United Nations

Reinforcement Training Package

United Nations Force Protection

for Commanding and Staff Officers of Military and Police Units in United Nations Peacekeeping Operations

United Nations Department of Peace Operations

The United Nations (UN) Force Protection Reinforcement Training Package (RTP) for Contingent Commanders, Staff, and Unit leaders for United Nations Peacekeeping Operations has been developed by the Integrated Training Service (ITS) of the UN Department of Peace Operations (DPO) in consultation with Member States and UN offices.

This version has been released for use by Member States in their pre-deployment training for United Nations Peacekeeping Operations. However, this RTP will be regularly updated so that it is fully responsive to the needs on the ground. Therefore, we strongly suggest checking for updated versions before training is conducted.

The latest version 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 found in the resource hub at the same location.

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

Integrated Training Service

Department of Peace Operations

United Nations

New York, NY, 10017, USA

Preface

Background

Since the Security Council first established peacekeeping missions, the operational environment has evolved significantly, growing both in size and complexity. Military and police units are a key element for mandate implementation in many Peacekeeping Operations. Unit performance has sometimes become the yardstick against which the success of mission is measured, and it is essential to understand units' deployment and performance is one of the most challenging aspects for both mission leadership and unit commanders.

The Department of Peace Operations has developed a suite of specialised training materials (STM) and Reinforcement Training Packages (RTP) to prepare military units for their deployment in UN Missions. There are also unique training packages on the Protection of Civilians (POC), Child Protection and Conflict-Related Sexual Violence. These activities alongside other military and police activities enable mandate implementation.

Experience has also shown that force protection tasks, despite their distinct nature, generate significant overlap with other mission activities. This is particularly true at the tactical level, where the assessment of threats, as well as the planning for and response to complex crises, is likely to simultaneously involve elements from the POC, Child Protection and Conflict-Related Sexual Violence realms. In order to reflect these realities and prepare peacekeepers for the multi-dimensional realities on the ground, this force protection training package aims to demonstrate the complex linkages between protection tasks, and provide training guidance on how to prevent, deter and respond to the interrelated threats.

Aim

According to the 2017 United Nations dos Santos Cruz report on peacekeeping fatalities[1], the peacekeeping environment features armed groups, terrorists, organised crime, street gangs, criminal and political exploitation, and other threat groups that attack UN units and civilian populations. The dos Santos Cruz report notes that some units and personnel lack an appropriate mindset to operate in the peacekeeping environment: "If the United Nations and T/PCCs do not change their mindset, take risks, and show a willingness to face these new

[1] "Improving Security of United Nations Peacekeepers."

challenges, they will be consciously sending troops into harm's way.[2]" The dos Santos Cruz report states that hostile groups do not understand a language other than force. To deter and repel attacks and to defeat attackers, the United Nations needs to be seen to be strong and not fear to use force when necessary. To improve security, missions should identify threats to their security and take the initiative, using all the tactics, to neutralise or remove the threats. Missions should go where the threat is, in order to neutralise it.

This RTP provides troop and police-contributing countries with a training package that combines conceptual, legal, and operational aspects to support the tactical planning of units to operate in peacekeeping operations. The training package is designed for application in both pre-deployment and in-mission training.

Target audience

The target audience of this package is military and police unit decision-makers, leaders, and staff at the tactical level. Also, this material is beneficial for the leadership and staff at the Mission/Force / Sector Headquarters levels and equivalent police command levels. The materials may lend themselves to a wide audience. Also, the audience can include personnel identified as decision-makers and staff officers who may be assigned to train, equip, employ, coordinate, or deploy the Unit. Member state trainers and course directors will benefit from these materials.

Structure of the training materials

Module 1: Conceptual Framework

Module 2: Legal Framework

Module 3: Operational Framework

Annex A: Lessons- PowerPoint Slide Presentations

Annex B: Tabletop Exercise (TTX); Scenario-based Exercise (SBE)

Annex C: Additional Lessons in support of force protection

[2] 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.

Acknowledgements

DPO would like to thank the subject matter experts from across the UN system, UNMAS, OHCHR, Member States listed alphabetically below, and other regional and international organisations who helped in the development of this training material.

People's Republic of Bangladesh
Republic of Ghana
Republic of Guatemala
Republic of Indonesia
Italian Republic
Kingdom of Morocco
Federal Democratic Republic of Nepal
Islamic Republic of Pakistan
Republic of Rwanda
Kingdom of Sweden
United Kingdom of Great Britain and Northern Ireland
Oriental Republic of Uruguay
United States of America

Contact person

For any proposals of updates, improvements, or any questions pertaining to 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 this site regularly.

Table of Contents

Guidance

General considerations for instructors

This package of materials is not a course but rather a compendium of critical training content for comprehensive contingent police and military tactical planning in UN Peacekeeping. No training material can cover the entire complexity of tasks arising from tactical planning. This training package should, therefore, be viewed as a supplemental package to assist the contingent training efforts for units. When designing a training programme, trainers can adapt and translate (language) the lessons to the needs of their audience. As a result, the duration of lessons and exercises delivered in the package may vary.

It is recommended that personnel receiving this training are already proficient in their basic unit tasks and technical skills (individually and collectively) at the tactical level. It is expected that the staff officers are fully capable of performing staff officer duties. It is also critical for all participants to have received the Core Pre-Deployment Training Materials (CPTM) and any of the mandatory Specialised Training Materials (STM) as a pre-requisite before this training. The CPTM and specified STM contain the fundamental principles, concepts, and ideas for UN Peacekeeping operations, which trainees should grasp well before participating in this RTP.

Instructor Profile

This training package is best presented by military and police instructors who master the CPTM, and their respective STM and have previous experience working in a UN peacekeeping mission. Having planning experience at the tactical level is important. Specific knowledge of the actual mission where trainees are to be deployed is advisable to be able to deliver a targeted course based on real experience. Finally, instructors should be familiar with and capable of facilitating scenario-based and tabletop exercises.

Scenario-Based Exercises (SBE) / Tabletop Exercises (TTX) Considerations

Contained in the RTP is a TTX. This exercise is a scenario and situation-driven learning activity to help consolidate learning outcomes and reinforce the lesson "Take Aways". 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 hypothetical scenarios and specific situations. The exercise will help participants understand the process of integrating into a peacekeeping operation that is focused on force protection and implementing the array of tasks that support the mandate by assisting in creating a safe and secure environment in the area of operations.

Methodology: Using their national problem-solving doctrine, methodology, military/police decision-making processes, and troop/police leading procedures, participants will analyse situations and tasks and present courses of action based on threats presented. 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 complexity, threats and political environment when operating in support of peacekeeping operations. Also, they should assist participants in bridging gaps in the transition from operations in a national context to peacekeeping operations. Instructors must emphasise that command and control (C2), the support structure, risk assessments of threats and coordination with the various actors in a peacekeeping operation can be challenging.

Training Characteristics

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

- Training should be interactive and encourage trainees' participation
- To help reinforce practical discussions, the training should bring in actual examples and anecdotes from peacekeeping missions
- Training methodology should be based on learning activities and practise
- Training should emphasise the political nature of a UN Mission and address how best to leverage and interact with all components
- Training should be evaluated

Symbols legend

💡	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.

Abbreviations/acronyms

For all practical purposes, throughout the Reinforcement Training Package documents, lessons, and slides, we will use Unit as an abbreviation to refer to both UN police and military units both in singular and in the plural forms and FP for force protection. The lessons use the acronym UNPKO for United Nations peacekeeping operation.

Module 1

Conceptual Framework

Module 1 at a Glance

Aim

The aim of this module is to familiarise participants with the:

- UNPKO environment and characteristics
- How tactical unit operations support the UN mandate
- Decision making and how intelligence support tactical units
- Force Protection (FP) introduction; threat-based analysis approach to risk analysis and mitigation for units
- Improvise explosive devices (IED) familiarisation
- Understanding the nature of and how cyber-attacks impact UNPKO
- Understanding the nature of and how misinformation and disinformation attacks impact UNPKO

Overview

Module 1 provides an overview of the conceptual framework related to FP in a UNPKO to support and contribute towards the successful achievement of the Mandate. It also the introduces types of attacks against UN units.

Introduction

Slide 1

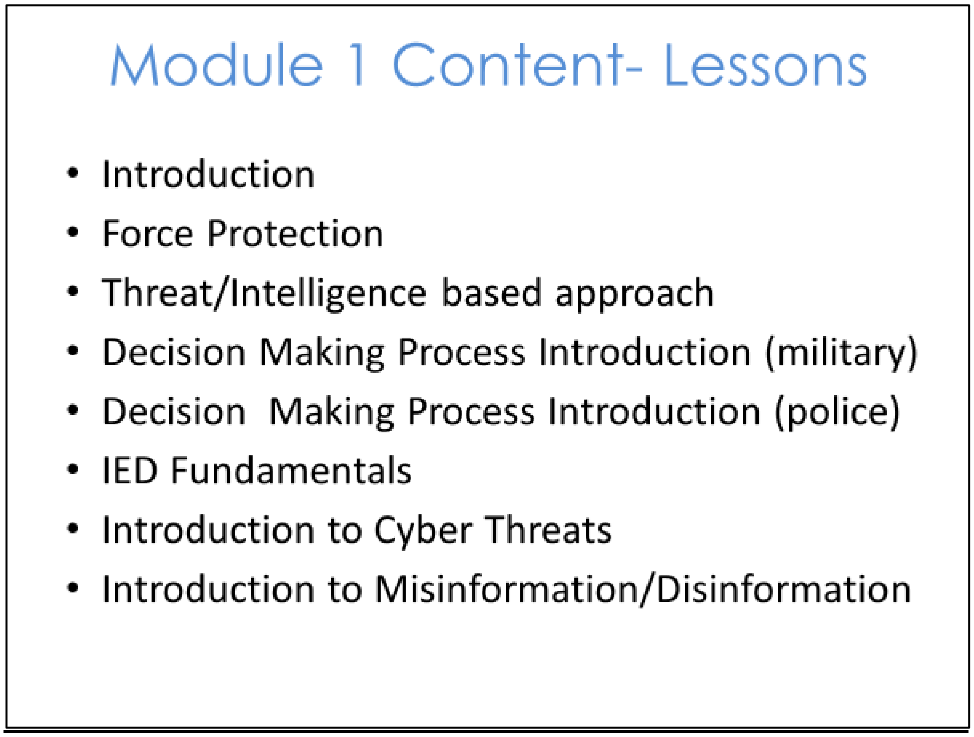
Module 1
Conceptual Framework
United Nations Force
Protection
in Peace Operations

Key Message: United Nations police and military units contribute to implementation of the UN Mission's mandate. These units must be able to operate in a high threat environment and be able to mitigate risks to their units and freedom of movement while accomplishing their tasks.

Module 1 is designed to provide you with an understanding of the complex and high-risk environment in which United Nations' police and military units operate during peacekeeping missions. Its primary focus is to familiarise you with peacekeeping intelligence, decision making, and force protection planning in a UNPKO environment.

The training package incorporates learning exercises, discussions, as well as annexes and references to enhance your comprehension. To solidify your grasp of FP planning, a comprehensive scenario-based exercise, known as a Tabletop Exercise (TTX), can be conducted at the conclusion of the course. This exercise will help reinforce your understanding of effective FP planning. Throughout the reinforcement training packet, lessons, and slides, we will use the abbreviation/acronym "UNFORPRO" to refer to United Nations Force Protection, while the term "unit" will encompass both singular and plural references to police and military tactical units. "FP" will serve as an abbreviation for force protection.

Slide 2



Module 1 Content- Lessons

- Introduction
- Force Protection
- Threat/Intelligence based approach
- Decision Making Process Introduction (military)
- Decision Making Process Introduction (police)
- IED Fundamentals
- Introduction to Cyber Threats
- Introduction to Misinformation/Disinformation

In Module 1, in the Conceptual Framework, we will cover these areas / lessons.

Lesson 1.1

Introduction

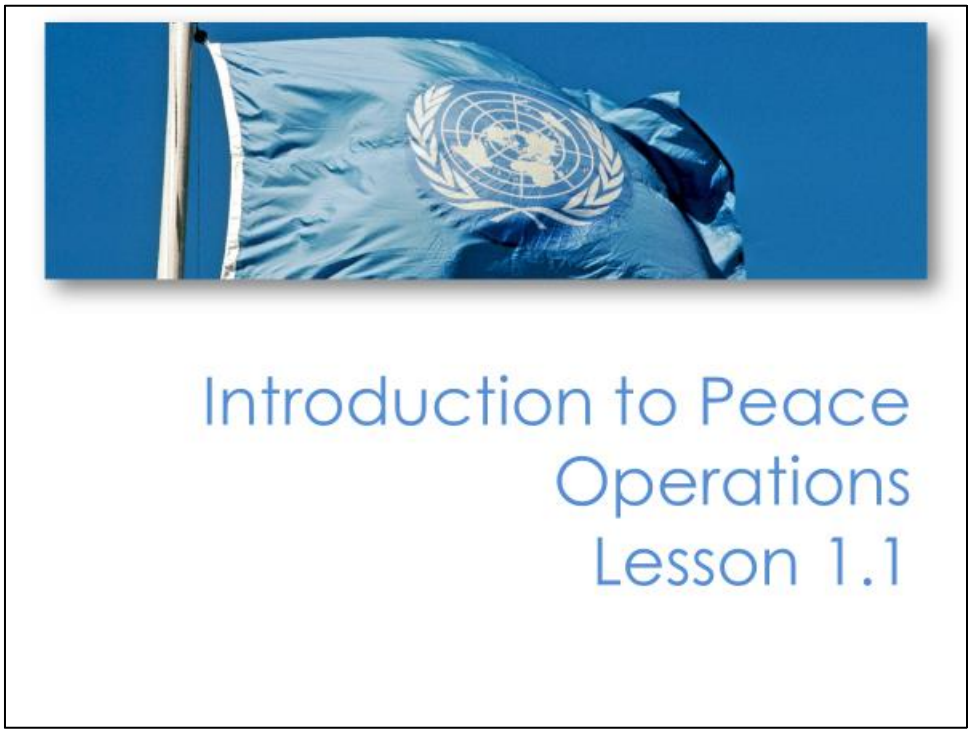
The Lesson

Starting the Lesson

For an interactive start to this Lesson, ask the participants if they have had experience in a UNPKO. Ask them to tell the group about their specific challenges with command and control, logistics, threats, security, tasking orders, and deployment.

☞***Note to instructor** – recommend that lesson 1.1 is presented by a trainer who has personal experience operating in a UN military or police unit in a UNPKO. The instructor should also encourage questions from the participants and aim for an interactive discussion. All participants should be encouraged to contribute to the group discussions and learning activities. The instructor should review the latest UNFORPRO DPO Handbook [Comment – does this exist?]. Learning involves some words, terms and phrases that may be unfamiliar and/or seem awkward. Reassure learners: "Don't let new language get in the way of learning". "As you move through the training, review the definitions of key words; ask your instructor to clarify definitions, abbreviations, and acronyms." Note that this training material uses a slightly modified FP definition that focuses on tactical units and the risks associated with a high threat environment.*

Slide 3

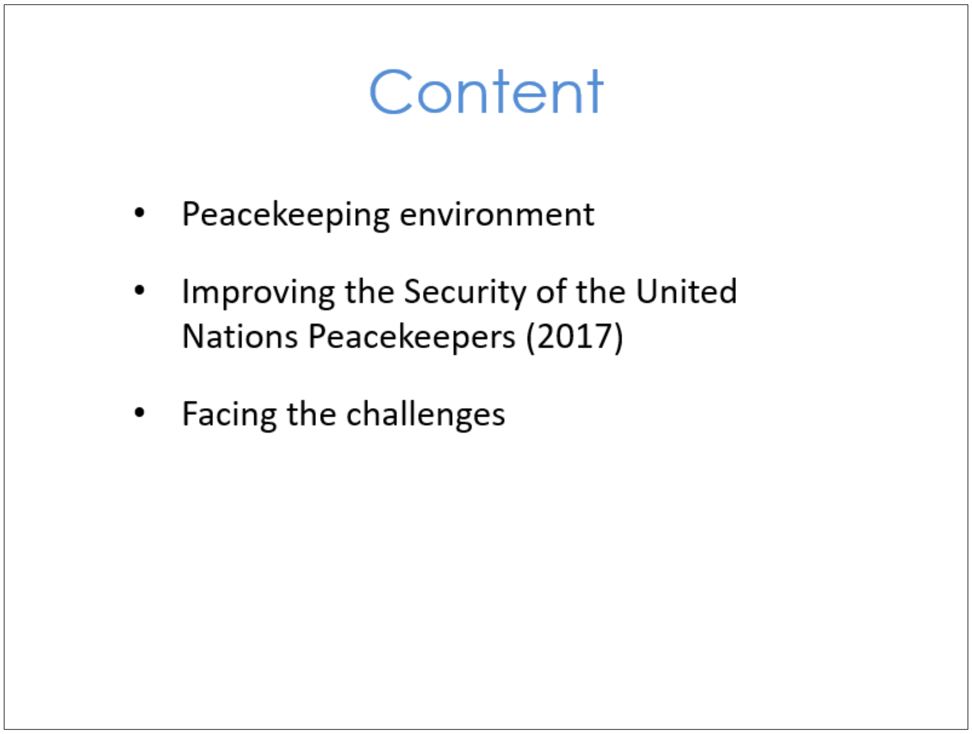


Introduction to Peace Operations
Lesson 1.1

UN tactical units play a vital role in peacekeeping missions, as they possess unique capabilities that directly impact the attainment of mandate objectives. It is of utmost importance that decision-makers, staff officers, and leaders at the tactical level who are involved with or oversee UN units have a comprehensive understanding of the operational environment and the capabilities these units bring to the table.

To facilitate this understanding, we will provide a concise overview of the current United Nations Peacekeeping Operations (UNPKO) environment. It is crucial that, from this point forward, we adopt the mindset of wearing the Blue Beret, symbolising the UN's presence and commitment in the intricate and challenging landscape of peacekeeping operations. By doing so, we can better grasp the complexities and demands faced by UN personnel operating in this environment, fostering a deeper appreciation for the role and responsibilities associated with UN tactical units.

Slide 4

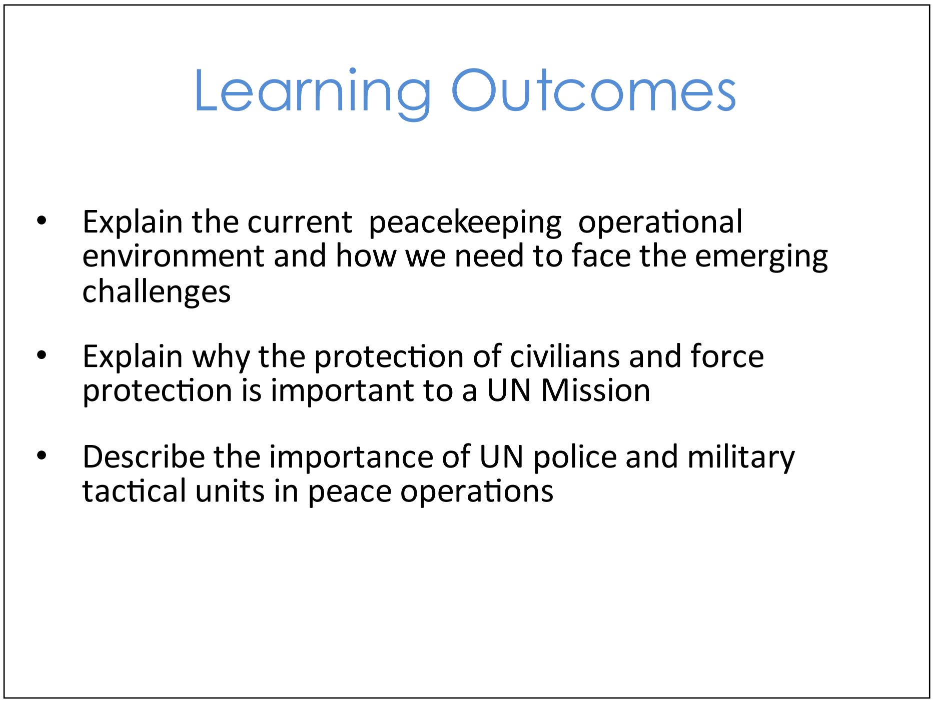


Content

- Peacekeeping environment
- Improving the Security of the United Nations Peacekeepers (2017)
- Facing the challenges

Here are the subject areas we will be covering.

Slide 5



Learning Outcomes

- Explain the current peacekeeping operational environment and how we need to face the emerging challenges
- Explain why the protection of civilians and force protection is important to a UN Mission
- Describe the importance of UN police and military tactical units in peace operations

At the end of the lesson, our aim is for you to be able to assimilate the essential roles and responsibilities of UN units in a UN Mission. We must first understand the UNPKO environment and what skills, and characteristics assist in support of the mission's security. Please take a moment to read and understand the requirements.

It is important to understand that UN units do not operate in total isolation but work in close coordination with other United Nations mission components, agencies and stakeholders including host nation security forces. By emphasising this collaborative approach, we aim to highlight the interconnectedness and interdependence that characterises UN operations. Understanding this fundamental aspect is vital for comprehending the dynamics and complexities involved in the successful execution of peacekeeping missions. It underscores the importance of effective communication, cooperation, and coordination among different entities, ultimately leading to enhanced mission outcomes and the achievement of overarching objectives.

Slide 6

The complex and lethal Peacekeeping Environment

6

Here is a UN vehicle after sustaining an IED attack. IEDs have become the leading cause of casualties for the United Nations. Their improvised nature makes them easy to construct and emplace.

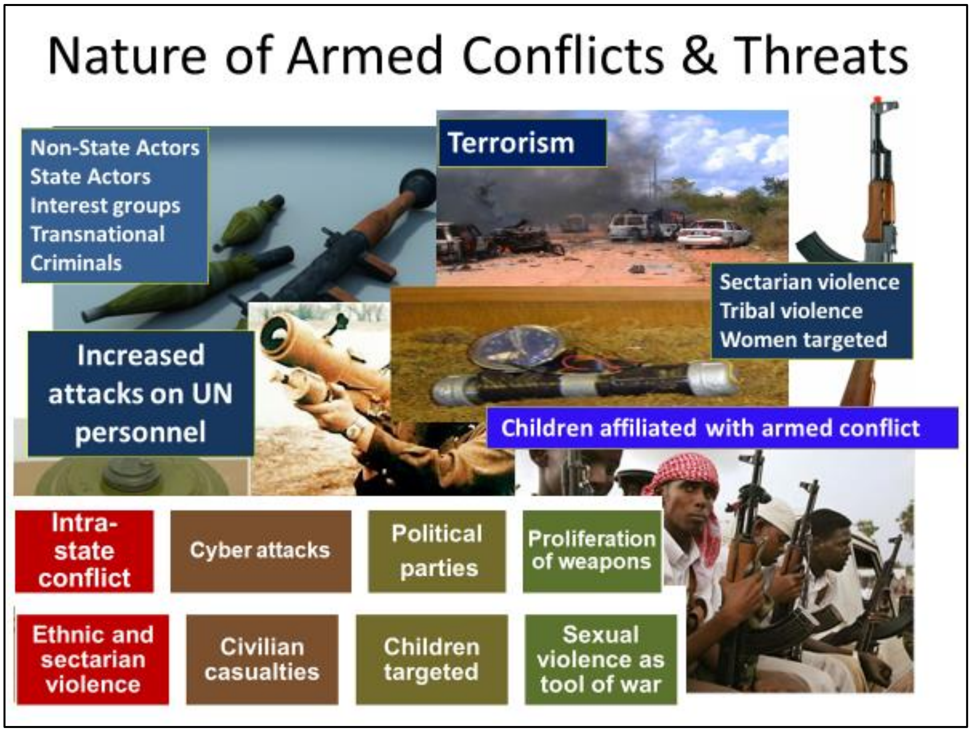
- *Initiate a classroom discussion on the characteristics of the current United Nations Peacekeeping Operations (UNPKO) environment. Allocate 10 minutes for this discussion. Encourage the students to share their thoughts and perceptions regarding the nature of the UNPKO environment.*

- *If the discussion lacks participation, prompt the students by asking about specific examples. For instance, inquire about mission areas known for their high level of lethality. Additionally, invite them to consider what is happening on the ground in these missions and the prevailing threats faced by peacekeepers.*

- *Transitioning from the discussion, inform the class about the increase in peacekeeper fatalities resulting from violent acts, which have been on the rise over the past years. Emphasise that these numbers exceed what would be considered a normal or acceptable level of risk. Furthermore,* *stress that if the planning process, posture, and mindset remain unchanged, it is highly likely that these fatalities will continue to escalate.*

- *By highlighting these facts, the intention is to underscore the urgent need for a shift in our approach to planning and mindset. It is crucial that we adapt our strategies and take necessary measures to mitigate the risks faced by peacekeepers, ensuring their safety and well-being in the challenging UNPKO environment.*

Slide 7



Nature of Armed Conflicts & Threats

Non-State Actors
State Actors
Interest groups
Transnational
Criminals

Terrorism

Sectarian violence
Tribal violence
Women targeted

Increased attacks on UN personnel

Children affiliated with armed conflict

Intra-state conflict

Cyber attacks

Political parties

Proliferation of weapons

Ethnic and sectarian violence

Civilian casualties

Children targeted

Sexual violence as tool of war

It is important that we have a general understanding of the characteristics of conflicts and threats that may continue after a UNPKO has been established. Contemporary armed conflicts are characterised by several trends, including the following:

- Shift from International to Internal Conflicts: Today we see fewer country-versus-country or international armed conflicts. Most ongoing conflicts are internal conflicts over power and resources, social and economic inequality, or ethnic or religious divides. While they often have regional implications, these conflicts are, in many cases played out within national borders.

- Complex Intra-State Conflicts: Intra-state conflicts involve a mix of state and non-state actors with varying capabilities and resources. Weaker parties often resort to terrorism and cyber-attacks. Parties involved in these conflicts increasingly target UN units and bases.

- Multiplicity of Conflicting Parties: Unlike international armed conflicts involving a limited number of states, intra-state conflicts often witness the involvement of numerous non-state groups. In certain instances, these groups splinter into competing factions, further complicating conflict resolution processes.

- Cross-Border Spill over: Conflicts frequently spill over across borders, leading to the influx of weapons or refugees. The widespread availability of weapons enables armed groups to sustain prolonged violence.

- Ethno-Sectarian Dimension: Intra-state conflicts, initially driven by political grievances, often acquire an ethnic or sectarian dimension. Leaders skilfully manipulate these conflicts along ethnic or sectarian lines, making them highly charged and challenging to resolve, leaving lasting impacts on societies.

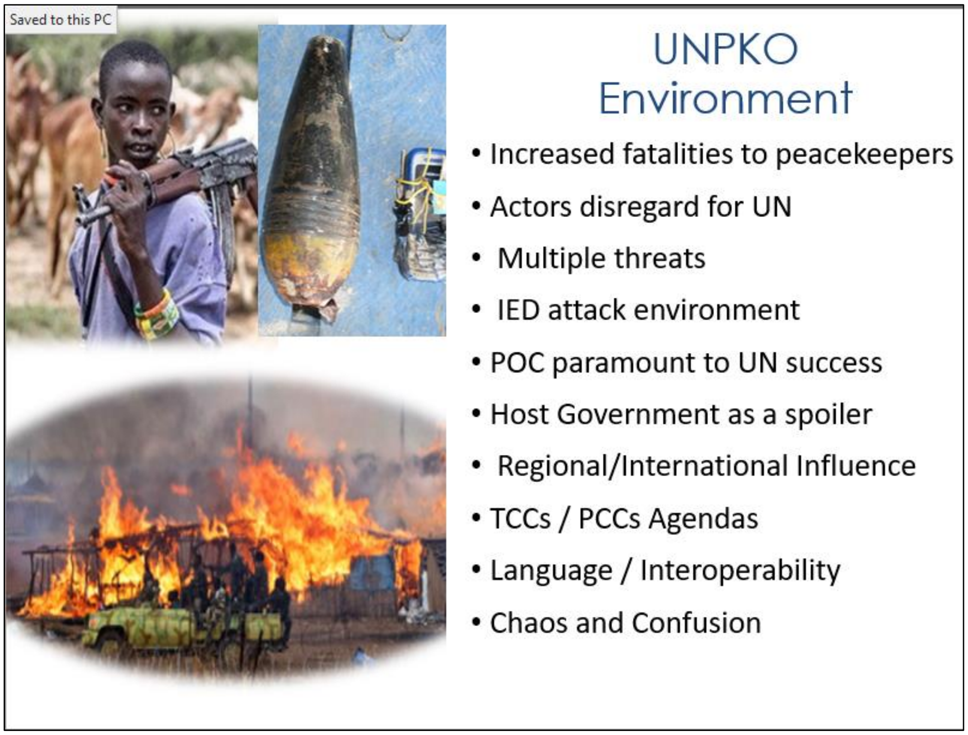
- Impact on Civilians: Current conflicts significantly affect civilians, directly targeting them or indirectly causing loss of life, livelihoods, and the denial of basic rights. Violations of human rights and international humanitarian law, as well as disrespect for the lives and well-being of civilians and civilian objects, are common occurrences. Urbanization of conflict and prolonged besiegement exacerbate the plight of civilians in protracted conflict situations.

- Plight of Children: Children bear a disproportionate burden in armed conflicts, being recruited as child soldiers, and subjected to abduction, sexual abuse, and even death or injury. Attacks on schools and hospitals, along with restricted humanitarian access, further intensify the adverse impact on children. Special attention must be given to child protection measures.

- Sexual Violence as a Strategic Tool: Parties to conflict increasingly employ sexual violence as a strategic tool of war. Women and girls are primarily targeted for rape and other forms of sexual violence, while men and boys are also victims. A comprehensive discussion on conflict-related sexual violence will be presented later in the module.

By recognising and comprehending these characteristics, we can better appreciate the multifaceted nature of contemporary conflicts and the urgent need for effective peacekeeping strategies that address these challenges.

Slide 8



Saved to this PC

UNPKO Environment

- Increased fatalities to peacekeepers
- Actors disregard for UN
- Multiple threats
- IED attack environment
- POC paramount to UN success
- Host Government as a spoiler
- Regional/International Influence
- TCCs / PCCs Agendas
- Language / Interoperability
- Chaos and Confusion

Recent years have seen a significant increase in casualties within the United Nations due to acts of violence. This grim reality necessitates a critical adaptation by the United Nations, as well as troop- and police-contributing countries, to a new paradigm. The traditional assumption that the blue helmet and the United Nations flag provide inherent protection is no longer valid. Peacekeeping environments now confront the presence of armed groups, terrorists, organised crime syndicates, street gangs, and various other threats. The era of peacekeeping resembling "Chapter VI-style" operations is a thing of the past.

In areas where internal security is lacking and governments struggle to enforce the rule of law, civilians find themselves in constant danger. It becomes the responsibility of the United Nations to fill this void and safeguard civilians from hostile groups and predators. When mandates are directed, it is now the norm within the Security Council to include tasks related to the protection of civilians, explicitly authorizing the use of "all necessary means," including deadly force.

The United Nations (UN) peacekeeping environments are complex and challenging. The characteristics mentioned here represent critical aspects that can significantly complicate peacekeeping operations. Let's delve into each one:

Increased fatalities to peacekeepers: Peacekeepers often face heightened risks and dangers, leading to higher casualty rates. These risks can arise from armed groups refusing to accept peace agreements, engaging in confrontations with civilians, or deliberately targeting UN personnel.

Groups that disregard the UN mandate: In some peacekeeping environments, involved parties may dismiss the authority or mandates of the UN peacekeeping mission. This obstruction hampers the mission's ability to mediate effectively and implement peace agreements. Host nations may publicly accept the mandate but covertly sabotage or support groups that disrupt the peace process.

Difficulty in distinguishing between combatants and civilians adds to the complexity.

IED attack environment: The use of Improvised Explosive Devices (IEDs) is on the rise and poses a significant risk to peacekeepers, making movements and operations in the area extremely hazardous.

POC (Protection of Civilians) operations are paramount to UN success: Safeguarding civilians in conflict zones is a central objective of many UN peacekeeping missions. Ensuring their safety and well-being is crucial for mission success. Failure to protect civilians can erode public confidence in the UN and hinder future support. Furthermore, a series of thematic resolutions addressing the Protection of Civilians (POC), Conflict-related Sexual Violence, and Children and Armed Conflict have been adopted. In essence, if the leadership of a UN Mission fails to protect its own personnel and neglects the duty to safeguard and protect civilians, it signifies a failure to save lives and a failure to fulfil the mission's objectives. Moreover, it has adverse implications for the global perception of the United Nations.

Host government as a spoiler: In certain cases, the host government may not cooperate with the peacekeeping mission or may actively work against its objectives, making sustainable peace hard to achieve. Some host nations might even oppress their own population or support groups that counter the UN mandate.

Regional/international influence: Conflicts are often influenced by regional and international actors pursuing their own interests and agendas. This external involvement further complicates peacekeeping efforts, with armed groups receiving support and funding from outside sources.

TCCs / PCCs Agendas: troop-contributing countries (TCCs) and police-contributing countries (PCCs) may have their own national or regional interests and priorities. These agendas may not always align perfectly with the UN's goals, affecting the dynamics within the peacekeeping mission.

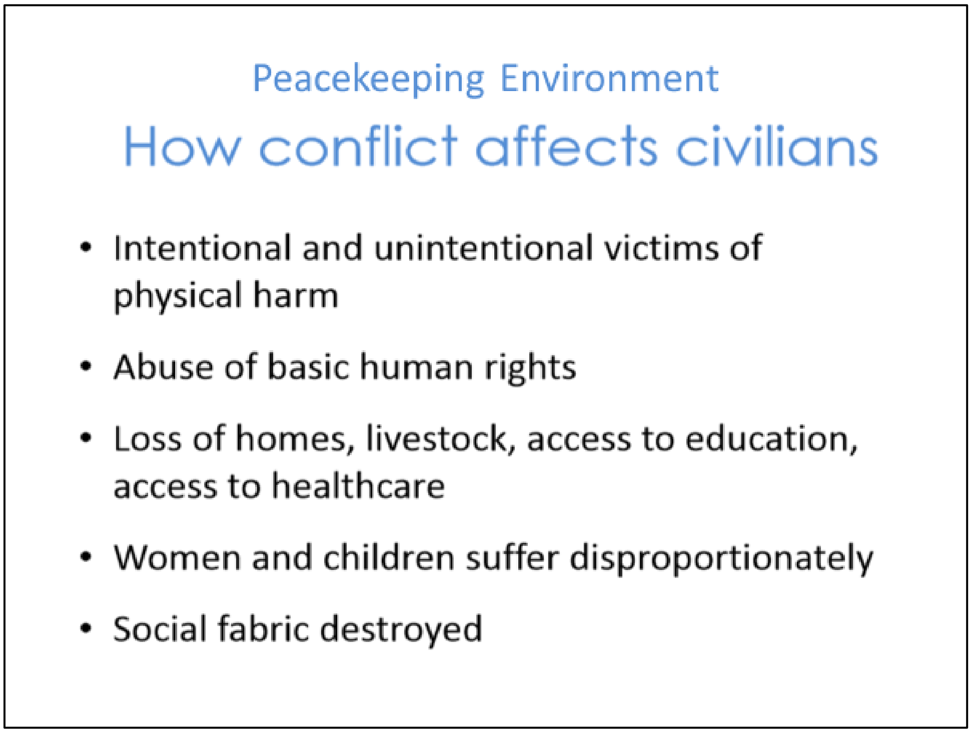
Language / Interoperability: Peacekeeping operations involve personnel from various countries who may not share a common language. This language barrier is exacerbated by the complexity of the UN Mission. Effective communication and interoperability among different contingents and with the local population are essential but not always achieved due to limited language assistance at the tactical level.

Chaos and confusion: Conflict zones can be chaotic, making it challenging to distinguish between combatants and civilians, understand shifting alliances, or ascertain the true intentions of various actors. The lack of clear command and control (C2) and peacekeeping-intelligence further complicates the situation. Military operations must consider humanitarian and political aspects, which may limit operational initiatives.

Addressing these complexities demands meticulous planning, diplomatic skills, adaptability, and a deep understanding of the local context. Well-trained, well-resourced peacekeeping missions, backed by strong international support, are crucial to effectively fulfil mandates and contribute to lasting peace.

Recognising the gravity of these circumstances, it becomes imperative for the United Nations and its partners to reassess and enhance their strategies, approaches, and capabilities. Adapting to this new reality is essential to ensure the effective protection of UN personnel, the preservation of civilian lives, and the successful realization of the mission's objectives. It is only by addressing these challenges head-on that the United Nations can maintain its credibility and fulfil its crucial role.

Slide 9



Peacekeeping Environment

How conflict affects civilians

- Intentional and unintentional victims of physical harm
- Abuse of basic human rights
- Loss of homes, livestock, access to education, access to healthcare
- Women and children suffer disproportionately
- Social fabric destroyed

The Key Message: The predominant UN missions of today and the future will focus on the POC because of the horrendous consequences conflicts have on civilians.

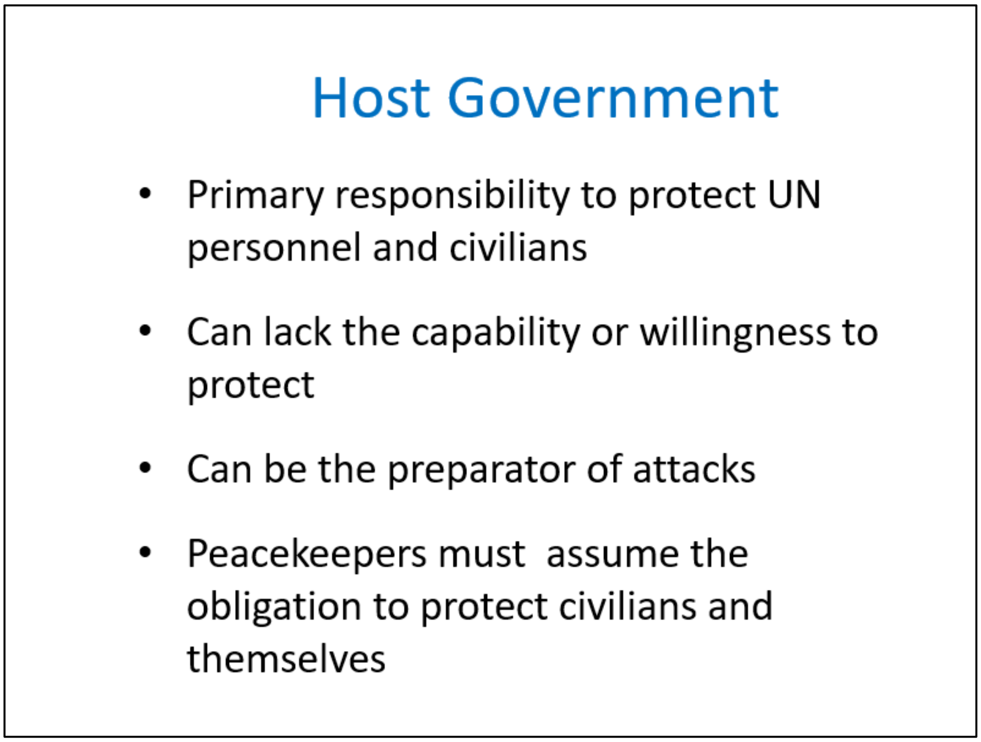
This slide underscores the sobering reality that civilians bear the brunt of casualties during times of conflict. They can fall victim to intentional targeting or suffer as an unintended consequence of violence. The impact of violent conflict extends beyond immediate physical harm, leading to widespread violations and abuses of basic human rights, such as the right to life and physical integrity, for civilians.

Displacement becomes a common occurrence as civilians lose their homes and are forced to flee. They also experience significant economic losses, including the destruction of livelihoods and the means to earn income. Access to essential services, such as education and healthcare, is disrupted when vital infrastructure like schools and hospitals are destroyed.

In particular, women and children endure disproportionate suffering in armed conflicts. They face pervasive levels of sexual violence and abuses, exacerbating their vulnerabilities. Additionally, conflict has a profound impact on communities, fostering hatred and tearing apart the social fabric, making reconciliation and the establishment of sustainable peace incredibly challenging.

To address the multifaceted impact of conflict, it is essential to evaluate how it specifically affects vulnerable groups. This includes adopting a gender perspective, considering the different needs and experiences of individuals based on age, disability, and personal circumstances. By understanding these dynamics, efforts can be directed toward mitigating the harm caused to vulnerable populations and fostering inclusive and lasting peace.

Slide 10



Host Government

- Primary responsibility to protect UN personnel and civilians
- Can lack the capability or willingness to protect
- Can be the preparator of attacks
- Peacekeepers must assume the obligation to protect civilians and themselves

Key Message: The primary responsibility for safeguarding civilians and UN personnel, including UN forces, from physical violence lies with the host state. However, when the host government is dysfunctional or not fully supportive of the mandate, it becomes crucial for the United Nations Peacekeeping Operations (UNPKO) to not only be mandated with the task of Protection of Civilians (POC) but also equipped with the necessary means and capabilities to fulfil this responsibility. Additionally, to effectively carry out POC, it is imperative to ensure the protection of UN units.

Before delving into our next topic, it is important to provide a comprehensive understanding of the responsibilities associated with the protection of civilians (POC) and force protection (FP) for United Nations personnel and units. The capability of the host nation to implement POC plays a pivotal role in shaping the PKO Mission Concept (MC). Let us explore this in more detail.

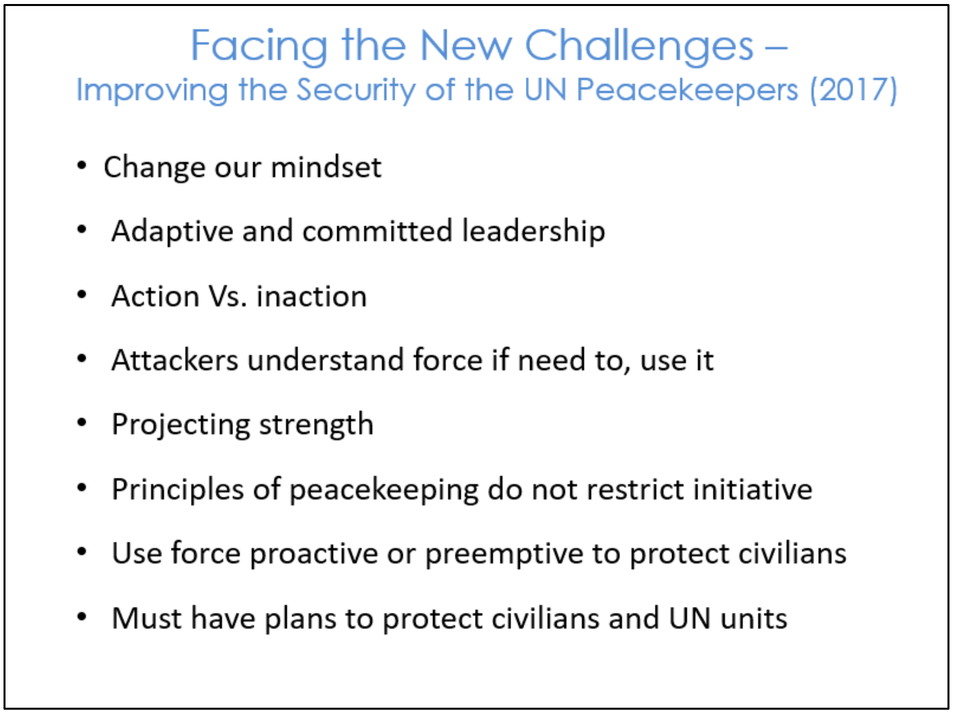
The primary responsibility for protecting civilians and UN personnel, including UN forces, from physical violence rests with the host state. The mandate for the protection of civilians does not undermine the primary and sovereign responsibility of the host state. This principle aligns with their obligations under international human rights, humanitarian, and refugee law and standards, which will be covered in Module 2.

The first step in implementing a POC mandate and an FP strategy is to support the government in fulfilling its responsibility. This approach ensures the sustainability and long-term impact of a mission's actions. In situations of armed conflict, non-state parties to the conflict also bear the responsibility to protect civilians and refrain from using physical violence against UN personnel in the areas under their control.

However, in many peacekeeping missions, host governments may lack the capacity or willingness to protect their citizens or the United Nations. In some cases, the host government may even pose a threat. In such challenging circumstances, peacekeepers assume the obligation to act and protect civilians and themselves.

By recognising the complexities and nuances of these responsibilities, the United Nations can effectively navigate the intricate landscape of peacekeeping, fulfilling its obligations to protect civilians and ensuring the safety of UN personnel in high-risk environments.

.Slide 11



Facing the New Challenges –

Improving the Security of the UN Peacekeepers (2017)

- Change our mindset
- Adaptive and committed leadership
- Action Vs. inaction
- Attackers understand force if need to, use it
- Projecting strength
- Principles of peacekeeping do not restrict initiative
- Use force proactive or preemptive to protect civilians
- Must have plans to protect civilians and UN units

To address the concerning trend of peacekeeper casualties and enhance the security of UN peacekeepers, Lieutenant General (Retired) Carlos Alberto dos Santos Cruz (Brazil) was appointed by the Secretary-General in November 2017 to conduct a comprehensive review of peacekeeping fatalities and injuries resulting from hostile acts.

The resulting document, titled "The Report on Improving Security of Peacekeepers," aims to identify the reasons behind the significant number of casualties caused by acts of violence in recent years and proposes measures to reduce these losses. The report emphasises the urgent need for a change in mindset, a willingness to take risks, and a proactive approach to confronting the new challenges within the peacekeeping operational environment.

In order to improve the security of UN peacekeepers, several key areas require attention and action:

1. Demonstrating Leadership: UN leaders must exhibit initiative, commitment, and determination to adapt. Military, police, and civilian personnel should actively seek solutions rather than waiting for casualties to occur.

2. Enhancing Operational Behaviour: Fatalities often arise from inaction rather than decisive leadership. The interpretation of mandates, rules of engagement, and other relevant documents should support a proactive approach and discourage unjustified inaction.

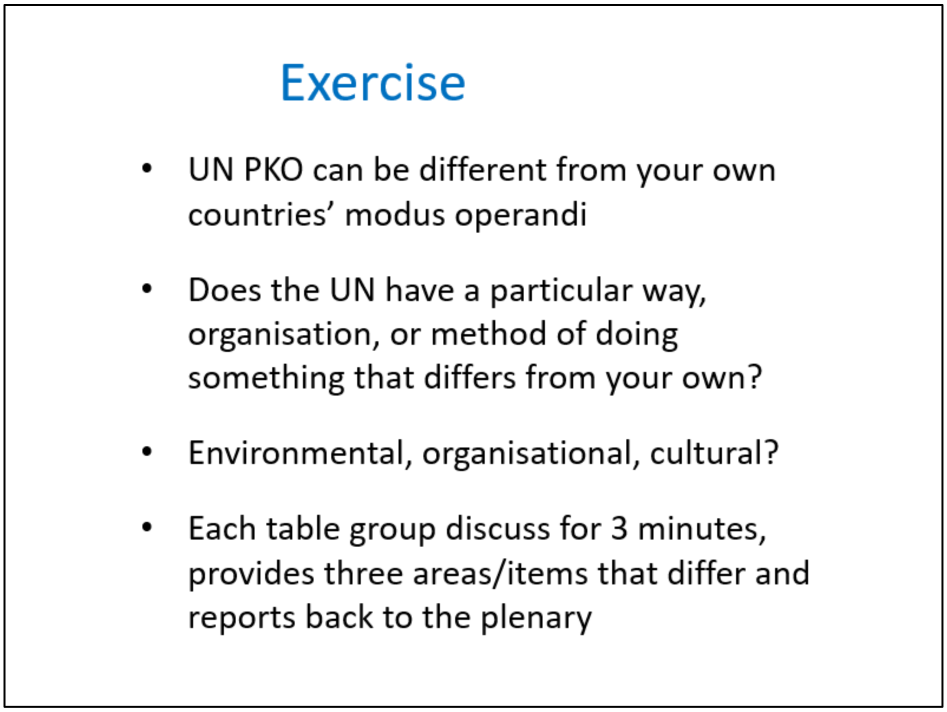
3. Effective Use of Force: The UN must recognise that hostile forces respond to strength. To deter and repel attacks, it is necessary to project strength and employ force when required. Risk-averse missions must understand that projecting strength provides security for both UN personnel and the civilian population. Night operations should be leveraged, using technological advantages to neutralise threats.

4. Embracing UN Principles: UN principles should not be seen as restrictions on initiative and the use of force. In high-risk areas, the UN should employ overwhelming force, adopting a proactive and pre-emptive approach. Failure to use the force in the current peacekeeping environment jeopardises mandates and puts the lives of troops, police, and civilians at risk.

5. Integrated Threat-Based Planning: Effective planning at both tactical and mission levels necessitates an integrated approach based on threat assessment and risk mitigation.

By addressing these areas of improvement as highlighted in the report, the UN can work towards reversing the trend of peacekeeper casualties and ensuring the security of its personnel. It is essential to embrace a proactive mindset, utilise force when necessary, and prioritise integrated planning and risk mitigation strategies. These actions will strengthen peacekeeping operations and contribute to the overall safety and success of UN missions.

Slide 12



Exercise

- UN PKO can be different from your own countries’ modus operandi
- Does the UN have a particular way, organisation, or method of doing something that differs from your own?
- Environmental, organisational, cultural?
- Each table group discuss for 3 minutes, provides three areas/items that differ and reports back to the plenary

- *Engage in comparative analysis: Initiate a discussion with the class to explore the differences between United Nations Peacekeeping Operations (UNPKOs) and their own countries' modus operandi. Encourage participants to consider whether the UN has distinct approaches, organisational structures, or methods that set it apart from their national practises and doctrine.*

- *Highlight distinctive aspects: Prompt the class to identify specific areas where the UN's operational framework diverges from their own. Encourage them to consider environmental factors, organisational structures, and cultural considerations that shape the UN's approach to peacekeeping.*

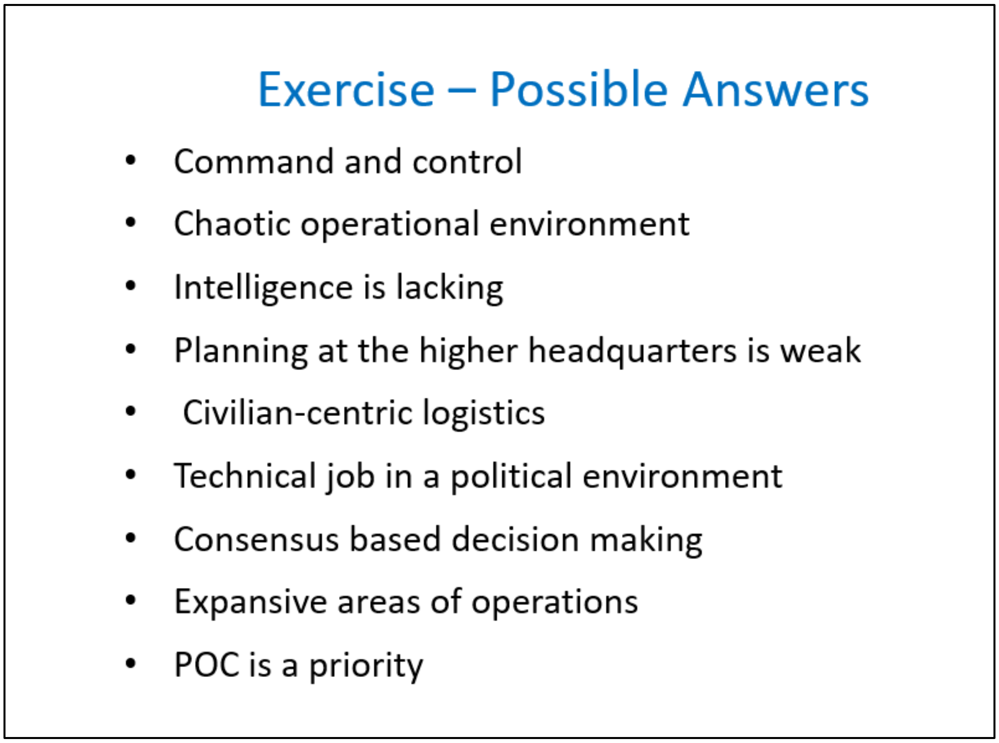
- *Group discussion: Divide the class into table groups and allocate 10 minutes for each group to discuss and identify three key areas or items that differentiate the UN's modus operandi from their own country's practises. Emphasise the importance of active participation and engagement during the discussion.*

- *Plenary Reporting: After the group discussions, reconvene the class for a plenary session. Each group should share their findings, and the key points can be recorded on a "butcher/flip chart" or whiteboard to visualise the progress and foster a comprehensive understanding of the differences identified.*

- *Facilitate Plenary Discussion: Allocate approximately 15 minutes for a lively plenary discussion, allowing participants to ask questions, seek clarifications, and share their perspectives. Use the next slide to present some examples and further enrich the discussion based on the points raised by the class.*

- *By structuring the session in this way, participants will actively engage in comparative analysis, fostering a deeper understanding of how UNPKOs differ from their own countries' practises and doctrine. This exercise encourages critical thinking, collaboration, and a broader perspective on the complexities of international peacekeeping operations. Note, if students use the word enemy to describe attackers or groups that pose a threat, remind them that we do not have an enemy in a UNPKO.*

Slide 13



Exercise – Possible Answers

- Command and control
- Chaotic operational environment
- Intelligence is lacking
- Planning at the higher headquarters is weak
- Civilian-centric logistics
- Technical job in a political environment
- Consensus based decision making
- Expansive areas of operations
- POC is a priority

Here are some examples of a UNPKO that may differ.

