

Items of High Importance List:

Weapons caches;

IED makers;

Religious leaders;

Military commanders;

Financial enablers (financiers, front businesses).

Slide 36

MDCOA.

IK will conduct an aggressive campaign of complex attacks on UNMIGAR FOBs throughout Sector West. These complex attacks will involve IDF, SVBIEDs, PBIEDs, and ground troops to assure maximum casualties, denying UNMIGAR access to most urban areas.

Intent/Purpose. To deny UNMIGAR access to all rural and most urban areas of Sector West, and to disrupt TCC political willingness to sustain UNMIGAR.

End state. Being forced to increase security at its bases makes UNMIGAR a static force, unable to deploy to more than a handful of urban areas. IK increases its control to more areas of Sector west.

SOM:

Shaping. Online hate speech targeting UNMIGAR increases. UNMIGAR becomes the target of radical preachers. The local population is warned not to cooperate with UNMIGAR, and those that do are targets for reprisal. IK moves weapons caches and a large number of fighters into key urban areas and increases IED/SVBIED/PBIED construction. Several safe houses are occupied. Reconnaissance and surveillance of UNMIGAR FOBs are conducted. IDF launch sites are prepared, and target registration begins from multiple launch sites.

Decisive. A series of attacks on UNMIGAR FOBs occur.

Sustainment. IK increases its control throughout the sector west, including in urban areas. Messaging/propaganda campaign to undermine UNMIGARs standing as a credible security provider in the eyes of the local population is maintained and increased.

Tactical Functions:

Protection. The group has no access to armour, but its structure, disposition, and ethnic composition provide a high level of OPSEC. The group also has good COMSEC.

Information and Intel. Can move within the local population—benefits from a local, albeit relatively small, support base which offers information on UNMIGAR movement.

Firepower. Small arms and IEDs (PBIEDs and SVBIEDs). Effective against UNMIGAR convoys.

Manoeuvre. IK is highly mobile. 4x4 vehicles offer an off-road capability, which reduces in the wet season. IK can also operate on foot over long distances and in urban areas.

Logs. Fighters can self-sustain for short periods. Use of local population/services possible due to support network and strong financial position.

C2. The group is widely dispersed, and its decentralised command structures offer operational freedom to individual groups.

Identifying Indicators & Warnings

Increase in anti-UNMIGAR propaganda (online, graffiti, religious sermons);

Reports of increased movement of IK cadres into urban areas, including the presence of extremists;

Reports of IK taking over safe houses in the area;

Increased surveillance of UNMIGAR FOBs;

Testing of UNMIGAR security procedures involving unarmed personnel by day and night;

Reports of movement of arms/explosives into urban areas;

Reports of large-scale attack rehearsals taking place;

IDF attacks from multiple launch sites indicative of ranging and target acquisition ongoing;

A significant change to the pattern of life in and around UNMIGAR bases;

Large gatherings of military-aged males in and around UNMIGAR bases;

Vehicles are moving at speed towards UNMIGAR gates.

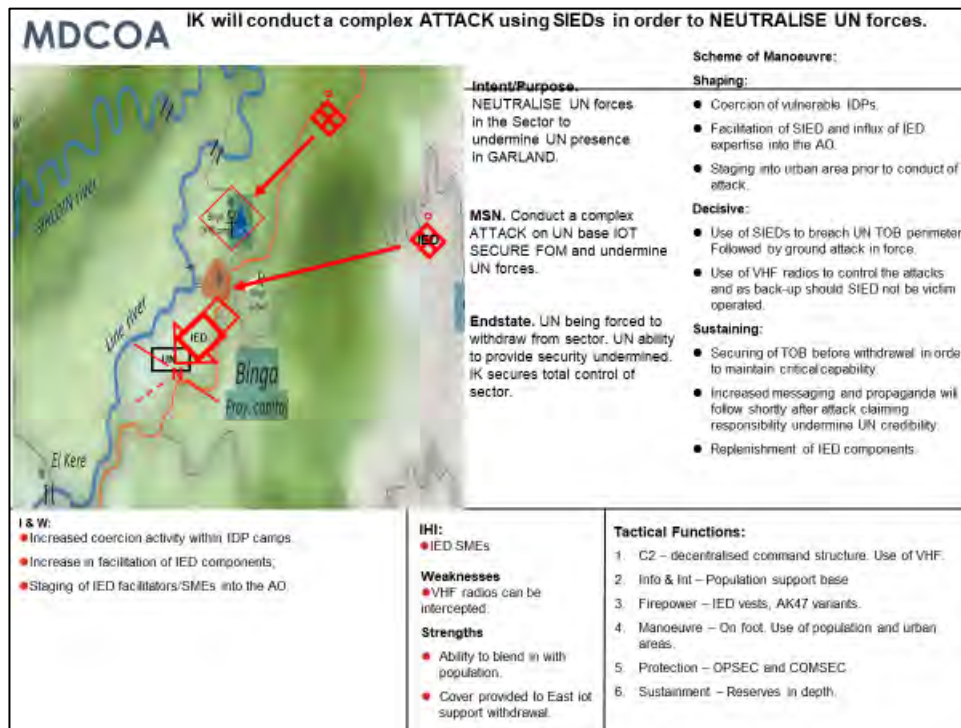Items of High Importance List:

Weapons caches;

IED makers;

Religious leaders;

Military commanders;

Financial enablers (financiers, front businesses).

Slide 37

Here are the MAI and TAIs transcribed on the event overlay.

Slide 38

This slide is used to inform the commander what the MPKI staff believe are the current PIRs relating to this AOE. This is an opportunity for the commander to confirm/change the MPKI effort. In addition, the MPKI staff should inform the commander where they have critical intelligence gaps, and this will enable the commander to prioritise acquisition assets, at this stage, to close some of the intelligence gaps.

Slide 39

Verbal Briefs – Tips

- Remove distractions
- Follow formats, avoid scripts
- Determine time to brief- stick to it
- Identify and arrange aids
- Pertinent information only
- Briefer- experience more important than rank
- Eye contact
- Rehearse – this is vital

Here are some briefing tips.

Remove distractions. The instructor should inform the students that it is important to remove distractions prior to briefing the commander.

Follow formats / avoid scripts. Formats are useful in order to structure the brief coherently. The P1B format in the handbook is a simple structure against which the MPKI can look to identify useful headings to inform no detail is missed.

Determine the time and stick to it. Ensure that you ask the commander how long you must brief. Should you P1B time be limited, it allows the MPKI staff to prioritise what is briefed to the commander – e.g. focus on the situation integration.

Identify and arrange aids. Ensure that the MPKI staff are aware of stage managing the P1B – ensure that overlays and briefing products are arranged coherently and logically. That transitions between overlays are rehearsed.

Pertinent information only. Do not brief the commander all that you know. Brief the commander what they need to know.