- Command and Control: In a UNPKO operation, command and control structures can be more complex due to the multinational nature of the mission. Different contingents from various countries may have different operational procedures, communication systems, and reporting structures, which can introduce challenges in achieving seamless coordination and unity of command. Some tactical units come under the tasking authority of the Mission / logistical civilian leadership while at the same time under the tactical/operational control of a police or military commander.

- Chaotic Operational Environment: UNPKOs are often in an environment where chaos and confusion prevail. The absence of a stable security environment, lack of peacekeeping-intelligence, complex C2, and conflicting requirements can pose additional challenges for mission planning, coordination, and the execution of tasks.

- Intelligence is Lacking: UNPKOs may face intelligence gaps due to limited access to information, language barriers, and local resistance to sharing sensitive information. This can impact the effectiveness of decision-making, threat assessment, and proactive measures to mitigate risks.

- Planning at the Higher Headquarters is Weak: The planning process in UNPKOs can be affected by limited resources, time constraints, and diverse perspectives among contributing nations. These factors can lead to challenges in developing comprehensive and robust operational plans at the higher headquarters level.

- Civilian-Centric Logistics: The UN mission logistic system operates under civilian leadership. As a result, logistical operations must consider the unique requirements of delivering humanitarian assistance, supporting local infrastructure, civilian components, and the military and police.

- Technical Job in a Political Environment: UNPKOs operate in a political environment where decisions and actions are influenced by political considerations and diplomatic engagements. Balancing technical military or police tasks with the need to navigate political sensitivities and engage with various stakeholders can create unique challenges for mission personnel.

- Consensus-Based Decision Making: Decision-making often involves seeking consensus among contributing nations, the host nation and other relevant actors. This process prioritises diplomatic efforts, multilateral cooperation, and inclusivity, but it can also lead to longer decision-making cycles and compromises on certain operational aspects.

- Expansive Areas of Operations: UN tactical units may operate in vast and diverse areas, encompassing multiple regions or even entire parts of a country. The wide geographical scope introduces logistical, operational, and security challenges, requiring effective coordination and adaptive strategies.

- Protection of civilians (POC) is a Priority: POC is a fundamental aspect of UNPKOs. Ensuring the safety and well-being of civilians, especially in conflict zones, becomes a primary objective and can significantly influence the planning, decision-making, and execution of operational tasks.

Here are other areas that my come up in the conversations:

- Mandate and Objectives: UNPKOs often operate under a specific mandate authorised by the UN Security Council, which sets out the mission's goals, tasks, and limitations. In contrast, national military or police operations may have different objectives aligned with their country's interests.

- Multinational Composition: UNPKOs involve personnel from various countries, creating a diverse multinational force. This contrasts with national operations that primarily consist of personnel from the country conducting the operation.

- Rules of Engagement (ROE): UNPKOs adhere to a standardised set of ROEs that prioritise the protection of civilians, focus on humanitarian rights and maintain peace. National operations focus on national interests and national security.

- Decision-Making Process: The decision-making process within UN PKOs often involves consultations and consensus-building among different countries and stakeholders. In national operations, decisions may be more centralized and driven by the country's chain of command.

- Resource Constraints: UNPKOs often face resource constraints, including limited funding, equipment, and personnel. National operations may have more extensive resources at their disposal.

- Language and interoperability: Issues can arise due to different languages used by both other TCC/ PCCS and the local population. Also, TCCs and PCCs have their own tactical doctrine and communications gear that do not necessarily align or are interoperable with the UN.

These factors highlight the unique operational environment and considerations that differentiate UNPKOs from national military or police operations. They underscore the complexity and challenges faced by UN peacekeepers in their efforts to maintain peace, protect civilians, and navigate the political landscape of the mission area.

Remember, these are just examples, and the actual differences may vary based on participants' countries and specific contexts. Encourage participants to share their own experiences and insights to further enrich the discussion and foster a deeper understanding of the divergences between UNPKOs and their own countries' practises.

Slide 14

Police and Military Units in Peacekeeping

Now, let us shift from the UNPKO environment and introduce the importance of UN tactical units.

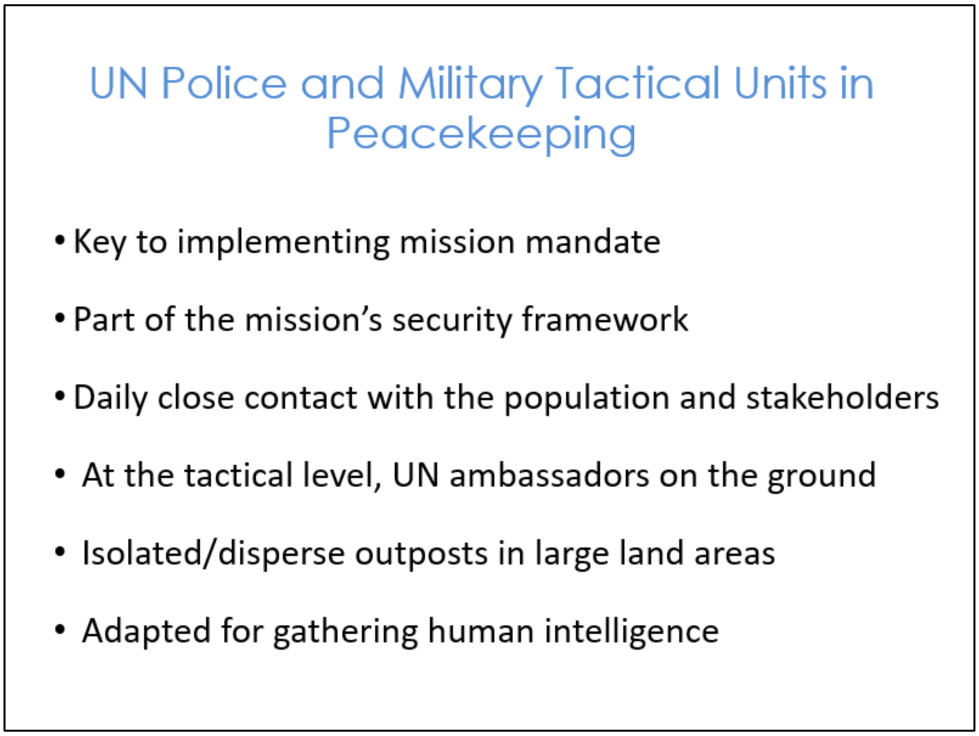
- *Enquire with the class why the military and police units are important in peace operations and what makes them special and suited to support a UN mandate.*

- *Inquire with the class why it is important that the UN units should be able to take a proactive approach to defend and protect themselves from attacks.*

- *Record the key points on a "butcher/flip chart" or whiteboard so the class can view the progress.*

- *A plenary discussion should take about 10 minutes.*

Slide 15



UN Police and Military Tactical Units in Peacekeeping

- Key to implementing mission mandate
- Part of the mission's security framework
- Daily close contact with the population and stakeholders
- At the tactical level, UN ambassadors on the ground
- Isolated/disperse outposts in large land areas
- Adapted for gathering human intelligence

The tactical UN units operating in a PKO environment possess special characteristics, including:

- Military and police units play a pivotal role in peacekeeping missions. Their specialized training and capabilities enable them to provide security, deter armed groups, protect civilians, and maintain law and order. This joint effort creates a stable environment, builds community trust, and supports the mandate implementation, making them key to mission success.

- Supporting the Security Framework: The primary role of these units is to provide support to the overall security framework of the mission. They contribute to deterring threats, protecting civilians, and enforcing peace and stability within the mission area.

- Emphasis on the Human Dimension: Tactical UN units rely on the human dimension of individual peacekeepers. Their success depends on the skills, training, discipline, and initiative of each peacekeeper in the Unit.

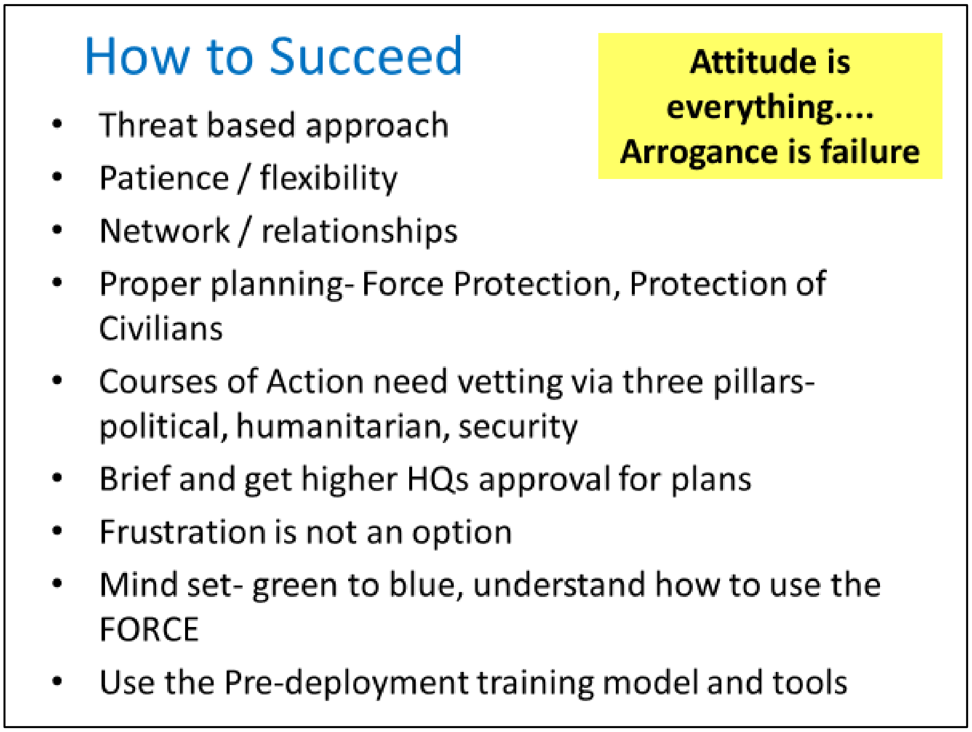
- Operating in Isolated and vast Areas of Responsibility: Often stationed far from their headquarters, support assets, and other units, these tactical units must operate in isolated areas and are responsible for large land areas. They demonstrate small unit discipline and initiative, acting decisively and independently in challenging situations, showcasing adaptability and effective decision-making in dynamic and complex environments. Additionally, they must maintain agility and mobility to swiftly move across various terrains and challenging conditions.

- Ambassadors on the Ground: Serving as the first line of engagement with the local population, these units represent the UN mandate on the ground. They directly interact with the community, building relationships, fostering trust, and demonstrating the mission's commitment to promoting peace, security, and the well-being of the local population.

- Valuable Information and Knowledge Sources: Tactical units possess a wealth of information and knowledge about the ground situation. Through their patrols and engagement with the local community, they gather crucial information and peacekeeping-intelligence that contribute to building a comprehensive operational picture for higher headquarters and the UN Mission.

By embodying these characteristics, tactical UN units play a vital role in the success of peacekeeping operations. They contribute to the mission's overall objectives and exemplify the UN's dedication to promoting peace and security in conflict-affected regions.

Slide 16



How to Succeed

Attitude is everything.... Arrogance is failure

- Threat based approach
- Patience / flexibility
- Network / relationships
- Proper planning- Force Protection, Protection of Civilians
- Courses of Action need vetting via three pillars- political, humanitarian, security
- Brief and get higher HQs approval for plans
- Frustration is not an option
- Mind set- green to blue, understand how to use the FORCE
- Use the Pre-deployment training model and tools

These points highlight key aspects crucial for success in a UNPKO (United Nations Peacekeeping Operation).

The Threat-Based Approach: Identify and analyse potential threats and risks in the operational environment. Tailor plans and actions to address specific threats and effectively mitigate risks. Continuously monitor and reassess threats to adapt and respond accordingly.

Patience/Flexibility: Understand that operational situations may change rapidly and unpredictably. Be patient and adaptable in adjusting plans and actions as necessary. Embrace flexibility to respond to emerging challenges and opportunities.

Network/Relationships: Build and maintain strong networks and relationships with key stakeholders. Collaborate with partner forces, local authorities, and international organisations. Leverage these relationships to gather peacekeeping-intelligence, share information, and coordinate efforts effectively.

Proper Planning - Force Protection and Protection of Civilians: Include force protection measures in all operational plans to ensure that units have operational freedom of action and safeguard their personnel. Develop strategies to protect civilians. Integrate humanitarian and Protection of Civilians (POC) considerations into planning to mitigate violence on civilian populations.

Courses of Action Need Vetting via Three Pillars - Political, Humanitarian, Security: Evaluate potential courses of action against political objectives and considerations. Assess the impact of proposed actions on humanitarian principles and the well-being of affected populations. Analyse the security implications and risks associated with each course of action.

Brief and Obtain Higher HQ Approval for Plans: Prepare comprehensive briefings to communicate plans, objectives, and anticipated outcomes. Seek approval from higher headquarters to ensure alignment with overall strategic objectives. Address feedback and incorporate necessary changes based on the guidance received.

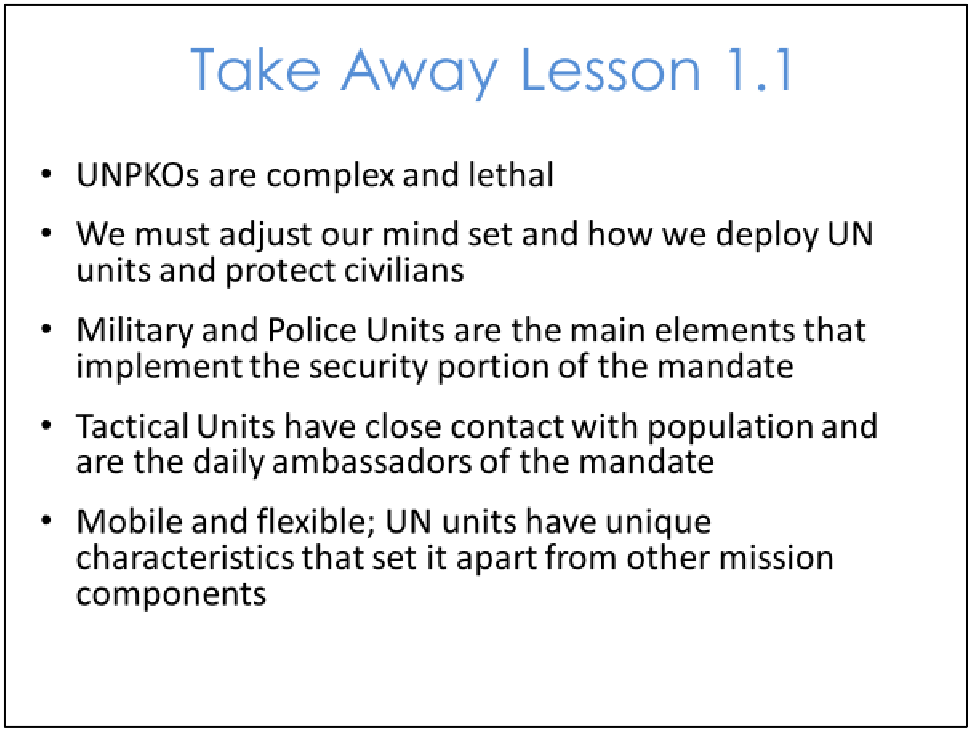
Frustration is not an Option: Emphasise the importance of maintaining composure and professionalism in challenging situations. Avoid allowing frustration to impede decision-making or hinder the mission's progress. Focus on problem-solving and seeking constructive solutions.

Mindset - Green to Blue, Understanding the Use of Force: Transition from a peacetime mindset (green) to an operational mindset (blue) when deployed. Understand the rules of engagement and appropriate use of force in accordance with international laws and conventions. Exercise judgment in applying force, considering the consequences and potential impact on the mission's objectives.

Attitude is Everything: Most leaders would say they prefer someone with a great attitude and a lower skillset over someone with a bad attitude and a higher skill set. No one will work with an individual who is not a team player. Emphasise the importance of a positive attitude and being a collaborative member of the team.

Use the Pre-deployment Training Model and Tools: Participate in pre-deployment training programmes tailored to the specific mission and environment. Acquire the necessary skills, knowledge, and cultural awareness to operate effectively in the deployment area. Utilise training tools such as simulations, scenario-based exercises, and cultural sensitivity training to enhance readiness.

Slide 17



Take Away Lesson 1.1

- UNPKOs are complex and lethal
- We must adjust our mind set and how we deploy UN units and protect civilians
- Military and Police Units are the main elements that implement the security portion of the mandate
- Tactical Units have close contact with population and are the daily ambassadors of the mandate
- Mobile and flexible; UN units have unique characteristics that set it apart from other mission components

Summary

- Police and military units are assets that contribute to achieving the mandate objectives.
- Peacekeeper fatalities have significantly increased over the years, emphasizing the need for a change in mindset and tackling new challenges.
- Protection of Civilians (POC) and Force Protection (FP) are crucial for mission success and UN credibility, necessitating POC/FP plans at all levels.
- UN tactical units rely on the human dimension of individual peacekeepers on the ground, possessing the ability to operate in diverse environments and engage with the local population as the first line of contact.
- Mobile and flexible, UN tactical units have unique characteristics that set them apart and enable them to fulfil their responsibilities effectively.

Lesson 1.2

Introduction to Force Protection

The Lesson

Starting the Lesson

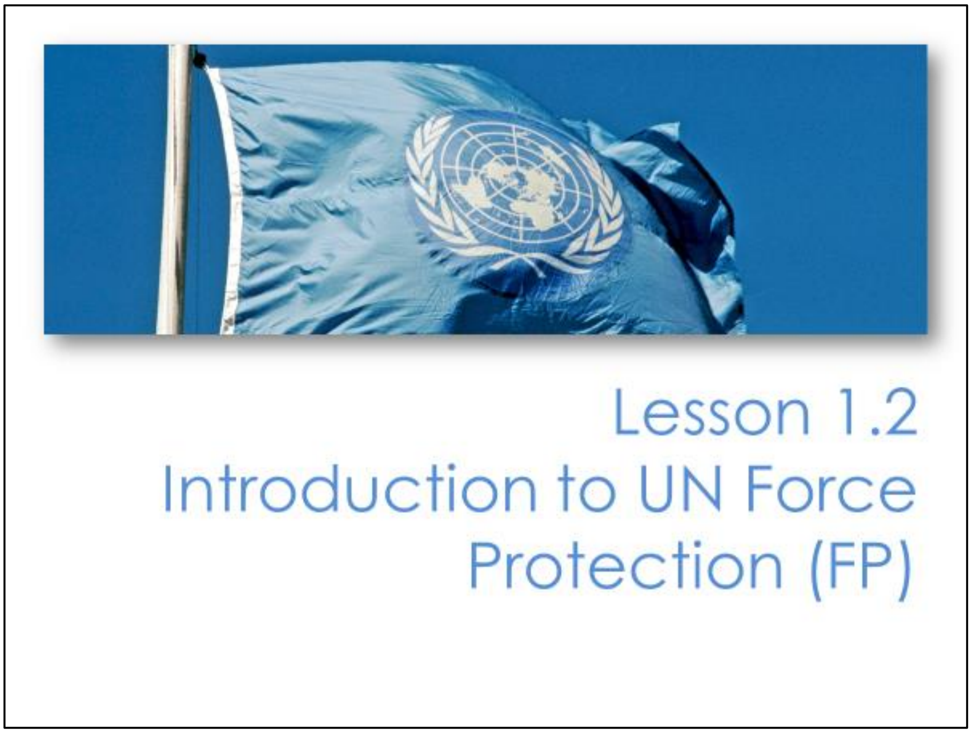
To facilitate a discussion on Force Protection (FP) in a Peacekeeping Operation (PKO), follow these steps:

- *Divide participants into small groups. Instruct each group to brainstorm and define what Force Protection means in the context of how a police or military tactical unit should consider FP before undertaking an operation or task,*
- *Allocate a specific timeframe for group discussions, such as 15 minutes. After the discussions, have each group report back to the plenary session to share their findings. Encourage group representatives to present their understanding of FP in PKOs and provide examples of how a tactical unit might prioritise and incorporate FP measures into their operational planning.*
- *As the facilitator, summarize the key points from each group's report on a whiteboard or chart to visualise the progress and foster a comprehensive understanding of FP in PKOs. Engage the plenary in a broader discussion to explore similarities, differences, and additional insights from the various group perspectives.*

The aim of this lesson is to provide the participants with a basic understanding of Force Protection (FP) in the United Nations Peace Operations framework.

- FP terminology/definitions
- Introduction to the principles and nature
- Introduction to FP threat, risk analysis
- FP Coordination

Slide 1

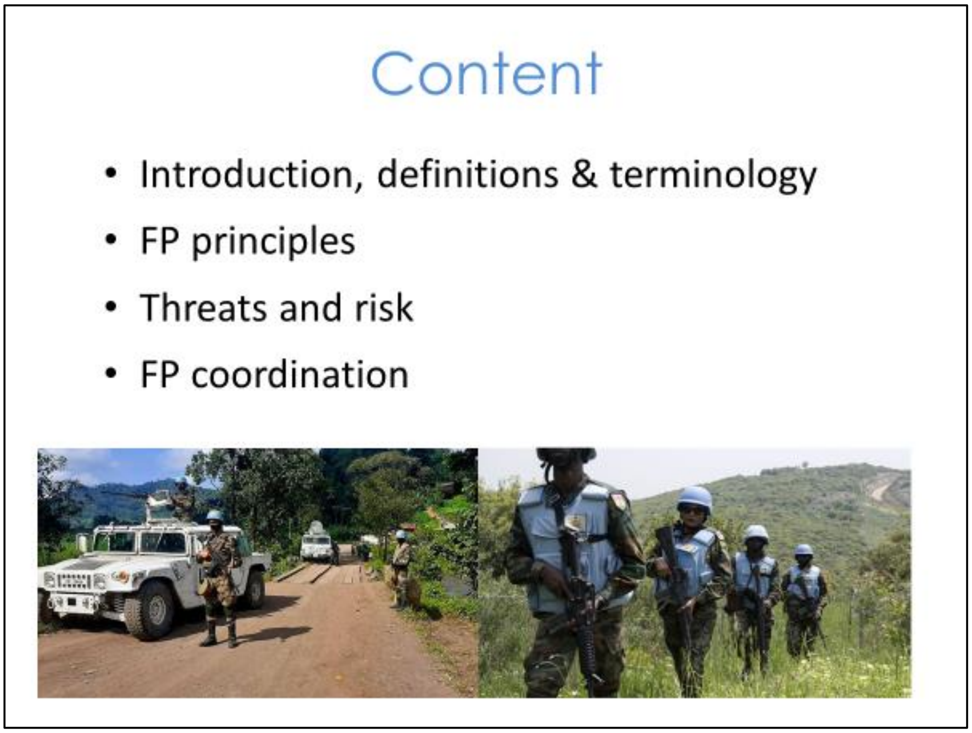


Lesson 1.2
Introduction to UN Force Protection (FP)

Force Protection (FP) is a crucial responsibility for all UN units operating in Peacekeeping Operations (PKOs). It must be integrated into the planning process of every mission. The rise in violent incidents targeting UN forces has underscored the criticality of FP. The escalating fatality rates among UN peacekeepers can be attributed to the capabilities of hostile actors and their deliberate targeting of UN personnel. To confront these emerging threats and mitigate risks, it is imperative to prioritise comprehensive education on FP tactical planning and execution.

Throughout this lesson, we will delve into the conceptual framework of FP within a UNPKO. Additionally, in module 3, we will explore the operational aspects of FP, addressing tactical considerations for developing and implementing a robust FP strategy. By equipping ourselves with a deeper understanding of FP principles and practises, we aim to enhance the safety and security of UN personnel, bolster mission effectiveness, and safeguard the well-being of those entrusted with upholding peace in challenging environments.

Slide 2



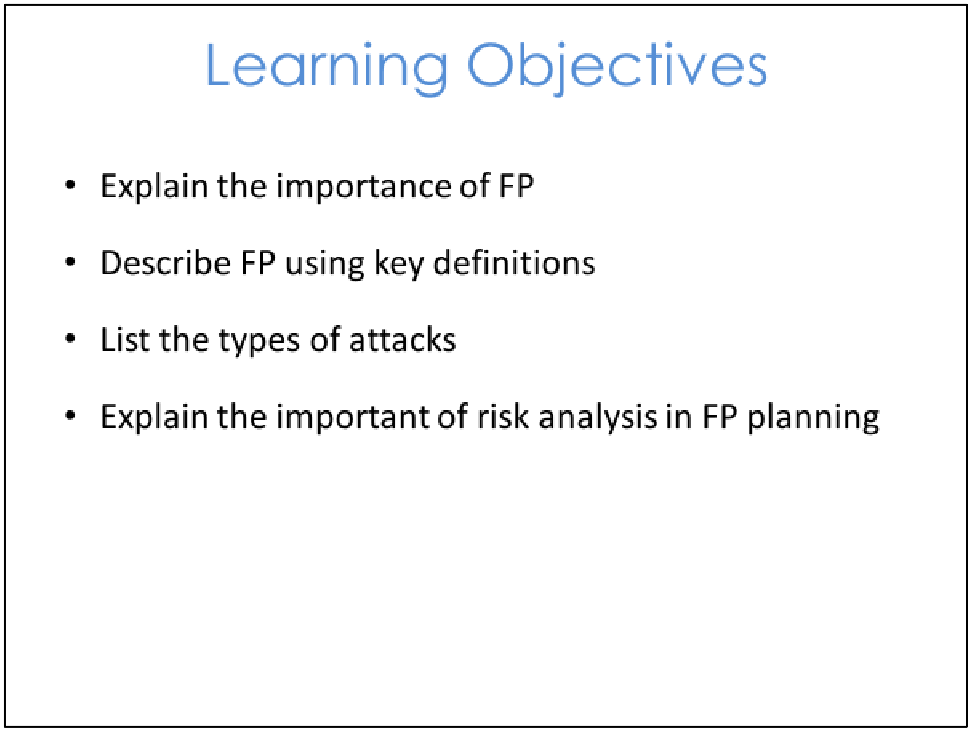
Content

- Introduction, definitions & terminology
- FP principles
- Threats and risk
- FP coordination

Here is the content for this lesson addressing the FP framework.

- Introduction, definitions & terminology
- FP principles
- Threats and risk
- FP coordination

Slide 3



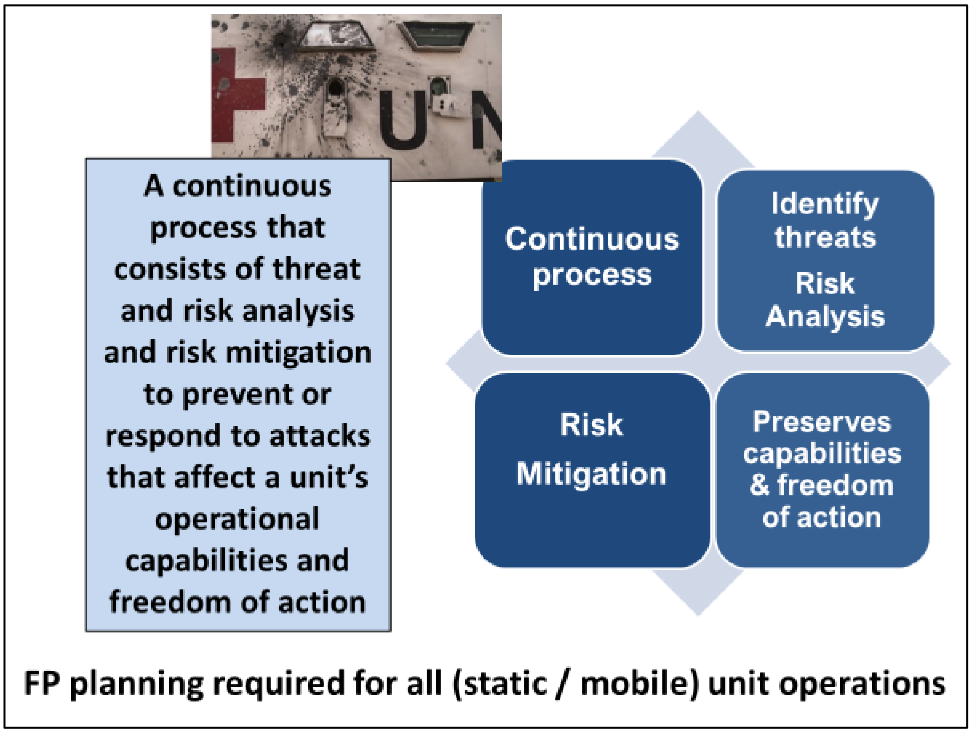
Learning Objectives

- Explain the importance of FP
- Describe FP using key definitions
- List the types of attacks
- Explain the important of risk analysis in FP planning

By the conclusion of this lesson, you will acquire the skills necessary to execute the tasks outlined on the slide. Take a moment to carefully review and comprehend the outlined requirements. This will enable you to prioritise and concentrate on the essential aspects that are most pertinent to your objectives.

- Explain the importance of FP
- Describe FP using key definitions
- List the types of attacks
- Explain the importance of risk analysis in FP planning

Slide 4



A continuous process that consists of threat and risk analysis and risk mitigation to prevent or respond to attacks that affect a unit's operational capabilities and freedom of action

Continuous process

Identify threats

Risk Analysis

Risk Mitigation

Preserves capabilities & freedom of action

FP planning required for all (static / mobile) unit operations

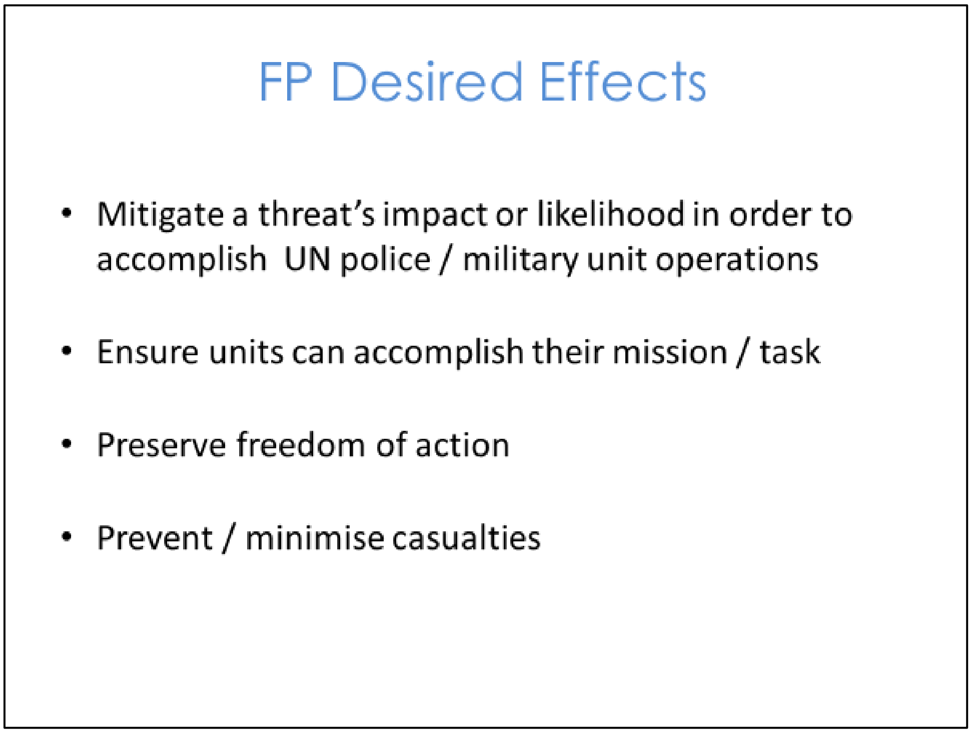
Force Protection (FP) is a continuous process that consists of threat and risk analysis and risk mitigation to prevent or respond to attacks that affect a unit's operational capabilities and freedom of action.

Force Protection (FP) is an ongoing process that encompasses analysing threats and risks, as well as implementing measures to prevent or respond to attacks that could hinder a unit's operational capabilities and freedom of action. It serves as a fundamental principle in all military operations, ensuring the successful completion of missions for UN tactical units. FP involves employing strategies to identify, prevent, and mitigate the likelihood and impact of threats.

FP entails a systematic approach to risk management, identifying risks to personnel, equipment, and mission, followed by the timely implementation of measures to address these risks to ensure the operational freedom of UN units.

In this lesson, we will provide a conceptual overview of the FP framework in Module 1. In Module 3, we will delve into planning considerations for unit operations, including threat and risk analysis specifically related to attacks.

Slide 5



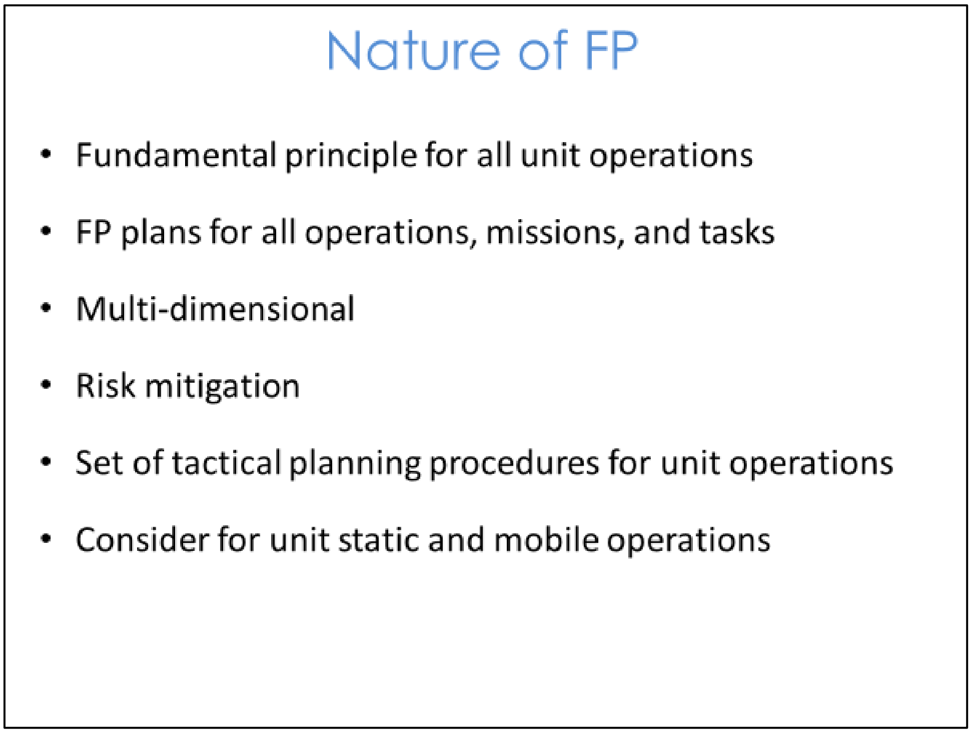
FP Desired Effects

- Mitigate a threat's impact or likelihood in order to accomplish UN police / military unit operations
- Ensure units can accomplish their mission / task
- Preserve freedom of action
- Prevent / minimise casualties

In every operation, it is a good practise to develop and set desired outcomes. Here are a few outcomes that we have set for UNFORPRO:

- Prevent violent attacks from threat actors; and if we cannot prevent then mitigate the impact or likelihood of the threat
- Reduce the vulnerability of UN troops and, police operations and provide the freedom of action for UN units to operate in support of the UN mandate
- Preserve freedom of action for UN units' operational capabilities and be able to use the force at a decisive time and place
- FP strategies support the ability to execute POC and to contribute to mandate implementation
- Minimise losses and casualties

Slide 6



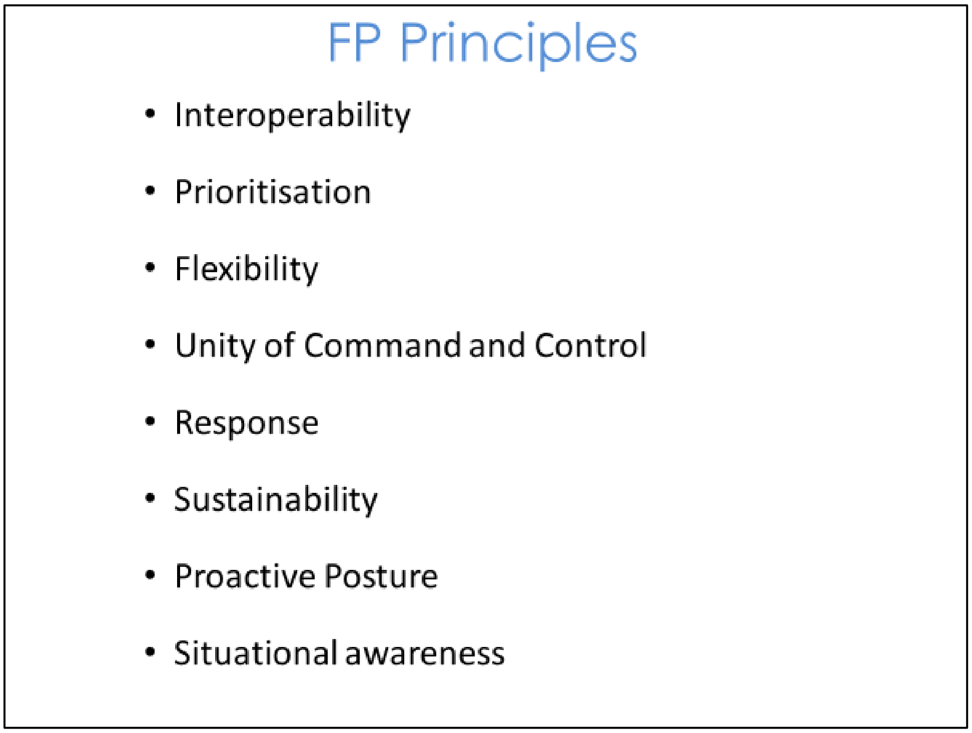
Nature of FP

- Fundamental principle for all unit operations
- FP plans for all operations, missions, and tasks
- Multi-dimensional
- Risk mitigation
- Set of tactical planning procedures for unit operations
- Consider for unit static and mobile operations

Let us look at the nature of FP:

- We consider it in all operations and systematically conduct FP planning in all operations
- FP mitigation management is organisational cross-organizational and multi-dimensional, providing a multi-layered approach to planning, resourcing, and executing
- FP includes a systematic risk management process
- Set of tactics, techniques, and procedures

Slide 7



FP Principles

- Interoperability
- Prioritisation
- Flexibility
- Unity of Command and Control
- Response
- Sustainability
- Proactive Posture
- Situational awareness

As in almost every conceptual framework, there is a set of principles. Here are the UNFORPRO principles:

Interoperability: Establishing liaison, conducting cross-training, coordinating measures, and engaging in rehearsals to ensure effective collaboration and coordination between different entities.

Prioritisation: Giving higher priority to the risks that pose greater threats.

Flexibility: Being adaptable to rapidly changing threats and adjusting plans and actions accordingly.

Unity of Command and Control: Recognising that negligence or insufficient compliance can compromise the overall success of the mission. Maintaining a clear chain of command and effective control systems.

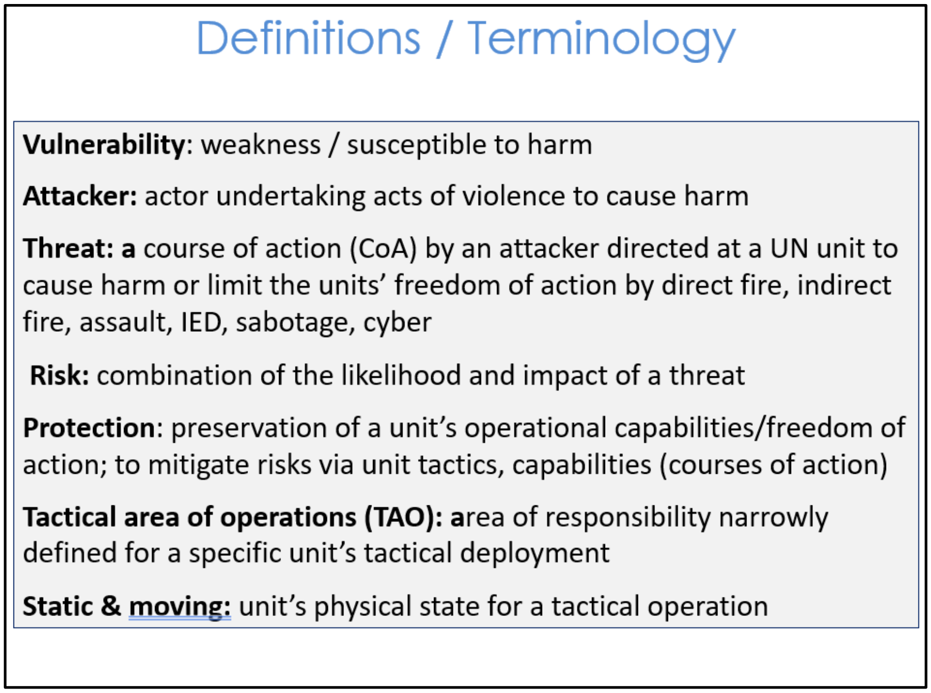
Response: Swift action and movement of units may be necessary to mitigate risks.

Sustainability: Ensuring the ability to maintain a consistent level of force protection posture over an extended period.

Proactive Posture: Taking an peacekeeping-intelligence-led approach based on comprehensive risk assessments and being willing to take the initiative to deter, prevent, and respond to threat events.

Operational Situational Awareness: This refers to having a comprehensive understanding of the operational environment in which operations are conducted. It involves real-time knowledge and understanding of factors that impact the mission, including the status, capabilities, and intentions of friendly forces, as well as the activities, capabilities, and intentions of potential adversaries or threats.

Slide 8



Definitions / Terminology

Vulnerability: weakness / susceptible to harm

Attacker: actor undertaking acts of violence to cause harm

Threat: a course of action (CoA) by an attacker directed at a UN unit to cause harm or limit the units' freedom of action by direct fire, indirect fire, assault, IED, sabotage, cyber

Risk: combination of the likelihood and impact of a threat

Protection: preservation of a unit's operational capabilities/freedom of action; to mitigate risks via unit tactics, capabilities (courses of action)

Tactical area of operations (TAO): area of responsibility narrowly defined for a specific unit's tactical deployment

Static & moving: unit's physical state for a tactical operation

In this training material, we will focus on essential definitions and terms related to the Force Protection framework, specifically concentrating on unit tactical protection. Our objective is to address threats that can temporarily or permanently hinder the operational capabilities or freedom of action of affected units in fulfilling their assigned tasks. Commanders must identify these threats and develop mitigation plans to ensure operational success.

These plans will involve tactical actions aimed at reducing risks to the unit. While other threats and hazards could also be considered and mitigated appropriately, our training material primarily focuses on tactical FP planning considerations concerning attacks against police and military units. These attacks encompass direct and indirect fire, assaults, IEDs, sabotage, and cyber threats. Natural hazards and other non-malicious threats, such as accidents and diseases, are crucial but may require procedural actions in coordination with the UN Mission civilian components, which take the lead. Safety incidents typically lack malicious or intentional components and are classified as accidents, hazards, or occupational safety events.

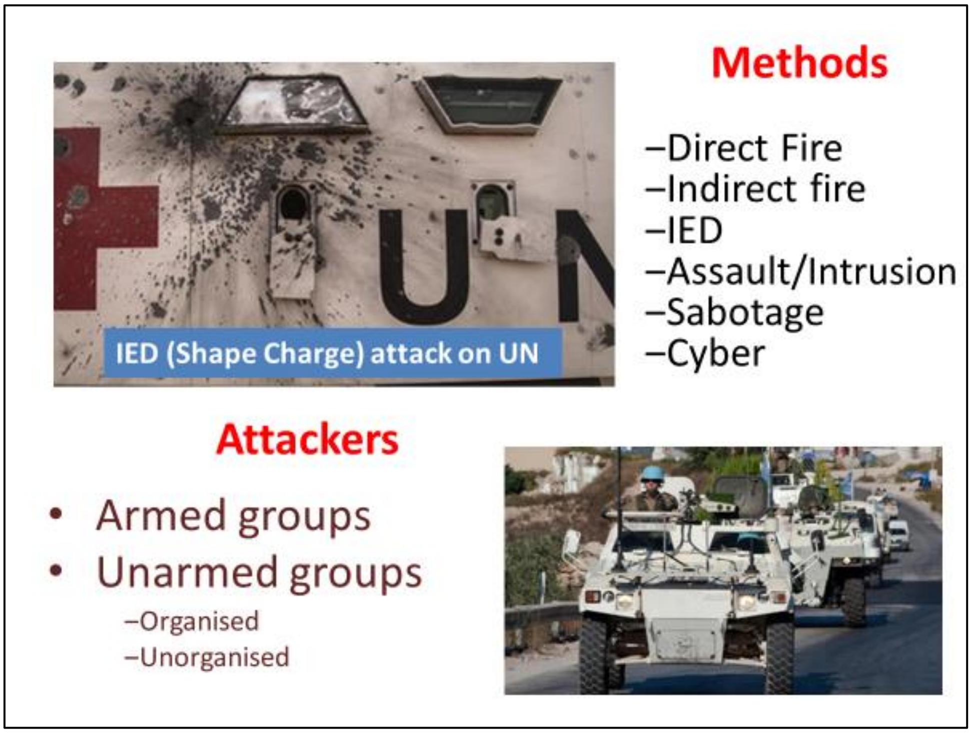
In Module 3 (Operational Framework), we will delve into a tactical approach to mitigating risks that have the potential to disrupt the operational capabilities of the affected unit.

We will use the following terms and definitions:

- Vulnerability: A weakness that exposes one to potential harm or danger

- Attacker: An individual or entity that carries out acts of violence or threats with the intention of causing harm
- Threat: actions or courses of action by attackers that result in casualties and or restrict a unit's freedom of action
- Risk: The combination of the likelihood and impact of a given threat
- Protection: The safeguarding of a unit's operational capabilities and freedom of action by mitigating risks through tactical courses of action
- Tactical Area of Operations (TAO): A narrowly defined area of responsibility assigned for the tactical deployment of a specific unit
- Static and Moving: The physical states of a unit during a tactical operation, indicating whether they are stationary or in motion (transit)

Slide 9



IED (Shape Charge) attack on UN

Methods

–Direct Fire
–Indirect fire
–IED
–Assault/Intrusion
–Sabotage
–Cyber

Attackers

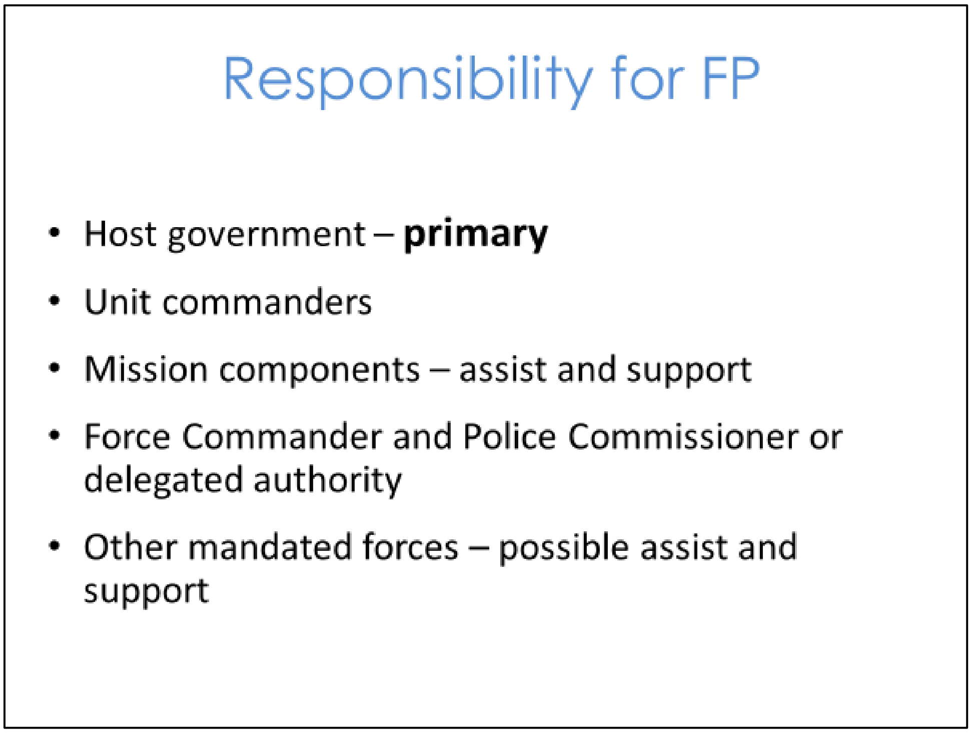
- Armed groups
- Unarmed groups
  - –Organised
  - –Unorganised

Ask the class to provide definitions and examples in these incidents, describing attacks, that pose a risk to UN units. Guide the discussion using the following list of defining attackers and their methods on the slides shown. explanations of these examples.

Here are the categories of the attacker and their methods. Take note of the compiled list of attack methods/types on the upper right side of the slide. Cyber-attacks encompass misinformation and disinformation campaigns targeting the UN and UN units. Additionally, we have categorized the attackers displayed on the bottom left-hand side of the slide. Attackers are classified as armed or unarmed groups, with a subcategory of organised or unorganised

For the purpose of this training, our focus will be on the tactical aspects of these types of attacks that intentionally aim at UN tactical units. Commanders must identify potential attackers/actors and understand their methods of attack, predicting them as threats. Each threat is analysed from a risk perspective and prioritised. A course of action (COA) plan is necessary to mitigate the risks they pose to the unit's operations.

Slide 10



Responsibility for FP

- Host government – **primary**
- Unit commanders
- Mission components – assist and support
- Force Commander and Police Commissioner or delegated authority
- Other mandated forces – possible assist and support

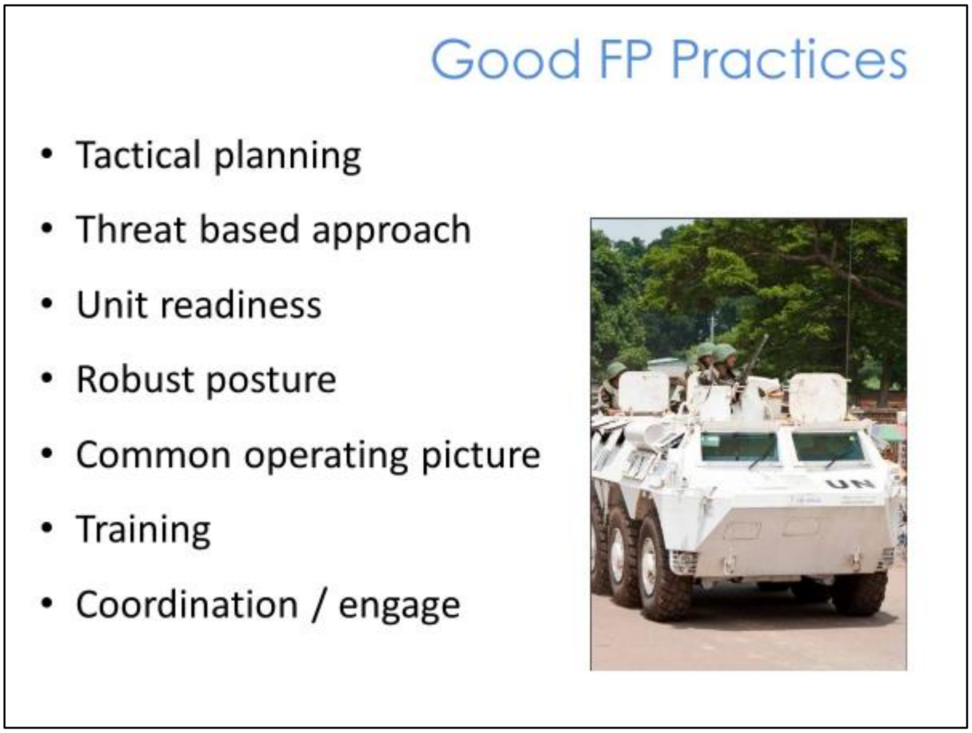
Who is responsible for Force Protection (FP) in a mission? Ultimately, at the tactical level, the unit commander bears the responsibility. The host state always holds the primary responsibility for protecting UN personnel within its borders. In cases where the state is unable or unwilling to provide protection, or where government forces themselves pose a threat, peacekeepers are authorised and responsible for offering force protection within their capabilities and areas of deployment.

In missions, it is the duty of the Special Representative of the Secretary-General (SRSG), the force commander, and the leadership of all military and police contingents to ensure the FP of all individuals under their command. The Force Commander and the Police Commissioner, or their delegated authorities, have responsibility for their units. The mission's civilian components also have a responsibility to support the mission's FP strategy.

Moreover, there may be mandated security forces or regional organisations' forces that support international and UN objectives, potentially reinforcing or assisting in the mission's FP strategy.

FP necessitates effective coordination of all its fundamental components and related assets. Unit commanders must provide clear FP direction and guidance at all levels of command to initiate operations planning and maintain consistency in applying FP measures, tasks, and activities. Mission-specific FP Standard Operating Procedures (SOPs) and directives should specify FP procedures from threat identification to the response phase, along with associated task elements, equipment, and infrastructure for FP.

Slide 11



Good FP Practices

- Tactical planning
- Threat based approach
- Unit readiness
- Robust posture
- Common operating picture
- Training
- Coordination / engage

Here are a few good practises when it comes to FP:

Emphasise the importance of a thorough planning process: FP plans should undergo a rigorous process and plans be approval by higher headquarters, ensuring effective command and control, unity of command, and adherence to standard operating procedures (SOPs).

Prioritise peacekeeping-intelligence and a threat-based approach for FP mission analysis: A comprehensive understanding of the peacekeeping-intelligence landscape and assessing potential threats is crucial for effective force protection.

Maintain unit readiness and project a robust security posture: Demonstrate a professional demeanour to deter potential attackers, consistently projecting an image of professionalism and readiness. Ensuring unit readiness is essential to avoid becoming an attractive target. Additionally, maintain solid physical security by regularly inspecting and maintaining bases, equipment, and defences to prevent vulnerabilities.

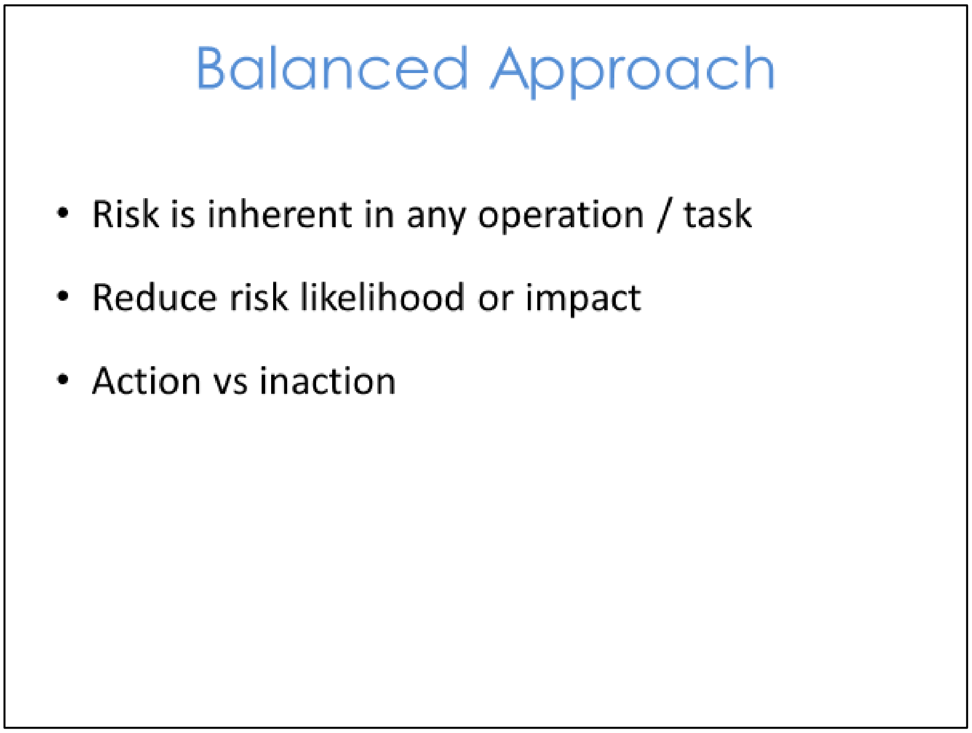
Foster good situational awareness and establish a common operating picture (COP): Maintaining a comprehensive understanding of the operational environment is vital for effective force protection. Establish early warning systems and maintain a network of named areas of interest (NAIs) that are actively integrated into the planning and execution processes.

Conduct regular rehearsals, exercises, and drills for tactical plans at all levels: Proactively prepare for potential contingencies by regularly practicing and refining tactical plans at various echelons. Key training elements should include actions on contact and rules of engagement (ROE), allowing for flexibility in adapting to dynamic situations.

Coordinate effectively with other units and entities: Collaboration and coordination with relevant stakeholders, including other units and supporting entities, are critical for comprehensive force protection measures. Foster effective communication channels and establish clear lines of coordination to ensure a cohesive approach.

These improvements aim to enhance clarity, coherence, and readability while conveying the original meaning and intent of the bullet points.

Slide 12



Balanced Approach

- Risk is inherent in any operation / task
- Reduce risk likelihood or impact
- Action vs inaction

Effective FP measures require a delicate balance between executing operations in high-threat environments and safeguarding the unit against costly attacks. While it is essential for staff to consistently mitigate high risks, it is equally important to acknowledge that risk is an inherent part of operations. There will be instances where units must accept that not all risks can be accounted for and not all threats can be fully eliminated. However, the mitigation of courses of action (COAs) can be planned.

In the past, a tendency toward risk aversion among UN units has placed them in a vulnerable position, attracting increased attacks and endangering personnel due to perceived weakness. Adopting a non-action approach and projecting a weak posture have only served to enhance the vulnerability of forces or reinforce the notion among hostile groups that the UN will not respond.

To enhance FP, units should proactively identify threats and risks to their security and take the initiative, employing all available tactics to neutralise or eliminate these threats. Missions should actively engage areas where threats are present, aiming to neutralise them effectively. Furthermore, operations conducted during night-time can leverage the unit's superior technology and provide an advantage. Adopting a reactive modality and passive posture only grants hostile forces the freedom to choose when, where, and how to attack.

Slide 13

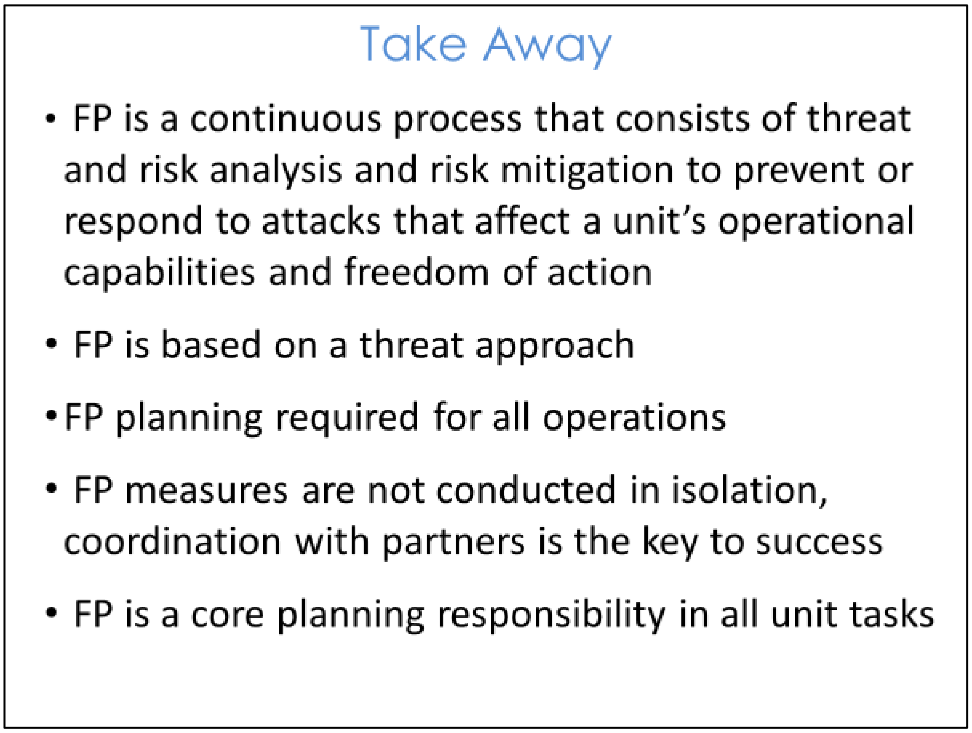
Coordination / Engagement

- Peacekeeping Intelligence cells
- Military, Police and Civilian Components
- Regional Offices
- HSSF, host nation law enforcement
- Other mandated UN forces
- Medical. CASEVAC
- Local governments, communities
- NGOs, regional / international organisations

Maintaining constant engagement with partners is paramount for the FP planning and execution success. Fundamentally, it requires the UN units, working together with the peacekeeping-intelligence framework, mission components, other partners, and support sections to identify the full range of threats and to support the FP support requirements. An IED threat can be mitigated and/or neutralised through the employment of special equipment and personnel for a convoy. Engineering units/sections should be consulted to ascertain what improvements of operating bases. A unit does not do FP in isolation. Here are some examples of elements that should be considered:

- Intelligence cells
- Military, Police and Civilian Components
- Regional Offices
- HSSF, host nation law enforcement
- Other mandated UN forces
- Medical. CASEVAC
- Local governments, communities
- NGOs, regional / international organisations

Slide 14



Take Away

- FP is a continuous process that consists of threat and risk analysis and risk mitigation to prevent or respond to attacks that affect a unit's operational capabilities and freedom of action
- FP is based on a threat approach
- FP planning required for all operations
- FP measures are not conducted in isolation, coordination with partners is the key to success
- FP is a core planning responsibility in all unit tasks

Summary

This lesson has established a foundation for comprehending the conceptual framework of UNPKO Force Protection (FP).

- FP serves as a strategic approach that operationalises continuous analyses, encompassing threat and risk analyses, and risk mitigation to prevent or respond to attacks that impede a unit's operational capabilities and freedom of action
- A threat-based approach should underpin FP planning, ensuring a comprehensive understanding of potential risks
- FP should be integrated into all operational tasks, becoming an inseparable component of mission planning and execution
- FP measures should not be conducted in isolation; success hinges on effective coordination with partners, fostering collaboration and synergy

FP Learning Activity 1.2

RESOURCES
Situations- Handout (attached below), chalk board or butcher paper and markers

TIME
Suggested time 30 min to one hour (dependant on the discussions).

PREPARATION
At the end of the lesson, choose some of the following situations/activities for review and discussion. Depending on the time available and the student's level of understanding, select all or the appropriate number of situations or activities below.

Divide the class into groups and give them the necessary time to read the narrative. Another option is to divide the plenary into three subgroups and ask to provide each group with a different topic. Ask the students to discuss and report back to the plenary. Provide the students with the Handout below (or provide the handout as a read-ahead the day prior to the lesson presentation).

NOTES TO INSTRUCTORS:
Reinforce the learning outcomes and access the knowledge of the group and individuals. Here are some suggested solution sets to help facilitate the discussions.

During the discussions, ask the students- What better planning (proactive) threat and risk analysis should have been done and what mitigating measures should have been implemented prior to the incident?

Instructor Notes- Situation #1

- If required, negotiations fail, and no further guidance from your headquarters, engage using force, if necessary, to restore the freedom of movement. Deploying the force in a tactical formation is considered using the force. When using force, do so in accordance with the Rules of Engagement (ROEs); any measures taken must prevent harmful consequences to civilians
- Comprehensive threat and risk analysis: Prior to the mission, a thorough assessment of the security landscape should have been conducted. This includes gathering peacekeeping-intelligence on potential armed groups or hostile actors operating in the area, identifying potential conflict zones, and analysing historical incidents that could indicate areas of heightened risk

- Route reconnaissance and selection: Careful planning of the route should have been undertaken, considering known or suspected threat areas, potential chokepoints, and areas of limited visibility
- By conducting detailed route reconnaissance, alternative routes or bypasses could have been identified to minimise exposure to risks
- Security coordination and information sharing: Prior to the movement, effective coordination with relevant local authorities, partner organisations, and peacekeeping-intelligence agencies could have provided valuable insights and warnings about potential threats. Sharing information with other UN units in the region could have enabled a collaborative approach to mitigating risks.
- Contingency planning: A proactive approach involves developing contingency plans for various scenarios, including encountering unknown armed groups. These plans should outline specific actions, communication protocols, and response strategies tailored to different threat levels
- In the event of an incident where the movement is halted by an unknown armed group, the immediate actions should prioritise the security of the UN unit and the mission ahead. This may involve maintaining situational awareness, establishing communication with higher headquarters and relevant authorities, and following established protocols for engaging with potential threats while minimising risks
- To better plan and mitigate such incidents in the future, the following measures can be implemented:
- Enhanced peacekeeping-intelligence gathering: Strengthen peacekeeping-intelligence capabilities to gather timely and accurate information about potential threats and armed groups operating in the area. This includes leveraging local sources, engaging with local communities, and utilising advanced surveillance technologies
- Pre-mission engagement: Establishing relationships with local communities and key stakeholders can provide valuable insights and early warning of potential threats. Regular engagement with local authorities, security forces, and community leaders can foster cooperation and support in mitigating risks.
- Continuous situational awareness: Implement a robust system for ongoing situational awareness, incorporating real-time peacekeeping-intelligence feeds, early warning systems, and regular threat assessments. This ensures timely updates on evolving security dynamics, allowing for proactive decision-making and adjusting operational plans accordingly
- Training and readiness: Regularly train personnel on response protocols, rules of engagement, and conflict management techniques. Conducting realistic scenario-based exercises and drills can enhance preparedness and decision-making abilities in high-stress situations
- By implementing these measures, UN units can better anticipate and mitigate incidents, ensuring the safety and security of personnel during movements to new operating bases

Instructor Notes- Situation #2

- Respond appropriately by exercising the inherent right of self-defence. Use the appropriate force to prevent casualties, and prevent the attackers from negating your freedom of action.
- The immediate action should prioritise the protection of the personnel and the integrity of the convoy to maintain freedom of action. This may involve engaging established response battle drills, implementing evasive manoeuvres, establishing effective communication with other convoy members, and requesting support from nearby security forces or higher headquarters
- Comprehensive threat and risk analysis: Prior to the convoy, a thorough analysis of the threat landscape should have been conducted. This includes identifying potential adversaries, assessing the likelihood of ambushes or attacks along the route, and understanding the local security dynamics. Factors such as known conflict zones, historical incidents, and peacekeeping-intelligence reports should be considered
- Route selection and reconnaissance: Conducting route reconnaissance is crucial to identify potential ambush points, vulnerable areas, or areas with limited visibility. Alternative routes should be explored, and the selected route should aim to minimise exposure to known or suspected threats. Additionally, gathering information from local sources, such as security forces or trusted contacts, can provide valuable insights into the security situation along the route.
- Security measures and convoy composition: Implementing appropriate security measures is vital for convoy protection. This includes selecting an appropriate convoy composition with adequate personnel, vehicles, and specialised security elements if necessary. Measures such as employing armed escorts, implementing communication protocols, and utilising armoured vehicles or protective equipment should be considered based on the assessed threat level
- Coordination and peacekeeping-intelligence sharing: Establishing effective coordination channels with local authorities, partner organisations, and peacekeeping-intelligence agencies can enhance the understanding of the local security environment. Sharing information and peacekeeping-intelligence regarding potential threats, recent incidents, or hostile activities can contribute to better preparedness and the implementation of proactive measures.
- Training and rehearsals: Regularly conducting training exercises and rehearsals specific to convoy operations is crucial. This includes practising convoy movement techniques, implementing standard operating procedures (SOPs), and training personnel on actions to be taken in the event of an ambush or attack. By simulating potential scenarios, personnel can improve their response capabilities and decision-making under pressure

Instructor Notes- Situation #3

- Conduct comprehensive threat and risk analysis: Prioritise the assessment of potential threats and risks along the designated routes. Utilise peacekeeping-intelligence resources, historical data, and local sources to identify key ambush sites and areas of concern
- Deploy reconnaissance and security patrols: Send out dedicated teams to gather information and conduct patrols in advance of identified key ambush sites. Their observations and findings can provide valuable insights for better planning and risk mitigation
- Determine priority locations/routes for force protection (FP): Consider various factors such as mission objectives, assessed threat levels, terrain and weather conditions, troop capabilities, available support assets, time constraints, and civil considerations. This evaluation helps determine the level of protection needed for specific locations or routes
- Ensure unit integrity: Maintain the integrity of smaller operational units (e.g., sections, platoons, companies) by implementing clear communication protocols, synchronized movement, and maintaining situational awareness. Cohesion and coordination within these units enhance overall force protection effectiveness
- Assess the size of the element requiring protection: Evaluate the composition and size of the element that needs protection. This analysis helps determine the appropriate resources, security measures, and force composition necessary to protect the unit
- Develop methods and reinforcement strategies: Establish proactive measures and contingency plans to address potential risks and threats. This includes determining protocols for medical evacuation, identifying evacuation routes, planning reinforcement actions, and establishing communication procedures during emergencies
- Identify and address restricted movement areas: Identify areas where movement may be restricted due to natural obstacles or manmade structures. Evaluate alternative routes, conduct necessary reconnaissance, and implement risk mitigation measures to safely navigate these areas
- Incorporate risk mitigation measures for identified Named Areas of Interest (NAIs): Identify NAIs, including potential ambush sites, and develop specific risk mitigation measures. Conduct prior reconnaissance and counter-ambush operations to gather peacekeeping-intelligence and improve situational awareness
- Plan for encountering obstacles or checkpoints: Develop procedures for encountering unexpected obstacles or checkpoints during the mission. Establish protocols for communication, engagement, and escalation of force to navigate such situations effectively

- Address mine or IED encounters: Prepare response protocols for encountering mines or improvised explosive devices (IEDs). Include procedures for identifying, marking, reporting, and safely neutralising or bypassing these threats. Include EOD or engineer support
- Establish medical emergency response protocols: Develop comprehensive medical emergency response plans, including procedures for casualty evacuation, communication with medical assets, and providing immediate medical care within the capabilities of the unit
- Plan for vehicle-related issues: Address potential issues such as lost vehicles, separated vehicles, broken-down vehicles, or vehicles getting bogged down. Develop procedures for communication, recovery, and ensuring the safety of personnel during vehicle-related incidents
- Account for communication challenges: Establish contingency plans for scenarios where communication systems fail or become compromised. Consider alternative communication methods, pre-arranged signals, and designated meeting points to maintain coordination and situational awareness.
- Plan for short and long halts: Develop protocols for conducting short and long halts during the mission. Consider security measures, surveillance, and maintaining situational awareness during these periods of reduced mobility.
- Prepare for landing zone operations: Establish procedures for landing zone operations, including coordination with air assets, securing the perimeter, rapid disembarkation, and regrouping to ensure the safety of personnel and equipment
- By expanding on these points, the planning process becomes more comprehensive, addressing a wider range of potential threats and scenarios, thus enhancing force protection and overall mission success

Instructor Notes- Situation #4

- Comprehensive risk assessment: Conduct a thorough risk assessment specific to the region and village in question. Analyse the local dynamics, historical incidents, and potential sources of tension to better understand the potential risks and challenges that may arise.
- Community engagement and consultation: Prior to the deployment, engage with local community leaders, representatives, and stakeholders to assess their concerns and expectations regarding the UN peacekeeping mission. Establish open lines of communication and foster a sense of trust and cooperation.
- Coordination with local forces and law enforcement: Establish coordination mechanisms and communication channels with local forces and law enforcement agencies. Share information, peacekeeping-intelligence, and situational updates to ensure a collaborative approach to maintaining security and protecting civilians.
- Crowd control capacity: Ensure that the deployed patrol has adequate training and resources for crowd control and managing public demonstrations. This includes equipping the patrol with appropriate non-lethal crowd control measures and ensuring personnel are trained in de-escalation techniques and respect for human rights.
- Rules of engagement and self-defence: Clearly define and communicate the rules of engagement for the patrol. This should include provisions for self-defence while prioritizing the protection of civilians. Ensure that peacekeepers are trained in proper self-defence techniques and aware of protocols for responding proportionately to threats.
- Continuous situational awareness: Establish mechanisms for monitoring the local security situation on an ongoing basis. This may involve regular patrols, peacekeeping-intelligence gathering, and liaising with local sources to detect any emerging tensions or potential threats.
- Joint planning and information sharing: Foster coordination and information sharing with other UN peacekeeping units, local authorities, and relevant international organisations operating in the area. Regular meetings and joint planning sessions can enhance situational understanding and enable a coordinated response to potential challenges.
- Cultural sensitivity and awareness: Provide cultural training and sensitization to peacekeeping personnel to better understand and respect local customs, traditions, and sensitivities. This fosters a positive relationship with the local population and reduces the likelihood of misunderstandings or tensions.

Student Hand Out Learning Activity FP Lesson 1.2

Situation 1

A UN unit was en route to establish a new operating base when, unexpectedly, their movement was abruptly halted by an unknown armed group for unknown reasons. To prevent such incidents and enhance proactive planning, what planning / preventive actions/improvements could have been made?

Situation 2

A UN unit is in transit, and unfortunately, they encounter an ambush where they become targets. In such a situation, what immediate action is necessary to ensure the safety and security of the unit? Additionally, to mitigate the incident and improve proactive planning, what steps could have been taken beforehand?

Activity 3

While planning a movement what are the main considerations for FP? What are the likely plans you might visualise to include in any FP planning?

Situation 4

A UN patrol was deployed to provide protection to a small village population, but unfortunately, protests erupted after two days, demanding the immediate withdrawal of the UN peacekeepers due to perceived failures in protecting civilians in the region. To prevent such incidents and enhance proactive planning, the following measures should have been implemented prior to the operation?

Lesson 1.3

The Lesson

Starting the Lesson

Overview

To foster an interactive and engaging start to this lesson, encourage active participation from the students. Begin by inviting them to share their perspectives on potential attackers and threats that could target a UN unit. Facilitate a discussion on how intelligence and a threat-based approach play a crucial role in analysing operational areas for effective tactical planning. Prompt the students to collaboratively generate a comprehensive list encompassing elements related to the physical terrain, human terrain, and information terrain.

Throughout the lesson, highlight the significance of intelligence in supporting peacekeeping operations. Encourage the students to identify the various benefits intelligence provides, such as enhanced situational awareness, early warning capabilities, and the ability to identify potential attackers. Record their insights on a whiteboard or a shared digital platform.

*Recommend that the instructor **review** the UN DPO Peacekeeping Intelligence Policy, and the Military Peacekeeping Intelligence Handbook.*

Slide 1

Lesson 1.3

Introduction to Intelligence and Threat-based Approach to Force Protection Planning

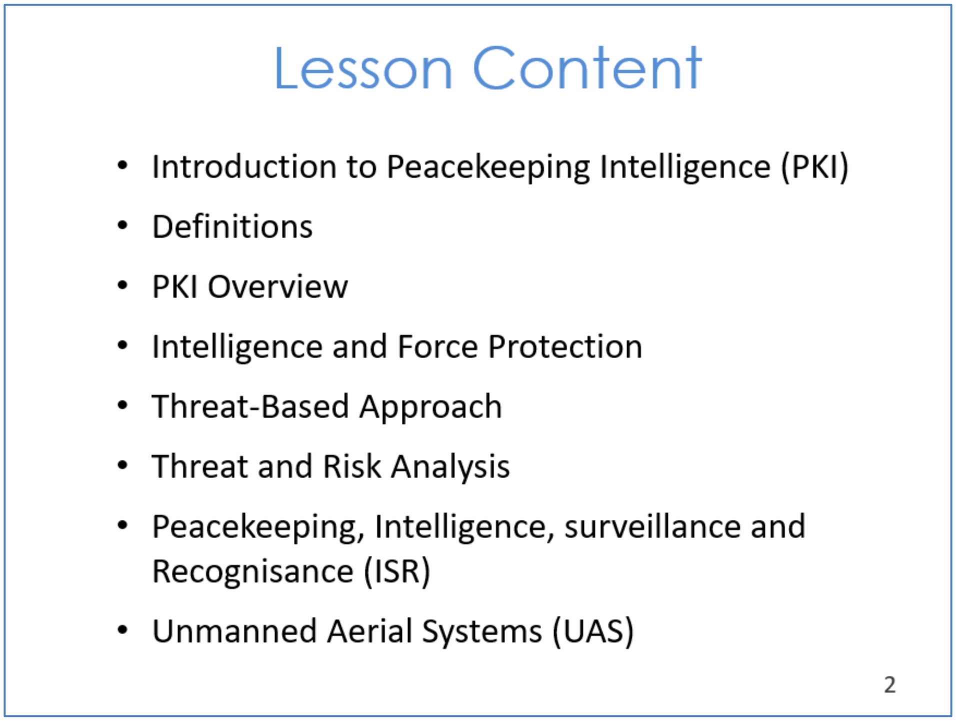
1

Leaders rely on a continuous stream of processed and analysed information, which equates to peacekeeping-intelligence, in order to make well-informed planning decisions prior to undertaking any task or mission. The United Nations (UN) has aimed to enhance situational awareness and deepen knowledge of threats in a particular region or area ever since the tragic events of the Srebrenica Massacre and the Genocide in Rwanda. Consequently, the UN has had to re-evaluate the concept of information operations within the context of complex peacekeeping missions.

It is of utmost importance that decision-makers, staff members, and leaders at the tactical level are fully cognizant of their capabilities and their role in the peacekeeping-intelligence cycle. Understanding the significance of accurate and timely peacekeeping-intelligence is vital for supporting the Force Protection plan.

Our focus also extends to the capabilities of peacekeeping peacekeeping-intelligence, surveillance, and reconnaissance (PKISR), specifically emphasising activities related to the acquisition phase of the peacekeeping-intelligence cycle. Furthermore, we will introduce the PKISR framework and provide a brief overview of the utilisation of unmanned aerial system (UAS) capabilities as a valuable resource for gathering information.

Slide 2



Lesson Content

- Introduction to Peacekeeping Intelligence (PKI)
- Definitions
- PKI Overview
- Intelligence and Force Protection
- Threat-Based Approach
- Threat and Risk Analysis
- Peacekeeping, Intelligence, surveillance and Recognisance (ISR)
- Unmanned Aerial Systems (UAS)

2

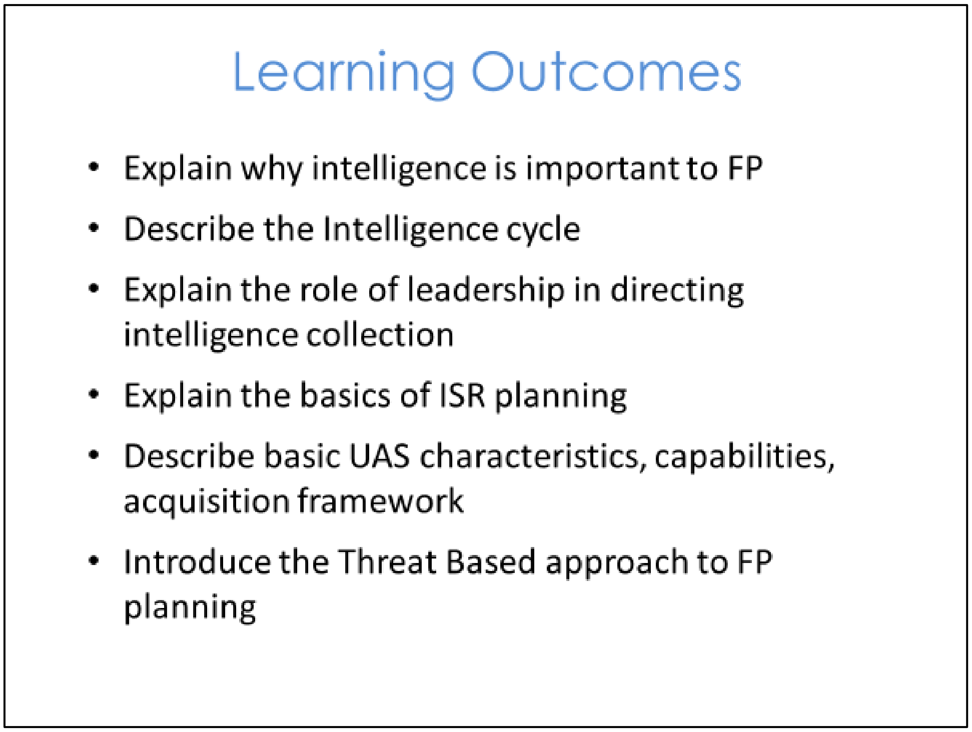
Here are the major components of this lesson:

- Introduction to peacekeeping-intelligence (PKI)
- Definitions
- PKI Overview
- Intelligence and Force Protection
- Threat-Based Approach
- Threat and Risk Analysis
- PK-Intelligence surveillance and Recognisance (PKISR)
- Unmanned Aerial Systems (UAS)

In this lesson, we will provide a comprehensive introduction to the peacekeeping-intelligence framework and the essential factors involved in conducting a threat-based and risk analysis of the area of operations, focusing specifically on the Force Protection process. It is crucial to recognise that police and military units possess distinct capabilities for patrolling and gathering information, which brings a unique perspective to the assessment of threats within a given area.

We will elucidate how peacekeeping-intelligence, surveillance, and reconnaissance (PKISR) have the potential to enhance operational safety through various means, primarily by improving our comprehension of the operational environment.

Slide 3



Learning Outcomes

- Explain why intelligence is important to FP
- Describe the Intelligence cycle
- Explain the role of leadership in directing intelligence collection
- Explain the basics of ISR planning
- Describe basic UAS characteristics, capabilities, acquisition framework
- Introduce the Threat Based approach to FP planning

This slide displays the learning outcomes.

- Explain why peacekeeping-intelligence is important to FP
- Describe the peacekeeping-intelligence cycle
- Explain the role of leadership in directing peacekeeping-intelligence collection
- Explain the basics of PKISR planning
- Describe basic UAS characteristics, capabilities, acquisition framework
- Introduce the Threat Based approach to FP planning

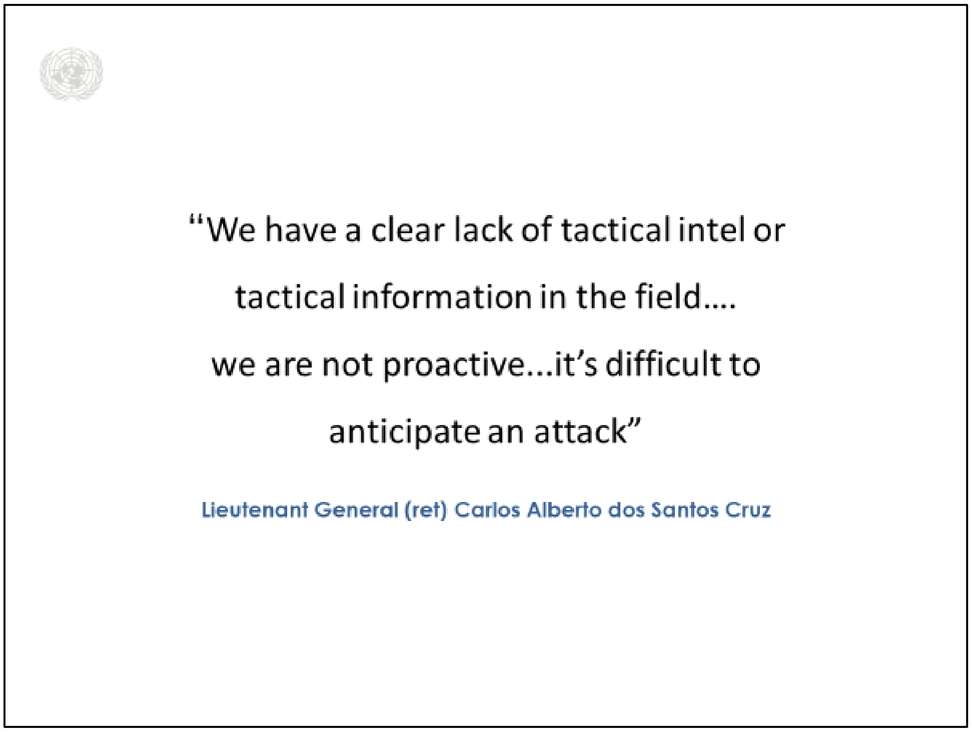
The learning outcomes are presented on this slide, representing the expected achievements by the end of the lesson. The primary objective of this lesson is to provide you with knowledge and familiarity regarding the UN peacekeeping-intelligence conceptual framework and its connection to the Force Protection process. Furthermore, we will introduce the framework of Peacekeeping-Intelligence, Surveillance, and Reconnaissance (PKISR), followed by a discussion on the utilisation of unmanned aerial system (UAS) capabilities as a valuable resource for information collection.

Slide 4

Too Frequent

The frequency of attacks against peacekeepers, UN facilities, and UN operating bases continues to be alarmingly high, leading to a steady rise in fatalities and injuries among peacekeepers. Tragically, over 4000 peacekeepers have sacrificed their lives in the pursuit of peace. In 2022, the number of peacekeepers who lost their lives amounted to 93. Similarly, in 2021, the figure stood at 135, and in 2020, it was 131. These statistics reveal the persistent threat faced by peacekeepers, despite the prioritisation of Force Protection measures and advancements in protective equipment.

Slide 5



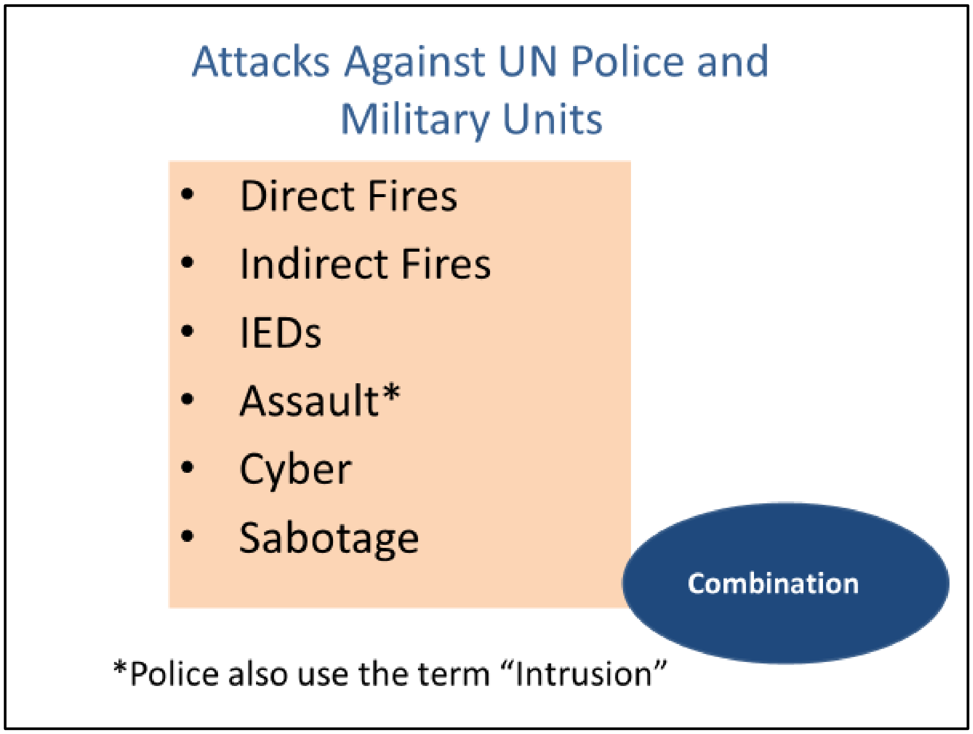
"We have a clear lack of tactical intel or tactical information in the field....
we are not proactive...it's difficult to anticipate an attack"

Lieutenant General (ret) Carlos Alberto dos Santos Cruz

The 2017 report by General Santos Cruz highlights the challenging peacekeeping environment characterised by armed groups, terrorists, organised armed crime gangs, and various threats against UN forces and civilian populations. The report emphasises that the United Nations and Troop/Police Contributing Countries (T/PCCs) often exhibit a "Chapter VI Syndrome," which, unless addressed, puts troops at risk. To avert casualties, peacekeeping missions require tactical peacekeeping-intelligence. However, the report underscores the lack of essential components such as a basic peacekeeping-intelligence system, management, human peacekeeping-intelligence networks, and situational awareness. According to the Cruz Report, peacekeeping-intelligence operations should be conducted as an integrated, crosscutting process for the following reasons:

- To prevent casualties
- To translate information into tasks and actions that enhance security
- Due to the absence of advanced collection platforms, the significance of human peacekeeping intelligence and informant networks increases
- Situational awareness and effective communication with the local population are crucial
- In missions where the Protection of Civilians (POC) is mandated, peacekeeping-intelligence gathering, and analysis play a vital role in predicting and preventing violence against vulnerable populations

Slide 6



Attacks Against UN Police and Military Units

- Direct Fires
- Indirect Fires
- IEDs
- Assault*
- Cyber
- Sabotage

Combination

*Police also use the term "Intrusion"

For this training material we will focus on the threats that focus on attacks against UN units. We do understand that there are many different forms of threats and not always in the form of hostile attacks. In this training material we will focus on these categories of threats to UN units,

- Direct fires
- Indirect fires
- Improvised explosive devises (IED)
- Assaults
- Cyber
- Sabotage

Also, an attack can include a combination of these actions at the same time. Cyber-attacks include misinformation and disinformation offenses against the UN and UN units.

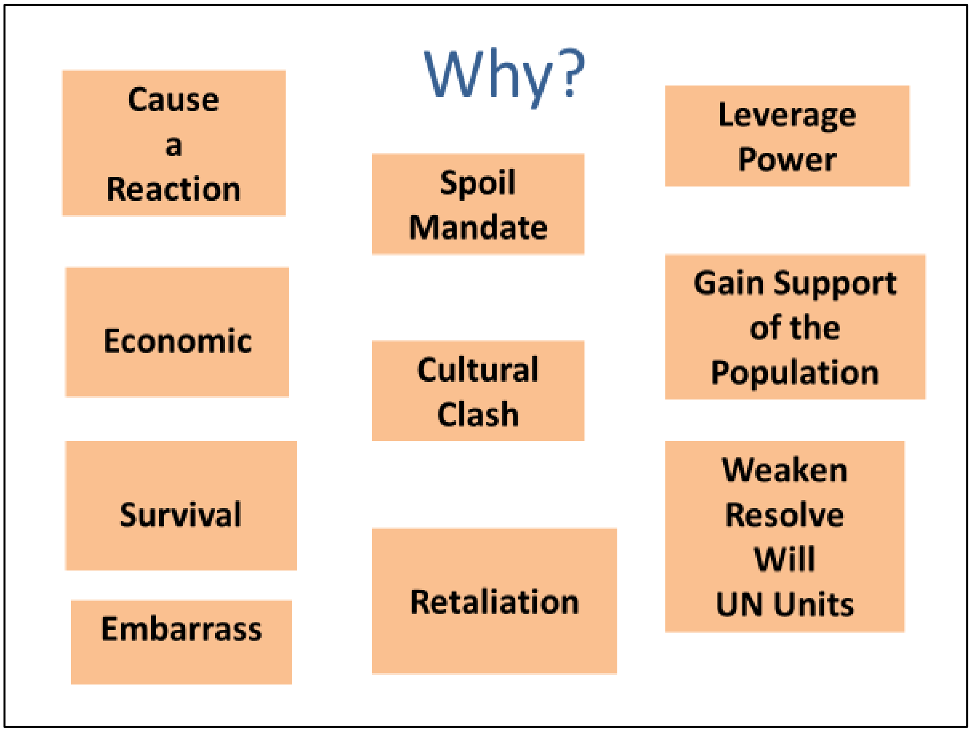
These attacks, conducted by actors targeting UN units during mobile or static operations, could impact the freedom of action that is required to accomplish its mandated tasks.

For the purpose of this training, we will focus on the tactical aspects of attackers that intentionally disrupt temporally or permanently the tactical capability of the affected units to discharge their mandated tasks. Commanders need to identify the potential attackers and how they will attack. Each threat is looked at from a risk analysis point of view and should be prioritised. A plan of action (CoA) is required to mitigate the risks they pose to the unit's operation.

For an interactive engagement:

To foster active participation and enhance comprehension, encourage the participants to share examples of potential motives behind attacks on UN units before advancing to the next slide. Make a note of their responses and subsequently compare them to the reasons outlined on the slide. This approach aims to gauge their understanding and perception regarding what they deem to be legitimate grounds for attacks.

Slide 7



Why?

Cause a Reaction

Spoil Mandate

Leverage Power

Economic

Cultural Clash

Gain Support of the Population

Survival

Weaken Resolve Will UN Units

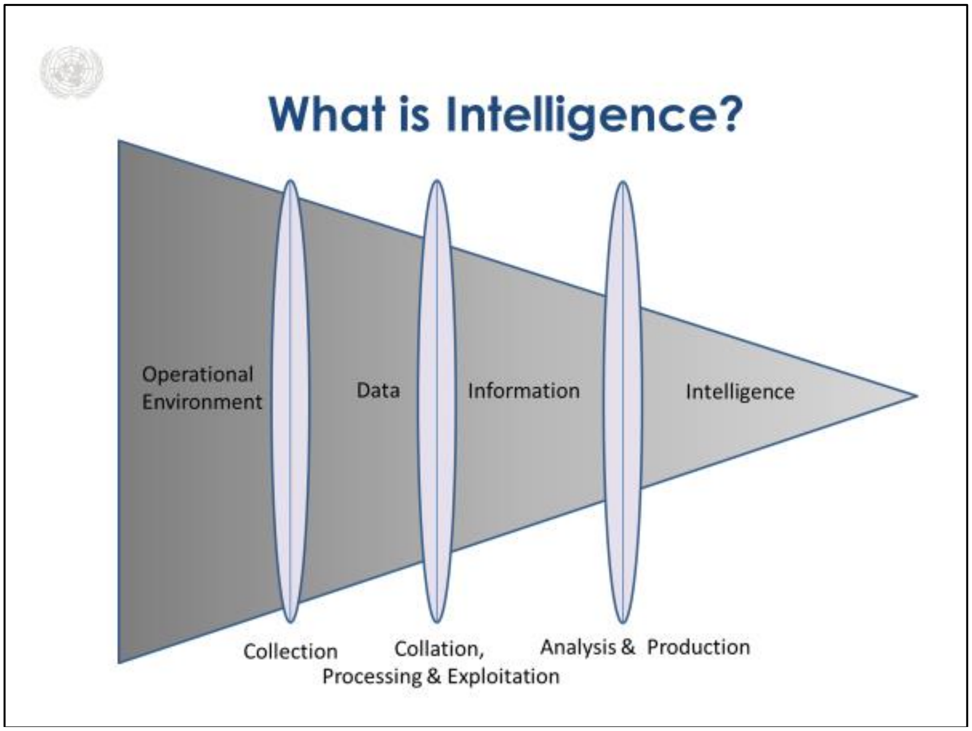
Embarrass

Retaliation

Here are some examples:

- Cause a reaction
- Economic
- Survival
- Embarrass the UN
- Spoil the mandate / UN Mission goals and objectives
- Cultural clash
- Retaliation, revenge, payback
- Leverage, influence for power or prestige / respect
- Gain the support of the population
- Weaken resolve, will, and morale, of UN units

Slide 8



What is Intelligence?

Operational Environment

Data

Information

Intelligence

Collection

Collation, Processing & Exploitation

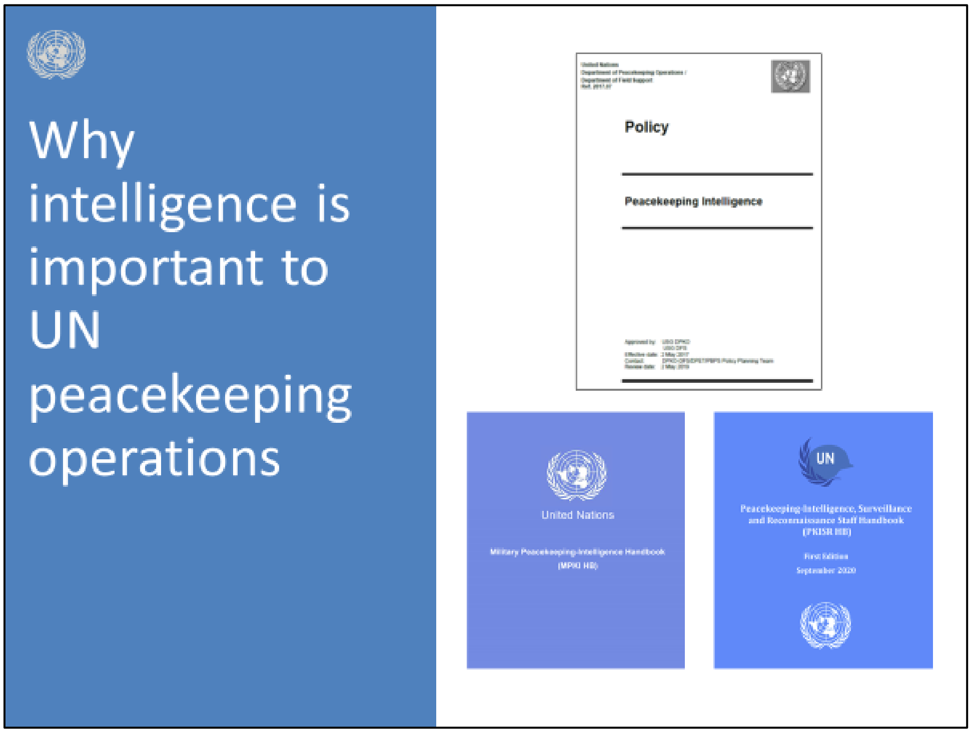
Analysis & Production

Intelligence is crucial in police and military UNPKO as it involves processing and analysing data and information to provide actionable insights for decision-makers. It enables us to discern meaningful information amidst the noise of data and information, aiding in a better understanding of the operational environment. Considering this, peacekeeping-intelligence (knowledge) becomes a key element for the success of any operation, making "Intel driven" approaches vital in UN operations.

Intelligence employs collection and analysis techniques to offer guidance and direction to commanders, enabling them to make effective decisions regarding resource deployment. The analysis processes serve as tools to help manage vast amounts of data, including both basic and current peacekeeping-intelligence, as well as raw incoming data.

Incorporating predictive analysis is essential for commanders utilising peacekeeping-intelligence. Predictive peacekeeping-intelligence not only assesses the capabilities of threats and other actors but also determines their intentions and likely courses of action. This information significantly contributes to the FP planning process.

Slide 9



Why intelligence is important to UN peacekeeping operations

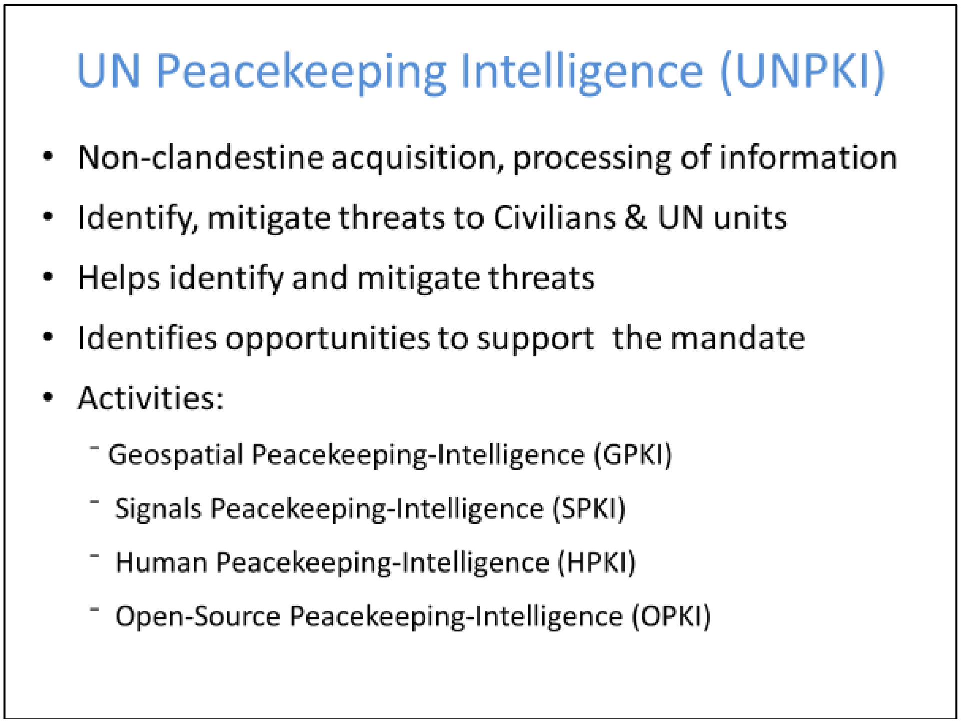
Policy
Peacekeeping Intelligence
United Nations
Military Peacekeeping-Intelligence Handbook
(MPKI HB)
UN
Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook
(PKISR HB)
First Edition
September 2020

This lesson draws upon the UN Department of Peacekeeping Operations, Peacekeeping Intelligence Policy, the United Nations Military Peacekeeping-Intelligence Handbook (May 2019) and the Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (Sep 2020).

The UN's transition from information to peacekeeping-intelligence reflects its recognition of evolving mandates and the operating environments within United Nations peacekeeping missions. With UN missions encountering complex, high-tempo, and lethal environments, the presence of diverse threats significantly affects both peacekeepers and civilian populations, jeopardising the successful implementation of mandates.

In such demanding circumstances, it becomes paramount for peacekeeping missions to bolster their comprehension of the operational environment. This entails maintaining a strategic and tactical view of unfolding developments and acquiring insights into the potential capabilities of threats and spoilers that may impede the efficient execution of peacekeepers' mandates.

Slide 10



UN Peacekeeping Intelligence (UNPKI)

- Non-clandestine acquisition, processing of information
- Identify, mitigate threats to Civilians & UN units
- Helps identify and mitigate threats
- Identifies opportunities to support the mandate
- Activities:
  - Geospatial Peacekeeping-Intelligence (GPKI)
  - Signals Peacekeeping-Intelligence (SPKI)
  - Human Peacekeeping-Intelligence (HPKI)
  - Open-Source Peacekeeping-Intelligence (OPKI)

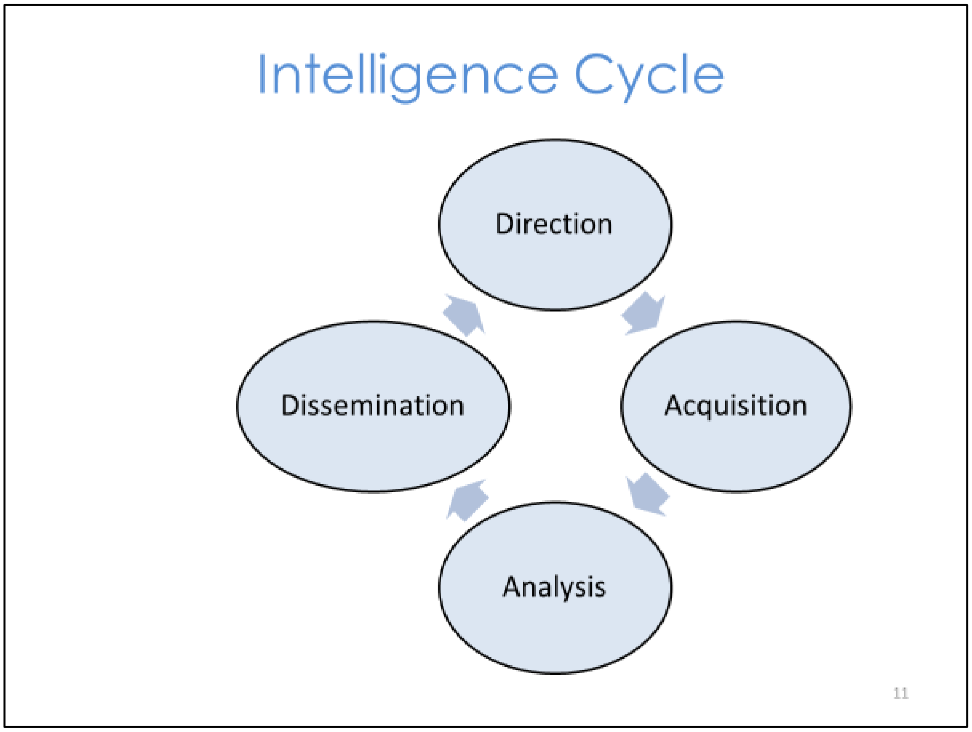
Military Peacekeeping Intelligence refers to the acquisition and processing of information by a mission within a directed peacekeeping-intelligence cycle, conducted openly and in accordance with legal frameworks. Its purpose is to fulfil decision-making requirements and support operations related to the safe and effective implementation of the Security Council mandate. This peacekeeping-intelligence framework facilitates threat and risk analysis, aiding the commander in developing Protection of Civilians and Force Protection plans.

Different types of Peacekeeping Intelligence activities include:

- Geospatial Peacekeeping Intelligence (GPKI): This involves analysing geographic imagery and geospatial data to gain valuable insights
- Signals Peacekeeping Intelligence (SPKI): This is in the developmental stage, and its scope must be determined in collaboration with the host nation's judicial system, defining the boundaries of permissible actions
- Human Peacekeeping Intelligence (HPKI): Human collection in peacekeeping operations must be conducted openly, with utmost consideration for the safety of the sources and their families. Proper management is essential
- Open-Source Peacekeeping Intelligence (OPKI): This involves the evaluation of a substantial volume of data obtained from open sources to determine its relevance and usefulness

Overall, these forms of Peacekeeping Intelligence contribute to informed decision-making and support the successful execution of peacekeeping missions.