Experience is more important than rank. The rank of the briefer is not important. Ensure that the commander is being briefed by the individual that has the most knowledge about the subject matter being briefed.

Eye contact. This helps the briefer engage with the audience; in doing so, it ensures the audience is more likely to assimilate the information being briefed.

Rehearse—the most critical element in preparing for a brief. The instructor should ensure that the students understand that they have to rehearse. That is planning the AOE timeline, that they factor in the time to do a full rehearsal. A rehearsal will enable the MPKI to identify areas for development, but also make an assessment on timings for each element.

Slide 40
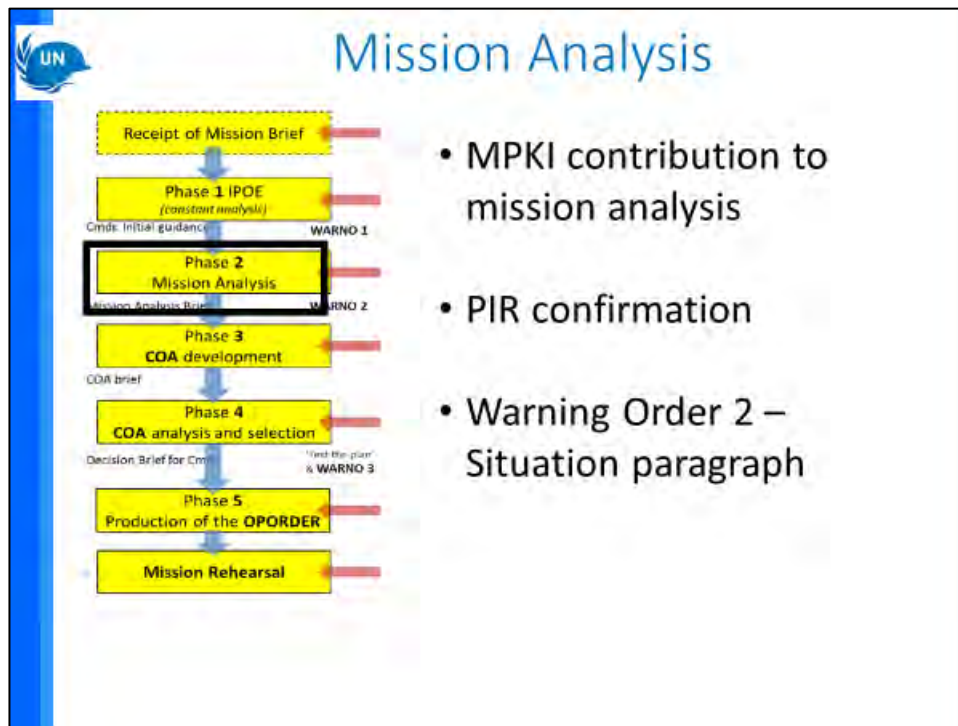
Phase Two is where the commander provides greater direction to their staff. This will enable the staff to understand the commander's thinking and identify the required COAs for further development.

MPKI support is critical to assist the commander and the planning staff. The MPKI staff should be aware that the commander will ask themselves at least four questions:

- What is my higher commander's intent?

- What are my specified and implied tasks?

- What are my freedoms and constraints?

- Has the situation changed, and in doing so, has it influenced my mission?

The MPKI staff should ensure that the Commander understands the threats and risks.

MPKI staff will confirm with the commander that the current PIRs are correct.

MPKI staff should look to update the situation paragraph for warning order 2 if that is required.

Slide 41
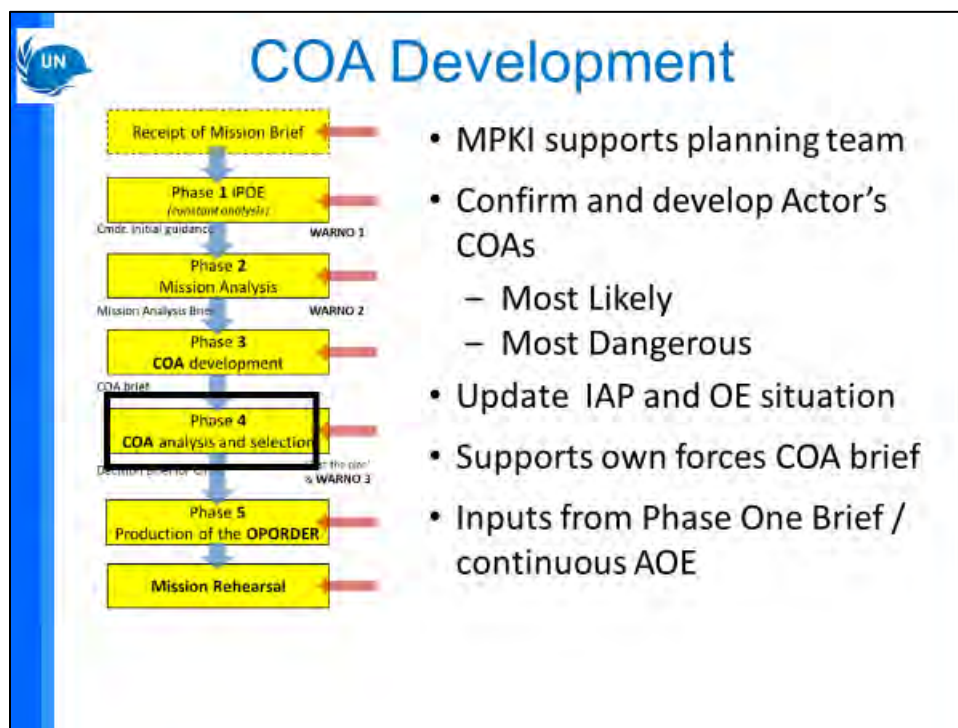
During this phase, the COA development teams will be working on possible COAs based on the commander's brief following mission analysis. The MPKI staff will provide support to each COA development group to provide SME advice regarding the AOE. MPKI Staff will still be conducting AOE and continue to develop understanding in addition to provide mission-specific AOE support. MPKI staff will support the COA development teams by 'testing' the COAs as they are being developed.