Slide 11



Intelligence Cycle

Direction

Acquisition

Analysis

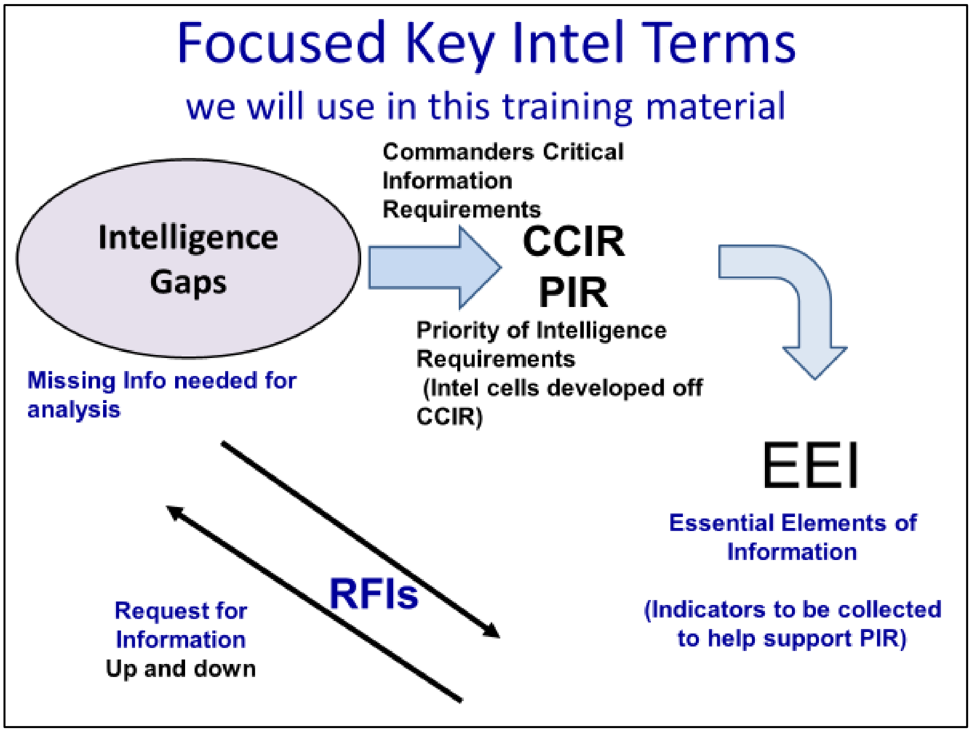
Dissemination

11

Presented here is the peacekeeping-intelligence cycle, which is commonly depicted as a continuous, systematic process encompassing several key activities: direction, acquisition, analysis, and dissemination.

- Direction: This step involves identifying the questions that need to be answered to guide peacekeeping-intelligence activities. Direction ensures that the leadership's information needs are addressed and helps focus the efforts of units and assets accordingly
- Acquisition: Once the requirements are determined and priorities are assigned, the next stage is acquiring the necessary data or information to support the analytical phase of the cycle. It is crucial to gather data and information from diverse sources and capabilities. Effective acquisition depends on clear requirements, ensuring that allocated resources are utilised in the most efficient manner
- Analysis: In this phase, the collected data and information are transformed into peacekeeping-intelligence. This is achieved by breaking down the information into its components and conducting a comprehensive analytical examination to uncover interrelationships, while also assessing reliability and credibility
- Dissemination: This step involves packaging and presenting peacekeeping-intelligence products to decision-makers and concerned personnel. It is the process of distributing the peacekeeping-intelligence in a format that is easily understandable and actionable. peacekeeping-intelligence that is not disseminated in a timely manner loses its value and utility

Slide 12



Focused Key Intel Terms

we will use in this training material

Intelligence Gaps

Missing Info needed for analysis

Commanders Critical Information Requirements

CCIR

PIR

Priority of Intelligence Requirements
 (Intel cells developed off CCIR)

EEI

Essential Elements of Information

(Indicators to be collected to help support PIR)

RFIs

Request for Information
Up and down

This slide is dedicated to introducing essential peacekeeping-intelligence terms and abbreviations that assist in prioritising the information requirements of mission leadership during the direction phase of the peacekeeping-intelligence cycle. While the MPKI handbook encompasses numerous terms utilised by peacekeeping-intelligence communities and cells, this training material will primarily focus on the commonly used terms by most TCCs/PCCs throughout the presentation and the training packet.

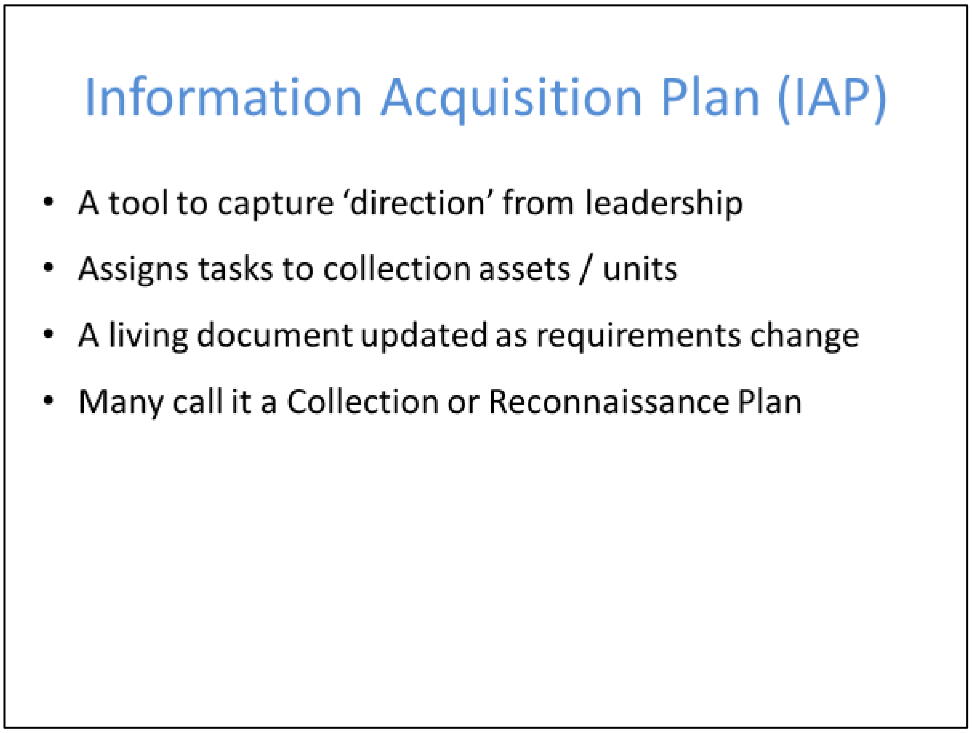
- Commander's Critical Information Requirements (CCIRs) are the paramount requirements established by the leadership. They encompass any information that the leadership deems crucial for the mission's success or signifies a threat to the mandate implementation. CCIRs should be defined during mission analysis and subsequently reviewed and modified throughout the decision-making process

- Effective coordination relies on aligning the acquisition of information with established priorities. Priority PK-Intelligence Requirements (PIRs) should primarily stem from the CCIRs but can also be derived from other sources. Well-written and focused PIRs serve as the foundation for acquisition and collection planning, guiding the tasking of assets. PIRs are likely to constitute a significant component of the Information Acquisition Plan (IAP).

- The Essential Elements of Information (EEIs) are crucial in breaking down Priority Peacekeeping Intelligence Requirements (PIRs) into specific, targeted questions that can be assigned to dedicated acquisition assets. These EEIs provide the necessary details to inform the development of the Information Acquisition Plan (IAP). When answered, EEIs should provide analysts with sufficient information to deliver comprehensive and satisfactory responses to each requirement. They are closely related to the PIRs, establishing a seamless connection that facilitates effective information gathering and analysis. In a scenario where the mission faces security threats, an EEI could be the identification of an armed group's weapon capabilities. For POC operations, an EEI might involve gathering information on the number and location of displaced persons, and where they go for access to get water

- The Request for Information (RFI) process enables any individual or entity within the Mission to pose a question that requires a response from Peacekeeping Intelligence, Surveillance, and Reconnaissance (PKISR) capabilities. To ensure efficient tasking of PKISR resources, the Force relies on a well-established process that allows all civilian and uniformed components of the Mission to submit RFIs. These RFIs can be prioritised against the Essential Elements of Information (EEIs), ensuring effective utilisation of PKISR assets

Slide 13



Information Acquisition Plan (IAP)

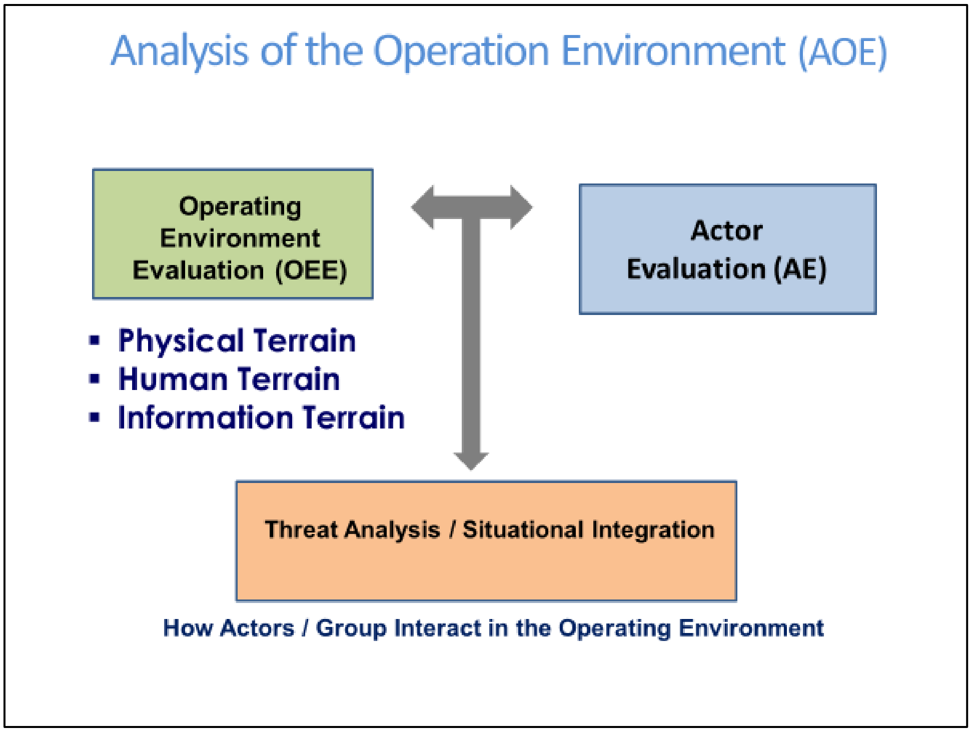
- A tool to capture ‘direction’ from leadership
- Assigns tasks to collection assets / units
- A living document updated as requirements change
- Many call it a Collection or Reconnaissance Plan

The Information Acquisition Plan (IAP) serves as a comprehensive tool that captures peacekeeping-intelligence requirements, outlining the questions that need to be answered utilising Peacekeeping Intelligence, Surveillance, and Reconnaissance (PKISR) assets. It is worth noting that some TCCs/PCCs also refer to the IAP as a collection plan.

The IAP is a dynamic and living document that necessitates regular review to ensure that all questions have been adequately addressed and that new requirements are incorporated into the plan. This plan serves as the foundation for consolidating peacekeeping-intelligence requirements, establishing priorities, and tasking collection assets, ensuring that the appropriate sensors / units are deployed to gather information in response to specific questions.

Within the mission, multiple IAPs may exist at different levels, aligning with the assets and inquiries pertinent to each level. The IAP forms the basis for executive orders, directing tasks and guiding acquisition assets in obtaining information that fulfils the requirements. The IAP should emphasise and concentrate on peacekeeping-intelligence or information gaps, enabling a focused approach to address critical knowledge shortfalls.

Slide 14


Analysis of the Operation Environment (AOE)
Operating Environment Evaluation (OEE)
Physical Terrain
Human Terrain
Information Terrain
Actor Evaluation (AE)
Threat Analysis / Situational Integration
How Actors / Group Interact in the Operating Environment

In a UNPKO, peacekeeping-intelligence serves as a critical pillar for mission success and risk mitigation. One key element of peacekeeping-intelligence is the Analysis of the Operational Environment (AOE), which involves a comprehensive assessment of various factors within a specific operational area. The importance of AOE and its subcategories, including Operating Environment Evaluation (OEE) and Actor Evaluation, to provide a holistic understanding of the operational environment is key to a successful mission analysis.

Operating Environment Evaluation (OEE):

The OEE is a crucial subcategory of AOE that encompasses a multidimensional assessment of the operational environment. It involves three key subcategories: Physical Terrain Assessment, Human Terrain Assessment, and Information Terrain Assessment.

Physical Terrain Assessment: This subcategory focuses on analysing the geographical features, natural obstacles, and infrastructure within the operational area. By understanding the physical terrain, such as mountains, rivers, urban areas, and road networks, peacekeeping-intelligence analysts can identify potential advantages, disadvantages, and logistical challenges for operations.

Human Terrain Assessment: Human Terrain Assessment involves studying the social, cultural, and political aspects of the operational environment. This includes evaluating the local population, their beliefs, customs, and socio-political dynamics. By assessing the human terrain, peacekeeping-intelligence analysts can gain insights into the local population's support, potential conflicts, and factors that may influence the mission's success.

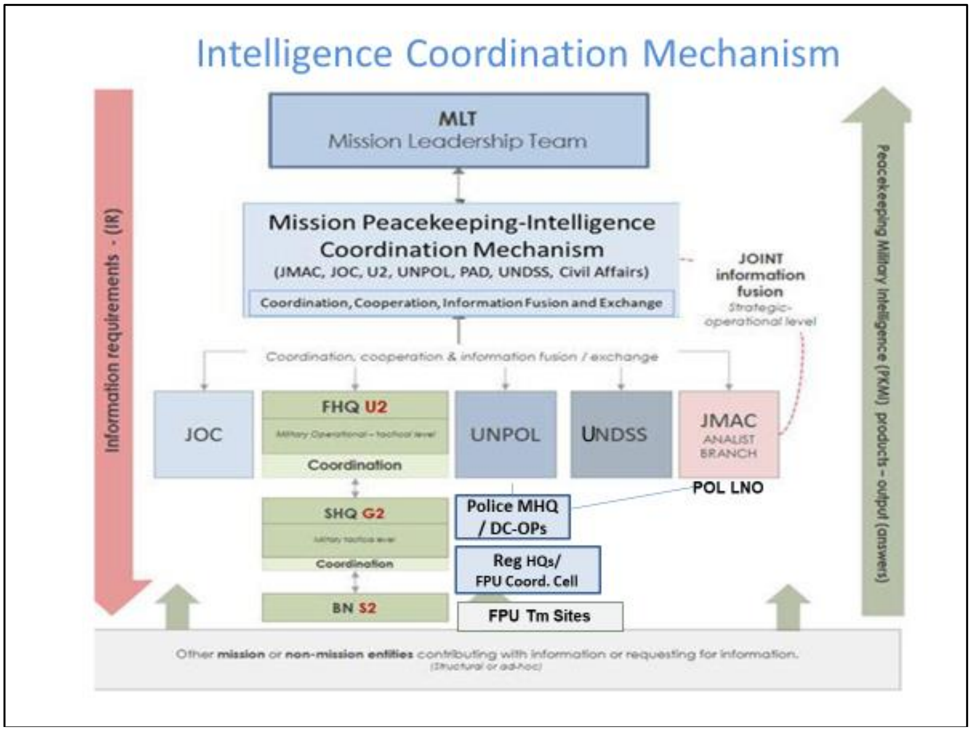
Information Terrain Assessment: In the digital age, the Information Terrain Assessment has become increasingly vital. It focuses on understanding the information environment, including communication networks, media channels, and online platforms. PK-Intelligence analysts assess the flow of information, propaganda, and disinformation campaigns that can impact the operational environment and influence public sentiment.

Actor Evaluation:

Another crucial aspect of AOE is Actor Evaluation, which involves assessing the various actors operating within the operational environment. This includes UN and host nation units and forces, potential attackers, non-state actors, and other influential entities. Analysts examine their capabilities, intentions, relationships, and potential threats they pose to the mission's objectives. By evaluating actors, peacekeeping-intelligence supports decision-makers in understanding the complex web of alliances, conflicts, and potential collaborations.

The Analysis of the Operational Environment (AOE) is an essential component of peacekeeping-intelligence in UNPKOs. By conducting a comprehensive assessment of the operational environment, including the subcategories of Operating Environment Evaluation (OEE) and Actor Evaluation, peacekeeping-intelligence analysts provide decision-makers with a holistic understanding of the challenges, opportunities, and potential risks. This knowledge enables informed decision-making, effective strategy development, and proactive measures to ensure the success and safety of military operations. Emphasising the AOE within peacekeeping-intelligence practises enhances situational awareness and strengthens the operational capabilities of UN units.

Slide 15



Intelligence Coordination Mechanism

MLT
Mission Leadership Team

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

JOINT information fusion
Strategic-operational level

Coordination, cooperation & information fusion / exchange

JOC

FHQ U2
Military Operational – tactical level
Coordination

UNPOL

UNDSS

JMAC
ANALIST BRANCH

POL LNO

SHQ G2
Military tactical level
Coordination

BN S2

Police MHQ / DC-OPs

Reg HQs/ FPU Coord. Cell

FPU Tm Sites

Information requirements - (IR)

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

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

Let's delve into the coordination mechanism that supports a robust UN peacekeeping-intelligence system. The peacekeeping-intelligence Coordination Mechanism (ICM) plays a crucial role in establishing an inclusive framework for information and peacekeeping-intelligence sharing. It effectively coordinates the mission-wide Peacekeeping Intelligence (PKI) function. The slide highlights the actors and components involved in this mechanism, showcasing the various peacekeeping-intelligence entities within a UN Peacekeeping Mission, each with their specific roles and responsibilities.

Establishing this mechanism is imperative to exercise centralized control over peacekeeping-intelligence activities, ensuring unity in peacekeeping-intelligence efforts throughout the mission. While the components, organisations, staff, and cells of a UN Mission individually contribute as good providers of operational peacekeeping-intelligence, their collaboration culminates in an effective operational peacekeeping-intelligence system. This cooperation is achieved through the Mission PK-Intelligence Coordination Structure (MICS), which may vary in its specific nature across missions but shares fundamental principles, including:

- Entities responsible for acquisition, analysis, and dissemination, such as the Joint Mission Analysis Centre (JMAC), Joint Operations Centre (JOC), United Nations Department of Safety and Security (UNDSS), Mission Support Component (MSC), mission components, and U2 staff, police component having a liaison office in the JMAC, along with peacekeeping-intelligence cells at regional headquarters

- Centralized control to enable decentralized execution
- Direction and coordination of the mission's peacekeeping-intelligence system
- The possibility of the JMAC acting as the primary coordinating body within the MICS
- Police and military components maintaining lines of coordination and support
- The military component incorporates peacekeeping-intelligence cells at Force and sector headquarters, as well as at the unit level
- The police component has a liaison office in the JMAC, along with peacekeeping-intelligence cells at regional headquarters, the Formed Police Unit (FPU) Coordination Cell, and Team FPU Sites
- As per the Policy and Guidelines for OPS/C2, peacekeeping-intelligence reports are processed and disseminated by the police, including Individual Police Officers (IPOs) and FPUs
- The MICS should have a civilian chair, with the Chief JMAC assuming this role when the JMAC functions as the coordinating body
- It draws strategic guidance from senior mission leadership and translates this guidance into peacekeeping-intelligence requirements
- It manages the Mission PK-Intelligence Acquisition Plan and the acquisition efforts to fulfil the peacekeeping-intelligence requirements
- It develops and maintains the mission's peacekeeping-intelligence Support Plan (ISP)
- By implementing the ICM and adhering to the principles of the MICS, the UN can establish a robust peacekeeping-intelligence system that effectively supports peacekeeping missions

For Interaction. *During the interaction, let's ask the students about how the MICM coordinates mission PKI entities. Some possible responses to consider are:*

- *The Mission-level Information Acquisition Plan (IAP): The MICM establishes an IAP that assigns each entity the responsibility of acquiring information for one or several Head of Mission Priority peacekeeping-intelligence Requirements (PIRs), as shown on the earlier slide. This ensures a systematic and coordinated approach to gathering relevant information.*

- *Regular Meetings and Information Sharing: The MICM facilitates regular meetings among all PKI entities, fostering an environment of collaboration and knowledge exchange. These meetings serve as platforms for sharing information and insights. For instance, the JMAC's acquisition of political information can enhance both military and police peacekeeping-*

intelligence cells' situational awareness and understanding, demonstrating the interconnectedness of peacekeeping-intelligence efforts.

Encourage the students to provide their personal perspectives on how the MICM coordinates mission PKI entities, emphasising the importance of information acquisition plans and the sharing of information among different peacekeeping-intelligence components.

☞ ***Note to Instructor****: The Chief of the JMAC will normally be a civilian, assisted by a specified number of information analysts and collection officers (civilian and military). Since most mission information gathering is either coordinated through, or processed by the JMAC, it is important to understand the structure and staffing of a generic JMAC. Ideally, all JMACs will have a separated analysis section from collection and data management.*

Missions without an established JMAC, have a requirement to conduct integrated analysis. This could be done through strategic meetings and individual components are tasked with drafting assessments.

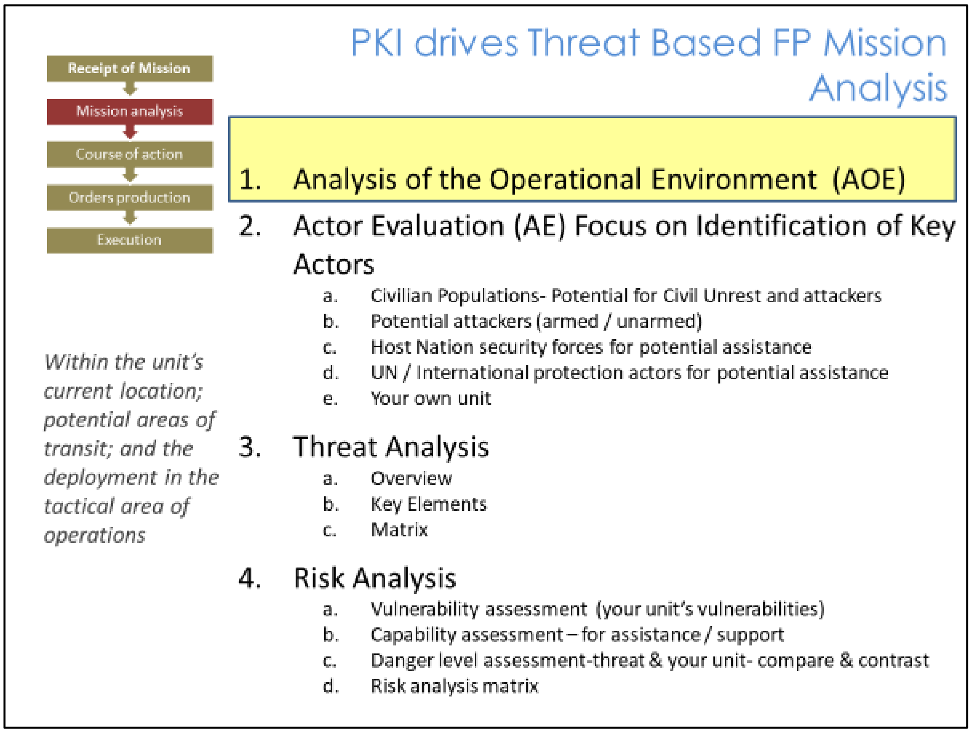
Slide 16

A Threat-based Approach- Intelligence drives the FP Mission Analysis

17

In the upcoming section of the lesson, we will delve deeper into the concept of a threat-based approach for FP mission analysis. This framework will serve as a valuable tool throughout module 3 lessons and the capstone tabletop exercise.

Slide 17



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

PKI drives Threat Based FP Mission Analysis

1. Analysis of the Operational Environment (AOE)
2. Actor Evaluation (AE) Focus on Identification of Key Actors
   a. Civilian Populations- Potential for Civil Unrest and attackers
   b. Potential attackers (armed / unarmed)
   c. Host Nation security forces for potential assistance
   d. UN / International protection actors for potential assistance
   e. Your own unit
3. Threat Analysis
   a. Overview
   b. Key Elements
   c. Matrix
4. Risk Analysis
   a. Vulnerability assessment (your unit's vulnerabilities)
   b. Capability assessment – for assistance / support
   c. Danger level assessment-threat & your unit- compare & contrast
   d. Risk analysis matrix

Within the unit's current location; potential areas of transit; and the deployment in the tactical area of operations

The FP planning process and the peacekeeping-intelligence cycle work in parallel, emphasising the significance of developing and refining the Analysis of the Operational Environment (AOE) in FP mission analysis. This is crucial to ensure effective FP planning. A seamless access to current, relevant, accurate, and comprehensive Peacekeeping-Intelligence from diverse sources is essential. This access involves analysing the physical terrain, human terrain, and information terrain, while also integrating them together.

During the phase of mission analysis, it becomes imperative to place a high priority on comprehending the human terrain and identifying key actors. By doing so, valuable insights into the social, cultural, and political dynamics at play can be gained. These insights enable more informed decision-making and strategic planning.

The FP planning process and the intel cycle complement each other, working concurrently to enhance mission analysis in the context of Force Protection. The Analysis of the Operational Environment (AOE) is a vital component of FP mission analysis, requiring continuous development and refinement.

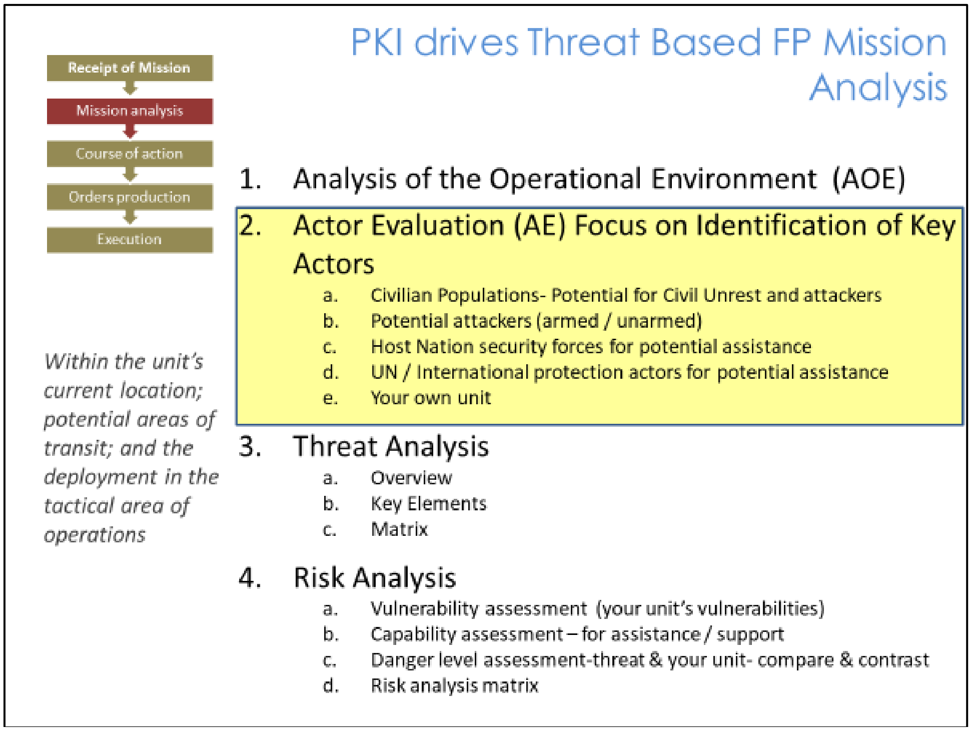
To ensure effective FP planning, it is necessary to have seamless access to a wide range of current and relevant Peacekeeping-Intelligence. This peacekeeping-intelligence should be accurate, comprehensive, and obtained from diverse sources. The information gathered must encompass various aspects, including the physical terrain, human terrain, and the information terrain.

Integrating these different sources of information is crucial to forming a comprehensive understanding of the operational environment. By analysing the physical terrain, we can assess factors such as geographical features, infrastructure, and potential threats. Understanding the human terrain involves studying the social, cultural, and political dynamics of the area, including the behaviour and motivations of key actors.

By placing a high priority on comprehending the human terrain and identifying key actors, FP planners can gain valuable insights into the complex dynamics at play. These insights enable them to make more informed decisions and develop strategic plans that consider the unique aspects of the operational environment.

In summary, the FP planning process, and the intel cycle work in parallel, with the Analysis of the Operational Environment (AOE) playing a central role in FP mission analysis. To ensure effective planning, access to current and comprehensive Peacekeeping-Intelligence is essential. This involves analysing the physical terrain, human terrain, and the information terrain, as well as integrating them together. By prioritizing the understanding of the human terrain and identifying key actors, FP planners can make more informed decisions and develop strategic plans that consider the social, cultural, and political dynamics at play.

Slide 18



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

PKI drives Threat Based FP Mission Analysis

Within the unit's current location; potential areas of transit; and the deployment in the tactical area of operations

1. Analysis of the Operational Environment (AOE)
2. Actor Evaluation (AE) Focus on Identification of Key Actors
   a. Civilian Populations- Potential for Civil Unrest and attackers
   b. Potential attackers (armed / unarmed)
   c. Host Nation security forces for potential assistance
   d. UN / International protection actors for potential assistance
   e. Your own unit
3. Threat Analysis
   a. Overview
   b. Key Elements
   c. Matrix
4. Risk Analysis
   a. Vulnerability assessment (your unit's vulnerabilities)
   b. Capability assessment – for assistance / support
   c. Danger level assessment-threat & your unit- compare & contrast
   d. Risk analysis matrix

Actor Evaluation (AE) is a critical and indispensable aspect of understanding the human terrain, particularly in relation to actors who are anticipated to exert significant influence on UN units. This evaluation entails employing a range of techniques to gather insights into various aspects of these actors, including their strengths, weaknesses, opportunities, potential attackers, groups that may offer support to the UN, positions, interests, capabilities, background, history, and relationships with the UN.

Thoroughly examining and assessing all relevant actors in the operational areas is of paramount importance in FP planning. By conducting comprehensive evaluations, we can develop a more profound understanding of the intricate social, political, and cultural dynamics at play. This understanding, in turn, enables us to make well-informed decisions and effectively engage with key stakeholders.

During the AE process, it is crucial to identify and evaluate the potential attackers and threats that may emerge from different actors in the operational environment. This involves assessing their motivations, intentions, and capabilities, as well as understanding the networks and relationships they have established. By delving into these aspects, we can anticipate and mitigate potential risks to UN units and develop appropriate strategies to address them.

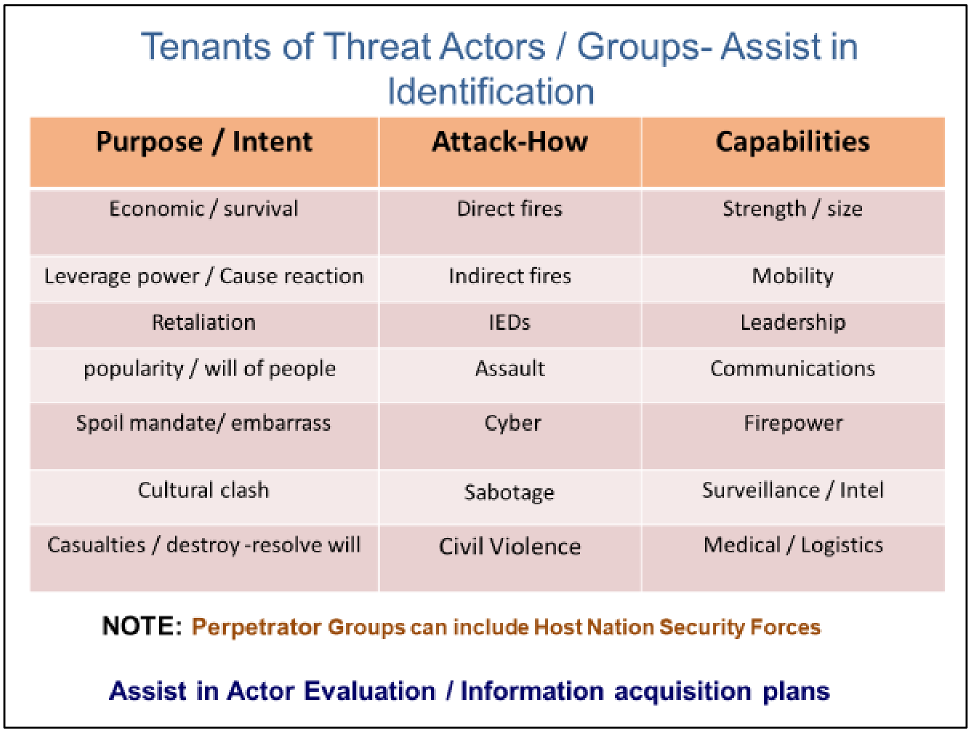
In addition, AE helps identify actors who may be supportive of the UN's mission and objectives. Understanding their positions, interests, and capabilities allows us to leverage these positive relationships and seek their assistance in achieving FP goals. Engaging with these actors can enhance cooperation, facilitate information sharing, and contribute to a safer operational environment.

Furthermore, AE contributes to the broader peacekeeping-intelligence picture by providing valuable insights into the complex web of relationships among various actors. This understanding is crucial for assessing potential alliances, rivalries, or conflicts among actors, which can have significant implications for FP planning. By recognising these dynamics, we can better anticipate the behaviour and actions of different actors and adjust our strategies accordingly.

To conduct effective AE, a variety of methods and sources should be utilised. This includes gathering information from open sources, such as media reports and public records, as well as using peacekeeping-intelligence sources, both human and technical. Collaborating with other UN agencies, partner organisations, and local stakeholders can also provide valuable insights and perspectives on the actors in the operational environment.

In conclusion, Actor Evaluation (AE) plays a pivotal role in understanding the human terrain and its impact on FP planning. By comprehensively assessing relevant actors, we gain a deeper understanding of their strengths, weaknesses, motivations, and relationships, enabling us to make informed decisions and engage with key stakeholders effectively. AE also assists in identifying potential attackers and threats while leveraging relationships with supportive actors. Through a thorough evaluation of actors, FP planners can enhance their understanding of the operational environment, contribute to the peacekeeping-intelligence picture, and develop strategies that mitigate risks and promote successful FP missions.

Slide 19



Tenants of Threat Actors / Groups- Assist in Identification

Purpose / Intent	Attack-How	Capabilities
Economic / survival	Direct fires	Strength / size
Leverage power / Cause reaction	Indirect fires	Mobility
Retaliation	IEDs	Leadership
popularity / will of people	Assault	Communications
Spoil mandate/ embarrass	Cyber	Firepower
Cultural clash	Sabotage	Surveillance / Intel
Casualties / destroy -resolve will	Civil Violence	Medical / Logistics

NOTE: **Perpetrator Groups can include Host Nation Security Forces**

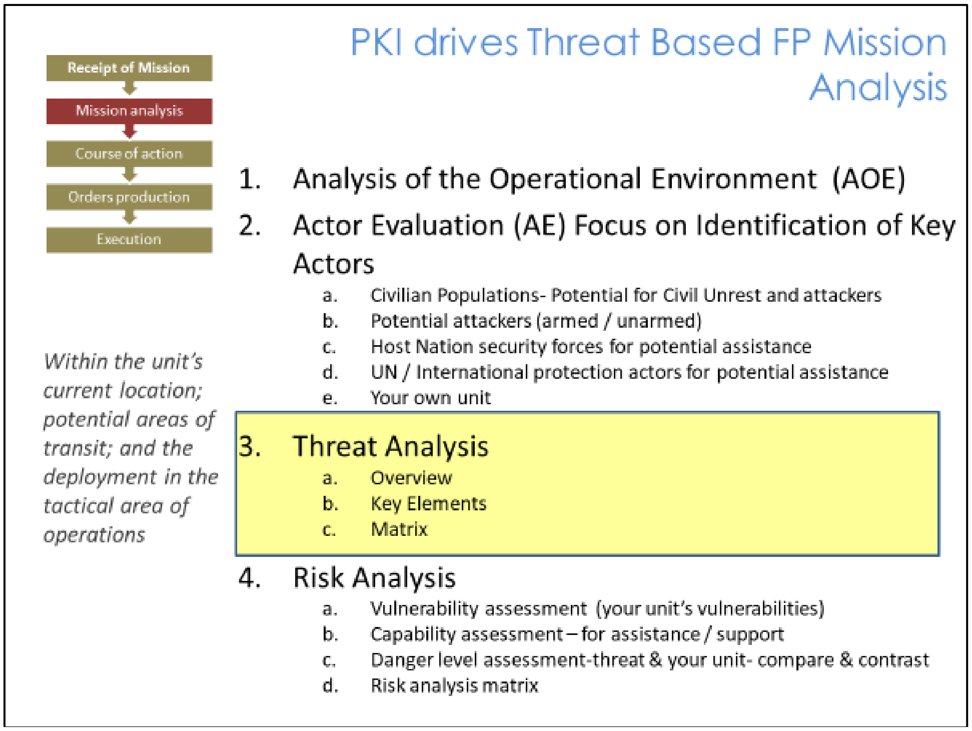
Assist in Actor Evaluation / Information acquisition plans

This chart serves as a valuable tool for understanding and identifying potential perpetrators of violence. It exemplifies an end, ways, and means framework, which proves beneficial in developing a comprehensive collection plan and establishing relevant indicators for input into the IAP.

By utilising this framework, we can systematically analyse the motives (ends), methods (ways), and resources (means) employed by potential attackers. This enables us to gather pertinent information and identification of potential attackers and their means / methods of attack.

The chart aids in organising and visualising the connections between various elements, allowing for a more holistic understanding of the dynamics at play. It provides a structured approach to identifying key actors, their motivations, tactics, and available resources, thereby contributing to enhanced situational awareness and informed decision-making.

Slide 20



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

PKI drives Threat Based FP Mission Analysis

1. Analysis of the Operational Environment (AOE)
2. Actor Evaluation (AE) Focus on Identification of Key Actors
   a. Civilian Populations- Potential for Civil Unrest and attackers
   b. Potential attackers (armed / unarmed)
   c. Host Nation security forces for potential assistance
   d. UN / International protection actors for potential assistance
   e. Your own unit
3. Threat Analysis
   a. Overview
   b. Key Elements
   c. Matrix
4. Risk Analysis
   a. Vulnerability assessment (your unit's vulnerabilities)
   b. Capability assessment – for assistance / support
   c. Danger level assessment-threat & your unit- compare & contrast
   d. Risk analysis matrix

Within the unit's current location; potential areas of transit; and the deployment in the tactical area of operations

A threat analysis is a crucial process that involves peacekeeping-intelligence-driven evaluation of potential threats within designated operational areas. It serves as a fundamental step in identifying and analysing threats, building upon the risk analysis process.

To effectively implement necessary protective measures while maximizing operational efficiency, continuous evaluation of the threat landscape is indispensable. This evaluation entails integrating information from diverse sources to ensure an accurate and up-to-date understanding of the evolving threat environment.

Threat analyses play a critical role in determining potential targets, identifying potential attackers, assessing their capabilities, and predicting the likely courses of action (CoA) they may undertake. It is essential to conduct threat analyses / assessments at all levels within the unit to ensure a comprehensive understanding of the threat environment and inform decision-making.

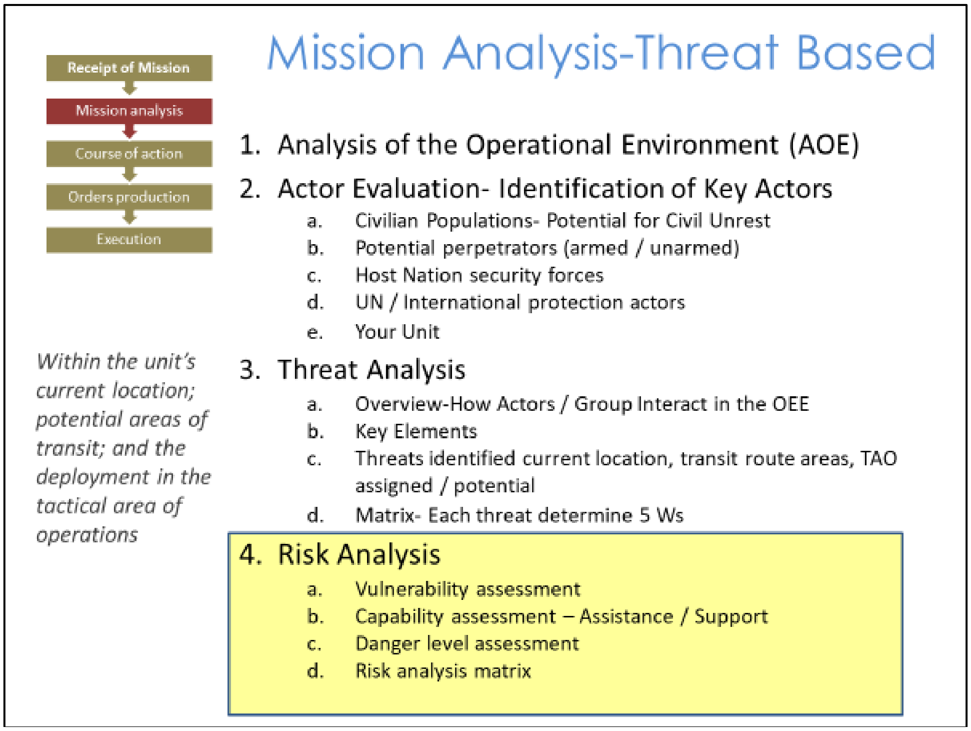
The highlighted areas, marked in yellow, serve as the foundation for our analysis and provide valuable insights for decision-making. By focusing on these areas, we can identify key factors and gather pertinent information that aid in understanding the threat landscape more effectively.

By conducting thorough threat assessments and analyses commanders and decision-makers are equipped with the necessary knowledge to implement appropriate protective measures and develop strategies to mitigate potential threats. These assessments enable proactive planning, resource allocation, and the implementation of countermeasures to safeguard personnel, assets, and mission objectives.

It is important to emphasise that threat analyses are not static but should be continuously updated and refined as new information becomes available. This ensures that the threat peacekeeping-intelligence remains relevant and responsive to the evolving nature of threats within the operational areas.

In conclusion, threat analyses are peacekeeping-intelligence-driven evaluations that form the foundation for identifying and analysing potential threats in designated operational areas. Continuous evaluation, integration of diverse information sources, and comprehensive assessments at all levels are vital for a thorough understanding of the threat landscape. By conducting effective threat analyses, decision-makers can make informed decisions, allocate resources effectively, and implement protective measures to mitigate risks and safeguard mission success.

Slide 21



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Mission Analysis-Threat Based

1. Analysis of the Operational Environment (AOE)
2. Actor Evaluation- Identification of Key Actors
   a. Civilian Populations- Potential for Civil Unrest
   b. Potential perpetrators (armed / unarmed)
   c. Host Nation security forces
   d. UN / International protection actors
   e. Your Unit
3. Threat Analysis
   a. Overview-How Actors / Group Interact in the OEE
   b. Key Elements
   c. Threats identified current location, transit route areas, TAO assigned / potential
   d. Matrix- Each threat determine 5 Ws
4. Risk Analysis
   a. Vulnerability assessment
   b. Capability assessment – Assistance / Support
   c. Danger level assessment
   d. Risk analysis matrix

Within the unit's current location; potential areas of transit; and the deployment in the tactical area of operations

The threat analysis plays a pivotal role in conducting a comprehensive risk analysis, contributing to the identification of measures aimed at reducing risk and mitigating the potential consequences or likelihood of an attack or event.

Commanders, at all levels, must prioritise threats to determine situations where force protection actions or risk mitigation efforts are most crucial. This prioritisation process is facilitated through a thorough risk assessment, which evaluates two key factors:

- Likelihood: This factor assesses the probability of a threat materializing. By analysing the likelihood of each identified threat, commanders and staff can gauge its potential occurrence
- Impact: This factor considers the potential consequences if the threat were to materialise. Understanding the potential impact enables commanders to assess the severity and ramifications associated with each threat

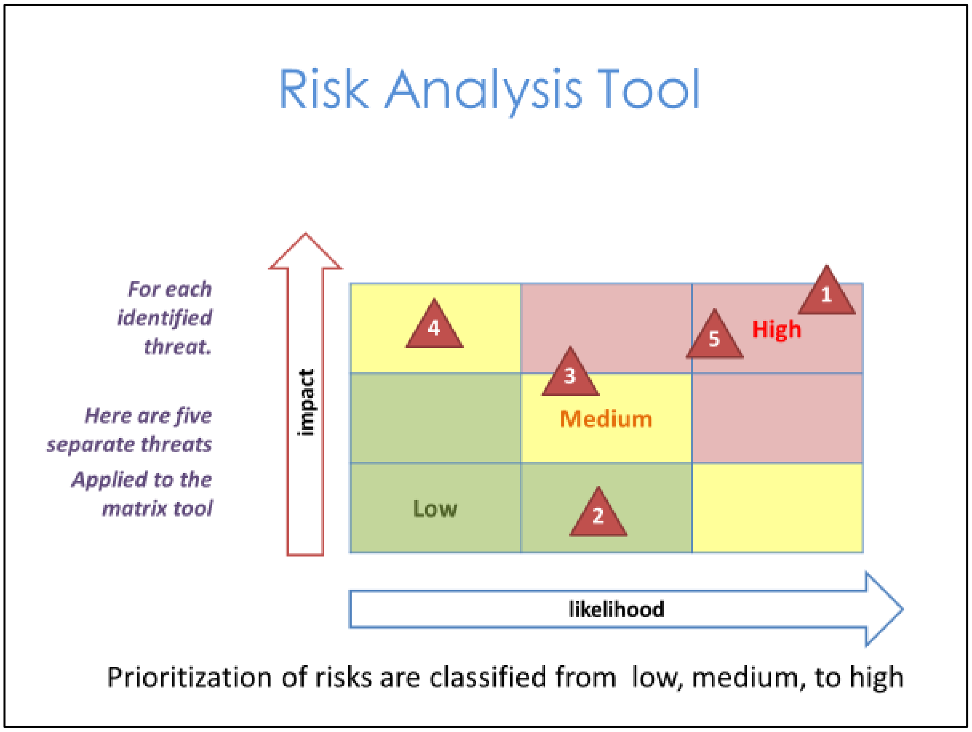
By considering the combination of likelihood and impact, commanders and staff can determine the level of risk associated with each identified threat. This risk assessment provides valuable insights for decision-making and resource allocation.

Risk mitigation principles recognise that while risk cannot be entirely eliminated, taking proactive steps to enhance protection measures against known or potential threats can significantly reduce their likelihood or impact. It is essential to adopt a proactive approach to risks, focusing on preventive measures and preparedness to minimise the vulnerability of the unit.

To effectively conduct FP risk analysis, reliable information and appropriate resources are indispensable for collecting, processing, and disseminating valuable peacekeeping-intelligence. The mission must prioritise the acquisition of accurate and timely information through various peacekeeping-intelligence channels. Human peacekeeping-intelligence remains a vital component in developing mission-wide collection plans and informing the analytical methods employed by analysts. Leveraging human peacekeeping-intelligence sources enhances the depth and accuracy of the overall threat analysis process.

In summary, the threat analysis is instrumental in conducting a comprehensive risk assessment within the unit. Prioritizing threats and conducting a thorough evaluation of likelihood and impact helps commanders identify areas where force protection actions and risk mitigation efforts are most needed. By adopting proactive risk management principles and leveraging reliable information, commanders can enhance protection measures and minimise the potential consequences of threats. Additionally, prioritizing the collection and analysis of human peacekeeping-intelligence contributes to a more robust and accurate threat analysis process.

Slide 22



Risk Analysis Tool

For each identified threat.

Here are five separate threats

Applied to the matrix tool

Prioritization of risks are classified from low, medium, to high

A valuable tool for visualising risk is the Risk Analysis Matrix, which combines the likelihood of an attack and the impact of that attack that identified threats have on a unit. This process can be used whether it pertains to civilians, UN forces, or UN facilities. Risk, in this context, is determined by both the vulnerability of specific groups and the threats they face. The Risk Analysis Matrix provides a useful framework for breaking down and analysing this information, as depicted on the slide.

On the graph, the vertical "Y" axis represents the Impact, which indicates the consequences that would arise if a threat materialised and affects the at-risk police or military unit. The "x" axis represents the Likelihood, denoting the probability of a threat materializing. Assessing the likelihood involves considering various factors such as existing human rights reporting, peacekeeping-intelligence inputs, and historical analysis.

In terms of risk assessment, Threat 2 on the graph is classified as low since it exhibits both low impact and low likelihood. On the other hand, Threat 1 is designated as high because it has a high likelihood of occurring and would result in significant impact. The displayed graph or matrix is a sample risk analysis representation, and we will utilise it during the lessons on Force Protection planning considerations in Module 3.

The Risk Analysis Matrix serves as a practical visual tool for evaluating risk, enabling decision-makers to prioritise resources and develop appropriate strategies to address threats. It allows for a systematic assessment of the likelihood and impact of different risks, facilitating informed decision-making and efficient allocation of protective measures. By utilising the Risk Analysis Matrix, organisations can enhance their understanding of the risk landscape and implement effective risk mitigation measures.

Slide 23

Intelligence, Surveillance and Reconnaissance (ISR)

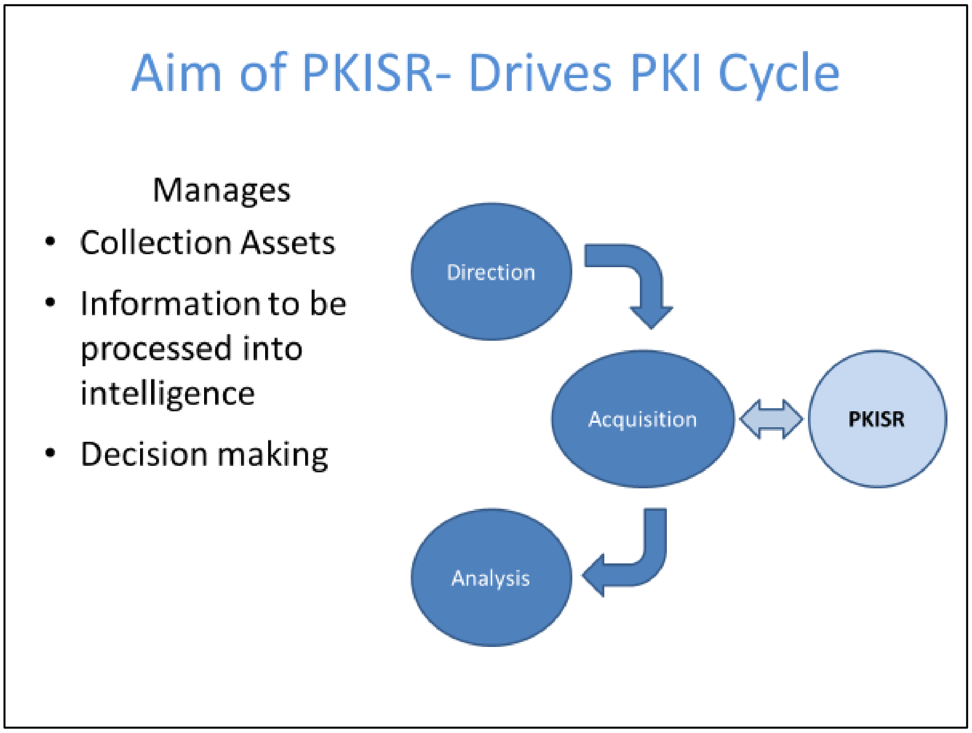
23

The subsequent part of the lesson centres on the acquisition of Peacekeeping Intelligence (PKI) and the role of Intelligence, Surveillance and Reconnaissance (ISR). The term ISR encompasses two fundamental meanings. Firstly, it describes the various entities utilised for acquiring PKI, such as Unmanned Aircraft Systems (UAS). Secondly, it refers to the process of managing the acquisition itself. It is essential to highlight that PKISR serves as the means to accomplish the acquisition step within the peacekeeping-intelligence cycle.

The objective is to provide you with a general understanding of ISR planning and the utilisation of UAS assets. It is crucial to comprehend that ISR assets are not solely dedicated to conducting Force Protection (FP) tasks; they also provide information for a range of other peacekeeping-intelligence-related requirements from various mission components. ISR assets exist in two distinct forms: UN units/assets and UN contracted systems. Planners must acknowledge the advantages and limitations offered by both types of assets.

By gaining insight into ISR planning and the use of UAS assets, you will develop a foundational understanding of how these resources contribute to the overall peacekeeping-intelligence capabilities in peacekeeping operations. Recognising the broader scope of ISR assets and their multifaceted role enables planners to effectively leverage them to meet diverse peacekeeping-intelligence requirements across mission components. It is important to evaluate the strengths and limitations of both UN-owned assets and contracted systems when considering their integration into the overall peacekeeping-intelligence framework.

Slide 24



Aim of PKISR- Drives PKI Cycle

Manages

- Collection Assets
- Information to be processed into intelligence
- Decision making

Direction

Acquisition

PKISR

Analysis

The aim of PKISR is to manage the acquisition of information. The core of tasking for PKISR assets should be from the Mission Information Acquisition Plan (IAP). Secondly, Requests for Information (RFI) should also be answered by prioritising the request against other tasks. What makes it complex, is the ability of the intel cells to interpret requirements and acquire the necessary data for it to be processed into peacekeeping-intelligence, all in a timely manner that supports decision making. ISR drives the intel cycle. Any component of the Mission can request information via an intel or information related question.