Slide 42
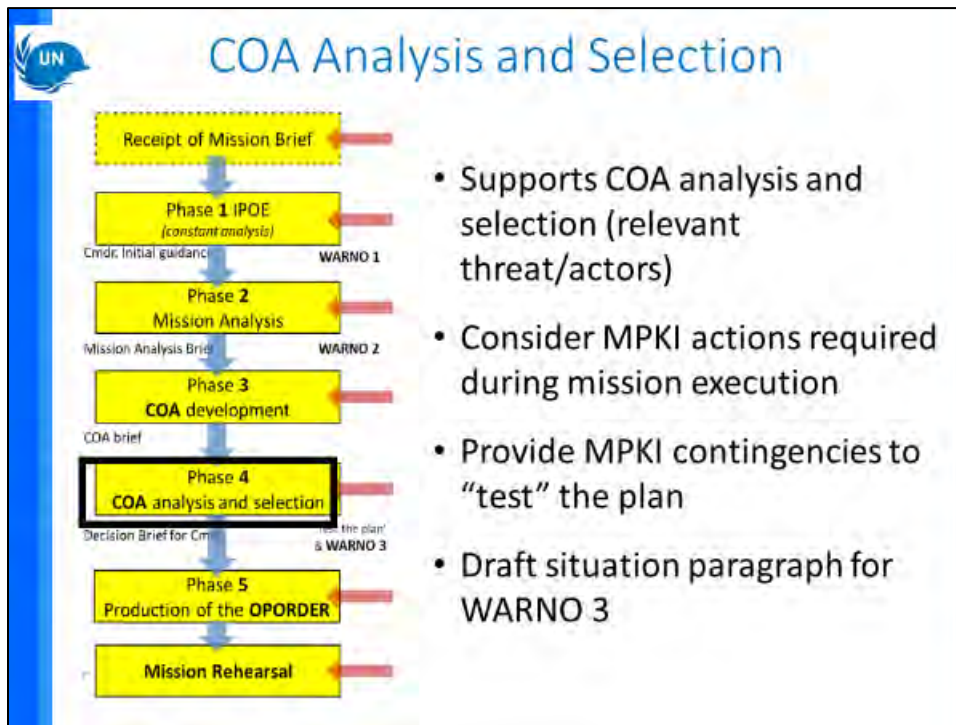
The commander will receive a back briefly from the COA development teams.
The commander will assess and analyse each brief and provide direction on which COA has been selected. The commander could also ask the staff to combine COAs and provide further development.

The MPKI staff should provide input to test the chosen COA. This will enable the identification and mitigation of known threats and risks. The MPKI staff should look to inform the commander where MPKI activity needs to take place during each stage of the chosen COA, such as acquisition activity. The MPKI staff should provide an update to the situation paragraph for warning order 3 if required.

Slide 43
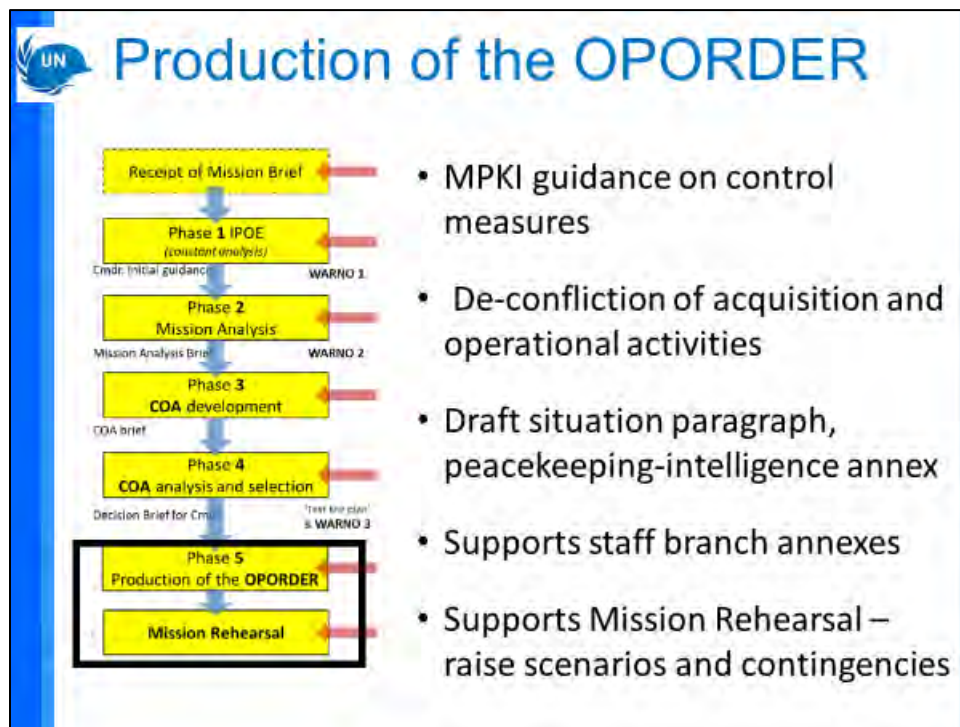
At this point in time, the staff will be writing an Operation Order to inform subordinate elements what missions and tasks are to be conducted, and the MPKI staff will draft the supporting intelligence annex and situation paragraphs. The MPKI staff should also look to provide guidance to the commander and planning staff regarding control measures, such as deconfliction of acquisition capabilities. Mission rehearsal – the role of the MPKI staff, is to raise realistic / testing scenarios. This confirms that the plan and its contingencies are viable.

Slide 44

Takeaway

- PKI support for the MDMP provides inputs to be integrated during all phases of the planning process

- The Phase One brief is the MPKI cell's moment to situate and inform the Command and Staff prior to the conduct of planning

- An updated peacekeeping-intelligence picture and 'testing' of the potential COAs will inform planning and shape the COA Brief

- The role of the MPKI staff during mission rehearsal is to raise realistic and relevant scenarios involving the physical, information and human terrains to test the plan and ensure that it is viable in relation to possible contingencies

Summary

In summary, the MPKI staff support all stages of the MDMP process. Staff must be proactive and look to provide expert situational awareness inputs.

The P1B is the MPKI staff's initial opportunity to situate the commander and the planning staff. The P1B products can be used throughout the MDMP to further assist planning.

Throughout, the MPKI staff should look to provide updates when new intelligence is raised or where the situation changes. The MPKI staff should also look to test the plan by including realistic actor scenarios in order to mitigate the identified risks and threats.

Lesson
3.6

POC Planning

Starting the Lesson

Slide 1

Lesson 3.6
Intelligence Support to POC
Planning

We have looked at how PKI can support military planning in the MDMP process. The tools we have taught you are highly adaptable, and we expect you to shape them to fit any intelligence requirements for your commander. An important planning requirement for a UN Mission is for the Protection of Civilians or POC Planning framework, which as an MPKIO, we need to be prepared to support.

Slide 2
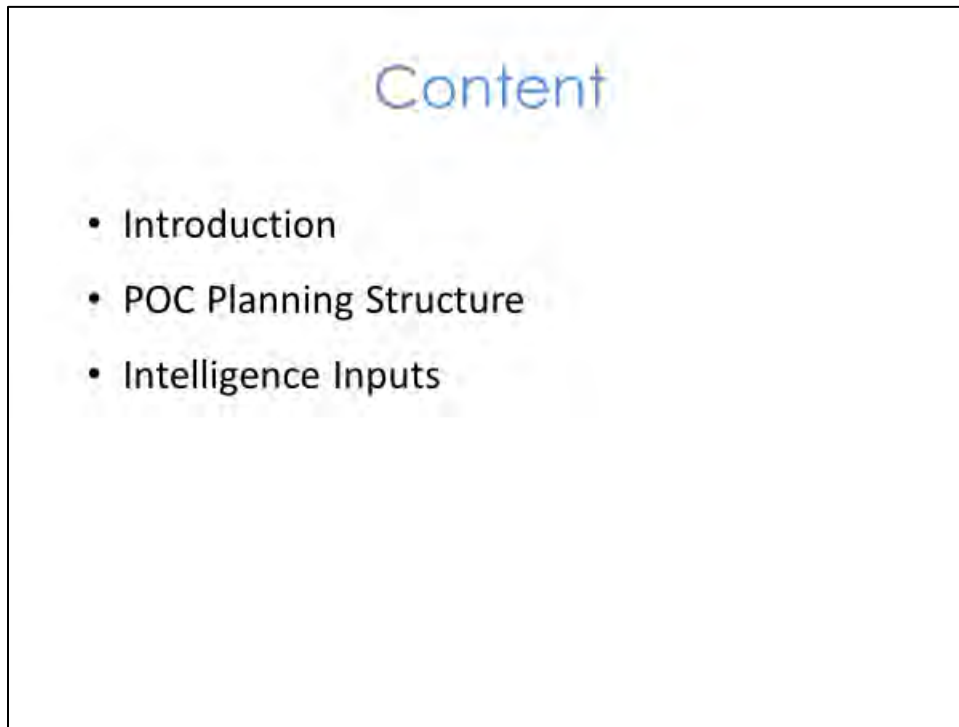
Here is the lesson content

Slide 3

Learning Outcomes

- Explain why POC Planning is important
- Identify intelligence inputs to POC Planning

On completion of this lesson, you will be able to explain the 3 Column Format and accurately derive, identify and fill in relevant factors, deductions and outcomes.

Slide 4

Above everything else is the fact that failure to protect may result in the loss of civilian life, which is tragic and the most important consequence. But POC is increasingly also coming to define the success and reputation of UN missions, meaning there are implications for the credibility and legitimacy of the United Nations and UN Peacekeeping involved.

Not all peacekeeping missions have a POC mandate. Yet, new mission routinely has been given a POC mandate. Additionally, since all the largest missions have a POC mandate, nearly all peacekeeping personnel work in a mission with POC mandate.

While agreement on the importance of POC was established quickly, finding consensus on what peacekeepers are expected to do in the context of POC has been difficult. In 2010, DPKO-DFS developed a commonly agreed upon Operational Concept, and 2015 the Policy on POC in Peacekeeping was created. It is important that MPKIOs understand the importance of POC and how best to focus their efforts to produce intelligence products that support POC planning.

Slide 5

POC Planning is similar to the MDMP process. Here is the basic POC Planning framework.   While it is the same overarching process as the MDMP, the component parts may be a bit different.

Slide 6
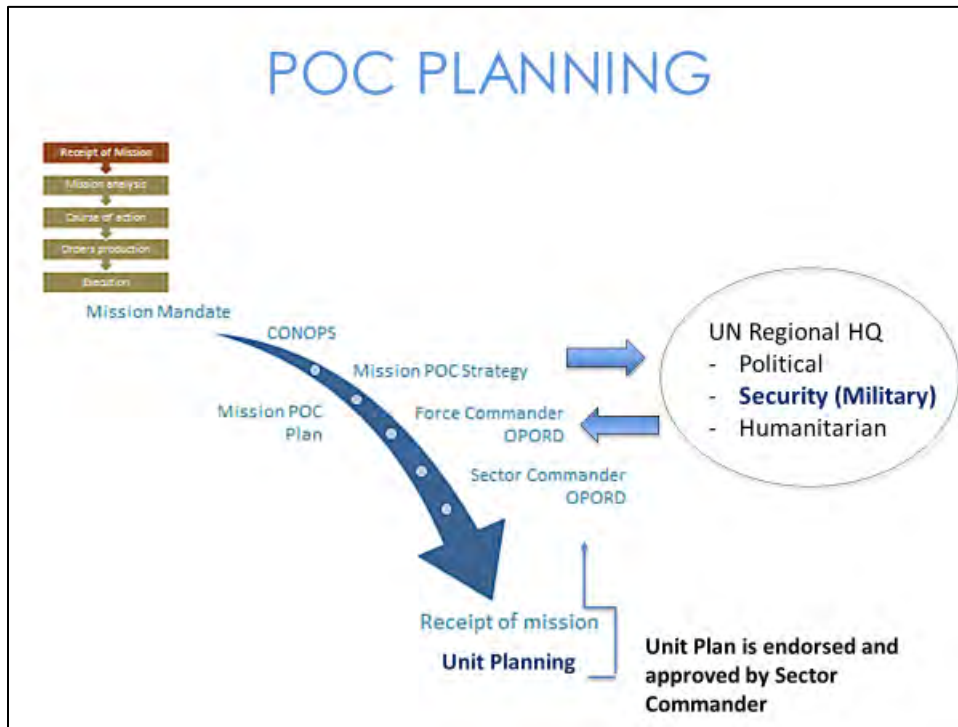
Key Message: POC Planning flows from the Mission Mandate through each planning level, culminating in a POC component of the OPORD/PLANORD to Unit Commanders. Commanders are required to consider POC Planning in all their mission planning.

The Mission Mandate is always going to comply with and reflect over-arching laws and policies that require the protection of civilians. The Mission Mandate triggers POC Planning in parallel with other mission planning. The product of POC Planning is not so much a plan, but POC considerations to be incorporated in all mission planning.

POC Planning flows down to the Force Commander's OPORD, Sector Commander's OPORD to Unit Commanders who will be tasked with conducting POC Planning in their AOR as a part of their Receipt of Mission.

Note that at the sector level, close liaison with the Regional HQ is essential in understanding the Political and Humanitarian aspects of POC, in addition to the Security aspect of POC. The three pillars of responsibility in a UN mission are Political, Security and Humanitarian. The Military component's primary responsibility is within the security pillar. Therefore, the sector and force HQs must ensure that they support the unit commanders by coordinating with and help create synergistic efforts in support of POC planning via the other Mission components.

Unit POC Planning will focus on understanding the specific vulnerabilities to civilians in their AOR and planning proactive measures to both prevent and pre-empt abuses against civilians. Reactive measures to respond to abuses and consolidate those

responses in order to reduce the effects of abuses against civilians that have not been prevented.

Force and Sector HQs will follow the POC planning process, but Unit Commanders may use their national planning processes to create the POC elements of their plans, though they will be tasked with providing POC outputs in the required POC format so that Sector and Force HQs understand the tactical POC challenges and threats.

Once a unit commander develops their plan, the next higher HQs must endorse and underwrite that plan. This includes accepting the risks and assisting the united commander in mitigating the risks. This may include accepting responsibilities for certain NAIs and TAIs inherent in the plans.