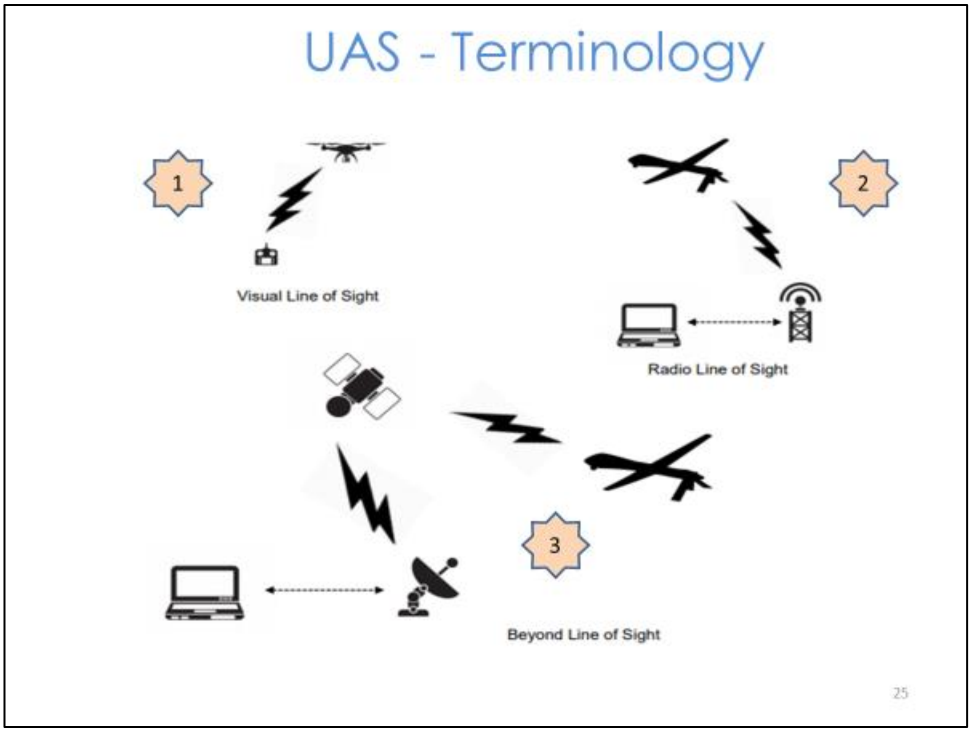
As previously stated, it is important to note that the tasking of ISR is not the sole domain of the military or police elements of the Mission. The Joint Mission Analysis Centre (JMAC) and the UN Police (UNPOL) within the Mission may equally request support from PKISR assets to acquire information on their behalf.

The mission leadership plays a key role in directing ISR. It is important that ISR resources collect information that supports the leadership's decision-making process. Because there is a finite number of resources, it is essential that peacekeeping-intelligence requirements are prioritised based on the needs of the leadership.

As such, it is important that the leadership provides continual direction and guidance as part of the ISR process. ISR is the enabler in providing situational awareness and supporting UN decision-making. The following therefore applies to ISR:

- Provide situational understanding and predictive PKI products to enhance peacekeeping planning and decision-making. Commanders who have access to good PKI are better able to take appropriate actions
- Provide warning of threats to the security of UN personnel, both uniformed and civilian
- Provide early warning of threats of physical violence to the local population, in support of POC
- Enhance the Mission leadership's understanding of shifts in the operational landscape through the identification of relevant trends and threats. This will facilitate the identification of risks and the development / planning of courses of action to mitigate the risks

Slide 25



The United Nations has been increasingly deploying Unmanned Aircraft Systems (UASs), also known as drones, or unmanned aerial vehicles (UAVs), in UN peacekeeping operations (UNPKOs). UASs are aircraft systems that operate without a human pilot onboard and consist of various components, including the unmanned aircraft itself, a ground control station (GCS) for flight management, and a communication link between the aircraft and the GCS. These versatile systems are designed for a wide range of applications, including surveillance, reconnaissance, data collection, and aerial operations in diverse environments.

To gain a comprehensive understanding of UASs, it is essential to familiarize oneself with the different types and terminology associated with them. In the context of the UN's use of UASs, there are specific terms that require clarification, one of which is "line of sight" (LOS), often mentioned in discussions on aircraft control. Let us delve into the distinctions between the various types of control.

The term "line of sight" (LOS) refers to the communication link between the GCS and the UAS, facilitating directional input and the transmission of sensor data. In the presentation, three types of "line of sight" control are depicted.

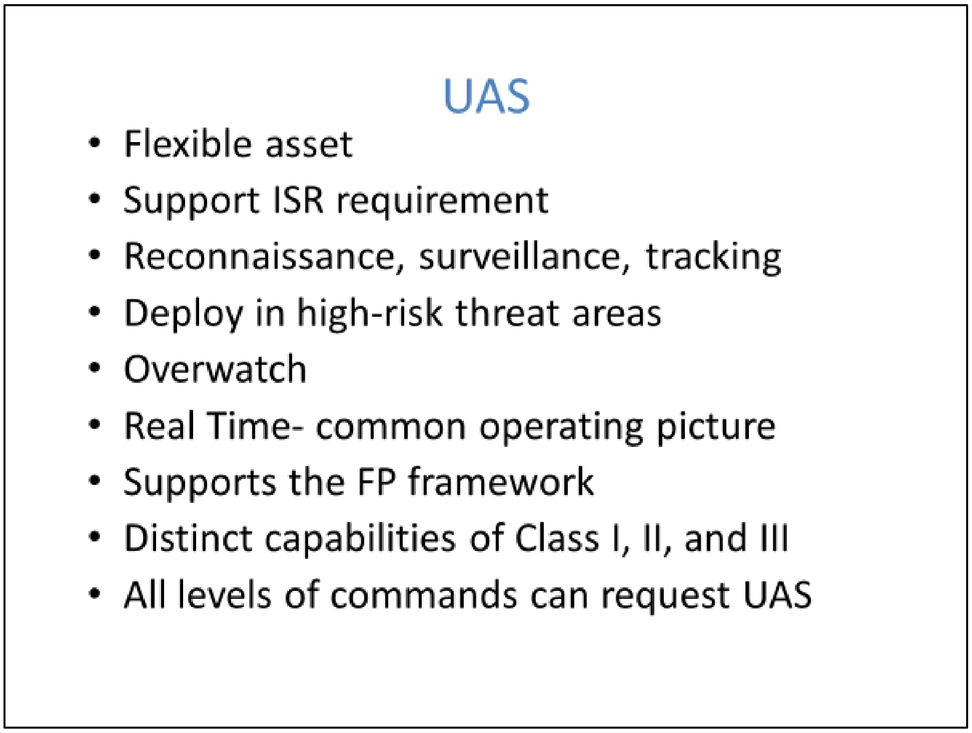
Firstly (#1), "visual LOS" is used to describe most Class I UASs. In this scenario, the aircraft pilot must maintain constant visual contact with the UAS to safely control it and avoid potential collisions with other aircraft, individuals, buildings, and terrain.

Next (#2), "radio LOS" characterises UASs that can operate beyond the visual range of the operator but are limited by obstacles presented by the surrounding terrain. This type of control is comparable to tuning into a radio station in a vehicle, where the strength of the signal can be affected by obstructions.

Lastly (#3), "beyond LOS" (BLOS) refers to the requirement of using satellite uplinks and downlinks to establish communication with the UAS. This type of control is primarily associated with Class III UASs, which rely on satellite connectivity to extend their operational range.

Understanding these distinctions enables stakeholders to appropriately classify and comprehend the control capabilities of different UAS classes. It is crucial to recognise the unique requirements and limitations posed by visual LOS, radio LOS, and BLOS control, as they significantly impact the operational range and capabilities of UASs.

Slide 26



UAS

- Flexible asset
- Support ISR requirement
- Reconnaissance, surveillance, tracking
- Deploy in high-risk threat areas
- Overwatch
- Real Time- common operating picture
- Supports the FP framework
- Distinct capabilities of Class I, II, and III
- All levels of commands can request UAS

Selecting the appropriate UAS type depends on size, capabilities, and operational requirements, ultimately bolstering acquisition and peacekeeping-intelligence gathering in peacekeeping missions.

- Flexible, versatile asset adaptable to various mission needs
- Support UNPKI by fulfilling peacekeeping-intelligence, surveillance, and reconnaissance (ISR) requirements
- Can conduct reconnaissance, surveillance, and tracking operations
- Deployment in high-risk threat areas to enhance situational awareness
- Providing overwatch capabilities for enhanced security
- Facilitating real-time sharing of information for a common operating picture
- Supports the FP framework
- Selecting an appropriate UAS type depends on size, capabilities, operational requirements
- Distinct capabilities of Class I, II, and III UASs for different mission needs

Concerning the bullet on the slide, “Distinct capabilities of Class I, II, and III UASs”, it is essential to better understand the categories. UASs are categorized into different classes, each serving specific purposes at various operational levels.

- Class I UASs are tactically focused and provide real-time situational awareness for ground units, without dedicated analysts
- Class II UASs, deployed at the Force level, offer enhanced capabilities and endurance. They operate day and night, receiving ISR tasking and utilising specialised sensors.
- Class III UASs, centrally held at the Force level, possess extended range, endurance, and advanced sensors, enabling comprehensive peacekeeping-intelligence gathering.

UAS sensors are highly effective for tactical tasks, such as persistent surveillance of armed groups. Larger UASs equipped with SAR and GMTI capabilities excel in wide-area surveillance. Smaller UASs are ideal for tactical missions like convoy overwatch and camp security, offering early warning and improved situational awareness.

Commanders and peacekeeping-intelligence cells have the authority to request UAS deployment at all levels, including UN Mission-level assets. A well-defined and comprehensive Request for Information (RFI) is crucial to justify and evaluate the criticality of identifying high-risk threats.

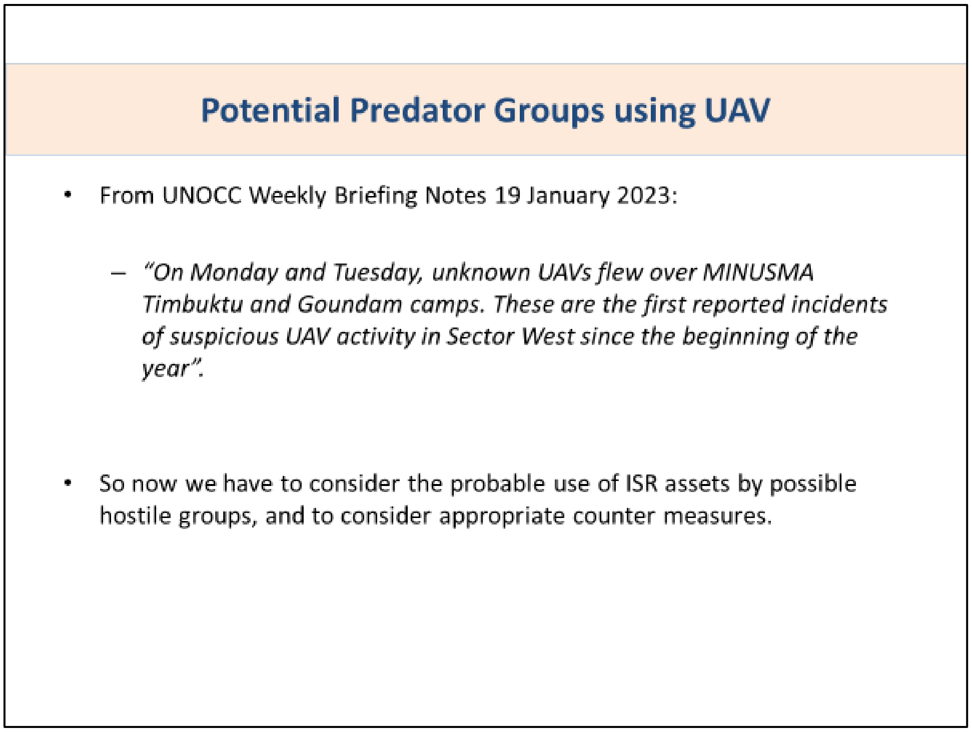
The RFI should outline specific operational requirements, emphasising how UAS deployment will enhance situational awareness and peacekeeping-intelligence gathering. It should highlight the unique capabilities of UASs in surveillance, reconnaissance, decision-making, and risk mitigation.

Furthermore, the RFI should address the types of surveillance capabilities, and operational parameters necessary for the UAS assets. This ensures that the deployed UASs are well-suited to meet the identified challenges and information needs.

Smaller UAS are better used for more tactical tasking such as overwatch of a convoy to look ahead for potential Improvised Explosive Device (IED) emplacement activity. A good communication link between the UAS operators and the unit within the convoy is essential for early warning of activity. Another good task for tactical UAS is enhancing camp security, providing overwatch to alert for potential enemy rocket or mortar action.

"SAR": SAR stands for Synthetic Aperture Radar. SAR is a radar imaging technology that can create high-resolution images of objects on the ground, even in adverse weather conditions. "GMTI": GMTI stands for Ground Moving Target Indicator. This capability allows UAVs to detect and track moving objects on the ground.

Slide 27



Potential Predator Groups using UAV

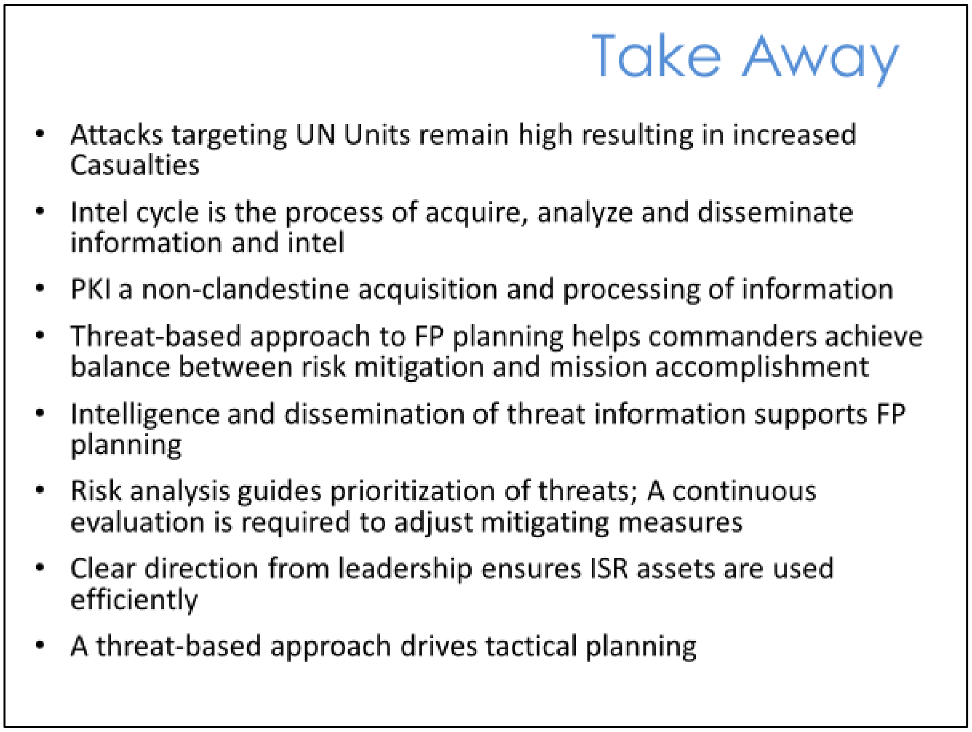
- From UNOCC Weekly Briefing Notes 19 January 2023:
  - *"On Monday and Tuesday, unknown UAVs flew over MINUSMA Timbuktu and Goundam camps. These are the first reported incidents of suspicious UAV activity in Sector West since the beginning of the year".*
- So now we have to consider the probable use of ISR assets by possible hostile groups, and to consider appropriate counter measures.

UNOCC Weekly Briefing Notes 19 January 2023.

"On Monday and Tuesday, unknown UAVs flew over MINUSMA Timbuktu and Goundam camps. These are the first reported incidents of suspicious UAV activity in Sector West since the beginning of the year".

Given recent developments, it is crucial to address the possibility of armed groups within the UN Mission area deploying unmanned aerial systems (UAS) or drones against UN units. This situation warrants a comprehensive assessment of how these potentially hostile entities utilise peacekeeping-intelligence, surveillance, and reconnaissance (ISR) assets. Additionally, it is essential to devise and implement effective countermeasures / counter UAS operations to mitigate the inherent risks associated with such activities.

Slide 28



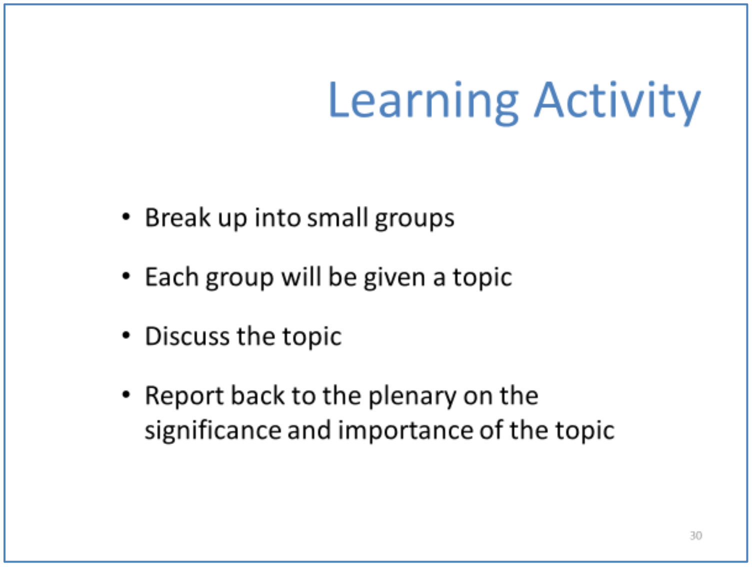
Take Away

- Attacks targeting UN Units remain high resulting in increased Casualties
- Intel cycle is the process of acquire, analyze and disseminate information and intel
- PKI a non-clandestine acquisition and processing of information
- Threat-based approach to FP planning helps commanders achieve balance between risk mitigation and mission accomplishment
- Intelligence and dissemination of threat information supports FP planning
- Risk analysis guides prioritization of threats; A continuous evaluation is required to adjust mitigating measures
- Clear direction from leadership ensures ISR assets are used efficiently
- A threat-based approach drives tactical planning

Summary

- The intelligence cycle encompasses a continuous sequence of activities: direction, acquisition, analysis, and dissemination
- The Information Acquisition Plan (IAP) serves as a tool for capturing all intelligence requirements specified by leadership, which can be addressed using ISR assets
- Threat analysis generates a predictive intelligence product, enabling the assessment of the threat's capabilities, intentions, and likely courses of action or scenarios. This analysis plays a crucial role in risk mitigation and Force Protection planning
- FP planning is a process primarily led by intelligence, requiring ongoing attention and involvement by unit staffs and leaders
- Risk analysis assists in prioritising threats, aiding in the determination of their relative significance
- ISR assets are valuable resources that can be employed for Force Protection planning purposes
- Planners must acknowledge the limitations of PKISR assets and make informed decisions about

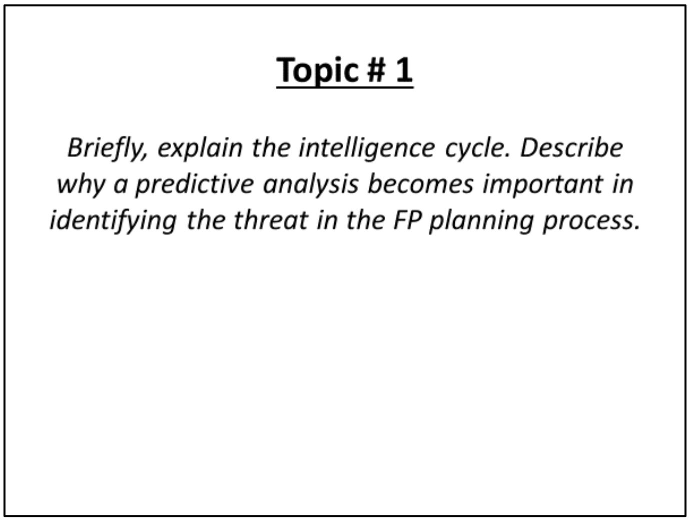
Learning Activity for Lesson 1.3



Learning Activity

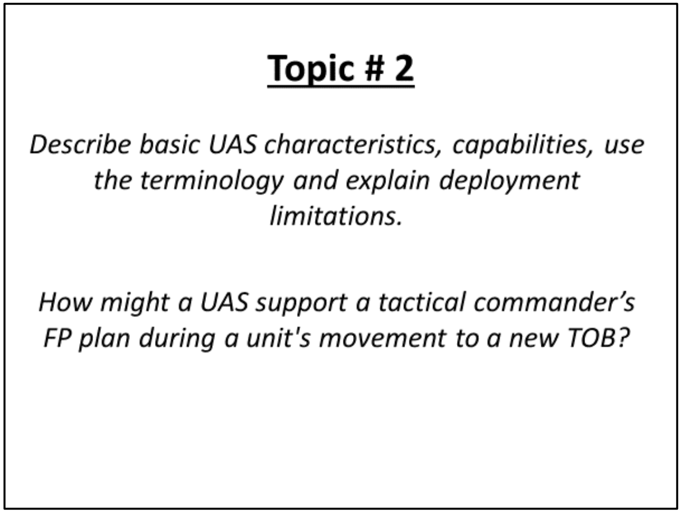
- Break up into small groups
- Each group will be given a topic
- Discuss the topic
- Report back to the plenary on the significance and importance of the topic

30



Topic # 1

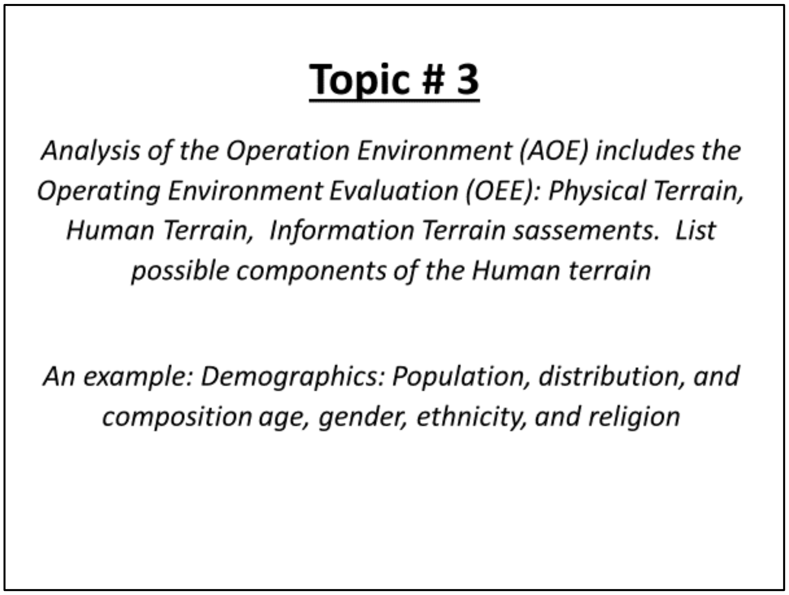
Briefly, explain the intelligence cycle. Describe why a predictive analysis becomes important in identifying the threat in the FP planning process.



Topic # 2

Describe basic UAS characteristics, capabilities, use the terminology and explain deployment limitations.

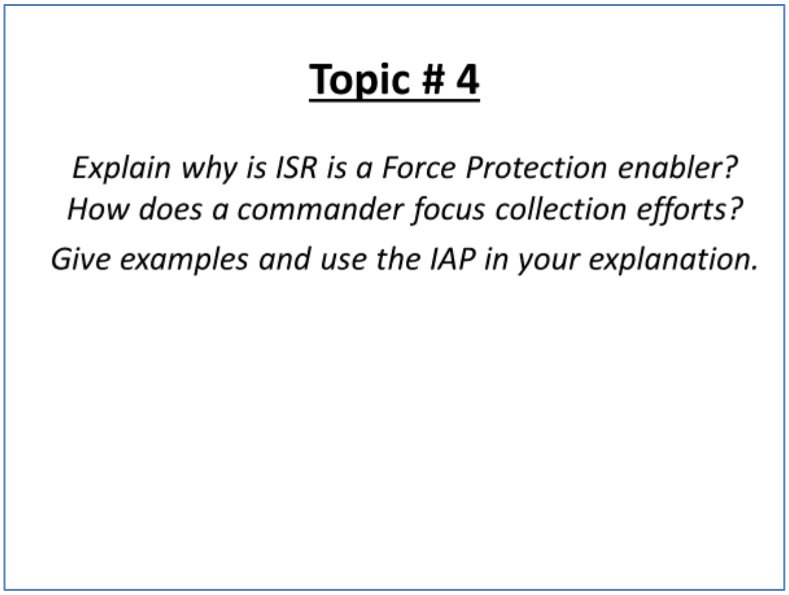
How might a UAS support a tactical commander's FP plan during a unit's movement to a new TOB?



Topic # 3

Analysis of the Operation Environment (AOE) includes the Operating Environment Evaluation (OEE): Physical Terrain, Human Terrain, Information Terrain sassements. List possible components of the Human terrain

An example: Demographics: Population, distribution, and composition age, gender, ethnicity, and religion



Topic # 4

Explain why is ISR is a Force Protection enabler? How does a commander focus collection efforts?

Give examples and use the IAP in your explanation.

Lesson 1.4

Intro to the Tactical Decision-Making Process (Military)

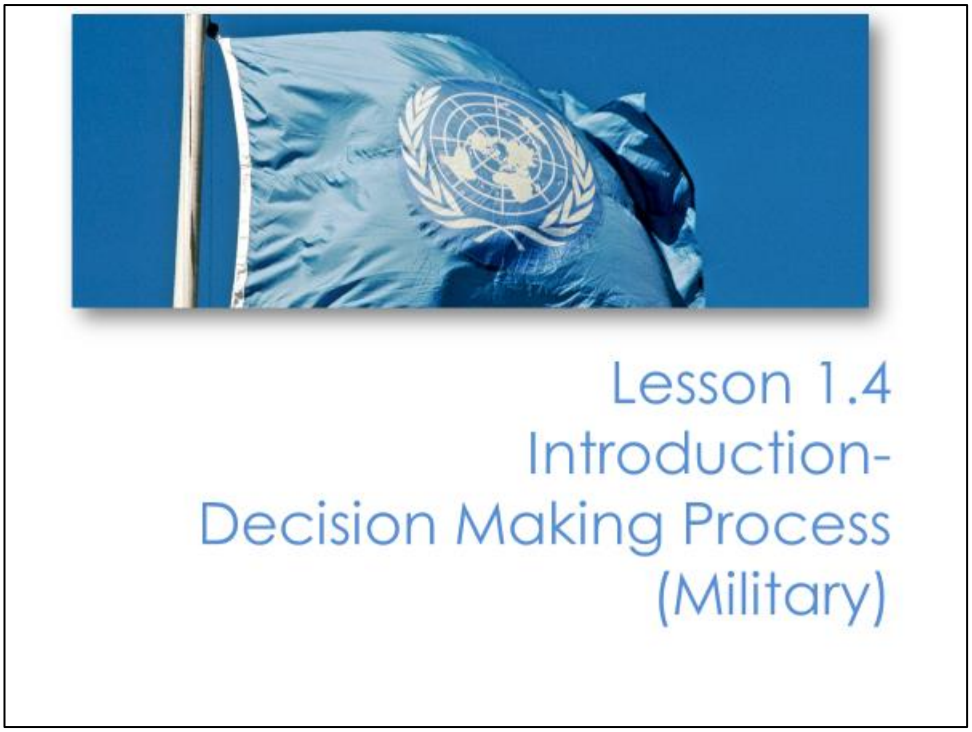
Starting the Lesson

The objective of this lesson is to familiarise participants with tactical planning guidance and considerations in a PKO. It is important for military officers to understand that tactical planning in peacekeeping operations is a multifaceted and diverse process that encompasses various components. The success of military operations relies on the adoption of a comprehensive planning and decision-making process, starting from the Force HQs to the Sector HQs, down to the field units and companies. This systematic approach empowers staff and commanders to seek optimal solutions and make decisions to achieve success.

In a traditional military operation, the planning process involves determining resource requirements, such as the necessary troops and equipment to accomplish the mission. However, in the context of a UN peacekeeping mission, many of these factors have already been established through strategic planning at the UNHQ, as outlined in relevant documents like the Security Council Resolution, Concept of Operations (CONOPS), Integrated Strategic Framework (ISF), and Mission Concept.

The purpose of this module is not to train participants on a specific decision-making or planning process dictated by any particular national doctrine. Instead, it aims to emphasize how commanders and their staff should integrate UN planning documents, such as Force Protection, Protection of Civilians (POC), Child Protection, Conflict-Related Sexual Violence (CRSV), and unique planning considerations. It also underscores the importance of understanding how military tasks support the mission. This lesson provides tactical PKO planning guidance for troop contributing countries (TCCs) to consider within their own planning processes.

Slide 1



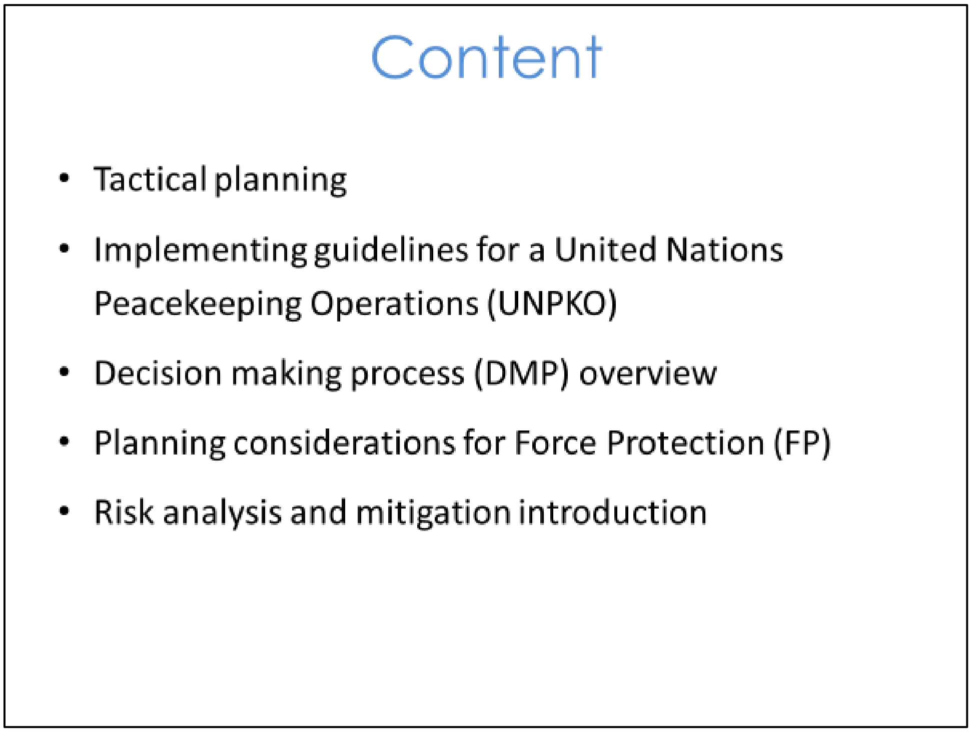
Lesson 1.4
Introduction-
Decision Making Process
(Military)

Military officers in a UN Mission must understand the unique tactical planning process in Peacekeeping Operations (PKO). Successful military operations depend on employing a planning process that involves staff and commanders working together to find optimal solutions and make decisions in a dynamic and dangerous PKO environment.

This planning process is not independent of the overall peacekeeping planning mechanism. It is complemented by other mechanisms such as liaison among different military and coordination with civilian and police components.

In this lesson, we will introduce you to tactical planning considerations and provide guidance to help member states integrate their own planning and military decision-making processes (MDMP) in a PKO. Specifically, we will focus on special tactical planning guidance and considerations for units operating within the United Nations Peacekeeping Operations (UNPKO) Force Protection (FP) framework.

Slide 2



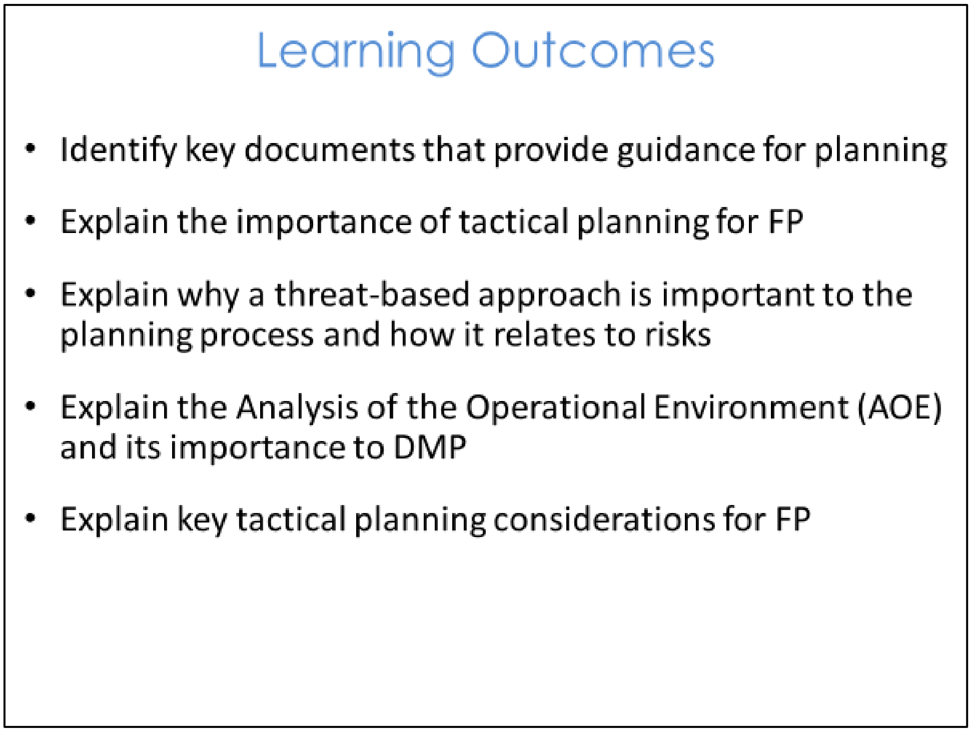
Content

- Tactical planning
- Implementing guidelines for a United Nations Peacekeeping Operations (UNPKO)
- Decision making process (DMP) overview
- Planning considerations for Force Protection (FP)
- Risk analysis and mitigation introduction

This lesson contains valuable information for the implementation of FP. We will discuss tactical considerations and provide guidance for planning FP. Additionally; we will examine the concept of risk analysis and assessment.

- Tactical planning
- Implementing guidelines for United Nations Peacekeeping Operations (UNPKO)
- Decision-making process (DMP) overview
- Planning Considerations for Force Protection (FP)
- Risk analysis and mitigation introduction

Slide 3



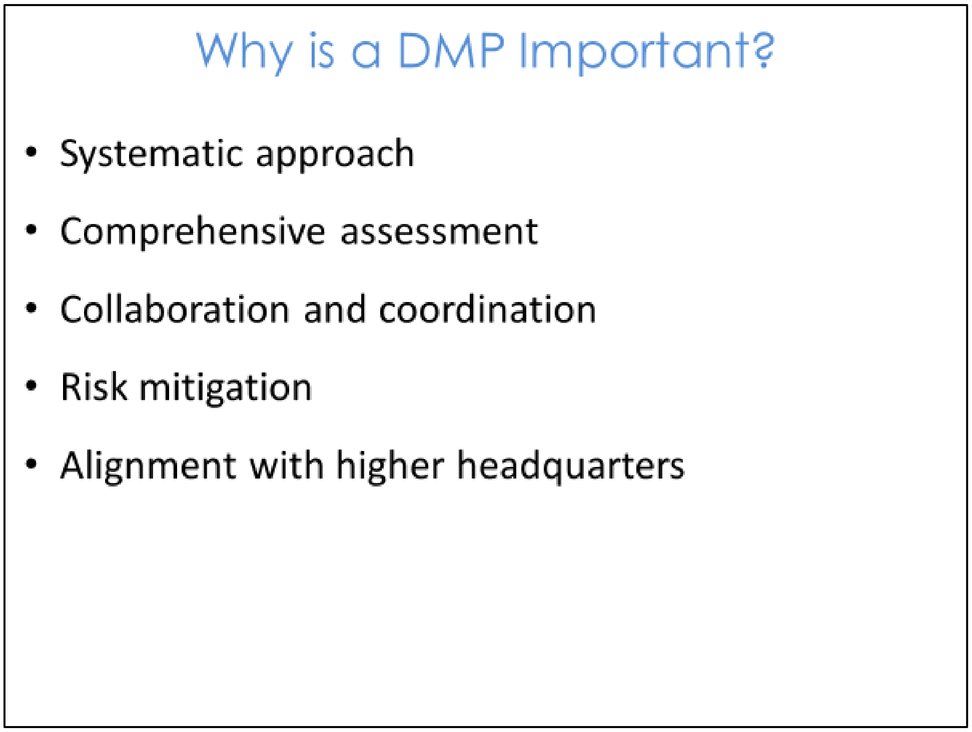
Learning Outcomes

- Identify key documents that provide guidance for planning
- Explain the importance of tactical planning for FP
- Explain why a threat-based approach is important to the planning process and how it relates to risks
- Explain the Analysis of the Operational Environment (AOE) and its importance to DMP
- Explain key tactical planning considerations for FP

As a good training practice, let us review the 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.

- Identify key documents that provide guidance for planning
- Explain the importance of tactical planning for FP
- Explain why a threat-based approach is important to the planning process and how it relates to risks
- Explain the Analysis of the Operational Environment (AOE) and its importance to DMP
- Explain key tactical planning considerations for FP

Slide 4



Why is a DMP Important?

- Systematic approach
- Comprehensive assessment
- Collaboration and coordination
- Risk mitigation
- Alignment with higher headquarters

Systematic approach: The military decision-making process offers a systematic and logical approach to analysing complex operational environments, assessing risks, and developing feasible courses of action. It ensures that all aspects of a mission are considered, enabling commanders to make informed decisions.

Comprehensive assessment: By considering multiple factors such as the political, humanitarian, and security dimensions, the decision-making process helps identify potential risks, opportunities, and constraints. This holistic assessment enhances situational understanding and supports effective planning.

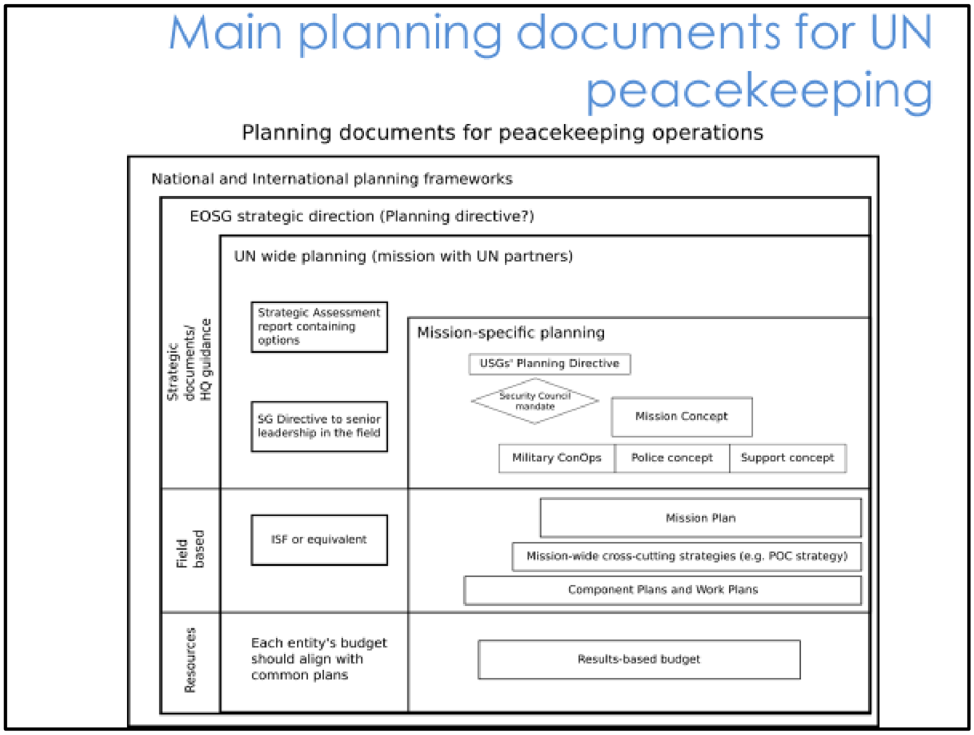
Collaboration and coordination: The decision-making process involves collaboration among staff members, commanders, and relevant stakeholders. It facilitates communication, information sharing, and coordination, ensuring that all stakeholders are involved and contributing to the planning process.

Risk mitigation: Through the decision-making process, commanders evaluate various courses of action and their potential consequences. This analysis enables them to anticipate and mitigate risks, minimising potential negative outcomes and maximizing mission success.

Alignment with higher headquarters: The military decision-making process ensures that plans are developed in accordance with strategic objectives and guidance from higher headquarters. By seeking their approval, it promotes unity of effort and alignment with the overall mission.

In summary, the military decision-making process is important because it provides a structured and comprehensive approach to planning military operations. It enhances situational understanding, facilitates collaboration, mitigates risks, aligns with higher headquarters, and promotes adaptability for mission success.

Slide 5



Main planning documents for UN peacekeeping

Planning documents for peacekeeping operations

National and International planning frameworks

EOSG strategic direction (Planning directive?)

UN wide planning (mission with UN partners)

Strategic documents/ HQ guidance

Strategic Assessment report containing options

SG Directive to senior leadership in the field

Mission-specific planning

USGs' Planning Directive

Security Council mandate

Mission Concept

Military ConOps

Police concept

Support concept

Field based

ISF or equivalent

Mission Plan

Mission-wide cross-cutting strategies (e.g. POC strategy)

Component Plans and Work Plans

Resources

Each entity's budget should align with common plans

Results-based budget

This slide provides an overview of planning processes in the UN system and their impact on ground operations. Understanding this complexity is crucial in the context of UN Peacekeeping:

- Mission-specific planning is part of the broader UN-wide planning process, guided initially by the Executive Office of the Secretary-General.

- At UN Headquarters, the Department of Peace Operations (DPO) develops a Mission Concept, which outlines the strategic goals and approach of the field mission. Military, police, and support concepts provide further details.

- The Mission Concept guides the development of a Mission Plan, which operationalizes the mandate and must align with the Integrated Strategic Framework (ISF) when applicable. The ISF brings together mission and UNCT (United Nations Country Team) mandates around agreed priorities.

- Each component within the Mission should have component-level plans, such as annual work plans, aligned with the Mission Concept and Mission Plan.

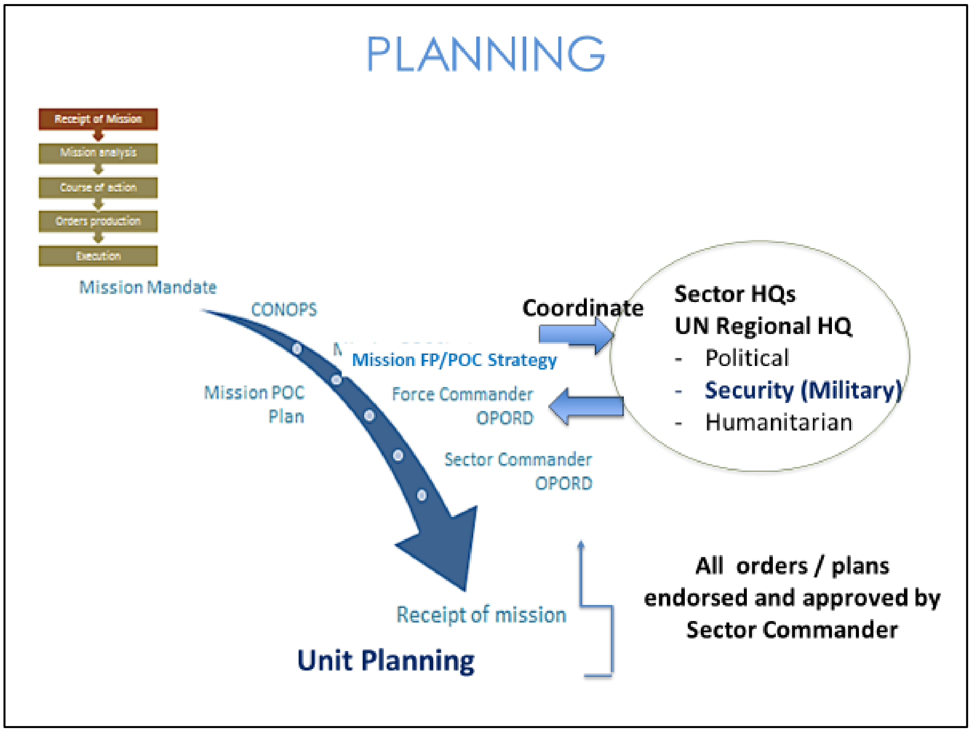
- The Mission may have mission-wide strategies addressing cross-cutting issues like the Protection of Civilians, child protection, and gender mainstreaming.

- The results-based budget (RBB) serves as the primary resource management tool at the mission level. It is derived from the Mission's plans for the following year and measures progress against mandated tasks and objectives.

- Plans should guide implementation, monitor on-ground impact, and be regularly updated based on evolving conflict analysis, determining the need for course corrections.

All strategic and operational planning processes related to Peacekeeping Operations must adhere to the appropriate UN policies.

Slide 6



PLANNING

Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Mission Mandate

CONOPS

Mission FP/POC Strategy

Mission POC
Plan

Force Commander
OPORD

Sector Commander
OPORD

Receipt of mission

Unit Planning

Coordinate

Sector HQs
UN Regional HQ
- Political
- Security (Military)
- Humanitarian

All orders / plans
endorsed and approved by
Sector Commander

This slide provides a comprehensive overview of the nested concept of planning and coordination among different layers of headquarters (HQs). It emphasises the importance of back briefs to higher HQs and the approval process for subordinate plans. When utilising the Military Decision-Making Process (MDMP) and planning process, it is crucial to involve and coordinate with all UN components, partners, interlocutors, and local governments.

Force Protection (FP) and Protection of Civilians (POC) planning stem from the Mission Mandate and cascade through each planning level, resulting in an Operations Order (OPORD)/Plan Order (PLANORD) issued to Unit Commanders. Commanders must incorporate FP and POC planning into all aspects of their mission planning.

The Mission Mandate always adheres to overarching laws and policies that prioritise the Protection of Civilians. FP and POC planning run parallel to other mission planning activities. The output of FP and POC planning is not a standalone plan but rather considerations to be integrated into mission planning.

Planning guidance is conveyed through the Force Commander's OPORD, and Sector Commander's OPORD, and ultimately reaches the Unit Commanders who are responsible for planning within their respective Area of Responsibility (AOR) as part of their Receipt of Mission.

Notably, at the sector level, close collaboration with the UN Country Team/Regional HQ is vital to grasp the political and humanitarian aspects. The three pillars of responsibility in a UN Mission are Political, Security, and Humanitarian. The Military component primarily focuses on the security pillar. Therefore, sector and force HQs must support unit commanders by coordinating and fostering synergistic efforts with other mission components in FP and POC planning.

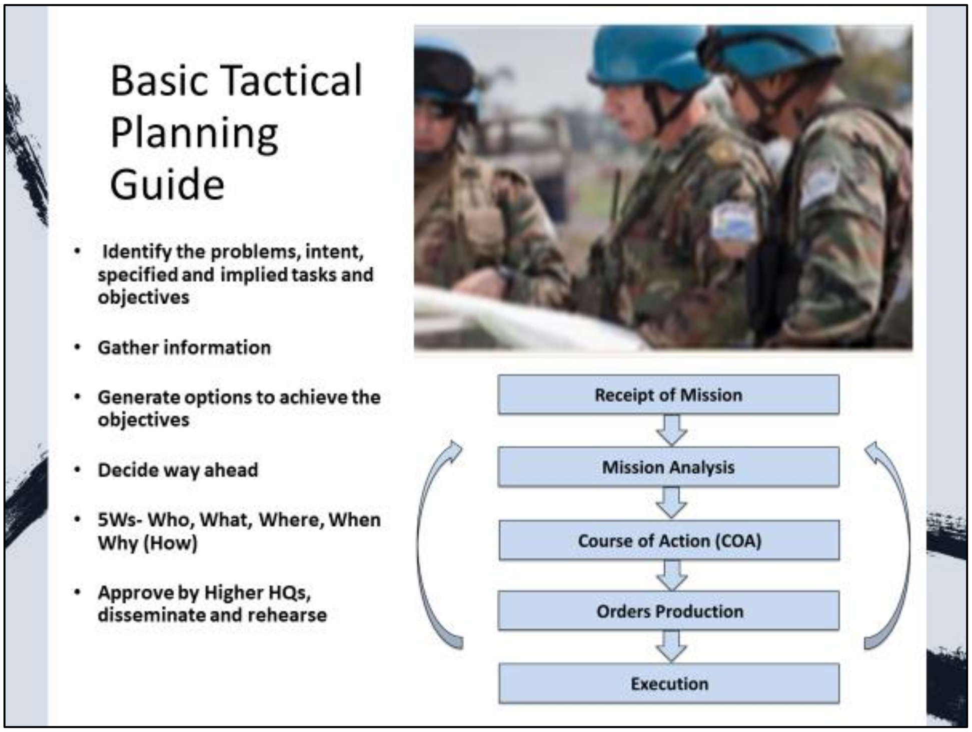
Unit-level FP planning entails understanding the specific vulnerabilities of UN forces and police units. Proactive measures should be incorporated into the planning process.

Force and Sector HQs generally follow the UN-MDMP planning process, while unit commanders utilise their national planning and decision-making processes to develop their plans. Referring to Standard Operating Procedures (SOPs) is advisable to ensure adherence to required formats for planning products. It is crucial for Sector and Force HQs to comprehend the tactical challenges and threats at the tactical level.

Once a unit commander devises their plan, it must be endorsed and supported by higher HQs. This includes accepting risks and aiding in risk mitigation. This may involve assuming responsibilities for specific Named Areas of Interest (NAIs) and Targeted Areas of Interest (TAIs) inherent in the plans.

For discussion:
To ensure successful planning, it is key that there exists a close liaison with the Sector HQs and, UN Country Team. The three pillars of responsibility in a UN Mission are Political, Secure Environment and Humanitarian. Ask the students how can we synergize the relationship with the interlocutors and partners?

Slide 7



Basic Tactical Planning Guide

- Identify the problems, intent, specified and implied tasks and objectives
- Gather information
- Generate options to achieve the objectives
- Decide way ahead
- 5Ws- Who, What, Where, When Why (How)
- Approve by Higher HQs, disseminate and rehearse

Receipt of Mission

Mission Analysis

Course of Action (COA)

Orders Production

Execution

Good planning is crucial for the success of UN military operations. Tactical units follow their respective national doctrines in their tactical planning processes. Each Troop Contributing Country (TCC) has its own planning process. However, the UN has also developed its own process to promote interoperability and facilitate combined operations at the Force and Sector HQs level. This UN planning process incorporates the UN military peacekeeping-intelligence framework, ensuring its inclusion in the planning efforts. A critical aspect of the process is the Analysis of the Operating Environment (AOE), which involves assessing the physical, human, and information terrain.

- Identify problems, intent, specified and implied tasks, and objectives; the decision-making process begins by clearly identifying the problems or challenges that need to be addressed. Commanders establish their intent, outlining their desired end state and key objectives. Specified tasks, which are explicitly defined, and implied tasks, which are inferred from the situation, are identified to achieve the objectives.

- Gather information: The decision process emphasises the collection and analysis of relevant information. Commanders and staff conduct peacekeeping-intelligence-gathering activities to gain a thorough understanding of the operational environment. They consider factors such as terrain, enemy capabilities, friendly forces, civilian considerations, and logistical constraints.

- Generate options to achieve the objectives: Based on the gathered information, commanders and staff brainstorm and develop multiple feasible options or courses of action. Each option considers different approaches, sequencing of tasks, allocation of resources, and potential risks and benefits. These options are evaluated against the identified objectives, constraints, and overall intent.

- Decide on the way ahead: The decision-making process involves evaluating and comparing the various options generated. Commanders consider the potential outcomes, risks, and alignment with strategic goals. After careful analysis, a decision is made on the preferred course of action or the way ahead.

- 5Ws - Who, What, Where, When, Why (How): The decision-making process requires, when deciding on a course of action, commanders, and staff to address the key questions of Who, What, Where, When, and Why (sometimes including How). These questions help define the details of the chosen course of action, including identifying the responsible units, tasks to be executed, operational areas, timing, and the underlying rationale.

- Plans approved by Higher HQs, disseminated, and rehearsed: Once a course of action is selected, it is presented to higher headquarters for approval. Plans are reviewed, refined, and adjusted as necessary based on feedback from higher headquarters. Once approved, the plans are disseminated to subordinate units, and rehearsals are conducted to ensure understanding and synchronization among all participating elements.

By following the military decision-making process, commanders and staff can effectively identify problems, establish objectives, gather information, generate options, make informed decisions, address key questions, obtain approval, and disseminate plans for execution. This systematic approach enhances the clarity and effectiveness of military operations.

Learning Activity: *Comparative Analysis of Military Decision-Making Processes (MDMP)*

Objective: This activity aims to facilitate a comparative analysis of the Military Decision-Making Process (MDMP) by exploring the differences between the provided DMP in the lesson materials and the students' own DMP doctrines. Through active engagement and group discussions, participants will identify distinctive aspects and consider potential associations between different DMPs.

Instructions:

Initiate Discussion: Begin the session by discussing the DMP shown on the slide that will be used as a planning tool throughout the lessons. Encourage the class to share their own DMP doctrines.

Stickie Notes: Distribute stickie notes to each student, providing one for each step of their respective DMPs. For instance, if there are 7 steps in their DMP, hand out seven stickie notes to that individual. Have the students write down each step on each stickie note.

Visual Representation: On a blackboard, whiteboard, or butcher paper, create a column with the following headings, leaving enough space between each step:

- ***Receipts of Mission***
- ***Mission Analysis***
- ***Course of Action***
- ***Orders Production***
- ***Execution***
- ***Unknown***

Categorize Steps: Have students come up in small groups and take turns placing their stickie notes on the corresponding step that best aligns with their own DMP. If a certain step cannot be associated or discerned, place it in the "Unknown" category.

Identify Distinctive Aspects: Prompt the class to identify specific areas where the suggested DMP diverges significantly from their own. Encourage open-mindedness and respectful discussions.

Encourage Adaptation: Encourage participants to consider how they might associate or combine steps to use the provided DMP effectively. Emphasise the value of assimilating their own MDMP with the one used in this RTP.

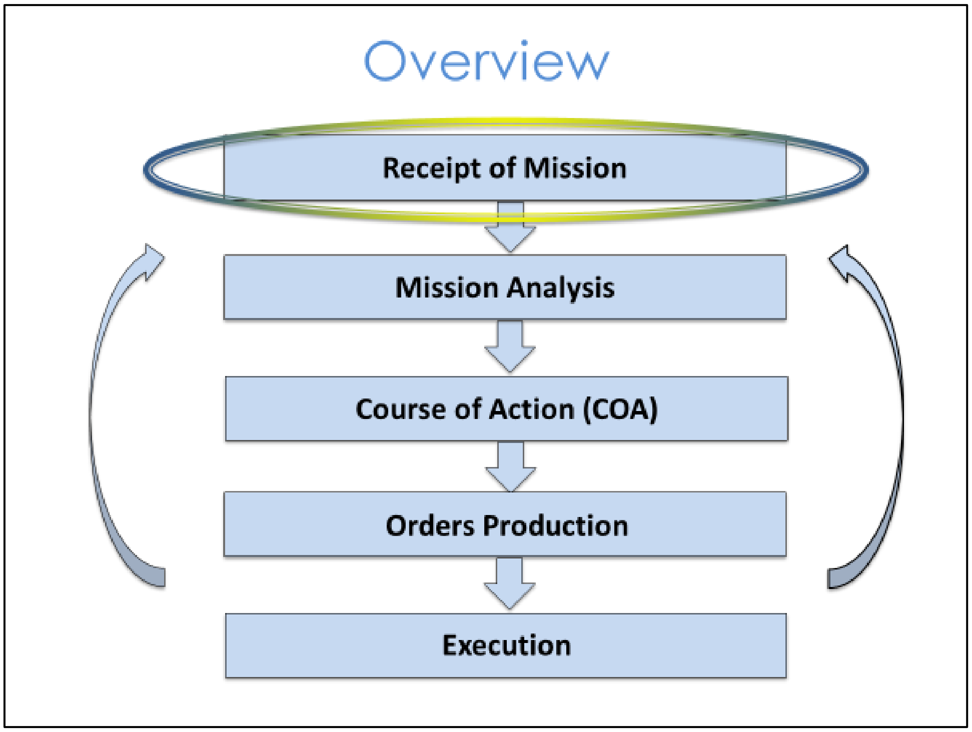
Facilitate Discussion: Allocate approximately 15-20 minutes for a discussion, allowing participants to ask questions, seek clarifications, and share their perspectives.

By structuring the session in this way, participants will actively engage in comparative analysis, fostering a deeper understanding of how their own country's practices and doctrines can be associated with the one used for instructional purposes throughout the lessons.

Before showing the next slide, ask the participants:

(1) What are the actions to be performed when a new mission is received?
(2) What could be the information collection activities that should be conducted?

Slide 8


Overview

Receipt of Mission

Mission Analysis

Course of Action (COA)

Orders Production

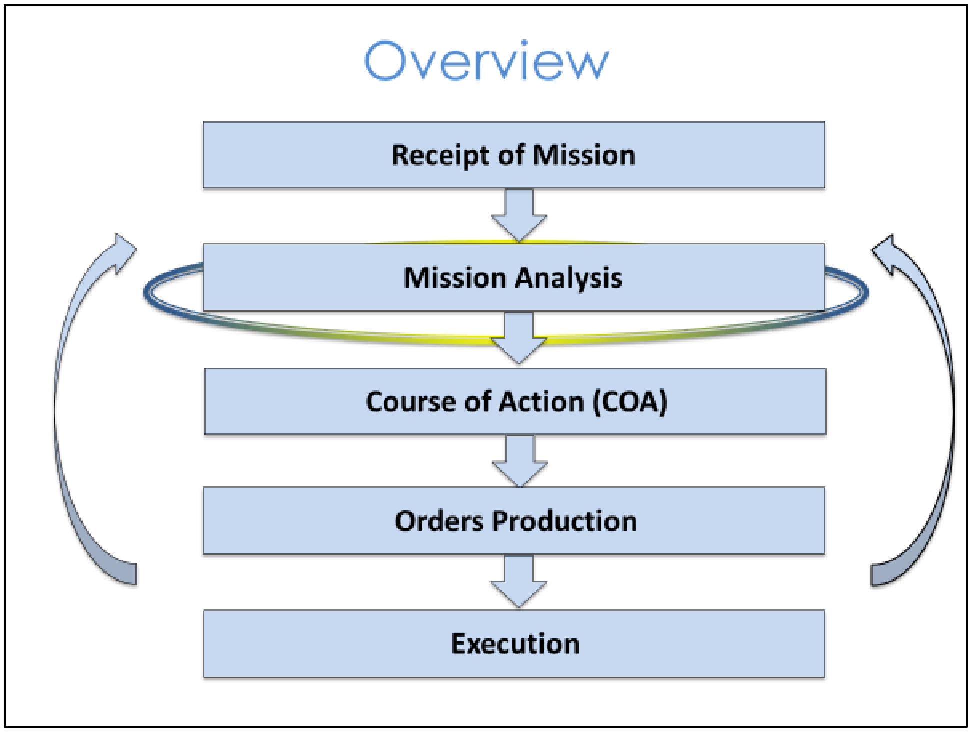
Execution

The objective of this initial step is to inform all participants about the planning requirements, including the available time for planning and the selection of a planning approach. When a new mission is identified, commanders and staff members undertake the following actions:

- Notify key participants
- Gather the necessary planning tools and documents, including the operation order from higher headquarters, maps, terrain information, and ongoing assessments
- Update and refine the Analysis of the Operating Environment (AOE) products
- Determine the required time for planning and mission preparation
- Begin identifying constraints and information needs
- Provide planning guidance to the commanders
- Conduct an initial assessment to determine specified tasks, implied tasks, and mission-essential tasks

- Authorise activities to acquire information, such as patrols, execution of matrices, open-source research, MPKI cell products, JOC/JMAC reports, and requests for information (RFIs) to higher headquarters
- Issue a warning order (WARNORD #1)

Slide 9



Overview

Receipt of Mission

Mission Analysis

Course of Action (COA)

Orders Production

Execution

Mission Analysis is a crucial planning tool that involves refining higher-level guidance, assessing facts and assumptions, and providing detailed mission and planning requirements. This process yields a restated mission, planning guidance, and Commander's intent, encompassing purpose, method, and end state. Key elements within this process include:

- Tasks: Refining and establishing specified, implied, and mission-essential tasks that drive mission success. Tasks are linked to desired effects on various actors, groups, terrain, or UN Forces
- Constraints: Identification and analysis of Constraints and Restrictions, considering limitations, restrictions, and freedom of action, Limitations that impact the plan
- Clarification: Requests for additional information from higher headquarters
- Planning Guidance: Conclusions that guide the staff
- Information Requirements (IR): Necessary information for planning purposes
- Identification and analysis of the Sector and Force Commander's intent, establishing the purpose of the UN Mission
- Identification and analysis of critical Facts and Assumptions
- Identification and analysis of Tasks, including specified tasks

- Assessment of Available Assets
- Classification of acceptable risks (high to low) for prioritisation and mitigation
- Consideration of key operational timings
- Identification of decisive terrain features and operational effects
- Drafting the Commander's intent, specifying the purpose, method, and end state of the mission

Additionally, Mission Analysis involves updating the Analysis of the Operating Environment (AOE). The MPKI cells play a vital role in this analysis, drawing information from various sources. The AOE is a continuous process requiring constant updates, particularly during operations. The AOE includes an analysis of:

- Physical terrain: Assessing the effects of terrain features on UN operations and mandate implementation
- Human terrain: Analysing the impact of human factors on UN operations, such as tribal, ethnic, and religious groups
- Information terrain: Evaluating the effect of communication infrastructure on UN operations
- Weather: Considering the impact of weather on mobility, visibility, and sustainability of operations

Mission Analysis also involves evaluating relevant actors in the area of operations, their intent, capabilities, strengths, weaknesses, and other critical factors. This analysis assists in contingency planning, risk mitigation, and informing operations, including the protection of civilians. Furthermore, integrating the understanding of the operating environment and actors helps generate future scenarios and evaluate non-UN actors' courses of action. This enables staff to plan for a range of scenarios, focusing on threat actors, and consider the impact of UN operations on other relevant actors and vulnerable population groups.

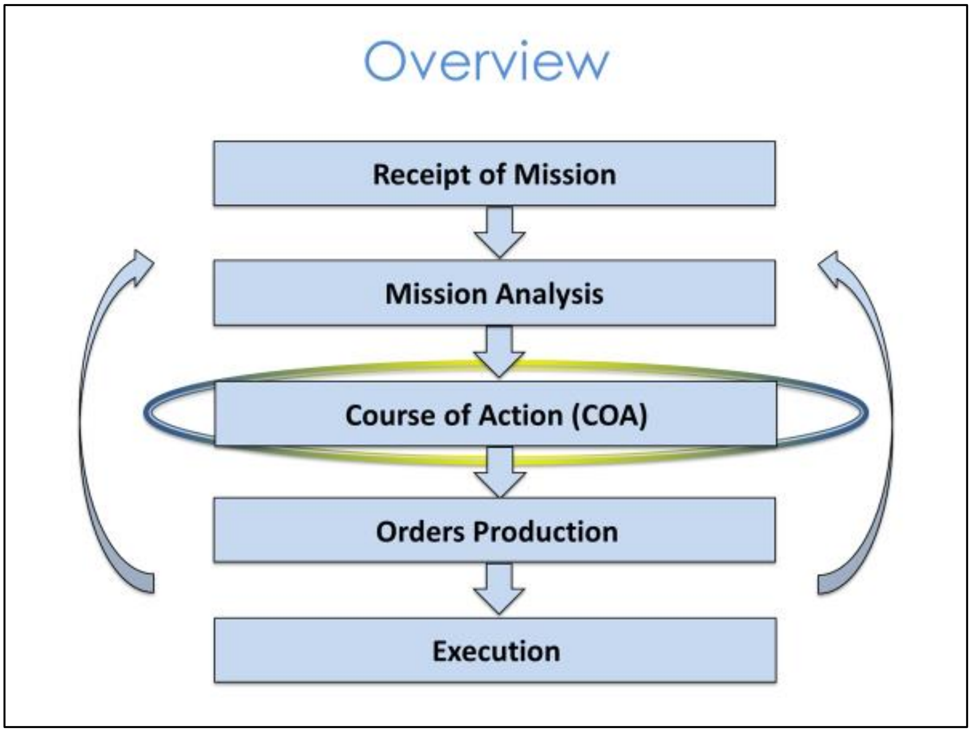
Internal and external staff communications are vital for planning/mission success. Discuss what you do to facilitate dialogue and sharing of information.

Ask the participants:

- *What are the essential elements of intent?*
- *What is the relationship between specified task, implied task/s, and mission essential tasks?*

Facilitate discussion and have them explain the purpose (of the Mission/Task), Method, and end state. Some students may find it difficult to phrase the end state. Have them give examples of End-State.

Slide 10



Overview

Receipt of Mission

Mission Analysis

Course of Action (COA)

Orders Production

Execution

The purpose of Course of Action (COA) development is to establish military options that fulfil the assigned mission or tasks. In a UN context, it is crucial to consider the second-order effects of a UN Mission, such as the impact on local key leaders and vulnerable civilian populations. A valid COA must be feasible, acceptable to UN policy and risk levels, and should include the following elements:

- What: Tasks to be executed
- When: Critical timing parameters
- Where: Locations where military effects will be achieved
- How: Concept of operation incorporating tasks
- Why: Purpose of the mission

COAs are often depicted visually and succinctly, typically on a board with the mission, commander's intent, scheme of manoeuvre, phases, purpose, method, end state, and information requirements. Staff should develop at least two COAs for a given task and consider them from the perspective of spoilers, threat actors, and vulnerability to civilians and our unit. This process, known as gaming, should be documented to address likely threat reactions and plan mitigation strategies.

Furthermore, it is essential to consider the impact of COAs on non-threat actors, such as civilians, local key leaders, and other important actors in the local environment.

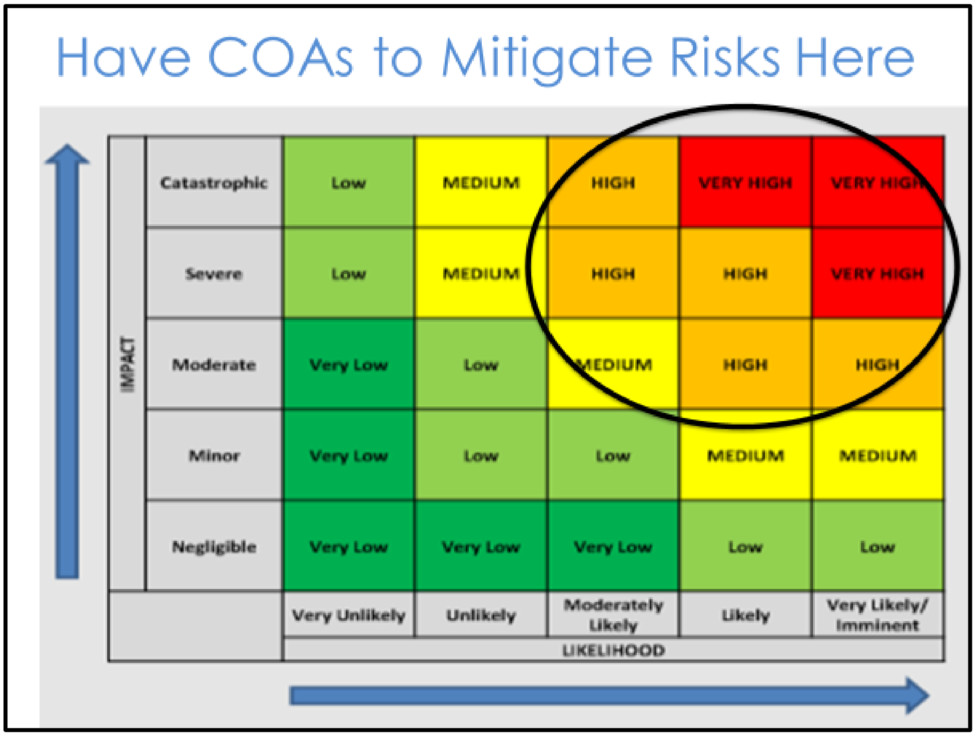
Methods for conducting COA analysis include:

- Developing decisive points and lines of operation
- Leveraging capabilities such as air operations, force mobility, and firepower
- Identifying vulnerabilities, such as limited forces and credibility
- Assessing critical requirements like consent, situation awareness, freedom of action, and rules of engagement (ROE)
- Evaluating critical capabilities of own forces that may be vulnerable
- Utilising an effects matrix or schematic

Each COA should consider aspects such as the significant effort, type of manoeuvre/movement, integration of other units, support, and civil partners, command, control, and communications, threats and risks, suitability, feasibility, acceptability, and political and humanitarian impacts.

The COA analysis and comparison are presented to the commander for decision-making. The commander reviews each COA, considering their strengths, weaknesses, likely reactions from spoilers, and UN-specific criteria (ROE, UN principles, FP, POC, etc.). Based on this information, an informed decision is made regarding which COA to refine and develop. The staff must provide a detailed Course of Action Analysis, Selection Comparison (COA Advantages/Disadvantages), and recommend a COA.

Slide 11



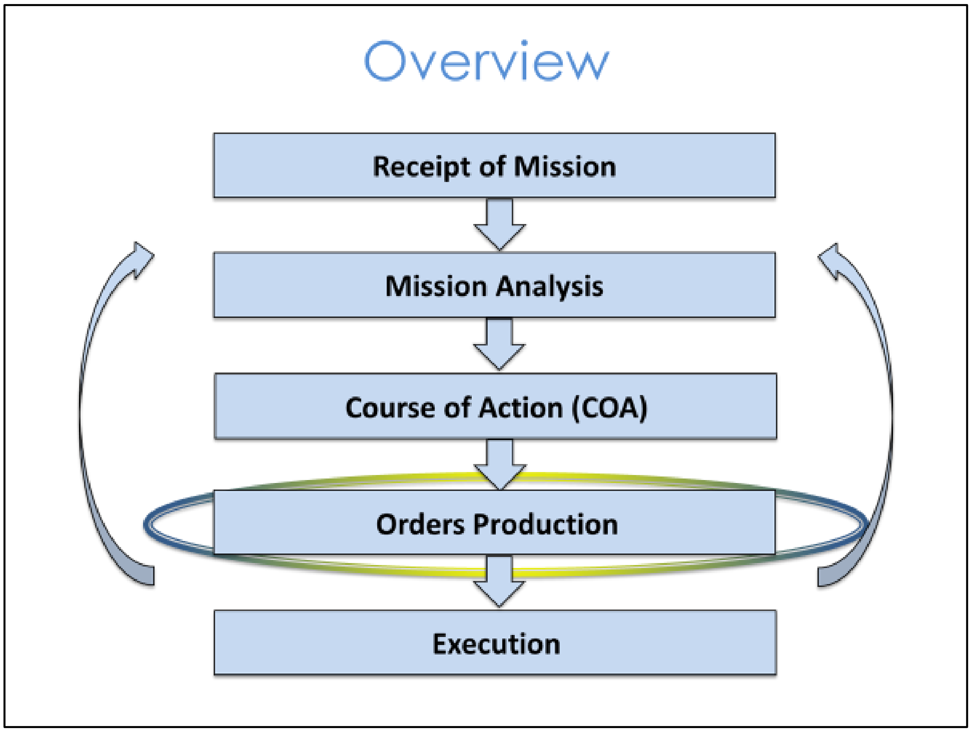
Have COAs to Mitigate Risks Here

IMPACT					
Catastrophic	Low	MEDIUM	HIGH	VERY HIGH	VERY HIGH
Severe	Low	MEDIUM	HIGH	HIGH	VERY HIGH
Moderate	Very Low	Low	MEDIUM	HIGH	HIGH
Minor	Very Low	Low	Low	MEDIUM	MEDIUM
Negligible	Very Low	Very Low	Very Low	Low	Low
	Very Unlikely	Unlikely	Moderately Likely	Likely	Very Likely/ Imminent
	LIKELIHOOD				

In the planning process, performing a comprehensive risk analysis of threats is crucial. Risk encompasses both the likelihood of a threat occurring and its impact on your operation and freedom of action. By prioritising planning efforts based on the level of risk posed by each threat, you can allocate resources and develop suitable strategies. Follow these steps for an effective risk analysis:

- Identify Threats: Analyse and identify potential threats that could jeopardise and impact your mission/ operation
- Assess Likelihood: Evaluate the probability of each threat using peacekeeping-intelligence and predictive analysis
- Evaluate Impact: Analyse the potential consequences of each threat on your operation
- Determine Risk Levels: Combine the likelihood and impact assessments to calculate the overall risk level for each threat, prioritising those with the highest potential impact and likelihood

Slide 12



Overview

Receipt of Mission

Mission Analysis

Course of Action (COA)

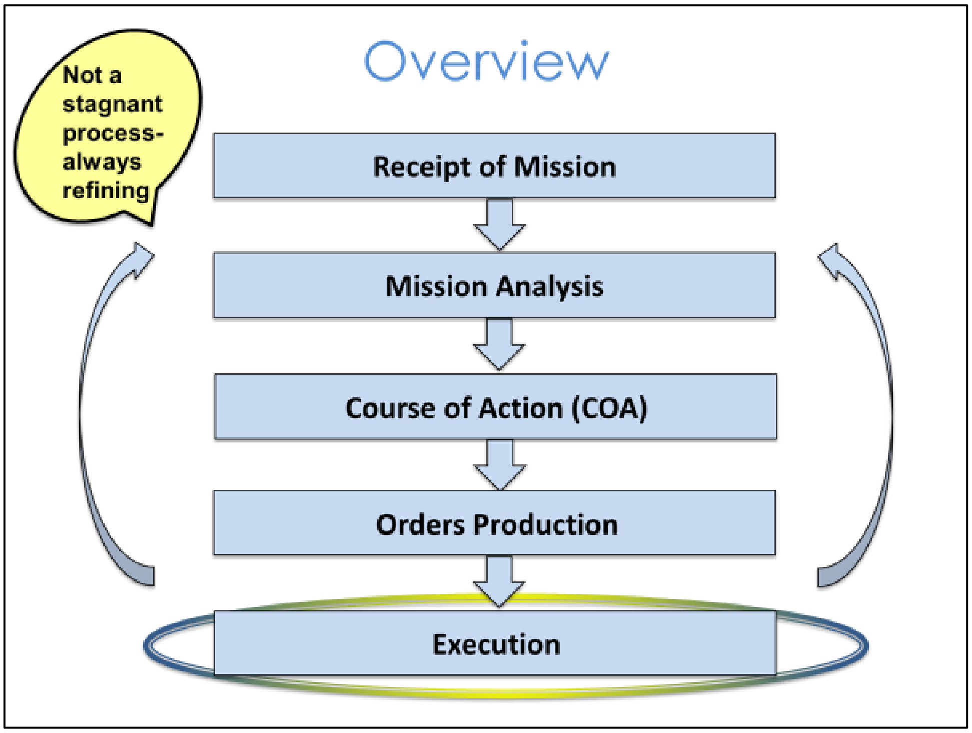
Orders Production

Execution

The staff takes responsibility for preparing, coordinating, authenticating, reviewing, publishing, and distributing orders and plans. The operations officer leads this process, while staff sections collaborate with staff primaries to develop the OPLAN or OPORD. The commander receives updates, stays informed about the content and process, and ultimately grants final approval.

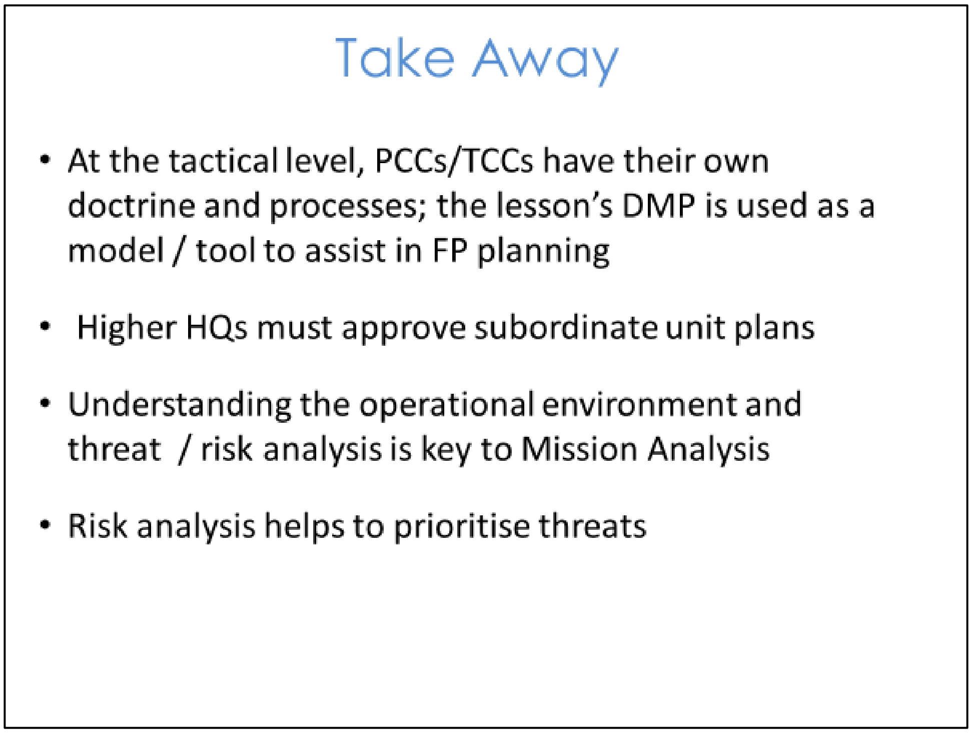
The headquarters ensures order consistency and alignment with the higher commander's intent through reconciliation and order crosswalks. The order undergoes briefing and presentation to the higher headquarters for final review and approval, with necessary resources provided by the higher HQs. This process remains dynamic and continuous, adapting to new information and changes in the environment.

Slide13



During the execution phase, both the staff and commanders maintain an ongoing assessment of the situation which may necessitate revisiting or restarting the planning cycle. Rehearsals play a crucial role in the execution process as they provide leaders troops and police with an opportunity to practise various aspects of the concept of operations. These rehearsals assist units in familiarising themselves with their assigned tasks, and the operational environment, and coordinating with supporting units prior to executing the operation. By engaging in these actions, units enhance their orientation and preparedness, ensuring a smoother execution of the operation.

Slide 14



Take Away

- At the tactical level, PCCs/TCCs have their own doctrine and processes; the lesson's DMP is used as a model / tool to assist in FP planning
- Higher HQs must approve subordinate unit plans
- Understanding the operational environment and threat / risk analysis is key to Mission Analysis
- Risk analysis helps to prioritise threats

Summary

- At the tactical unit level, PCCs/TCCs use their own DMP doctrine; this lesson provides a model and tool to support Force Protection (FP) planning efforts
- Subordinate unit plans require approval from higher headquarters, ensuring alignment and coherence with the mission objectives and support
- A comprehensive understanding of the operational environment and conducting a thorough threat/risk analysis are fundamental components of Mission Analysis
- Risk analysis plays a vital role in prioritising threats, allowing for the identification and focus on those with higher potential impacts and likelihood to manifest and helps in resource allocation and mitigation strategies

Lesson 1.5

Intro to the Tactical Decision-Making Process (Police)

Starting the Lesson

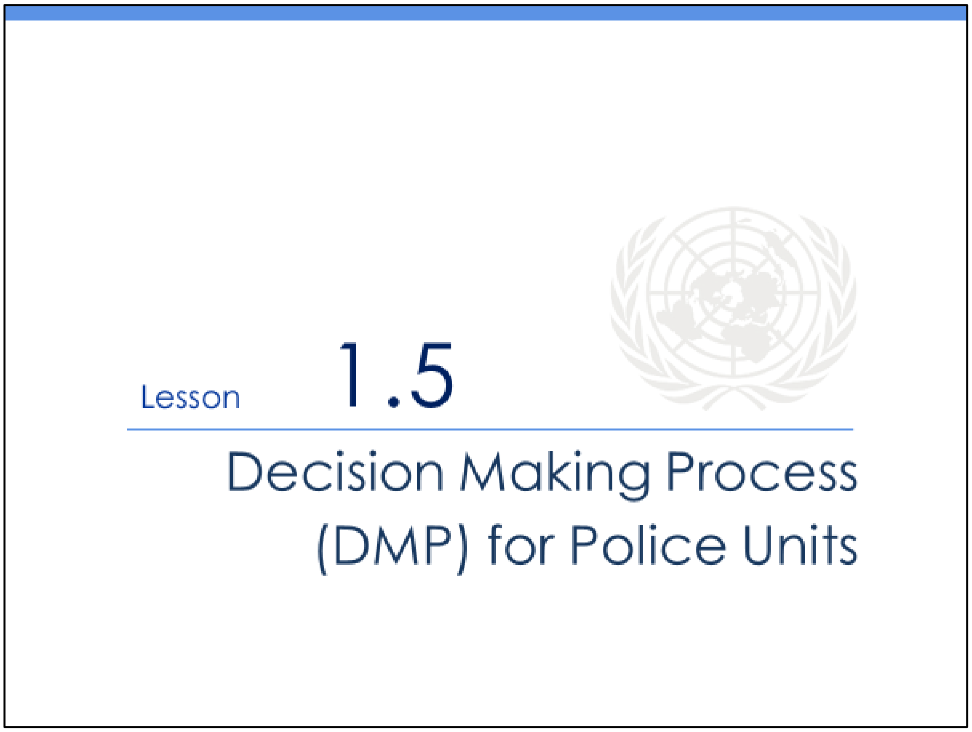
The goal of this lesson is to familiarise participants with tactical planning in PKOs. Tactical planning in peacekeeping operations is a complex and multidimensional process that includes various components. Successful operations require a comprehensive planning and decision-making process. Staffs and commanders must seek optimal solutions and make informed decisions.

The planning process determines requirements needed to accomplish the task. In a UN peacekeeping mission, the relevant planning documents, such as Security Council Resolutions, Integrated Strategic Framework (ISF), and Mission Concept, provide guidance.

At the tactical level, each police contributing country (PCC) has its own decision-making process based on national doctrine. This module aims to highlight how commanders and their staff must integrate UN planning documents, and also, must consider factors like Force Protection, Protection of Civilians (POC), Child Protection, Conflict-Related Sexual Violence (CRSV), and understand the police tasks that support the mission. The lesson provides tactical PKO planning guidance and tools for police contributing countries (PCCs) to incorporate into their planning process.

It is suggested that the instructor review the DPO Policy (Revised) on Formed Police Units in United Nations Peacekeeping Operations.

Slide 1



Lesson 1.5

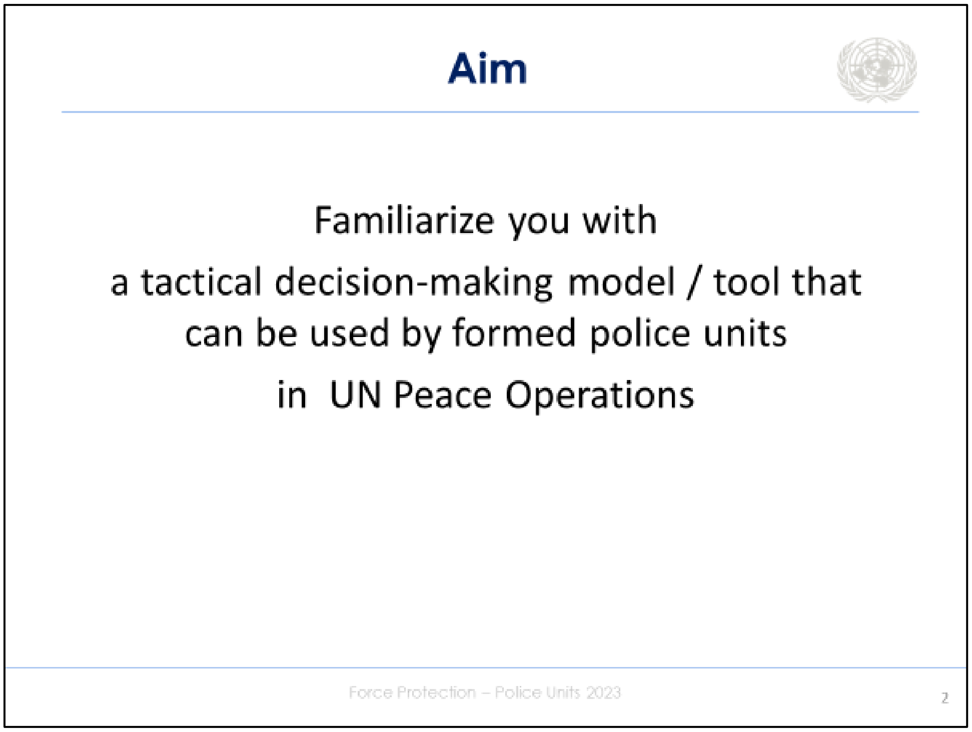
Decision Making Process (DMP) for Police Units

The police decision-making process is a continuous cycle that involves assessing the situation in uncertain and rapidly changing conditions. It requires systematic information collection, critical thinking, and the ability to assess and take initiative.

Understanding the unique process of tactical planning in a Peacekeeping Operation is crucial for successful police operations. It relies on a planning process that involves staff and commanders seeking optimal solutions and making decisions to achieve objectives in a dynamic and dangerous PKO environment.

This process is not an isolated planning mechanism. It is supported by mechanisms such as liaison among different layers of all mission components. In this lesson, we will introduce tactical planning considerations, tools and guidance that can assist member states in integrating and implementing their own planning and decision-making process.

Slide 2



Aim

Familiarize you with

a tactical decision-making model / tool that can be used by formed police units

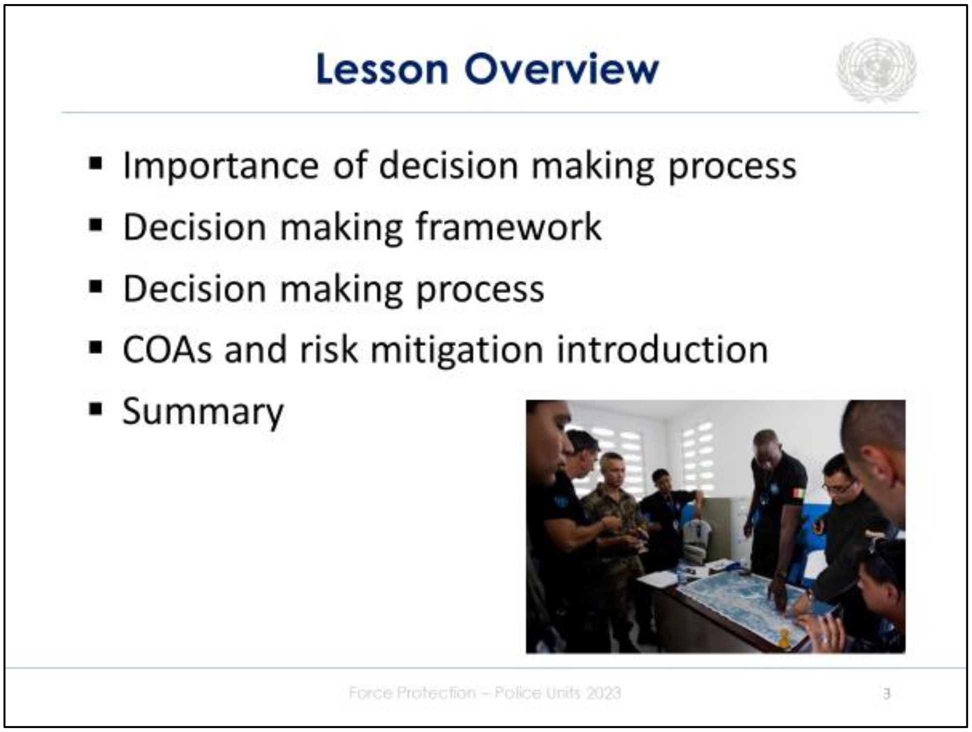
in UN Peace Operations

Force Protection – Police Units 2023

2

The aim of this lesson is to familiarise you with a tactical decision-making model / tool that can be used by formed police units in UN Peace Operations.

Slide 3



Lesson Overview

- Importance of decision making process
- Decision making framework
- Decision making process
- COAs and risk mitigation introduction
- Summary

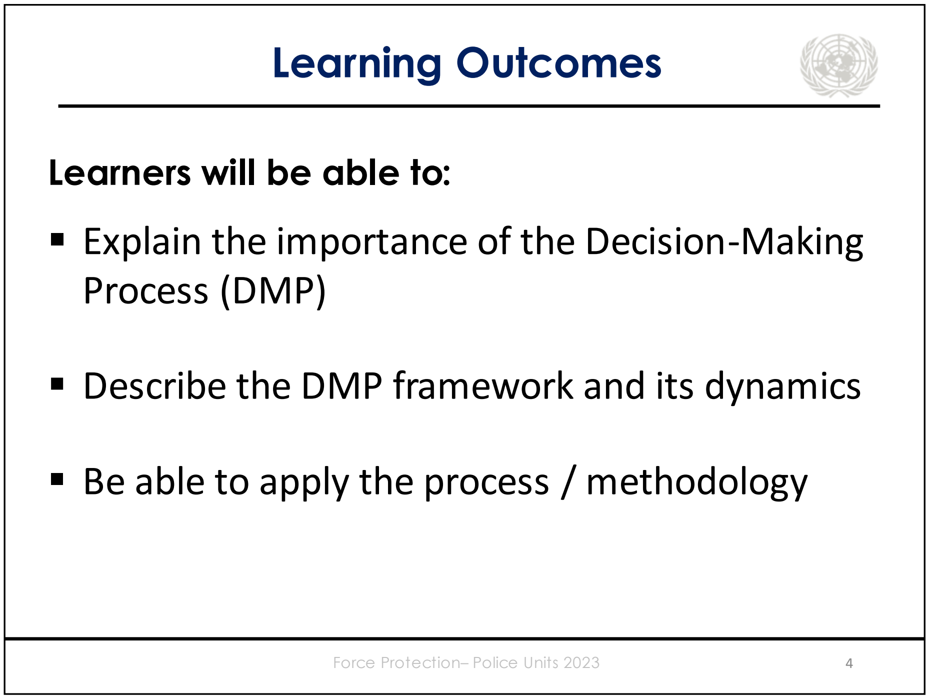
Force Protection – Police Units 2023

3

Here is the content of this lesson. We will explain tactical considerations and guidance to be used for planning for force FP. The lesson will also, review the risk analysis and assessment concept.

- Importance of a decision-making process
- Decision-making framework
- Decision-making process
- COAs and risk mitigation introduction
- Summary

Slide 4



Learning Outcomes

Learners will be able to:

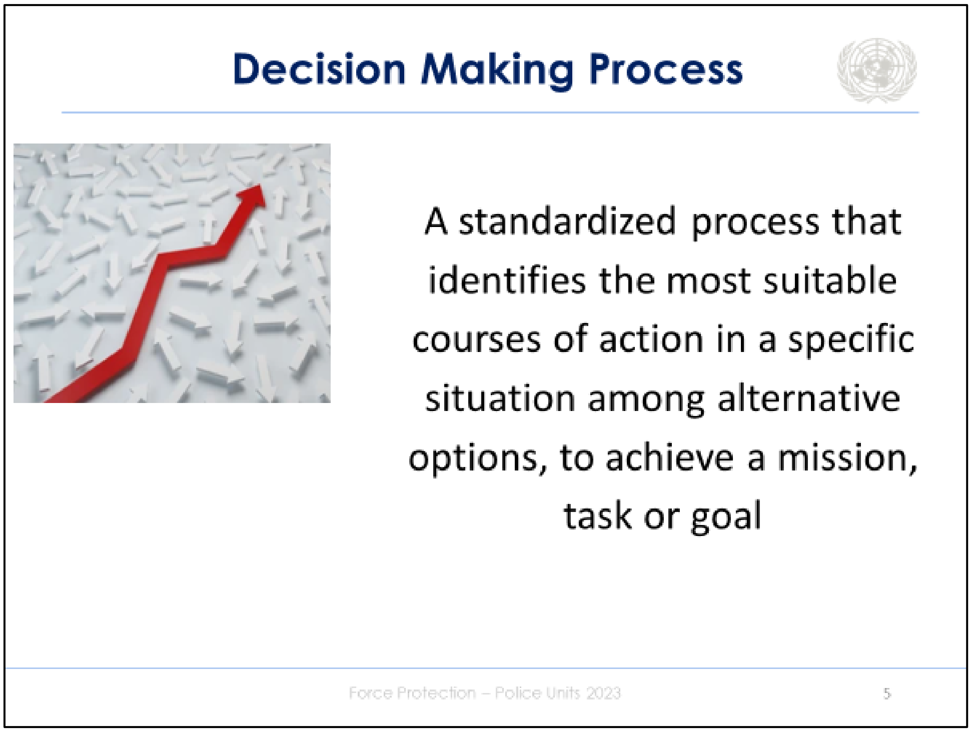
- Explain the importance of the Decision-Making Process (DMP)
- Describe the DMP framework and its dynamics
- Be able to apply the process / methodology

Force Protection– Police Units 2023 4

To ensure effective training, let's review the learning outcomes of this lesson. By the end of this lesson, you will acquire the skills necessary to perform the actions outlined on the slide. Please take a moment to carefully read and understand the requirements. This will enable you to focus on the most pertinent aspects. By completing this lesson, learners will be able to:

- Explain the importance of the Decision-Making Process (DMP).
- Describe the DMP framework and its dynamics.
- Be able to apply the process / methodology.

Slide 5



Decision Making Process

A standardized process that identifies the most suitable courses of action in a specific situation among alternative options, to achieve a mission, task or goal

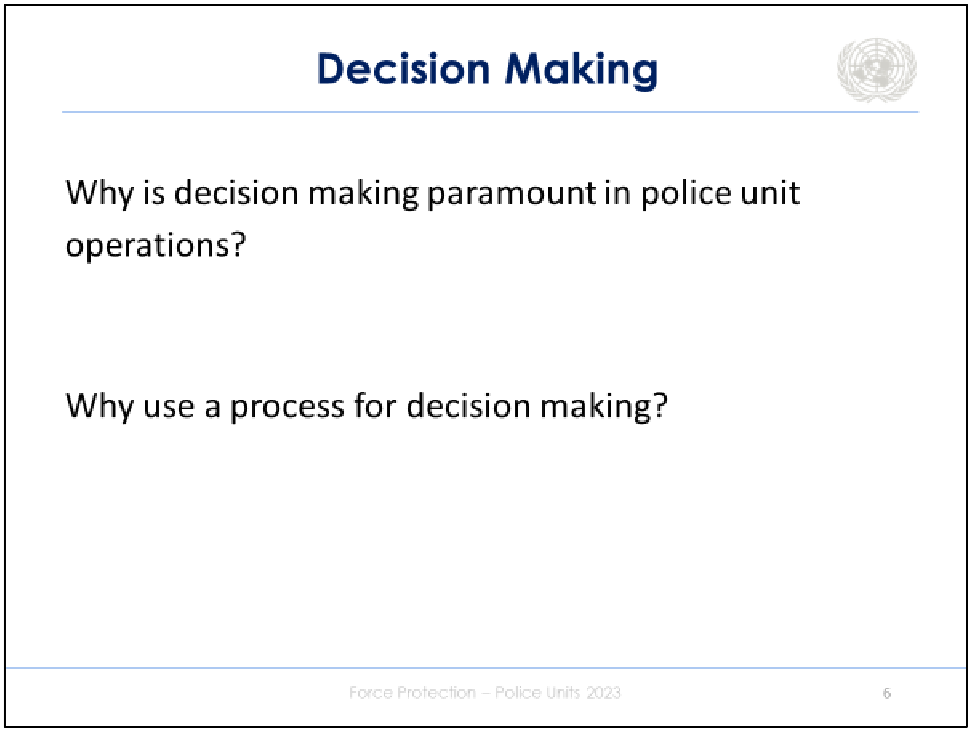
Force Protection – Police Units 2023

5

The Decision-Making Process (DMP) is a standardised approach that enables the identification of the most suitable course of action in a specific situation from various alternatives. Its purpose is to achieve a desired goal and effectively manage the resulting consequences. The process involves continuously assessing the situation, which is often characterised by uncertainty and rapid change. This necessitates systematic information collection, critical thinking, and the ability to assess and take initiative.

To conduct thorough information gathering, optimal cooperation, timely coordination, and high flexibility are crucial. It is important to recognise that the DMP is a methodology for thinking, not just a checklist. When applied correctly, it enhances understanding of the environment, enables problem analysis, identifies vulnerabilities, and promotes a proactive approach.

Slide 6



Decision Making

Why is decision making paramount in police unit operations?

Why use a process for decision making?

Force Protection – Police Units 2023

6

For discussion:

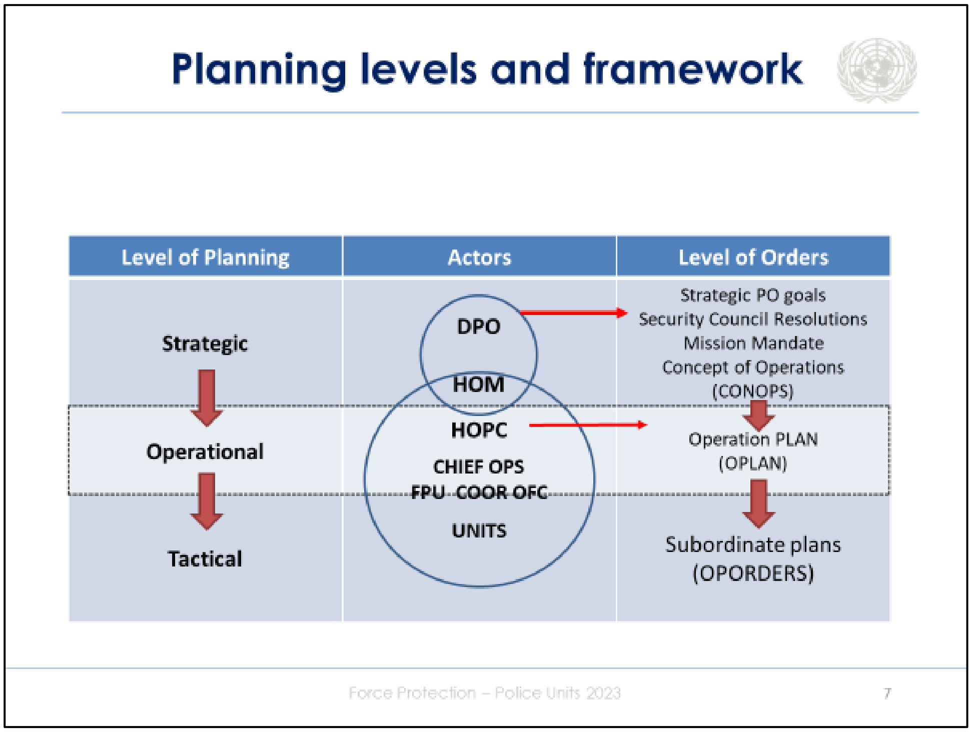
Ask the group to explain the following:

- *Why is decision-making paramount in police unit operations?*
- *Why use a process for decision-making?*

To ensure successful planning, it is key that police unit operations should be planned. Here are some points for discussion:

- *A systematic DMP supports the operator to ensure all aspects are considered in decision-making.*
- *When DMP is used, decisions will be guided on facts and assumptions, the rule of Rule of Law as it applies to the mission, the mandate.*
- *A nested approach to logically flow from strategic- and mission-level guidelines and orders to tactical orders.*

Slide 7



Planning levels and framework

Level of Planning	Actors	Level of Orders
Strategic	DPO HOM	Strategic PO goals Security Council Resolutions Mission Mandate Concept of Operations (CONOPS)
Operational	HOPC CHIEF OPS FPU COOR OFC	Operation PLAN (OPLAN)
Tactical	UNITS	Subordinate plans (OPORDERS)

Force Protection – Police Units 2023 7

This slide provides an overview of the different planning processes in the UN system and how they eventually impact tactical operations on the ground. This will help to understand the complexity of planning in the context of UN Peacekeeping:

- Mission-specific planning is part of the broader UN-wide planning process, which takes initial guidance from the Executive Office of the Secretary-General

- At UN Headquarters, DPO will develop a Mission Concept, which is a strategic level articulation of what the field mission will do and how. Under the Mission Concept are military, police and support concepts that provide more details

- The Mission Concept will inform the development of a Mission Plan, which is the Mission's operational plan of how to implement the mandate. The Mission Plan must be aligned with the Integrated Strategic Framework (ISF), where it exists. The purpose of an ISF is to bring together the mission and the UNCT's mandates around a set of agreed priorities

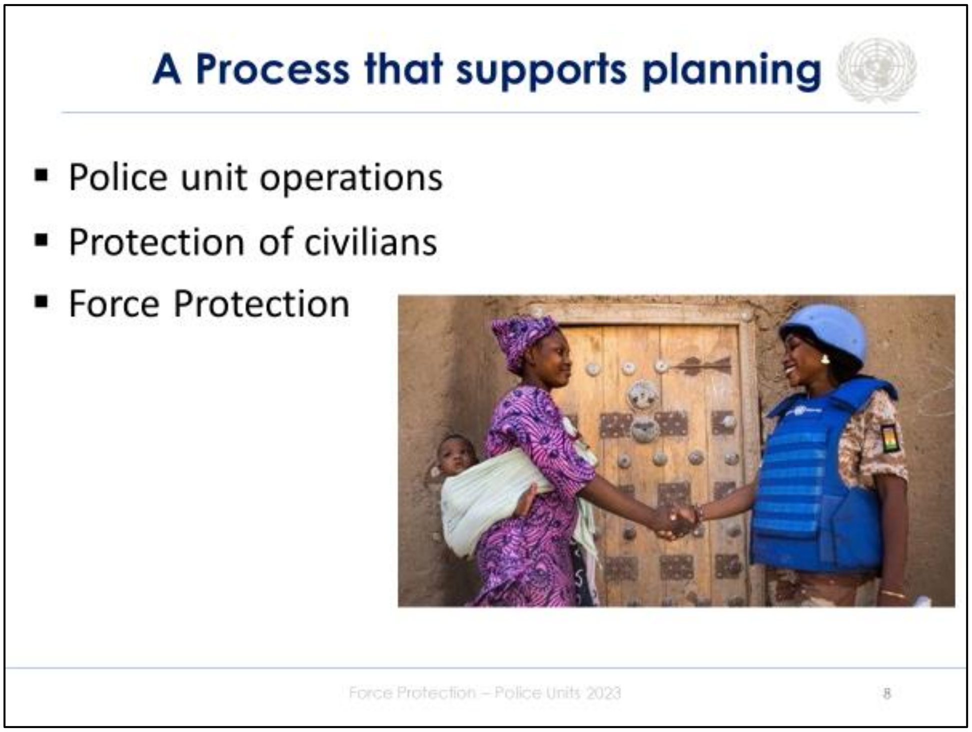
- Each component in the Mission should have component-level plans such as annual work plans aligned with the overall Mission Concept and Mission Plan

- The Mission may have mission-wide strategies on cross-cutting issues such as the Protection of Civilians, child protection and gender mainstreaming.

- The command of police units is vested in the HOPC or his or her delegates, Deputy-Chief Ops (FPU) and Regional Commanders. The police units receive missions via an OPLAN.

- Plans or OPORDERS will guide the unit’s implementation on the ground and should be continuously updated based on evolving conflict analysis and should help determine when a change of course is needed.

Slide 8



A Process that supports planning

- Police unit operations
- Protection of civilians
- Force Protection

Force Protection – Police Units 2023 8

The Decision-Making Process (DMP) plays a vital role in supporting the planning and implementation of various critical aspects within a peacekeeping operation. It extends its support to:

Police Unit Operations: The DMP aids in the planning and execution of police unit operations. It assists in determining the most effective strategies, tactics, and resources needed to fulfil the mission objectives.

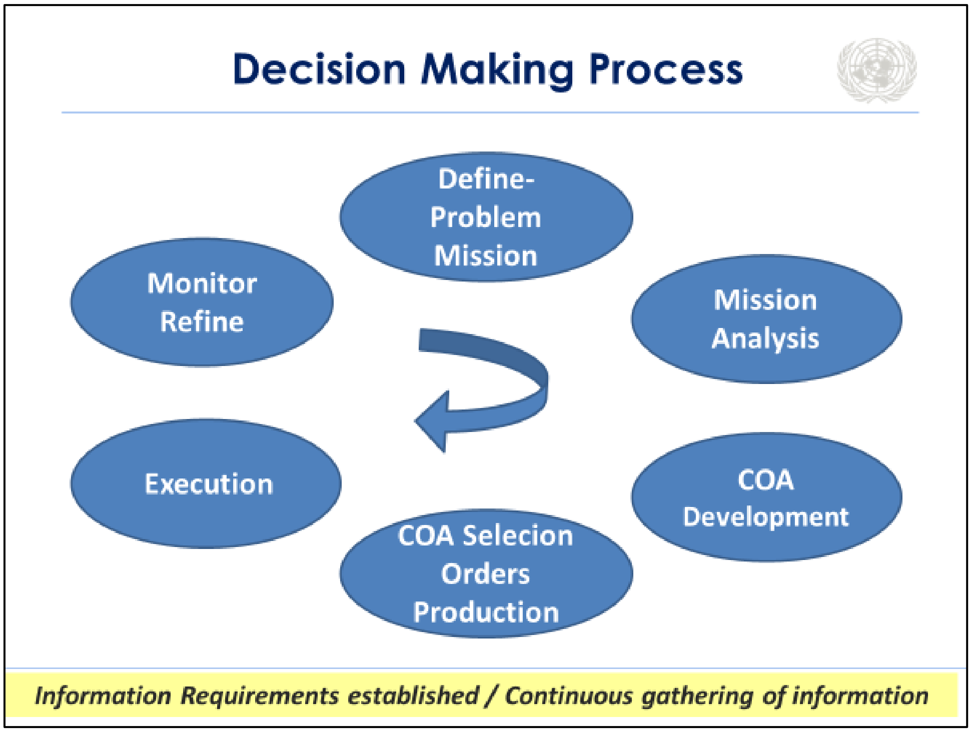
Protection of Civilians: Within the context of peacekeeping, protecting civilians is of utmost importance. The DMP provides a structured approach to assess the risks faced by civilians and develop comprehensive plans and actions to ensure their safety and security.