Slide 7
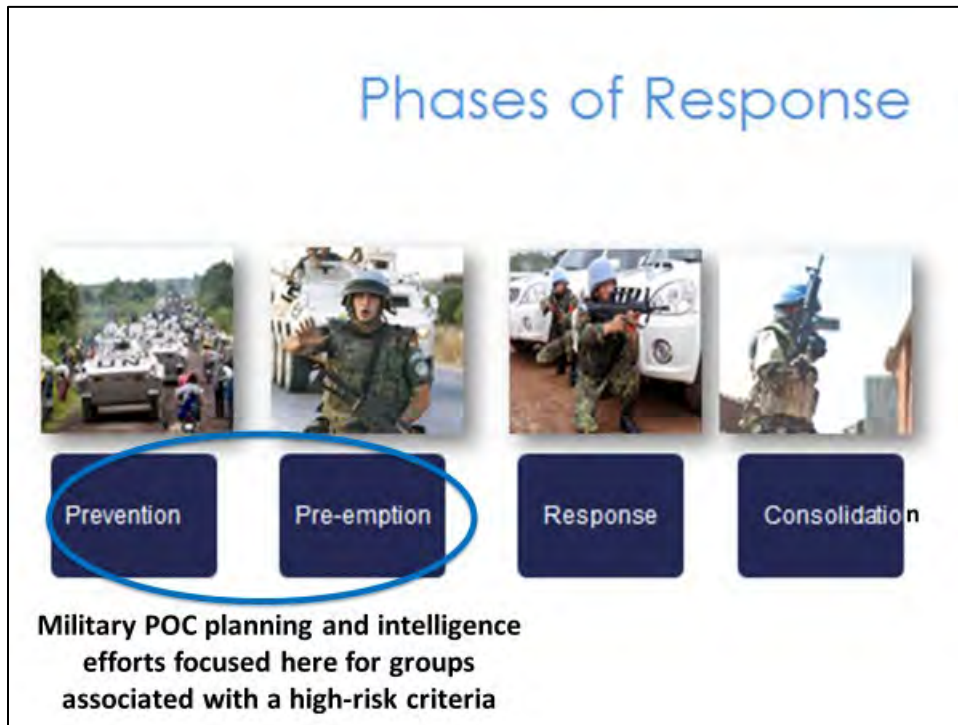
Key message: How UN peacekeeping missions respond to POC threats can be divided into four phases. The four phases are not sequential, and missions will often find their activities fall into different phases in different parts of the country at the same time, and some of the same activities may take place across all phases.

It is enough to know that the objective of this approach is to either eliminate a threat, or mitigate the risk to civilians associated with that threat. It must also be noted that these phases do not necessarily occur in sequential order and may be undertaken simultaneously or independently.

Here are the four phases:

- Prevention,
- Pre-emption,
- Response and
- Consolidation (threat has been mitigated/eliminated)

Action is necessary across all four phases, in line with the proactive approach taken by peacekeeping missions. In the prevention and pre-emption phase, the incident has not occurred yet, and missions can more effectively avoid violence by acting in these phases. In the response phase, missions respond to a violent incident that has already occurred, and in the consolidation phase missions support post-conflict activities. During

military planning for POC; intelligence efforts should be focused on the prevention and Pre-emption phases for groups associated with a high-risk criterion.

Slide 8
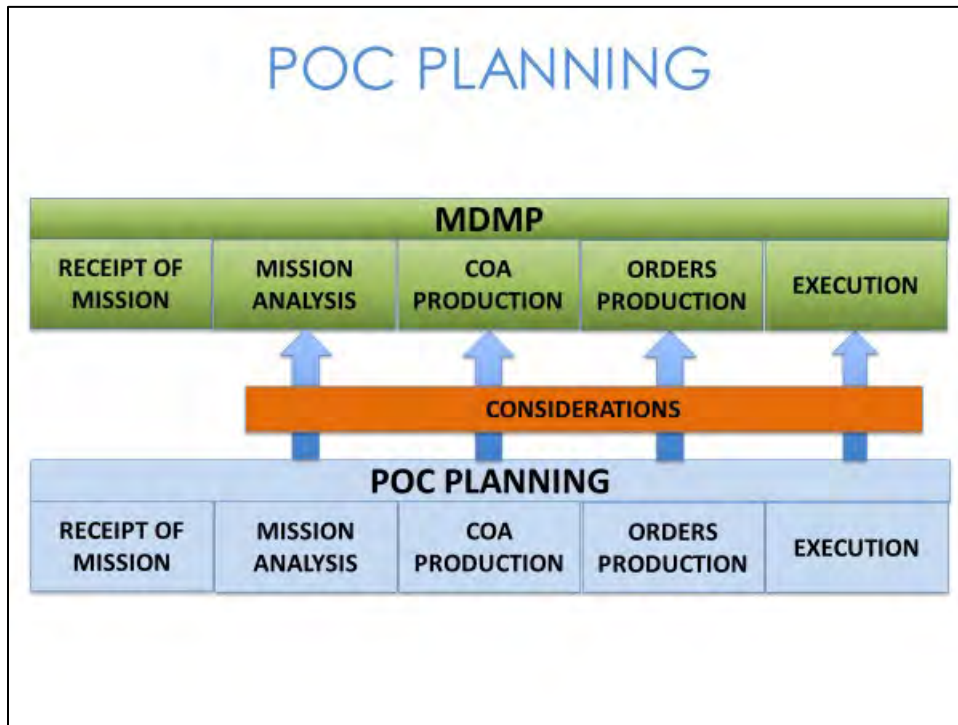
POC considerations are to be incorporated into all mission planning. While POC is considered separately in a wider MDMP planning, it is generally the same staff doing both.   POC planning produces considerations that are injected into mission planning to ensure that POC occurs effectively.

Slide 9
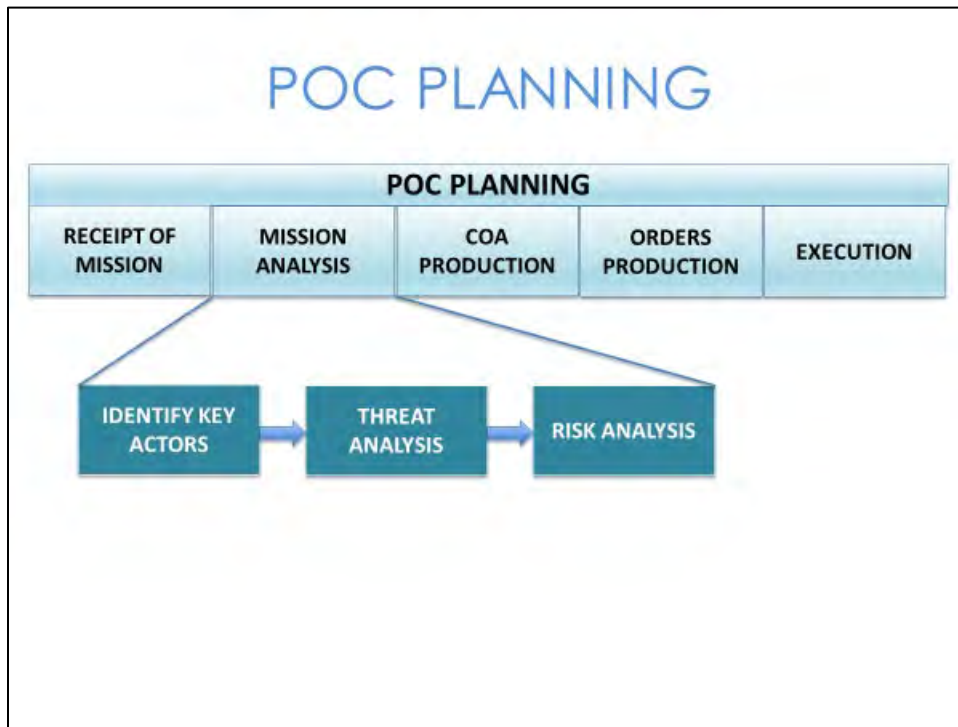
Mission Analysis is where intelligence can add critical value. Under the POC Mission Analysis step, POC planners follow the process of:

- Identify and analyse all key actors in the AOR based on their relevance to the Protection of Civilians

- Select those key actors that represent a threat to vulnerable civilians and further analyse them

- Determine the level of risk (impact and likelihood) that threat actors pose to vulnerable civilians

The threat actors and the level of risk they pose to vulnerable civilians is then injected into mission planning to allow commanders to determine which civilian population/groups they need to protect, and how they will protect them.

This is where intelligence products can assist in POC planning to develop effective planning considerations for commanders.

Slide 10
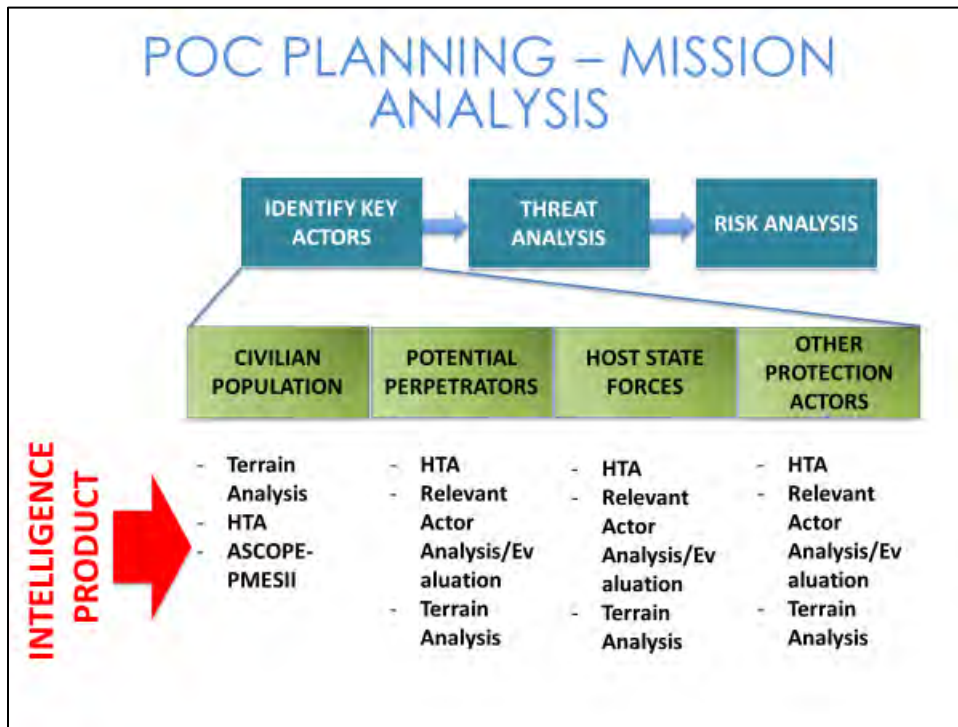
Key Message: The 'Identify Key Actors' step of POC Mission Analysis includes analysis of the Civilian Population, Potential Perpetrators, Host State Forces and Other Protection Actors, all of which can be enhanced with the contribution of Intelligence Products.

Under the Identify Key Actors step, POC planners consider Actors in the following groups:

▪ Civilian communities, to provide an understanding of where and who they are, their location and make-up; hospitals, schools, IDP / refugee camps all should be analyses (armed groups recruitment and areas of kidnapping etc.)

▪ Potential Perpetrators – those who may potentially present a risk to vulnerable civilians (threat actors who present a risk to the force may not present a risk to civilians, and some actors may not present a risk to the force, but do present a risk to civilians)

▪ Host State Forces – to determine their ability and/or willingness to protect civilians, and particularly if they themselves pose a risk to vulnerable civilians

▪ Other Protection Actors – these are other Actors in the AOR whose purpose is to protect civilians

Interaction. Ask the students how the students this question: – Who might some humanitarian Protection Actors be?

Answer: the humanitarian/human rights component of the UN mission, the host nation, Red Cross, Doctors Without Borders, local NGOs, etc.

In order to assist the POC planning process, we can contribute standard intelligence products as shown, to improve understanding of the Key Actors in the AOR.   The only difference between our normal threat-based analysis and analysis in support of POC is that we must orientate our thinking to focus on potential threats to civilians.

Slide 11
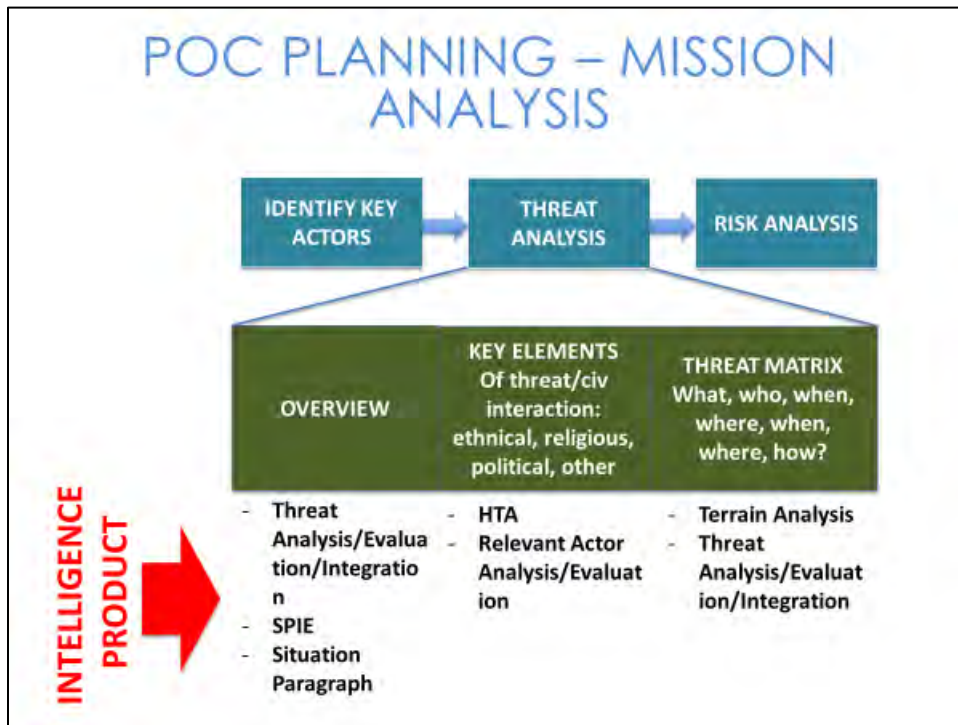
Key Message: The 'Threat Analysis' step of POC Mission focuses on the potential effect that identified threat actors could have on civilian communities, all of which can be enhanced with the contribution of Intelligence Products.