Force Protection: Ensuring freedom of action and mitigation of risks, FP is a key priority. The DMP assists in analysing threats, vulnerabilities, and risks to devise appropriate measures for force protection. It aids in identifying and implementing proactive measures to mitigate risks and maintain the mission's success.

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 FP and POC Planning in parallel with other mission planning. The product of FP Planning is a consideration to be incorporated in all mission planning.

Of note, all strategic and operational level planning processes related to Peacekeeping Operations must comply with the appropriate UN Policies, promote human rights, Strengthen the rule of law, Prevent / reduce conflicts, empower women, and help Deliver humanitarian and field support.

Slide 9



Decision Making Process

Define-Problem Mission

Mission Analysis

COA Development

COA Selecion Orders Production

Execution

Monitor Refine

Information Requirements established / Continuous gathering of information

Effective planning serves as the foundation for successful unit operations. Tactical planning processes for tactical units are aligned with their respective national doctrines. Each Police Contributing Country (PCC) has its own distinct planning process, while the UN has established a process aimed at enhancing interoperability.

The slide presents a tool that aids in explaining tactical planning considerations for PCCs to integrate into their planning process within a Peacekeeping Operation. To facilitate the seamless incorporation of Force Protection (FP) and Protection of Civilians (POC) into peacekeeping operations, staff members should consider utilising the tool provided as a guide. They can adapt it to suit their specific planning process, ensuring a comprehensive approach to planning and execution.

- Define the problem / the mission
- Mission analysis
- Course of Action (COA) development
- COA selection and orders production
- Execution
- Monitor the execution and refine the plan

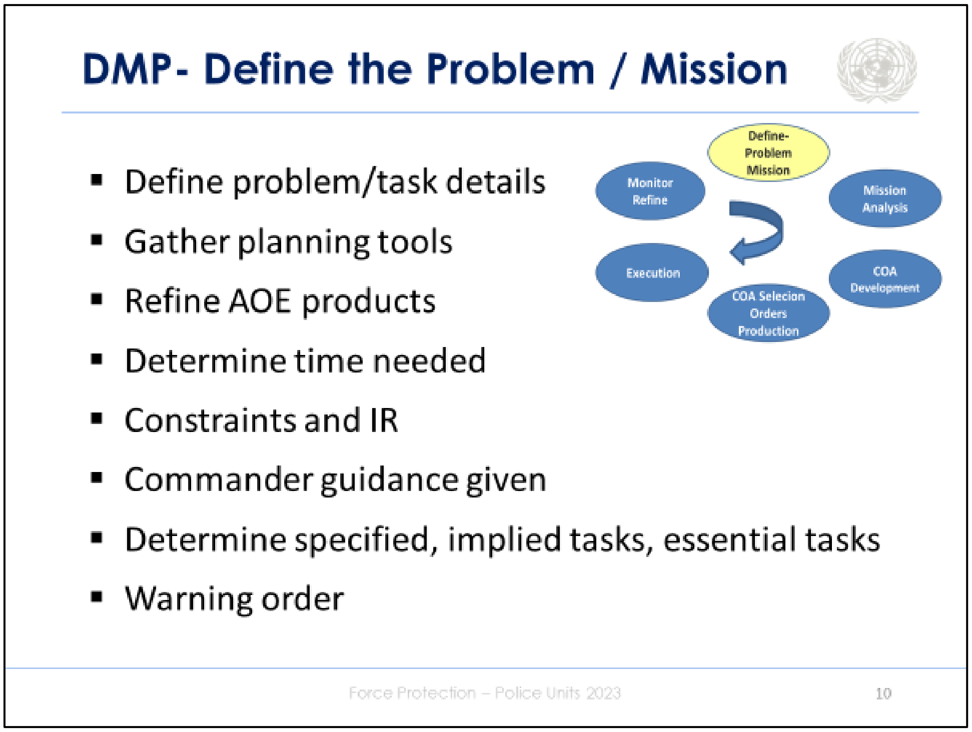
In the upcoming slides, we will delve into each step of this comprehensive planning guide. It is important to note that although the guide is presented in a linear and phased manner, the tactical planning process itself is far from being linear. It is a dynamic, cyclic, and continuous process that requires constant review and refinement.

Tactical planning is not a static endeavour; it necessitates ongoing updates to analytical products, decisions, and orders to accurately reflect the evolving threats, risks, environment, and objectives. It is crucial to recognise that tactical planning is an inclusive staff process, involving the collaboration and input of the entire staff.

Furthermore, Information Requirements (IRs) are continuously established, and units and staff engage in continuous information gathering. This ongoing information gathering assists in refining existing Courses of Action (COAs), and plans, or addressing planning assumptions and validating facts.

By understanding the iterative nature of the tactical planning process, continuously adapting to changing circumstances, and engaging in active information gathering, the staff can ensure that their planning remains agile, accurate, and responsive to the operational environment.

Slide 10



DMP- Define the Problem / Mission

- Define problem/task details
- Gather planning tools
- Refine AOE products
- Determine time needed
- Constraints and IR
- Commander guidance given
- Determine specified, implied tasks, essential tasks
- Warning order

Define-
Problem
Mission
Mission
Analysis
COA
Development
COA Selecion
Orders
Production
Execution
Monitor
Refine

Force Protection – Police Units 2023 10

The initiation step serves the purpose of notifying all participants about the planning requirements, the available time for planning, and establishing the planning approach. When a new mission is identified, commanders and staff engage in the following actions:

Define the Problem and Mission/Task Details: Clearly articulate the problem at hand and gather comprehensive details about the mission or task.

Gather Planning Tools and Documents: Collect the necessary planning-related documents, including the operation order from higher headquarters, maps, terrain products, and running estimates.

Update and Refine Analysis of the Operating Environment (AOE) Products: Continuously update and refine the analysis of the operating environment to ensure accurate situational awareness.

Determine Planning and Preparation Time: Assess the time required for effective planning and preparation for the mission.

Identify Constraints and Information Requirements: Begin identifying the constraints that may impact the planning process and determine the specific information requirements needed.

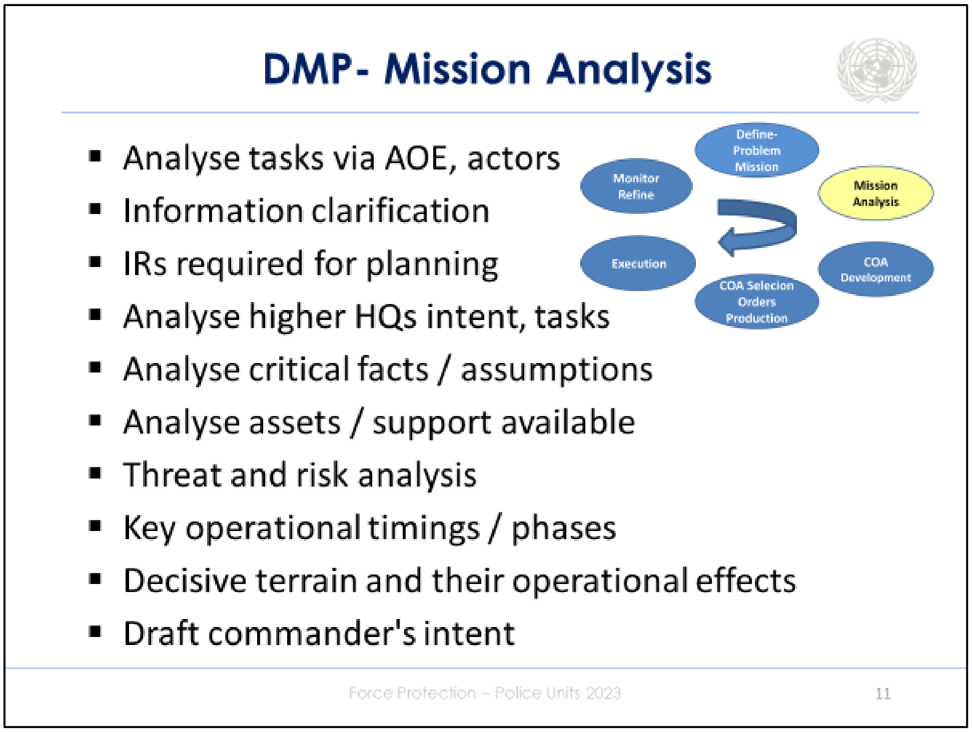
Commander's Planning Guidance: The commander provides planning guidance to the staff, outlining key objectives and priorities.

Conduct Initial Assessment and Identify Essential Tasks: Conduct an initial assessment to identify the specified tasks, implied tasks, and mission essential tasks.

Alert Key Personnel and Issue Warning Order: Notify key personnel about the upcoming mission and issue a warning order, providing initial instructions and highlighting critical information.

By initiating these steps, the planning process is set in motion, ensuring that all participants are informed, prepared, and focused on accomplishing the mission effectively.

Slide 11



DMP- Mission Analysis

- Analyse tasks via AOE, actors
- Information clarification
- IRs required for planning
- Analyse higher HQs intent, tasks
- Analyse critical facts / assumptions
- Analyse assets / support available
- Threat and risk analysis
- Key operational timings / phases
- Decisive terrain and their operational effects
- Draft commander's intent

Define-
Problem
Mission
Mission
Analysis
COA
Development
COA Selecion
Orders
Production
Execution
Monitor
Refine

Force Protection – Police Units 2023 11

Mission Analysis is a crucial tool within the planning process, serving as a foundation for effective decision-making. It involves taking the higher-level guidance provided to the planners, critically evaluating it against the facts and assumptions, and refining it to develop a comprehensive understanding of the mission and its planning requirements.

This process leads to the formulation of a restated mission, planning guidance, and Commander's intent, which incorporates the purpose, method, and desired end state of the mission. Deduction and analytical frameworks play a central role in this process, organising information under various headings, including:

Analysing Tasks through Analysis of the Operating Environment (AOE) and Actors: Examining the tasks required within the operational environment, considering the actors involved and their roles.

Information Clarification: Ensuring clarity and understanding of all relevant information pertaining to the mission.

Information Requirements (IRs) for Planning: Identifying the specific information needed to support the planning process.

Analysing Higher Headquarters' Intent and Tasks: Evaluating the intent and tasks set by higher headquarters and understanding their implications for the mission.

Analysing Critical Facts and Assumptions: Analysing the critical facts and underlying assumptions that affect the planning process.

Analysing Available Assets and Support: Assessing the assets and support available for the mission and considering their impact on planning.

Threat and Risk Analysis: Conducting a comprehensive analysis of threats and risks associated with the mission.

Key Operational Timings and Phases: Identifying the critical operational timings and phases that need to be considered during planning.

Drafting Commander's Intent: Developing a preliminary commander's intent that provides clear direction and objectives for the mission.

By undertaking these analytical steps, mission analysis enables planners to gain a thorough understanding of the mission, clarify information requirements, assess risks, and establish the commander's intent. It sets the stage for the subsequent planning process, ensuring a solid foundation for effective mission execution.

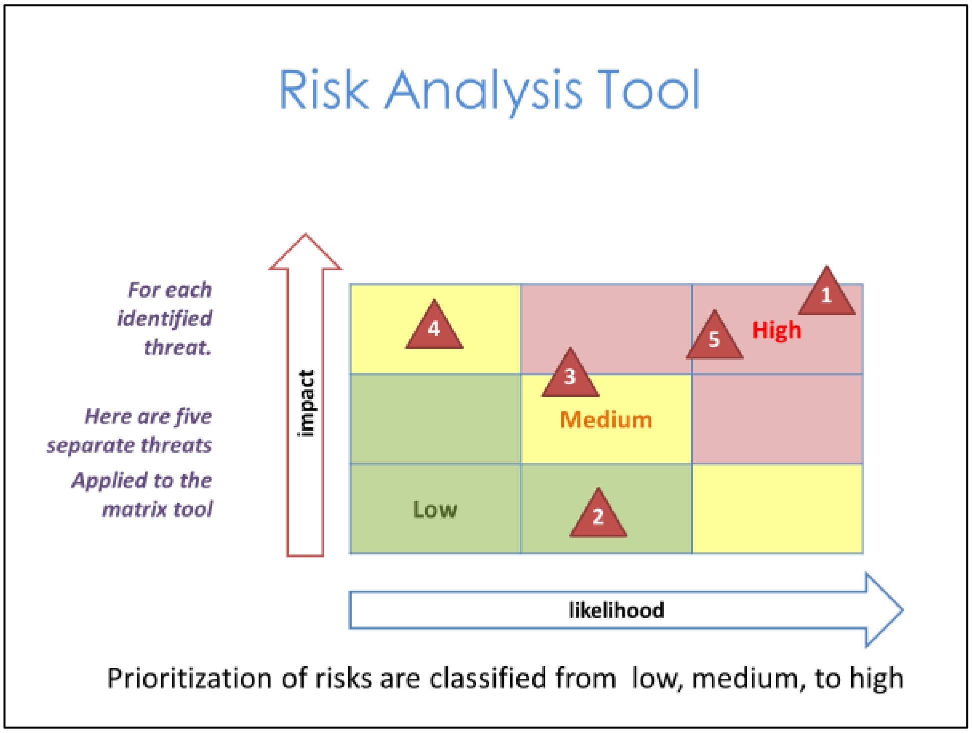
Internal and external staff communications are vital for planning / mission success. Discuss what you do to facilitate dialogue and sharing of information.

Ask the participants:

- *What are the essential elements of intent?*
- *What is the relationship between specified task, implied task/s, and mission essential tasks?*

Facilitate discussion and have them explain the purpose (of the Mission/Task), Method, and end state. Some students may find it difficult to phrase the end state. Have them give examples of End-State

Slide 12



Risk Analysis Tool

For each identified threat.

Here are five separate threats Applied to the matrix tool

Prioritization of risks are classified from low, medium, to high

When mitigating risks associated with threats against civilians and our units, conducting a risk analysis is essential for determining the best Course of Action (COA). This slide presents a matrix that can aid in the Decision-Making Process (DMP).

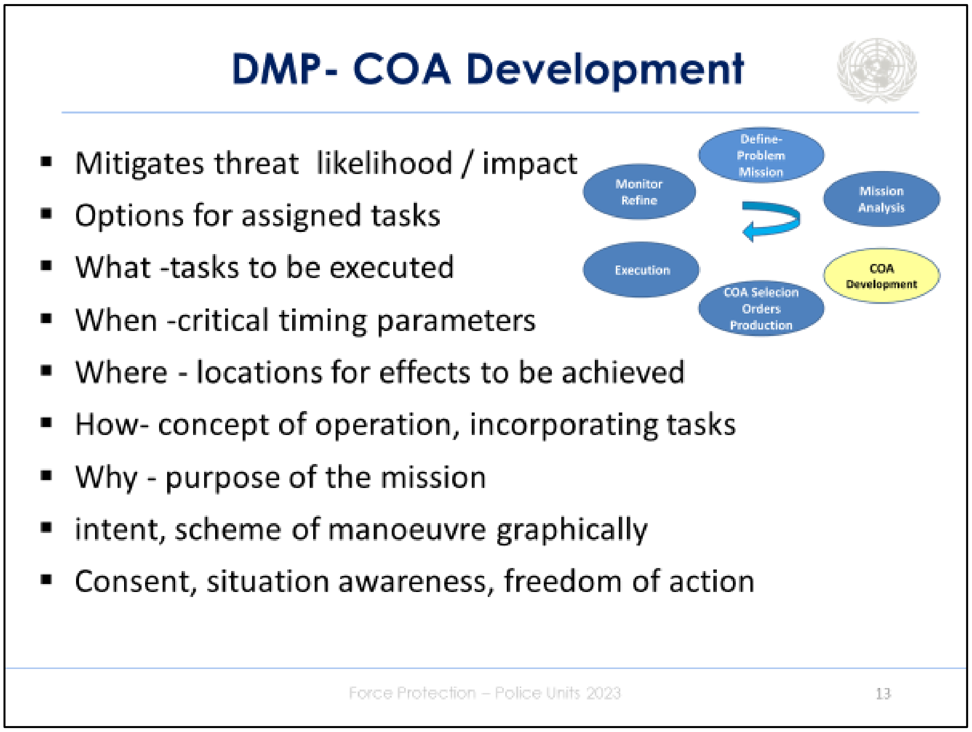
The Risk Analysis Matrix combines the likelihood of an attack and the impact of that attack that identified threats. This process can be used whether it pertains to civilians, UN forces, or UN facilities. Risk, in this context, is determined by both the vulnerability of specific groups and the threats they face. The Risk Analysis Matrix provides a useful framework for breaking down and analysing this information, as depicted on the slide.

On the graph, the vertical "Y" axis represents the Impact, which indicates the consequences that would arise if a threat materialised and affects the at-risk police unit, or civilian population. The "x" axis represents the Likelihood, denoting the probability of a threat materialising. Assessing the likelihood involves considering various factors such as existing human rights reporting, peacekeeping-intelligence inputs, and historical analysis.

In terms of risk assessment, Threat 2 on the graph is classified as low since it exhibits both low impact and low likelihood. On the other hand, Threat 1 is designated as high because it has a high likelihood of occurring and would result in significant impact. The displayed graph or matrix is a sample risk analysis representation, and we will utilise it during the lessons on Force Protection planning considerations in Module 3.

The Risk Analysis Matrix serves as a practical visual tool for evaluating risk, enabling decision-makers to prioritise resources and develop appropriate strategies to address threats. It allows for a systematic assessment of the likelihood and impact of different risks, facilitating informed decision-making and efficient allocation of protective measures. By utilising the Risk Analysis Matrix, organisations can enhance their understanding of the risk landscape and implement effective risk mitigation measures.

Slide 13



DMP- COA Development

- Mitigates threat likelihood / impact
- Options for assigned tasks
- What -tasks to be executed
- When -critical timing parameters
- Where - locations for effects to be achieved
- How- concept of operation, incorporating tasks
- Why - purpose of the mission
- intent, scheme of manoeuvre graphically
- Consent, situation awareness, freedom of action

Define-Problem Mission
Mission Analysis
COA Development
COA Selecion Orders Production
Execution
Monitor Refine

Force Protection – Police Units 2023 13

The purpose of Course of Action (COA) development is to create one or more options that effectively execute the assigned police tasks and fulfil the mission. Here are the key components involved in COA development:

Mitigates Threat Likelihood/Impact: The COA should address and mitigate the likelihood and impact of threats identified during the risk analysis phase. It aims to minimise risks to personnel, equipment, and the mission.

Options for Assigned Tasks: Various options should be considered that align with the assigned tasks and objectives. These options provide flexibility and enable the selection of the most suitable approach to achieve the desired outcomes.

COA should include / or answer the following questions:

- What - Tasks to be Executed: Clearly define the specific tasks that need to be executed as part of the COA. This includes identifying the actions required to address key challenges and accomplish mission objectives.

- When - Critical Timing Parameters: Determine the critical timing parameters associated with the COA. This includes identifying time-sensitive actions, synchronisation requirements, and key milestones that must be met for successful execution.

- Where - Locations for Effects to be Achieved: Identify the specific locations where desired effects and outcomes are to be achieved. This involves considering the geographic areas where the COA will be implemented and its impact on the overall mission.

- How - Concept of Operation, Incorporating Tasks: Develop a concept of operation that outlines how the COA will be executed. This includes integrating the identified tasks, resources, and coordination mechanisms necessary for effective implementation.

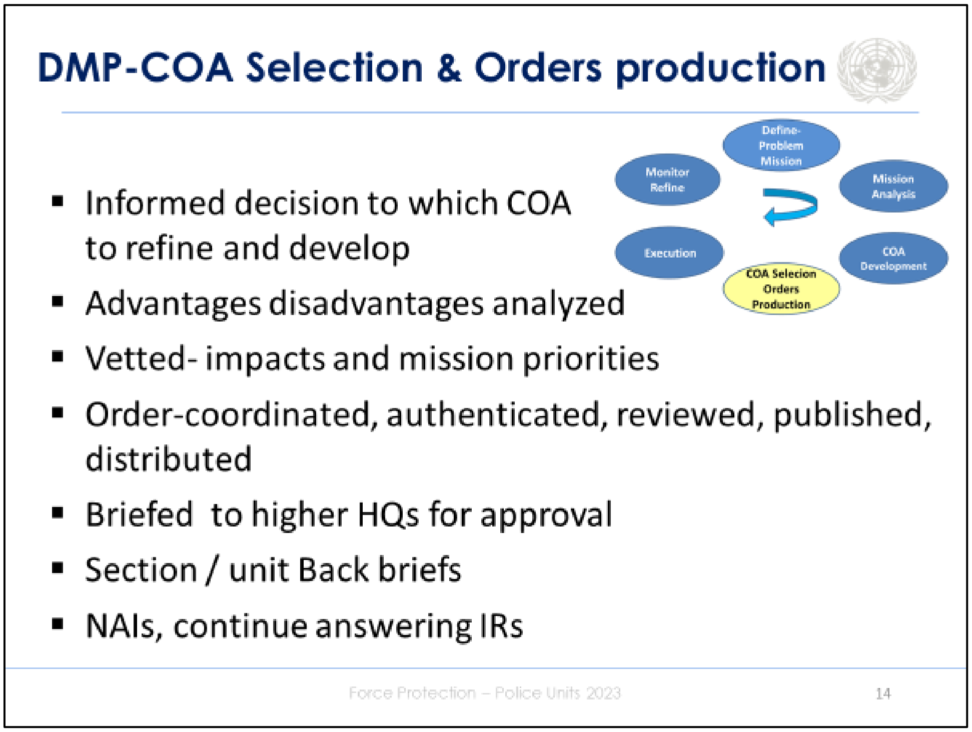
- Why - Purpose of the Mission: Clearly articulate the purpose and underlying objectives of the mission. This provides a strategic context and ensures that the COA aligns with the broader mission goals and intentions.

Intent, Scheme of Manoeuvre Graphically: Communicate the intent and desired outcomes of the COA through a graphical representation. This visual depiction helps convey the intended scheme of manoeuvre, highlighting key elements and operational considerations.

Consent, Situation Awareness, Freedom of Action: Consider the need for consent from relevant parties, maintain situational awareness, and ensure freedom of action to execute the chosen COA effectively. This involves assessing the political, legal, and operational aspects that may impact the mission.

By addressing these components during COA development, planners can create well-defined and comprehensive options that optimise the utilisation of resources, mitigate threats, and ensure successful mission execution.

Slide 14



DMP-COA Selection & Orders production

- Informed decision to which COA to refine and develop
- Advantages disadvantages analyzed
- Vetted- impacts and mission priorities
- Order-coordinated, authenticated, reviewed, published, distributed
- Briefed to higher HQs for approval
- Section / unit Back briefs
- NAIs, continue answering IRs

Define-Problem Mission

Mission Analysis

COA Development

COA Selecion Orders Production

Execution

Monitor Refine

Force Protection – Police Units 2023 14

The COA selection and order production involve several key components to ensure a well-informed decision-making process and the effective dissemination of operational instructions. Here are the important elements to consider:

Informed Decision on COA to Refine and Develop: The selection of a specific COA requires a thorough assessment and analysis of each option. This includes evaluating the feasibility, effectiveness, and alignment of each COA with the mission objectives. The decision-making process should be based on accurate and up-to-date information.

Analysis of Advantages and Disadvantages: Each potential COA should undergo a comprehensive analysis of its advantages and disadvantages. This evaluation helps identify the strengths, weaknesses, risks, and potential outcomes associated with each option. The aim is to select the COA that offers the highest probability of success while minimising potential negative impacts.

Vetted Impacts and Mission Priorities: Prior to the COA selection, the impacts and implications of each option must be thoroughly vetted. This involves considering how the COA aligns with mission priorities, operational constraints, available resources, and potential consequences.

Order Production: Once the COA has been selected, the production of operational orders is initiated. This process involves coordinating, authenticating, reviewing, publishing, and distributing the orders to relevant personnel and units. The orders provide clear and concise instructions for executing the chosen COA.

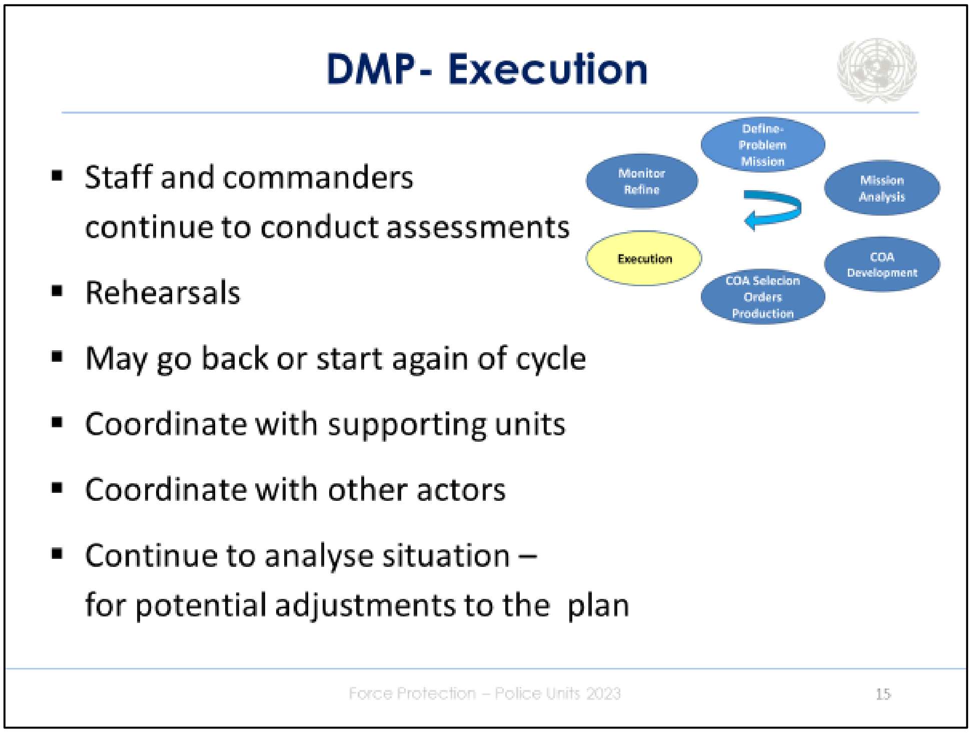
Briefing to Higher Headquarters for Approval: The operational orders, along with the selected COA, are briefed to higher headquarters for approval. This ensures that the decision-making process and the chosen COA are aligned with the strategic objectives and overall command direction. The briefing provides an opportunity for higher-level commanders to provide feedback, adjust if necessary, and grant final approval.

Section/Unit Back Briefs: To ensure effective communication and understanding, sections and units involved in the execution of the COA are required to conduct back briefs. These briefings provide an opportunity for subordinates to present their understanding of the operational orders, their assigned tasks, and any questions or concerns. Back briefs help verify that everyone is aligned and prepared to execute the mission.

NAI Continuation and Information Requirements (IRs): Throughout the COA selection and order production process, the identification and monitoring of Named Areas of Interest (NAIs) continue. Additionally, information requirements (IRs) must be continually addressed to support the planning and execution process. This ensures that the latest information is incorporated into decision-making, and adjustments are made as necessary.

By incorporating these key components into the COA selection and order production process, commanders and staff can ensure that the chosen COA is well-informed, addresses potential advantages and disadvantages, and is effectively communicated to the relevant personnel for successful mission execution.

Slide15



Define-Problem Mission
Mission Analysis
COA Development
COA Selecion Orders Production
Execution
Monitor Refine

DMP- Execution

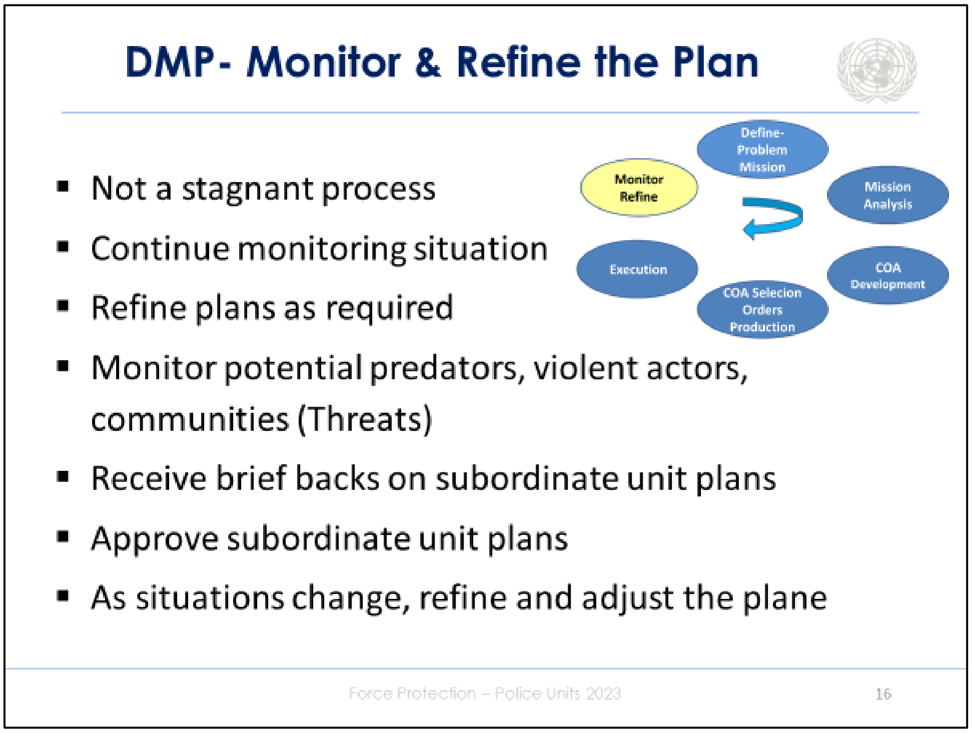
- Staff and commanders continue to conduct assessments
- Rehearsals
- May go back or start again of cycle
- Coordinate with supporting units
- Coordinate with other actors
- Continue to analyse situation – for potential adjustments to the plan

Force Protection – Police Units 2023 15

During the execution step, the staff and commanders continue to conduct assessments of the situation and may require the staff to go back or start again in the planning cycle. Rehearsals are a key element of execution that allows leaders and their troops to practise aspects of the concept of operations. These actions help units orient themselves to their tasks, and environment, and coordinate with supporting units before executing the operation.

- Staff and commanders continue to conduct assessments
- Rehearsals
- May go back or start the cycle
- Coordinate with supporting units
- Coordinate with other actors
- Continue to analyse the situation for potential adjustments to the plan

Slide16



DMP- Monitor & Refine the Plan

- Not a stagnant process
- Continue monitoring situation
- Refine plans as required
- Monitor potential predators, violent actors, communities (Threats)
- Receive brief backs on subordinate unit plans
- Approve subordinate unit plans
- As situations change, refine and adjust the plane

Define-
Problem
Mission
Mission
Analysis
COA
Development
COA Selecion
Orders
Production
Execution
Monitor
Refine

Force Protection – Police Units 2023 16

In the Decision-Making Process- Monitor & Refine the Plan phase, the following key components are involved:

Dynamic Process: The planning process is not stagnant but rather an ongoing and dynamic one. It requires continuous monitoring and evaluation of the situation to ensure that the plan remains relevant and effective.

Situation Monitoring: Throughout the execution phase, it is crucial to monitor the evolving situation. This involves gathering and analysing information, and keeping a close watch on potential threat actors, predator groups, and the communities affected by the operation. By staying informed, the planning team can make informed decisions and take appropriate actions.

Refinement of Plans: Plans may need to be refined and adjusted based on the changing circumstances. As new information becomes available or unexpected challenges arise, it is important to review and modify the plan accordingly. This flexibility allows for better adaptability and improves operational outcomes.

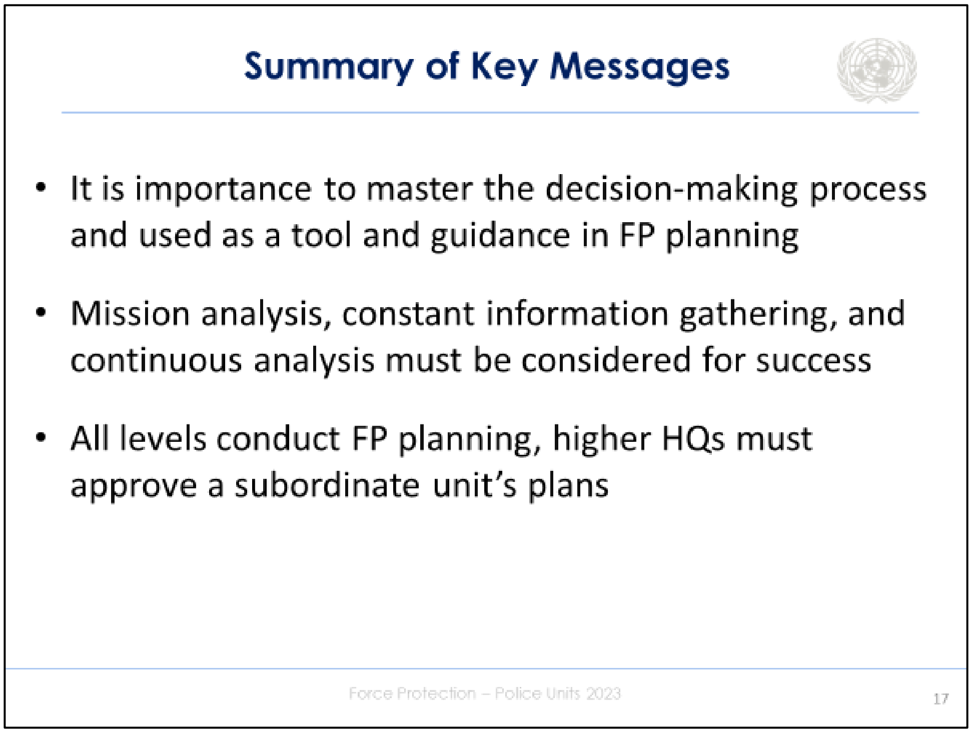
Brief Backs on Subordinate Unit Plans: As part of the monitoring and refinement process, the planning team receives briefings and updates from subordinate units regarding their individual plans. This information exchange ensures coordination and alignment between different units and helps identify any gaps or inconsistencies that need to be addressed.

Approval of Subordinate Unit Plans: The planning team, in its monitoring role, approves the plans developed by subordinate units. This ensures that the overall mission objectives and intent are met, and that the subordinate units are aligned with the larger operational strategy.

Continuous Plan Adjustment: Situations can change rapidly in a dynamic operational environment. Therefore, it is essential to continuously refine and adjust the plan as necessary. This may involve modifying tactics, reallocating resources, or revisiting the operational concept to better address emerging challenges and achieve mission success.

By emphasising the dynamic nature of the planning process, continuous situation monitoring, refinement of plans, monitoring potential threats, receiving briefings from subordinate units, approving their plans, and making necessary adjustments, the DMP - Monitor & Refine the Plan ensures that the mission remains responsive and adaptable to changing circumstances.

Slide 17



Summary of Key Messages

- It is importance to master the decision-making process and used as a tool and guidance in FP planning
- Mission analysis, constant information gathering, and continuous analysis must be considered for success
- All levels conduct FP planning, higher HQs must approve a subordinate unit's plans

Force Protection – Police Units 2023

17

Summary

- The DMP is an important tool used by planners in UNPKOs to facilitate effective decision-making and planning. It helps ensure that decisions are made in a structured and informed manner, contributing to the overall success of peacekeeping operations.
- Mastering the decision-making process is crucial in FP planning within a peacekeeping operation. The DMP serves as a guide, assisting commanders and staff in assessing threats, identifying vulnerabilities, and developing strategies to mitigate risks and protect personnel and assets.
- Mission analysis, continuous information gathering, and ongoing analysis are vital for successful FP planning. Through thorough mission analysis, planners gain a deeper understanding of the operational environment, allowing them to identify potential threats and risks. Constant information gathering keeps planners informed, enabling well-informed decision-making. Continuous analysis allows for adjustments to the plan based on new information and emerging threats.
- FP planning occurs at all levels in a peacekeeping operation. While subordinate units develop their specific plans, higher headquarters have the responsibility of approving these plans. This ensures coherence and alignment with mission objectives. The approval process also allows for a comprehensive review, providing guidance and identifying areas for improvement, ultimately ensuring that plans align with operational requirements and mandates.

Lesson 1.6

Explosive Remnants of War, Improvised Explosive Devices

Starting the Lesson

For an interactive start to this Lesson, ask the participants if they have had experience in a UN Peace Operation with the specific challenges dealing with exposure to explosive threats.

☞***Note to instructor –*** *recommend that the lesson be presented by a trainer who has some personal experience with explosive hazards, EOD expertise, or has worked with UNMAS*

☞ ***Recommend-*** *that instructors review the UN IED Threat Mitigation Handbook and the Landmine, ERW and IED Safety Handbook*

Slide1

Lesson 1.6
Improvised Explosive Devices
(IED)Fundamentals

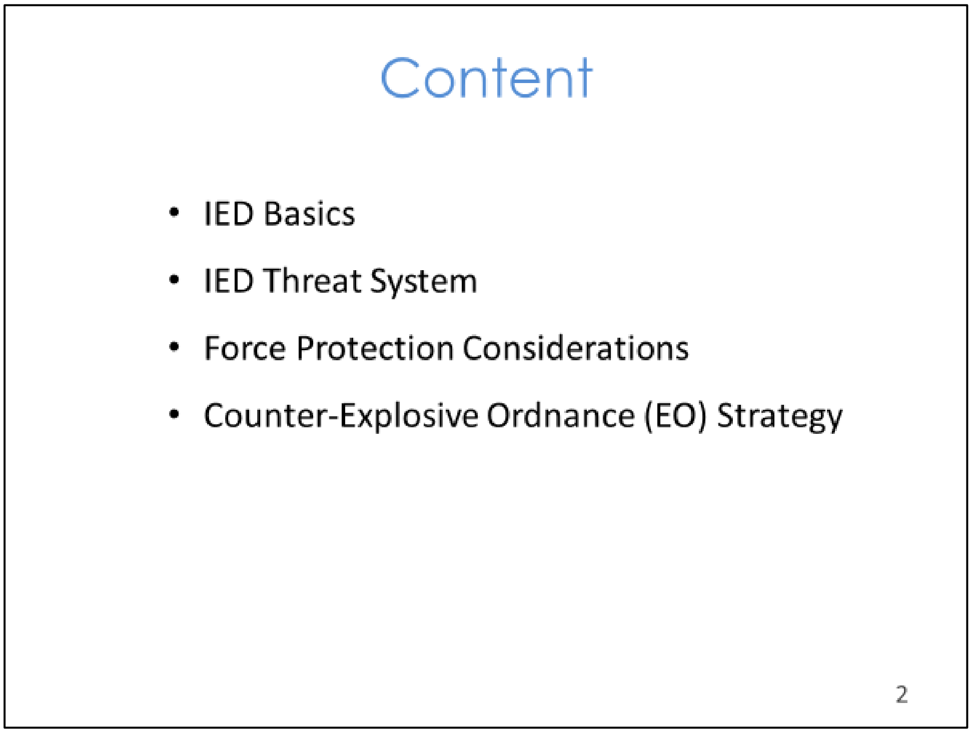
1

IEDs have become the leading cause of casualties for the United Nations. Their improvised nature makes them easy to construct and emplace – and they can have a deadly impact on a mission and UN forces/units. A UN unit operating in an IED environment must take unique and special FP considerations when developing its operational planning. We will help familiarize you with IEDs and some of the FP measures to mitigate risks to the UN force. Here is a UN vehicle after sustaining an IED attack.

Ask the class what are and what they think about the use of IEDs against UN personnel and civilians in the current UNPKO environment. This discussion should take 10 minutes

- *If this goes well, ask them to give a mission example; however, if the students are quiet, prompt them by asking what current missions they know of, what is happening on the ground with IEDs*
- *Follow up by saying that there is a consistent increase in peacekeeper fatalities due to violent acts that have drastically increased over the past years. These numbers go beyond a normal or acceptable level of risk, and they are likely to rise even higher if we do not change our FP posture and mindset*

Slide 2



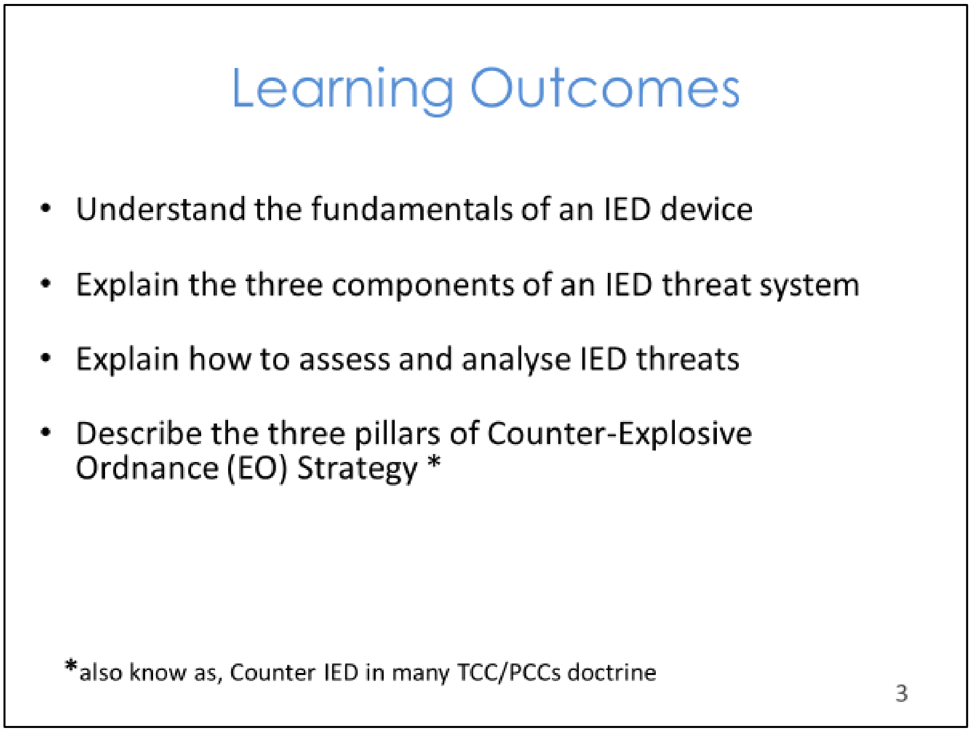
Content

- IED Basics
- IED Threat System
- Force Protection Considerations
- Counter-Explosive Ordnance (EO) Strategy

2

Here is the content of the lesson.

Slide 3



Learning Outcomes

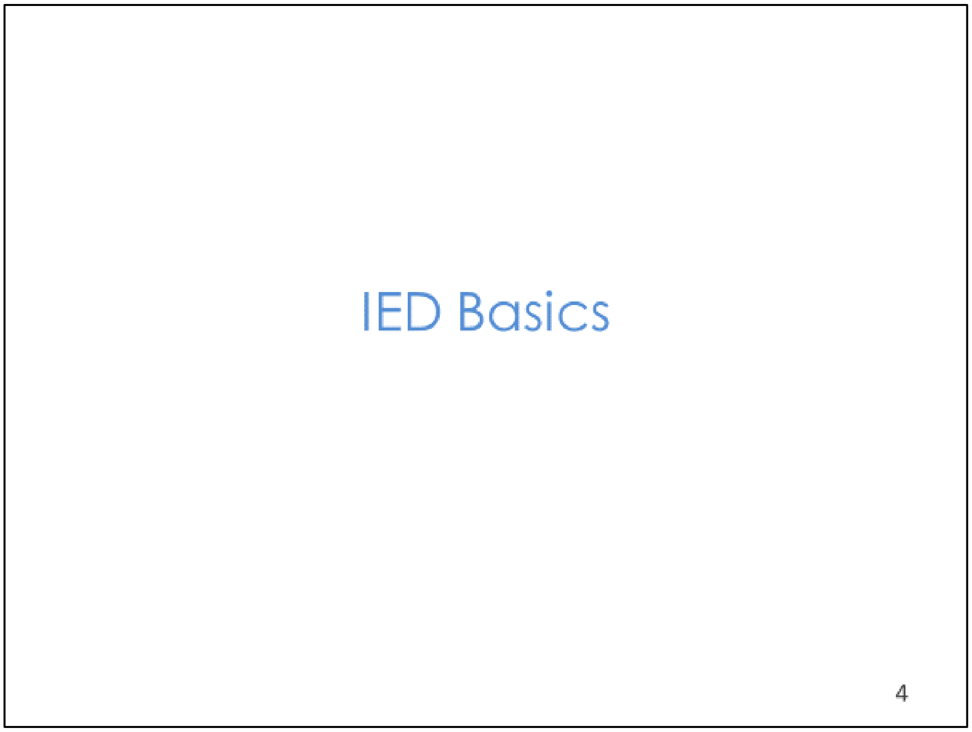
- Understand the fundamentals of an IED device
- Explain the three components of an IED threat system
- Explain how to assess and analyse IED threats
- Describe the three pillars of Counter-Explosive Ordnance (EO) Strategy *

*also know as, Counter IED in many TCC/PCCs doctrine

3

Let’s review the Learning Outcomes for this lesson. By the end of this lesson, you should have a basic knowledge and familiarisation of IEDs in a UN Mission area and the threat system framework. Take a few minutes to review.

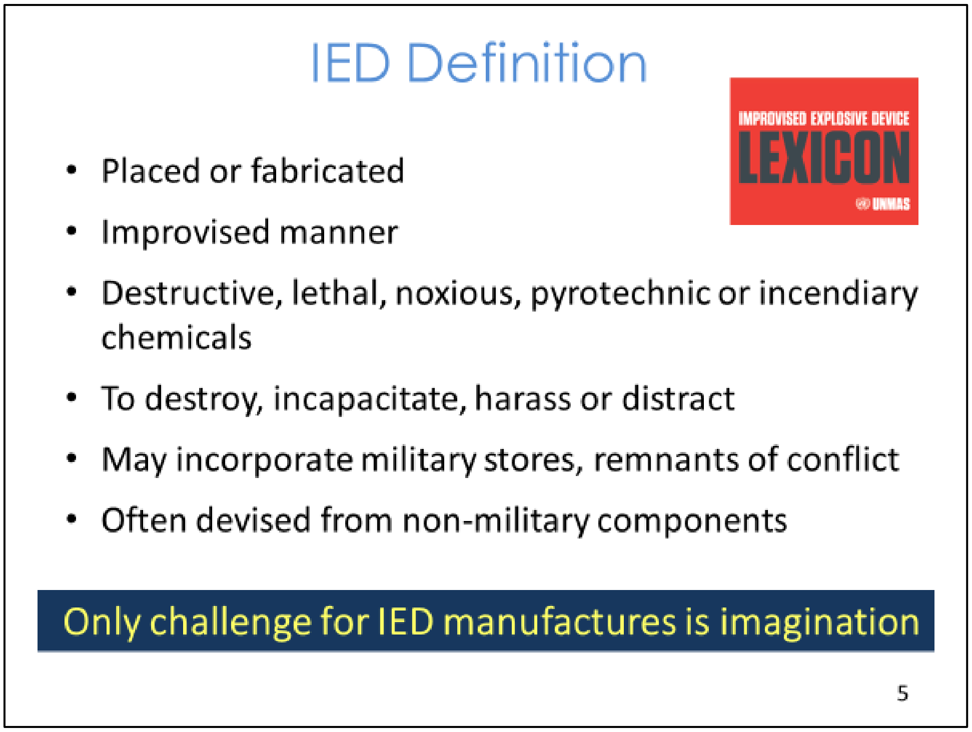
Slide 4



IED Basics

4

Slide 5



IED Definition

- Placed or fabricated
- Improvised manner
- Destructive, lethal, noxious, pyrotechnic or incendiary chemicals
- To destroy, incapacitate, harass or distract
- May incorporate military stores, remnants of conflict
- Often devised from non-military components

Only challenge for IED manufactures is imagination

5

IMPROVISED EXPLOSIVE DEVICE
LEXICON
UNMAS

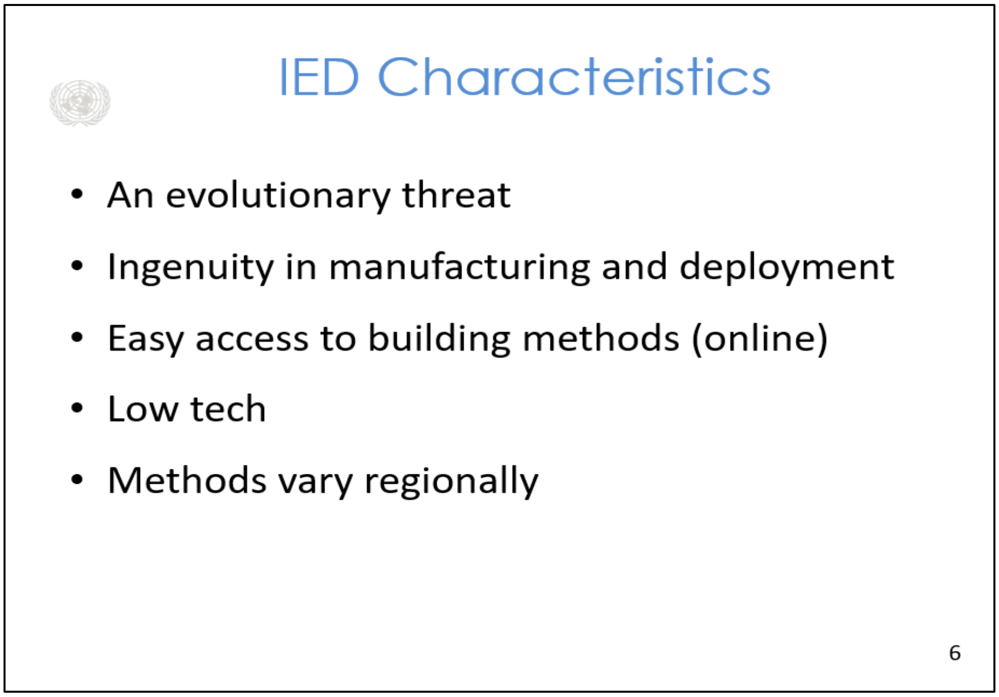
In this section of the lesson, we should focus on the basics of IEDs and be aware of their components. Knowledge of the material used to construct IEDs will assist the mission in determining the threat network. Here are a few points on this slide to help define an IED.

A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores but is normally devised from nonmilitary components.

In countries where strict weapons controls are in place, IEDs seem to form an increasingly attractive alternative or addition to illicit small arms. They are easily constructed and are improvised using many remnants of conflict explosives left in the country or chemicals easily obtained. IEDs can be simple to design, and components remain cheap and easily accessible, including through criminal networks and porous borders, as a result of corruption and poor ammunition stockpile management.

The threat of IEDs varies greatly from differing locations. Different group training, availability of materials, personnel knowledge, and experience, as well as geography all contribute to a different threat. Groups have recruited extensive cadres which can be trained to manufacture and use IEDs. These groups often aim at any gatherings of civilians, UN bases and convoys.

Slide 6



IED Characteristics

- An evolutionary threat
- Ingenuity in manufacturing and deployment
- Easy access to building methods (online)
- Low tech
- Methods vary regionally

6

IED Characteristics encompass a diverse range of aspects that make them a significant concern in modern security landscapes. These improvised devices possess the following attributes, contributing to their notoriety and wide-ranging impact:

An Evolving Threat: IEDs represent an ever-changing threat as malicious actors constantly adapt their tactics, techniques, and procedures. The dynamic nature of these devices makes them a challenging problem for security forces worldwide.

Ingenious Manufacturing and Deployment: One of the most alarming aspects of IEDs is the ingenuity displayed by those who create and deploy them. Utilising common and seemingly harmless materials, individuals with malicious intent can construct deadly devices that are hard to detect and mitigate.

Easy Access to Building Methods (Online): The proliferation of information on the internet enables easy access to a wealth of knowledge related to IED construction and deployment. This accessibility empowers individuals with malicious intentions, including lone-wolf attackers, to gain the know-how required for making these dangerous devices.

Low Tech, High Impact: Despite being relatively low-tech in comparison to conventional weapons, IEDs can cause devastating consequences. Their simplicity, coupled with their potential for mass casualties and infrastructure damage, makes them a potent threat.

Regional Variations in Methods: The methods used in IED construction can vary significantly from one region to another. This regional variation highlights the adaptability of those who employ IEDs, as they tailor their devices to suit local circumstances, which adds complexity to countermeasures.

Deceptive Appearance: IEDs often blend in with the surroundings, appearing like everyday objects or debris. This camouflage makes them difficult to spot, increasing the risk to civilians and military personnel alike.

Use of Triggers and Detonation Techniques: IEDs can employ various triggering mechanisms, such as pressure plates, remote-controlled devices, or even simple tripwires. Understanding and countering these different methods presents a constant challenge for security experts.

Psychological Impact: The fear and uncertainty surrounding IEDs go beyond the immediate physical impact. These devices create a sense of insecurity and can disrupt daily life, affecting communities and regions for an extended period.