Under the Identify Key Actors step, POC planners carry out the following:

- Provide an overview of the situation, including a summary of threats

- Analysis of the potential areas of concern between threat groups and civilian populations that may develop into abuses against vulnerable civilians – key areas of potential conflict include ethnical, religious, political or any other identified differences that may place specific civilian communities at risk from specific threat groups

- The Threat Matrix summarises threat actors and which communities they may target and how

In order to assist the POC planning process, we can contribute standard intelligence products as shown, to improve understanding of the Threat Actors in the AOR, nature of civilian communities, and how they may interact in a way that presents a risk to civilians. The only difference between our normal threat-based analysis and analysis in support of POC is that we must orientate our thinking to focus on potential threats to civilians from specific threat groups.

Interaction. Ask the students how the students this question: This is not an exhaustive list of suitable products – what else can you think of that we might be able to contribute?

Answer: Link Diagrams and Association Matrices showing interactions between civ communities and/or threat groups, Timelines if they show patterns of abuse that allow us to predict likely possible times that threats target civilians, etc. Analysts should consider contributing any product that clarifies the POC environment.

Slide 12
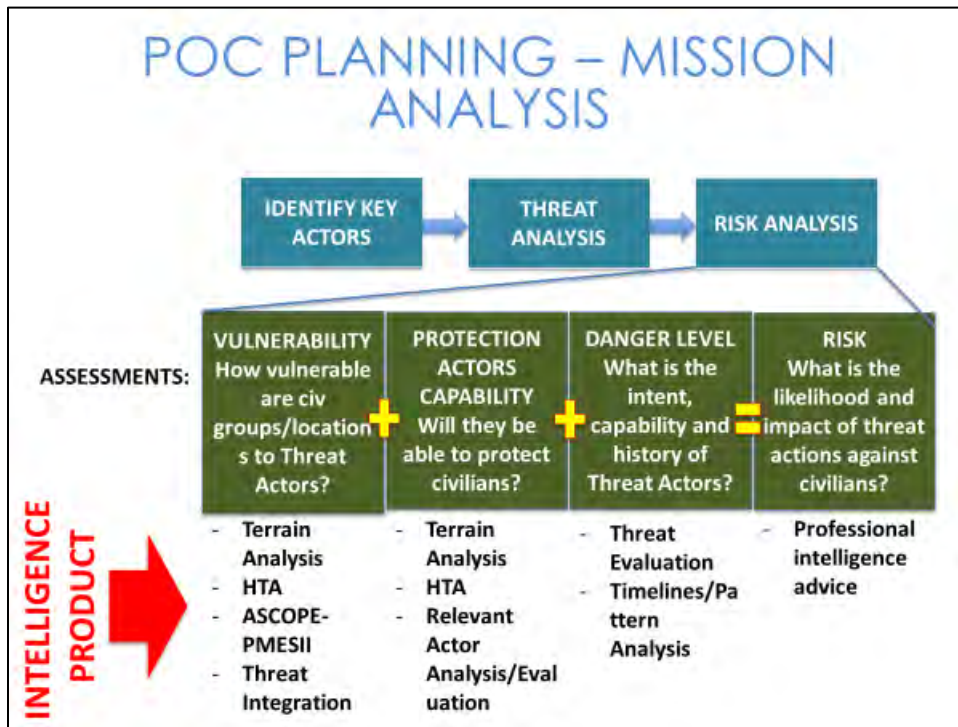
Key message: 'Risk Analysis' step of POC Mission Analysis considers how vulnerable civilian communities may be, how much protection they can rely on from other protection actors, and how dangerous each threat group is to each civilian community, which when put together allows planners to assess the risk to each civilian community, driving planning priorities.

Under the Risk Analysis step, POC planners consider the following:

- How vulnerable are specific civilian communities to each identified threat group? If a civilian community is not vulnerable to a threat group, they do not require protection

- How capable are other protection actors, such as Host Nation forces, of protecting the identified vulnerable civilian communities? If you cannot rely on other protection actors to protect vulnerable civilians, the UN Commander will need to plan to use their resources to protect those communities

- What is the level of danger (based on the capability, intent and historical actions against those identified vulnerable civilians) that identified threat actors present to identified vulnerable civilians? The level of danger contributes to determining the priority to protect

- Finally, taking into consideration the previous steps, what is the likelihood and impact of threat actions against vulnerable civilians? This determines the Commander's priorities for the protection of civilians

In order to assist the POC planning process, we can contribute standard intelligence products as shown, to improve understanding of building blocks of risk analysis.   The only difference between our typical threat-based analysis and analysis in support of POC is that we must orientate our thinking to focus on potential threats to civilians.

Slide 13
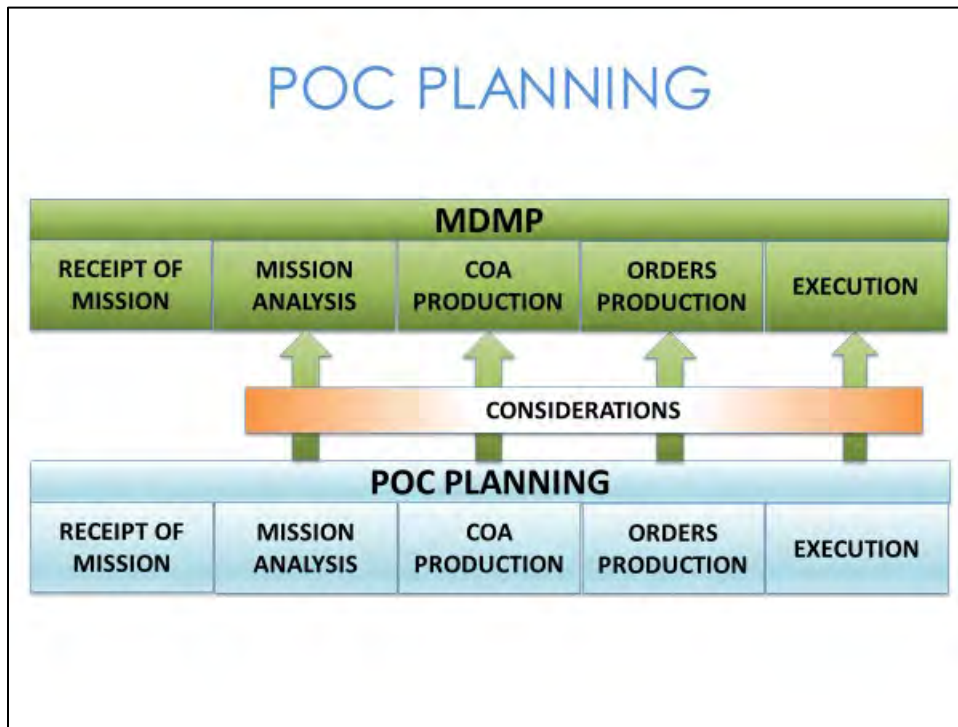
POC Planning continues from Mission Analysis to COA production, Orders and Execution, all of which an intelligence analyst can contribute to if engaged in the POC planning process. During the other POC Planning steps, intelligence personnel should remain engaged in order to provide advice as appropriate.

Slide 14

Take Away

- In parallel to the MDMP, each level of command will conduct POC planning that Intelligence Analysts need to support

- Analysts need to understand the products of POC planning in order to provide products that assist planners

- The only difference between threats to force and threats to civilians is perspective

Summary

Intelligence Analysts need to be aware of POC planning and provide intelligence products that inform POC planners, just like you support the MDMP

M o d u l e
3

Operational Framework Wrap Up

At the conclusion of Module 3, some key elements should become clearer:

- A general understanding of the key operational framework covering a MPKIO operating in UN peacekeeping operation

- The main skillsets required for MPKIO operating in UN PKOs

- The Tabletop Exercise (TTX) will give you a better understanding of the MPKIO operations in a UN PKO along with the essential planning parameters, skills and tasks performed

- The MPKIO is an enabling asset

- The TTX provides you with some tools to apply in the employment of MPKIO, decision-making processes that might be used in a PKO and provides a platform for understanding how MPKIO support the mandate

- A focus on the tactical level employment of a MPKIO and a general overview of the operational level concepts to help leaders understand how a MPKIO con contribute to the accomplishment of the UN mandate

☞ **Instructor Note:** *For the Capstone Learning Activity (LA) go to the MPKIO RTP Annex C – TTX*

R e f e r e n c e s

Glossary and Annexes

The following annexes and references can be found in separate folders to aid in the delivery of the modules:

- **Annex A:** PowerPoint Slide Lesson Presentations

- **Annex B:** Lesson Learning Activities and Capstone Tabletop Exercise (TTX)

- **Annex C:** Supporting documents, references and background material

Glossary (acronyms and abbreviations)

3CF	3 Column Format
ACH	Analysis of Competing Hypothesis
ACOA	Actor Course of Action
AE	Actor Evaluation
AII	Area of Intelligence Interest
AIR	Area of Intelligence Responsibility
AM	Acquisition Management/Manager
AOE	Analysis of the Operating Environment
ASCOPE	Areas, Structures, Capabilities, Organisations, People, Events
Bn	Battalion
CCIR	Commander's Critical Information Requirement
CIU	Crime Intelligence Unit
CMOS	Current Military Operations Service
COG	Centre of Gravity
COIST	Company Intelligence Support Team
Comd	Commander
COMINT	Communications Intelligence
Coy	Company
CC	Critical Capabilities
CR	Critical Requirements
CV	Critical Vulnerabilities
DPKO	Department of Peacekeeping Operations

DTG	Date Time Group
ELINT	Electronic Intelligence
EMP	Electro-Magnetic Pulse
EO	Event Overlay
FHQ	Force Headquarters
FOB	Forward Operating Base
FRAGO	Fragmentary Order
G2	Sector Level Intelligence Staff
GA	Gender Analysis
GEO	Geospatial
GEOINT	Geospatial Intelligence
HIPPO	High-Level Independent Panel on Peace Operations
HUMINT	Human Intelligence
I&W	Indicators & Warnings
IAP	Intelligence Acquisition Plan
IDP	Internally Displaced People
IE	Intelligence Estimate
IHI	Items of High Importance
IM	Information Management
IMINT	Imagery Intelligence
INTREP	Intelligence Report
INTSUM	Intelligence Summary
IO	Information Operations
IOTs	Integrated Operational Teams
IR	Intelligence Requirement
IR	Infra-Red
IRM	Information Requirements Management/Manager
ISR	Intelligence, Surveillance, Reconnaissance
JMAC	Joint Mission Analysis Centre
JOC	Joint Operations Centre
KT	Key Terrain
LN(s)	Local National(s)
MASIC	Military All-Source Information Cell
MICM	Mission Peacekeeping-Intelligence Coordination Mechanism
MDACOA	Most Dangerous Course of Action
MDMP	Military Decision-Making Process
MICS	Mission Intelligence Co-ordination Structure
MLACOA	Most Likely Course of Action
MSN	Mission
NAI	Named Area of Interest
OE	Operating Environment
OEE	Operating Environment Evaluation

OMA	Office of Military Affairs
OO	Office of Operations
OPINT	Operational Intelligence
OPO	Operations Order
ORBAT	Order of Battle
OS	Open Source
OSINT	Open Source Intelligence
OTHR	Over The Horizon Radar
PBIED	Person-borne Improvised Explosive Device
PICTINTSUM	Picture Intelligence Summary
PIR	Priority Intelligence Requirement
PK MIHB	Peacekeeping Military Intelligence Handbook
PKMI	Peacekeeping Military Intelligence
PI	Platoon
PMESII - PT	Political, Military, Economic, Social, Infrastructure, Information, Physical, Time
POC	Police Operations Centre
PPE	Personal Protective Equipment
Recce	Reconnaissance
RFI	Request For Information
ROMB	Receipt of Mission Brief
S2	Battalion Level Intelligence Staff
SAR	Synthetic Aperture Radar
SI	Situation Integration
SIGINT	Signals Intelligence
SIR	Specific Intelligence Requirement
SITMAP	Situation Map
SLT	Senior Leadership Team
SOPs	Standard Operating Procedures
SRSG	Special Representative of the Secretary-General
SPIE	Short Peacekeeping Intelligence Estimate
TAI	Target Area of Interest
TCC	Troop Contributing Country
TECHINT	Technical Intelligence
TPME	Task, Purpose, Method, End state
U2	Force level intelligence
UAS	Unmanned Aircraft System
UN	United Nations
UNHQ	United Nations Headquarters
UNDSS	United Nations Department of Safety and Security
UV	Ultraviolet
VBIED	Vehicle-borne Improvised Explosive Device
VG	Vital Ground

VHF   Very High Frequency
VLF   Very Low Frequency
VRN   Vehicle Registration Number
WARNO   Warning Order

[End of document]