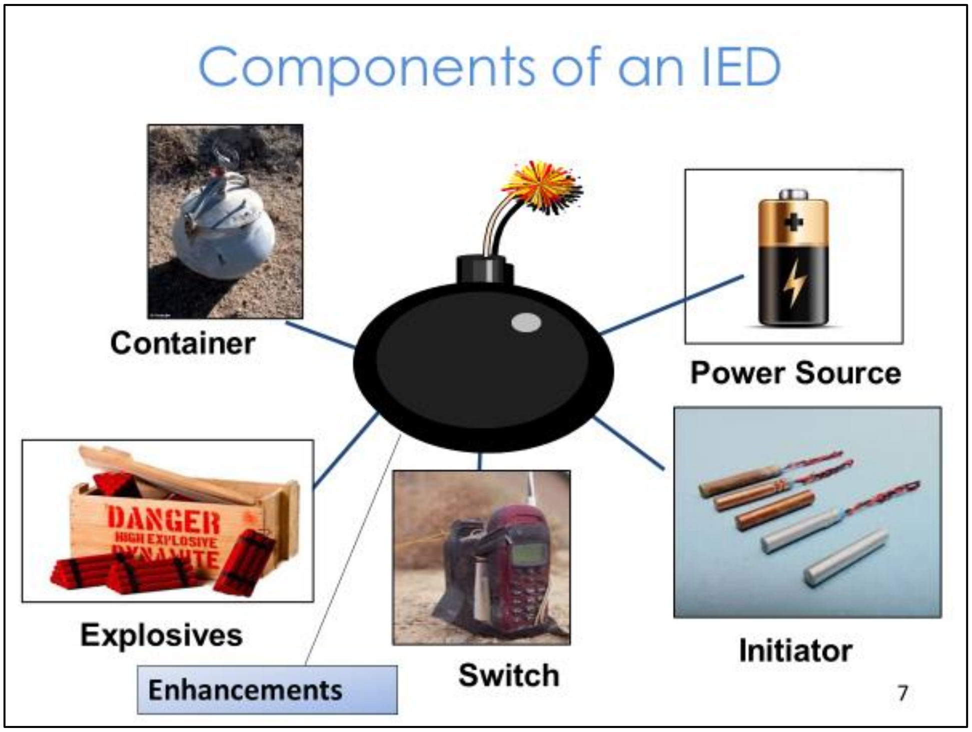
Violent Tool: IEDs are frequently used in terroir-type scenarios, where weaker adversaries attempt to offset the advantage of stronger organisations.

Challenges in Detection and Disposal: Detecting and safely disposing of IEDs require specialised training, equipment, and resources. Counter-IED teams face immense risks while carrying out their duties, as even a single mistake can lead to catastrophic consequences.

Constant Innovation: The ongoing arms race between those who build IEDs and those who counter them fuels a continuous cycle of innovation. This constant evolution necessitates a proactive and adaptive approach to counter-IED efforts.

In conclusion, the characteristics of IEDs make them an enduring and ever-evolving threat. Combating this menace demands international collaboration, continuous research, and a comprehensive understanding of the tactics and motivations driving those who employ these devices.

Slide 7



Components of an IED

Container

Power Source

Explosives

Enhancements

Switch

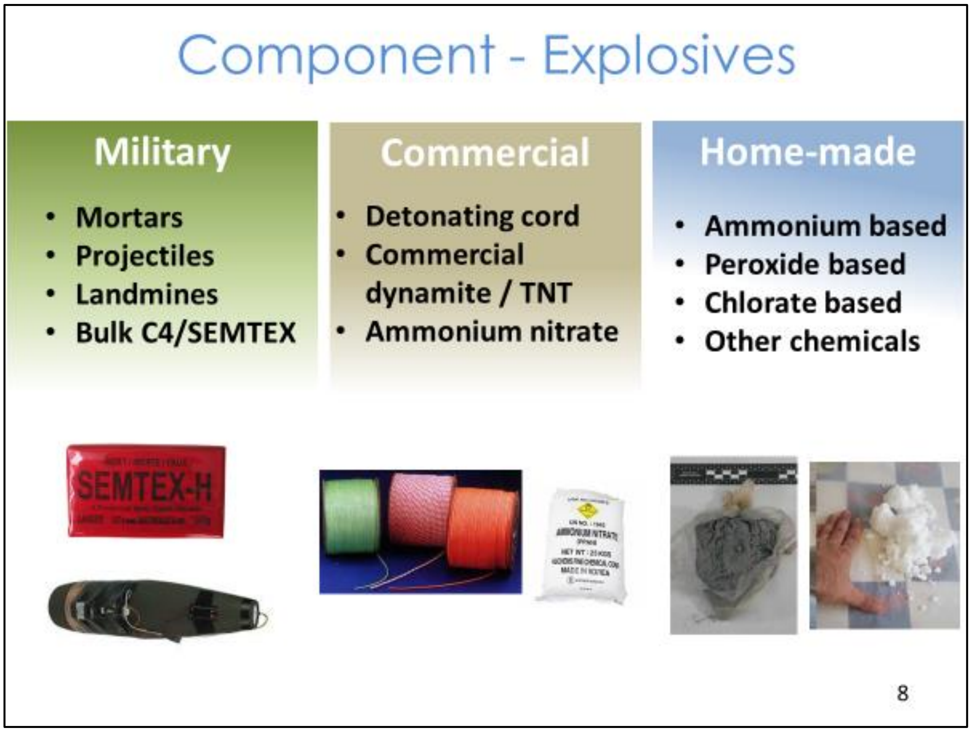
Initiator

7

IEDs are generally comprised of these components – A Switch, Power Source, Initiator, Container, and a Main Charge (Explosive)) but may also have additional enhancements added at time.

- A power source is required to ‘complete the circuit’ and detonate the device. Common power sources are 9-volt batteries
- An initiator is an item that is used to detonate the main charge. Initiators can be electric or non-electric and are very sensitive explosives. They are sometimes referred to as blasting caps and are very sensitive to heat, shock and friction and should never be touched
- The main charge or the explosives can be military-grade, such as C4 or home-made such as fertilisers
- The container for the explosives can be anything suitable, including backpacks, pressure cookers, plastic jugs
- Enhancements are any other items added that increase the effects; for example, ball bearings and nails
- A switch is what causes the IED to function. It can be a pressure plate, a phone, a passive infrared sensor, or a car alarm. There is no limit to what can be used to detonate an IED

Slide 8



Component - Explosives

Military

- Mortars
- Projectiles
- Landmines
- Bulk C4/SEMTEX

Commercial

- Detonating cord
- Commercial dynamite / TNT
- Ammonium nitrate

Home-made

- Ammonium based
- Peroxide based
- Chlorate based
- Other chemicals

SEMTEX-H
AMMONIUM NITRATE

8

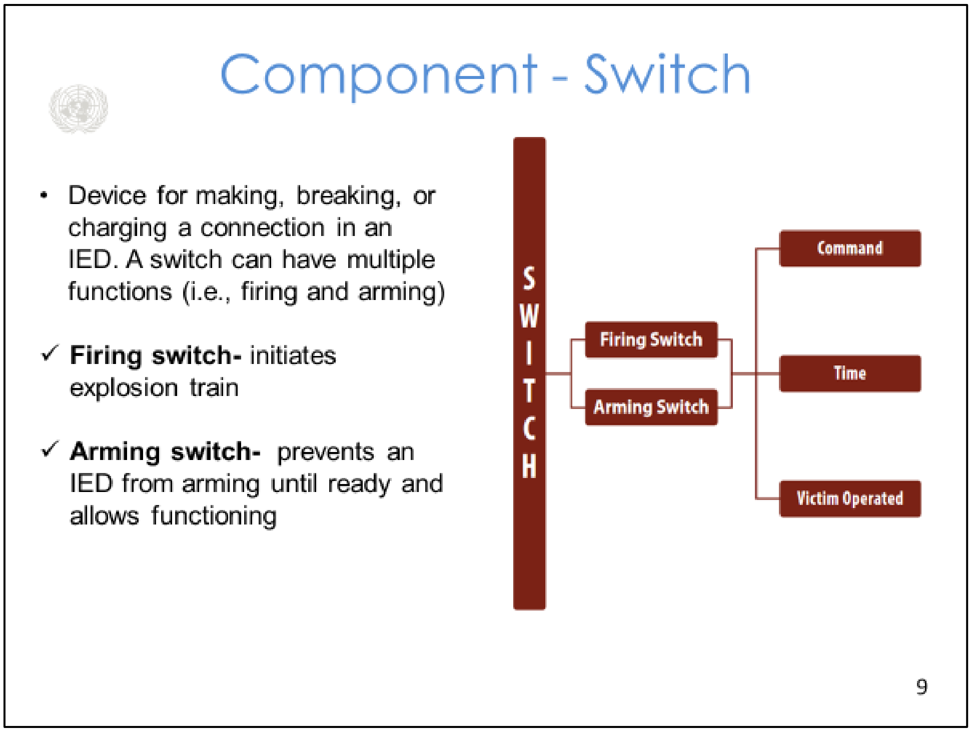
Explosives can come in many different forms; here are three common forms:

Military-grade explosives such as C4 or SEMTEX are difficult to procure. However, following a conflict, such as projectiles and bombs are often used as main charges. Aggressors are known to remove the main charge filing for use in IEDs. This is why it is critical to report any explosives found.

- Commercial explosives used for mining and other legitimate purposes can be stolen or diverted and incorporated into IEDs
- Homemade explosives are often fertilizer-based, so remain vigilant to indications of large amounts of fertilizer where no farming activity is conducted
- Homemade explosives may be more or less sensitive depending on the formulation, the substitutions, the purity, and the manufacture methods

Many of the chemical components can be purchased from a chemical supply store in pure form. Some homemade explosives may be found as small, crystalline solids that have settled to the bottom of a liquid filed container. Some may be flat on top of the liquid. Some sensitive homemade explosives may be manufactured in a cold and/or frigid water bath to prevent explosion. Some homemade explosives may be kept in a refrigerator or freezer.

Slide 9



Component - Switch

- Device for making, breaking, or charging a connection in an IED. A switch can have multiple functions (i.e., firing and arming)

✓ **Firing switch-** initiates explosion train

✓ **Arming switch-** prevents an IED from arming until ready and allows functioning

SWITCH

Firing Switch

Arming Switch

Command

Time

Victim Operated

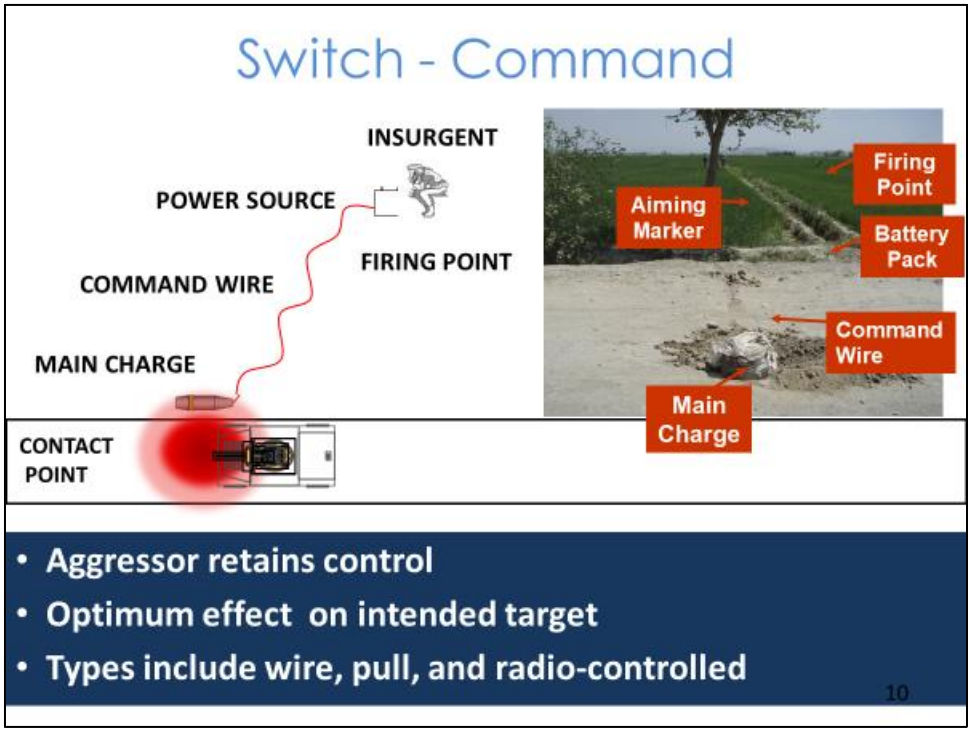
9

IEDs are categorized into 3 categories determined by how they are designed to function:

- Victim-operated - detonate when a person or vehicle conducts an action that subsequently causes the device to function. Things like pressure plates and PIR (passive infrared) switches are examples
- Command-initiated - detonate at the direction of the aggressor. This can be done remotely, as is the case with cell phones or key fobs in which the attacker is not physically connected to a device. Or directly, as is the case with command wire in which a long wire connects the IED to the attacker
- Time initiated- these are set to function after a set period of time and are typically attached to a digital or antilog clock

Some TCCs / PCCS also classify IEDs based on the carrier_ Vehicle-Borne IED (VBIED; Person-Borne IED (PBIED)/ Suicide IED; and Water-Borne IED (WBIED),

Slide 10



Switch - Command

- Aggressor retains control
- Optimum effect on intended target
- Types include wire, pull, and radio-controlled

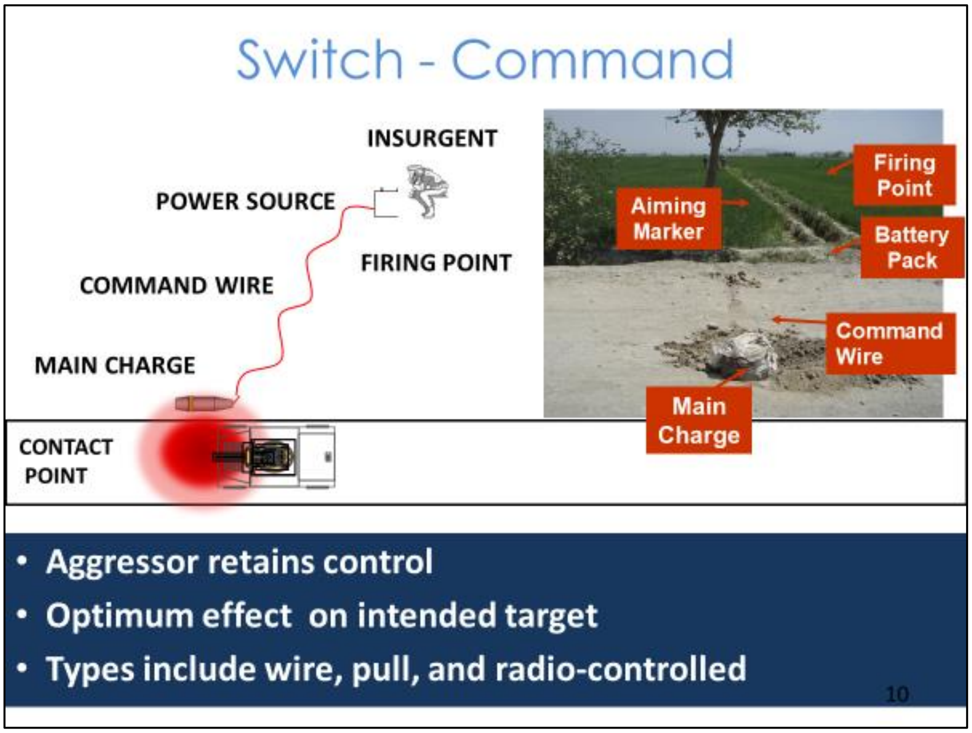
Here is an example of a Command-initiated IED. In this example, a command-initiated IED contains a switch that is activated by an aggressor in which they control the device. These IEDs normally feature separation between the main explosive charge and the firing switch.

This allows the aggressor to target from a safe distance. The aggressor who fires the command IED is referred to as a triggerman. An IED fired by command gives the aggressor full control. Command IEDs are especially suited to attacking mobile targets.

To implement an attack using a command-initiated IED, an aggressor needs to be able to select two suitable locations: where the IED is emplaced, and the triggerman's firing point

There are many methods to fire an IED by command. Two main methods are by radio control and by command wire. Other methods include pulling a string and technologies that complete an action.

Slide 11



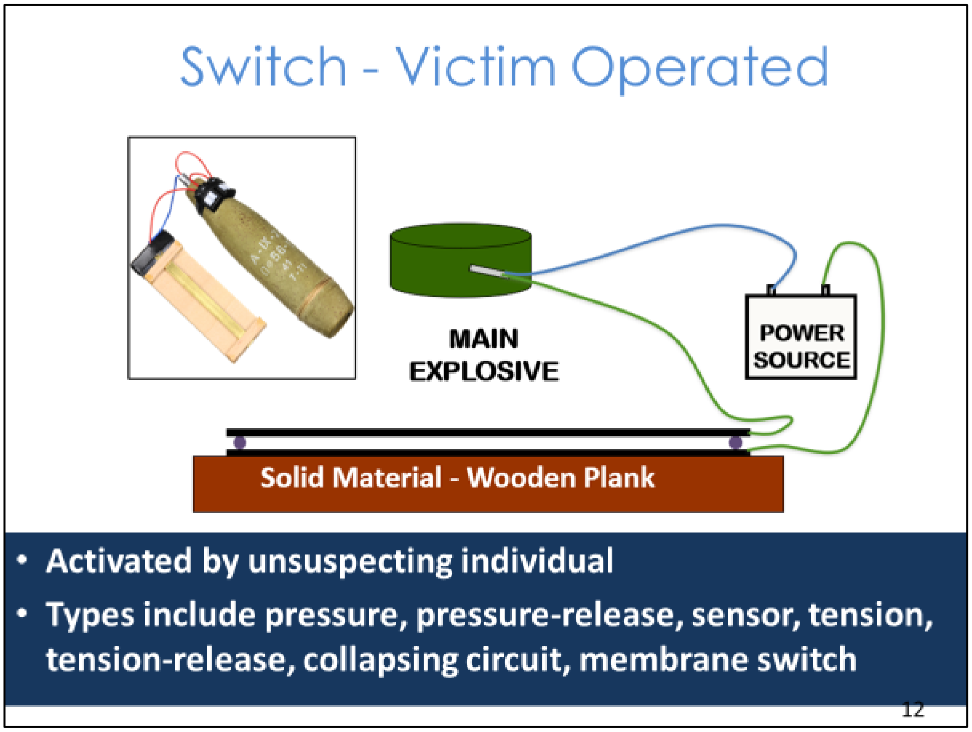
Switch - Command

- Aggressor retains control
- Optimum effect on intended target
- Types include wire, pull, and radio-controlled

10

IEDs can function through various sets of timed switches. These switches can be mechanical, chemical, or digital. Again, it is up to the creativity of the bomb-maker. Mechanical timers could include water displacement, where a container slowly leaks water until two metal plates come into contact and complete a circuit. Or it could be a version of a mechanical clock that pulls two wires together as time progresses. Chemical timers could be variations of a chemical reaction or pyrotechnic delay (time fuse). Electronic or digital timers could make use of digital watches wired to alarm speakers, a circuit that activates when a battery finishes draining, or any other variation.

Slide 12



Switch - Victim Operated

MAIN EXPLOSIVE

POWER SOURCE

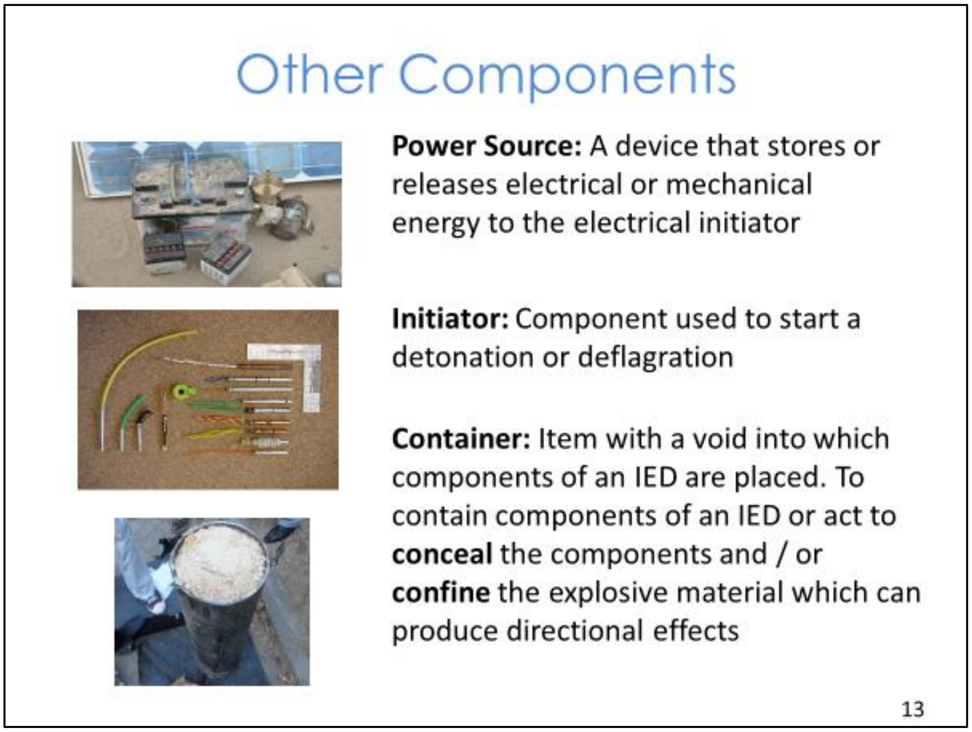
Solid Material - Wooden Plank

- Activated by unsuspecting individual
- Types include pressure, pressure-release, sensor, tension, tension-release, collapsing circuit, membrane switch

12

Shown in the picture above is a pressure plate IED, which is an example of an IED in which a pressure plate acts as the Victim Operated Switch which may involve a person standing on or a vehicle driving over the plate and the explosive main charge is an item of military ordnance in this case, you see the smaller picture showing a 155mm projectile.

Slide 13



Other Components

Power Source: A device that stores or releases electrical or mechanical energy to the electrical initiator

Initiator: Component used to start a detonation or deflagration

Container: Item with a void into which components of an IED are placed. To contain components of an IED or act to **conceal** the components and / or **confine** the explosive material which can produce directional effects

13

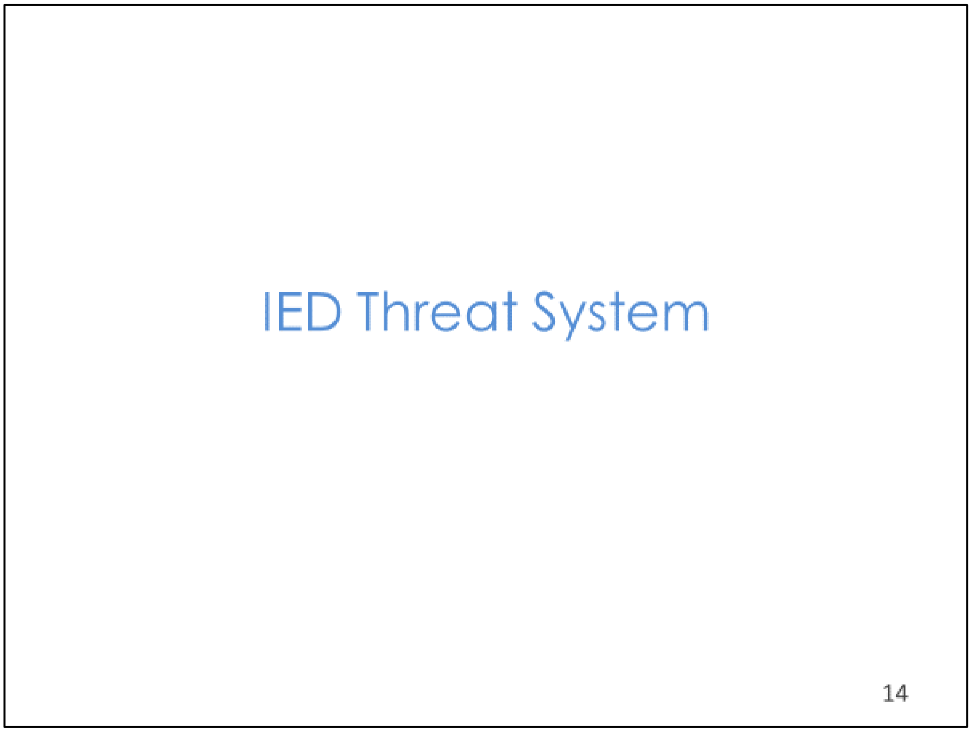
Other IED components you should be aware of, as mentioned earlier, include power sources, initiators, and the actual container for the device.

For power sources, IEDs could use a variety of electrical or mechanical energy. Electrical energy could be direct current through a battery (9V, 12V, capacitor, hand crank, etc.) or alternating currency (uninterrupted power supply). Mechanical energy sources could include storing applied energy through the physical movement of an IED component like a mechanical spring or a leaf spring.

Initiators could come from a variety of sources. They can be found in military stores or commercial sources. Also, initiators could be home-made, but the process is very dangerous due to the high sensitivity of the primary explosives required for these items.

Moreover, containers for an IED must consider concealment and confinement. Materials and types could be very diverse, including nylon, metal, plastic, cardboard, etc. Examples of different types of containers found in the past are pipes, human remains, tires, jugs, empty military ordinance, vehicles, and others.

Slide 14

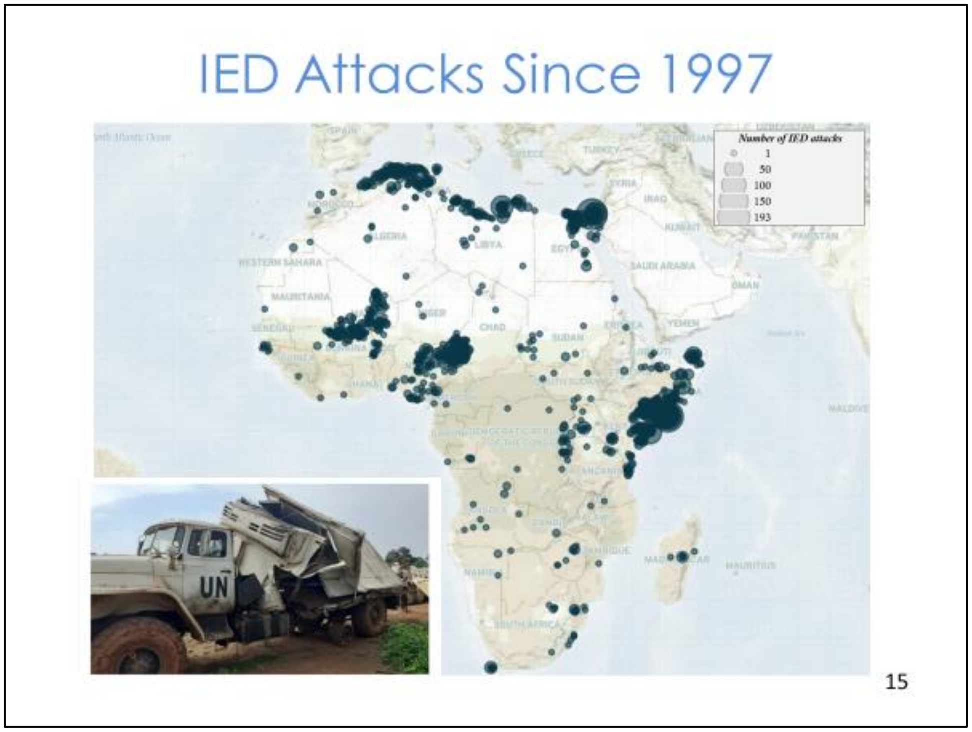


IED Threat System

14

Transition slide.

Slide 15



IED Attacks Since 1997

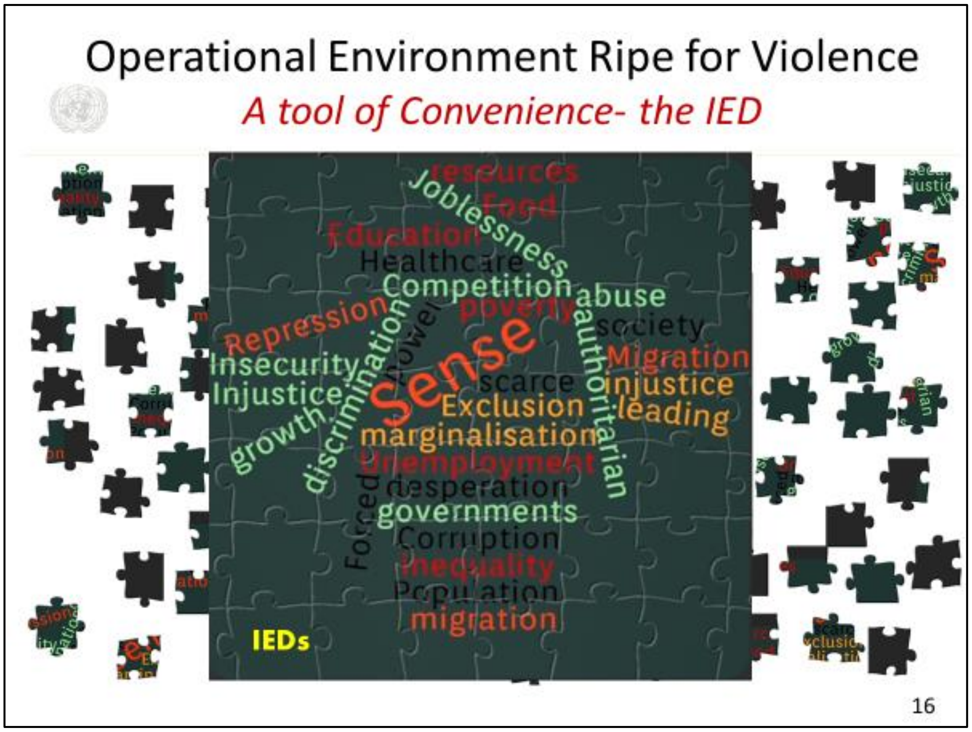
Annually, IED attacks kill and injure more people than do attacks with any other type of weapon except firearms. A review of selected international media reports from 2015 to 2021 revealed more than 6,300 recorded IED explosions, resulting in over 105,000 casualties. The proliferation of IED use is an unmistakable trend. About half of the world's countries have currently been impacted.

Why is IED use spreading? Because groups have made enduring gains in territorial control, creating areas where IED production facilities can go undetected for long periods of time. The financial and organisational prowess of several of these groups allows their IED manufacturers to continually adapt to counter-IED (C-IED) measures.

The spread of communications technology has greatly abetted IED knowledge-sharing. Online, groups share instructional videos or materials, both on IED construction and on the execution of attacks.

Moreover, foreign fighters have been returning to their home countries or have crossed borders into third countries, bringing the skills learned in conflict zones with them. Returnees have formed cells and networks providing access to weapons and materials for IED construction while capitalizing on acquired battlefield skills and explosives-related training.

Slide 16



Operational Environment Ripe for Violence

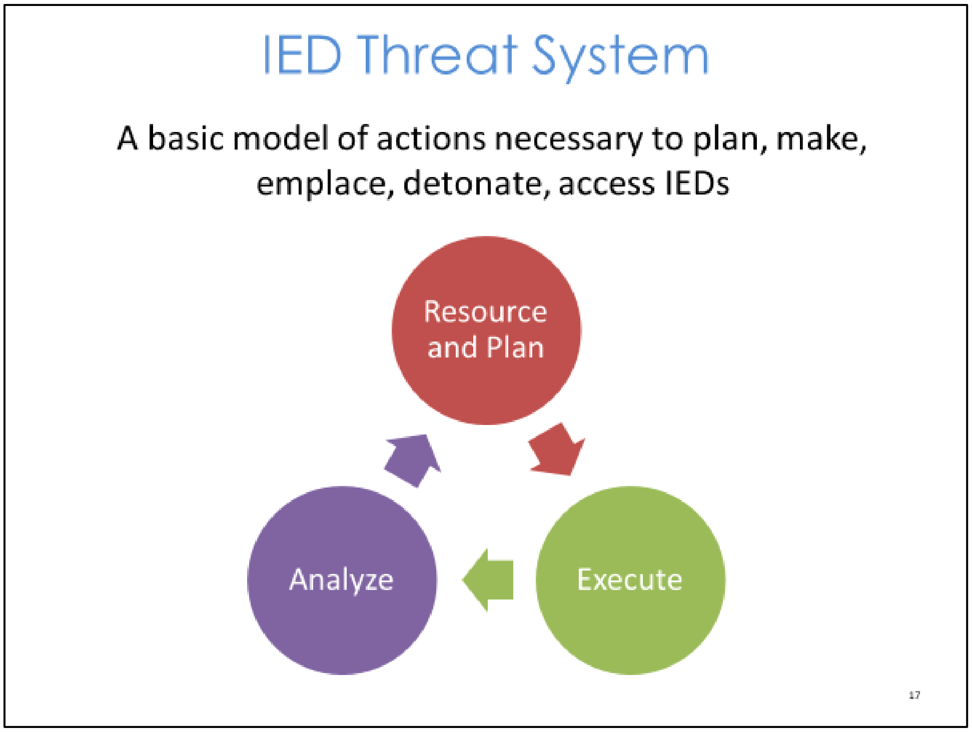
A tool of Convenience- the IED

16

This slide displays puzzle pieces that represent many factors when putting together, making an environment ripe for recruiting IED perpetrator actors.

- Corruption - abuse of power, authoritarian or repressive governments
- Sense of Injustice/repression
- Rigged elections
- Bias leaders
- Exclusion, discrimination, or marginalisation within the society
- Lack of fair and equal representation/power-sharing
- Overpopulation- population growth leading to migration and poverty
- Climate change
- Forced Migration
- Competition for scarce resources and food Insecurity
- Unemployment/joblessness
- Poverty
- Lack of hope and bleak outlook leading to desperation

Slide 17



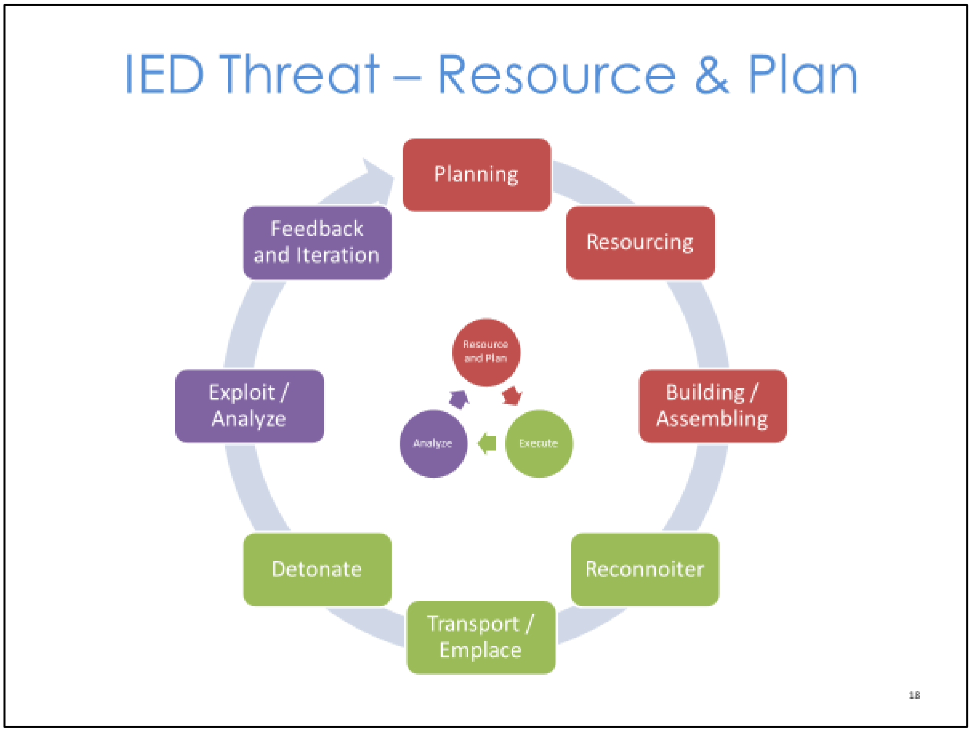
IED Threat System

A basic model of actions necessary to plan, make, emplace, detonate, access IEDs

The IED system is defined as the personnel, resources, and activities necessary to plan, build, execute, and exploit an IED event.

The IED system adopted by a perpetrator may or may not be structured. It involves multiple actions, from the collection and procurement of material for IED manufacturing to the placement of the IED at the point of attack. It can require elaborate planning and resources, including personnel, technical expertise and IED-making material. The actual IED attack is just one part of the whole system. IED systems are most effectively categorized according to three recurring phases seen on this slide: resource and plan, execute and analyse.

Slide 18



IED Threat – Resource & Plan

Planning

Resourcing

Building / Assembling

Reconnoiter

Transport / Emplace

Detonate

Exploit / Analyze

Feedback and Iteration

Resource and Plan

Execute

Analyze

18

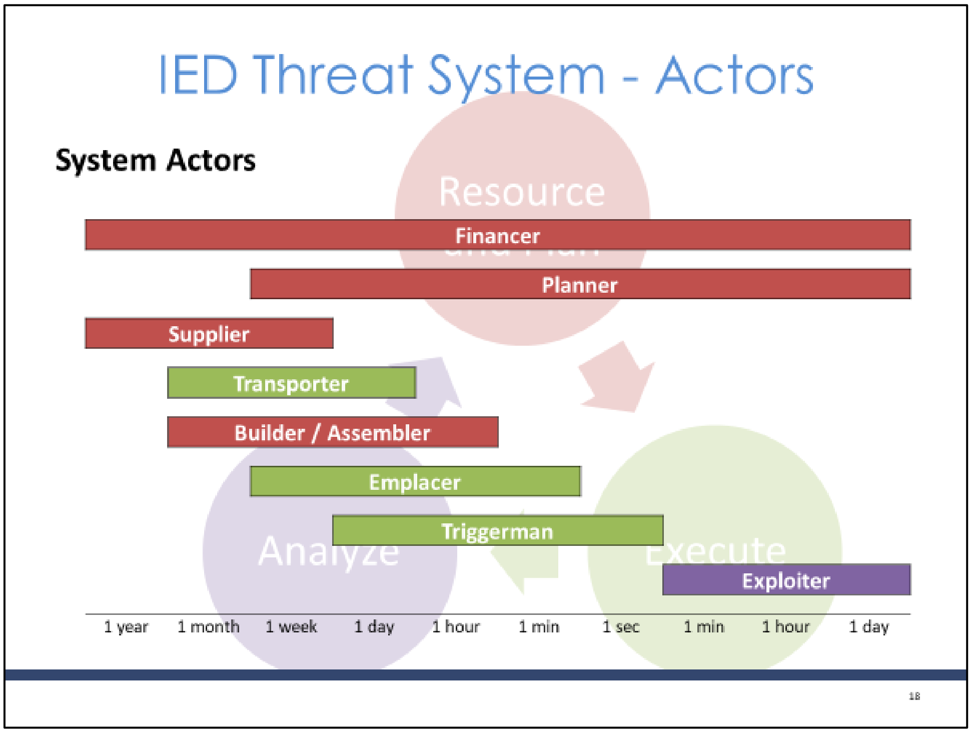
To achieve success, groups that systematically use IEDs must engage in a series of network operations or activities. These operational requirements encompass two main aspects: (1) securing funding and (2) obtaining necessary resources, such as explosive materials, as well as personnel like bomb makers who are motivated by ideology, economics, or other factors.

These network activities can take place concurrently or sequentially, but often, they operate independently, regardless of whether they occur simultaneously or in a specific order. Each function within the network may be organised into one or more cells, with participants in each cell often unaware of the existence of other cells. The various roles within the network include Planners (responsible for developing strategies), Suppliers, Transporters, Builders, Emplacers, Triggermen, and Exploiters.

At each stage of the threat chain, there are opportunities to disrupt the network and hinder its operations, either directly or indirectly. Direct intervention may involve blocking access to funding, materials, or personnel, including bomb-making components and individuals with bomb-making expertise. Indirectly, valuable information obtained from critical and noncritical functions can help identify, track, and exploit vulnerabilities within the network, leading to the impairment of potential attacks.

By detecting and tracking the IEDs network, as well as considering characteristics of the bomber, such as theft or unauthorised acquisition of precursor chemicals, agencies can gain insights into the structure, sustainability, and modus operandi of the network.

Slide 19



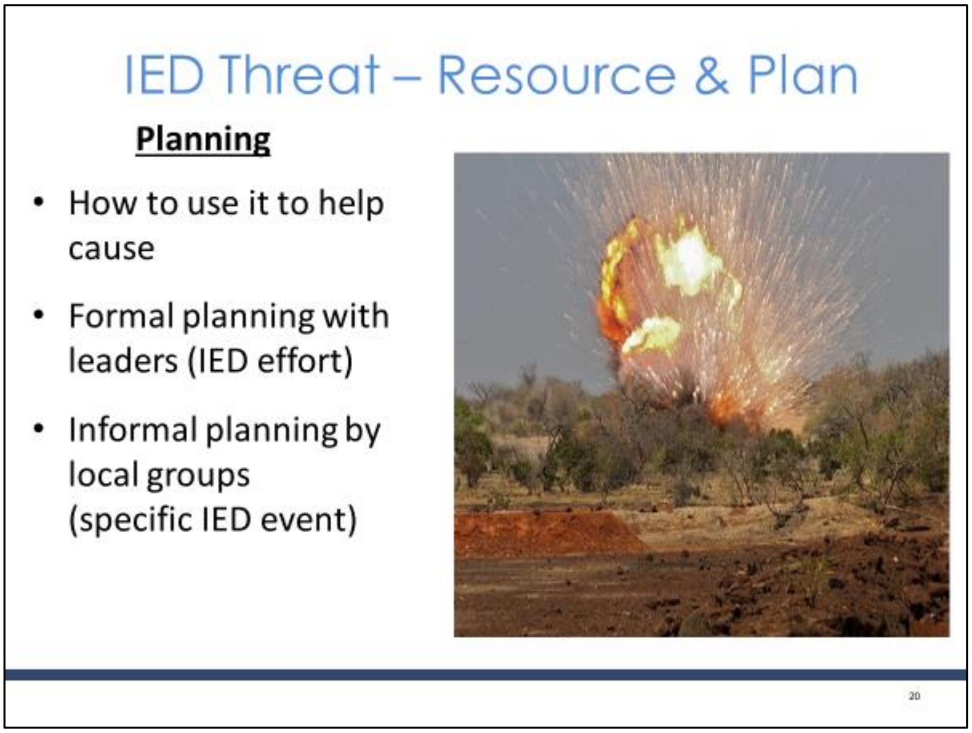
IED Threat System - Actors

System Actors

This graphic representation illustrates the IED network system, focusing on the timeline leading up to and immediately following an IED attack. It emphasises the specific timeframe in which tactical units have the potential to influence the situation. The green area highlights network personnel who are more susceptible to tactical-level reconnaissance and observation.

To disrupt or intervene the network operations, the red line representing network personnel depicted in the slide suggests that a more strategic approach is required. This entails leveraging mission-specific strategies and garnering support from the host nation to effectively detect and monitor the network's activities.

Slide 20



IED Threat – Resource & Plan

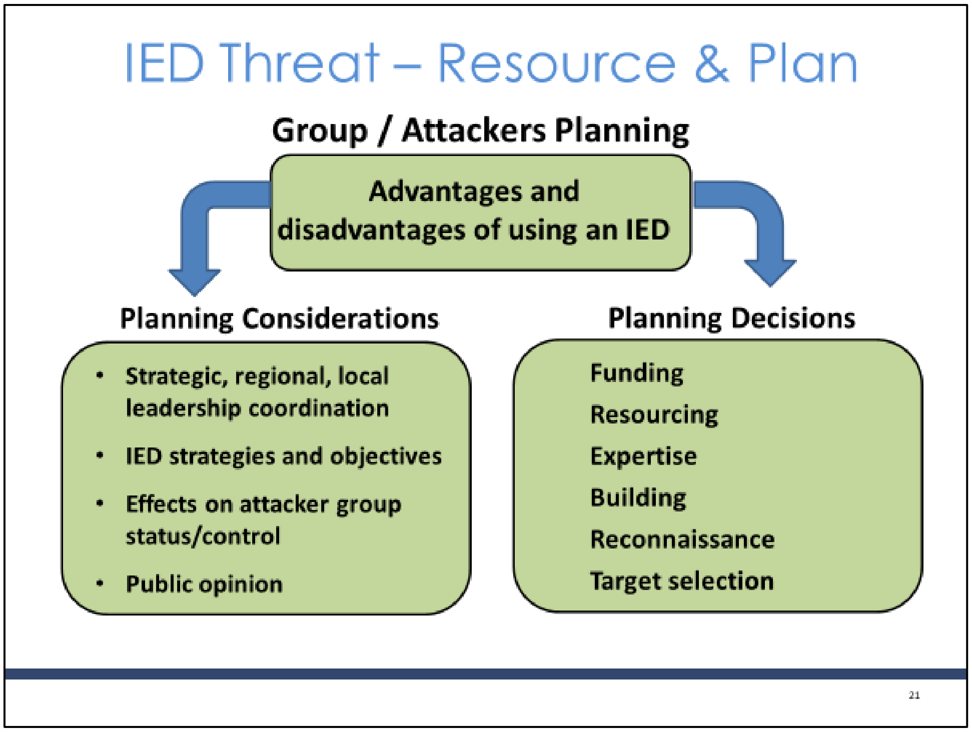
Planning

- How to use it to help cause
- Formal planning with leaders (IED effort)
- Informal planning by local groups (specific IED event)

20

The potential attackers using IEDs must carefully contemplate the use of IEDs when devising a strategy. Within the planning process, there are inherent advantages and disadvantages associated with the use of IEDs that require thorough consideration. Such planning takes place across multiple tiers within the network / organisational structure, with decisions ultimately falling upon leaders at various levels. The overarching question they face is whether the deployment of IEDs proves advantageous and, if so, what justifications exist for such a choice.

Slide 21



IED Threat – Resource & Plan

Group / Attackers Planning

Advantages and disadvantages of using an IED

Planning Considerations

- Strategic, regional, local leadership coordination
- IED strategies and objectives
- Effects on attacker group status/control
- Public opinion

Planning Decisions

Funding
Resourcing
Expertise
Building
Reconnaissance
Target selection

21

In this slide, we delve into the crucial considerations and decisions involved in planning an IED operation. The actions of armed group leaders who employ IEDs have the potential to impact, alter, or advance their existing goals or strategies. A critical aspect to assess is whether there is adequate organisational control to effectively manage an IED operation. Additionally, it is vital to anticipate the sentiments and reactions of the local population towards such activities.

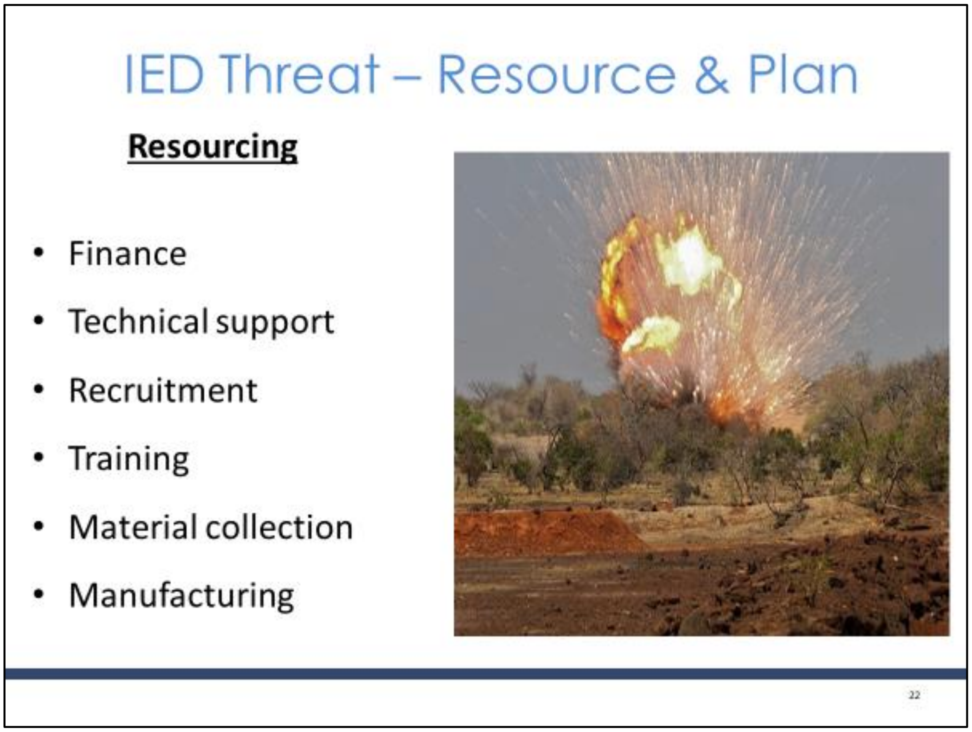
As these factors are meticulously weighed, leaders at all levels face a continuous stream of decisions pertaining to crucial aspects like funding, resourcing, IED construction, and more. Constructing and executing an IED entails several key components, including:

- Funding: Securing the necessary financial resources to support the operation
- Resourcing: Acquiring the required materials and equipment for the construction and deployment of the IED
- Expertise: Recruits and personnel that possess the specialised knowledge and skills related to IED assembly and deployment
- Building: Physically constructing the IED, considering its design, components, and functionality

- Reconnaissance: Gathering peacekeeping-intelligence and conducting surveillance to identify suitable targets and assess the operational environment
- Target selection: Choosing specific targets that align with the group's objectives and maximise the desired impact

These aspects form the foundation of constructing and executing an IED operation, necessitating careful planning and decision-making at each step along the way.

Slide 22



IED Threat – Resource & Plan

Resourcing

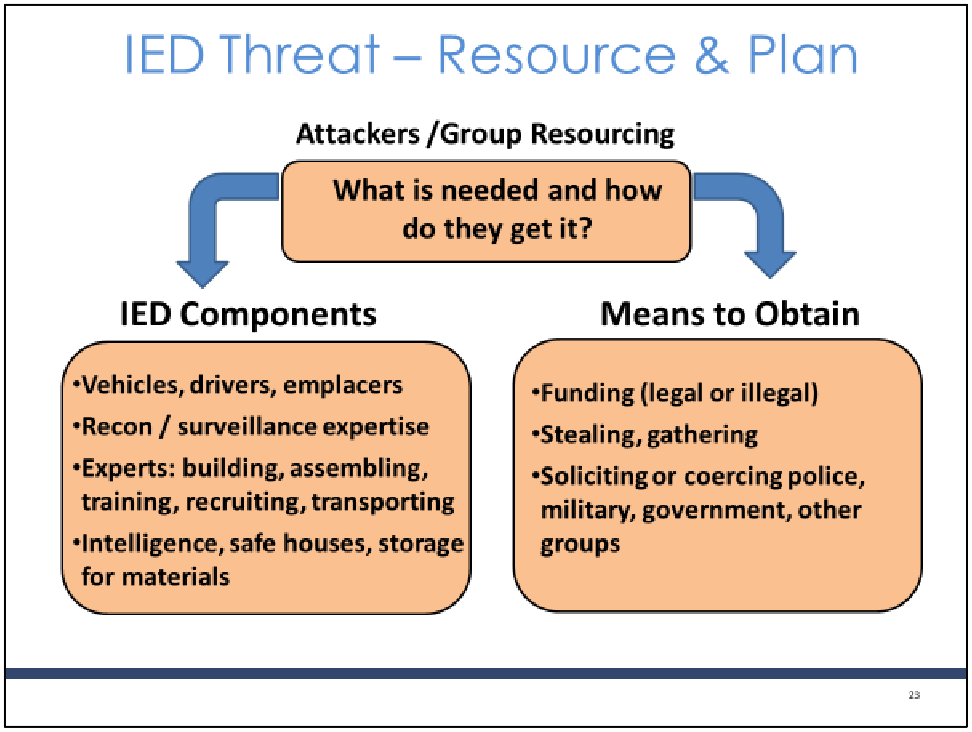
- Finance
- Technical support
- Recruitment
- Training
- Material collection
- Manufacturing

22

The armed group engages in a comprehensive assessment of their needs and strategies on how to obtain them. Their considerations extend beyond relying solely on illegal funding as they explore alternative avenues such as theft, purchasing from businesses, or seizing resources from the battlefield. The availability of specific parts and components plays a significant role, influencing factors like the type of IED to be used and target selection. In some cases, limited parts availability may compel the group to revisit their planning process, reevaluating their objectives and what they aim to achieve through the utilisation of IEDs.

Resourcing involves acquiring the necessary training to support their operations. This may entail hiring experts to perform crucial tasks or investing in training their own personnel. Training efforts could involve either bringing experts to their location or sending their personnel to receive training from experts elsewhere. This information highlights critical requirements that the Counter-Explosive Ordnance (C-EO) Strategy, also known as the Counter-Improvised Explosive Device (C-IED) effort, can utilise to disrupt the network. By preventing the construction of IEDs and implementing changes to protective techniques, the CIED effort can effectively mitigate the impact of these devices.

Slide 23



IED Threat – Resource & Plan

Attackers /Group Resourcing

What is needed and how do they get it?

IED Components

- •Vehicles, drivers, emplacers
- •Recon / surveillance expertise
- •Experts: building, assembling, training, recruiting, transporting
- •Intelligence, safe houses, storage for materials

Means to Obtain

- •Funding (legal or illegal)
- •Stealing, gathering
- •Soliciting or coercing police, military, government, other groups

23

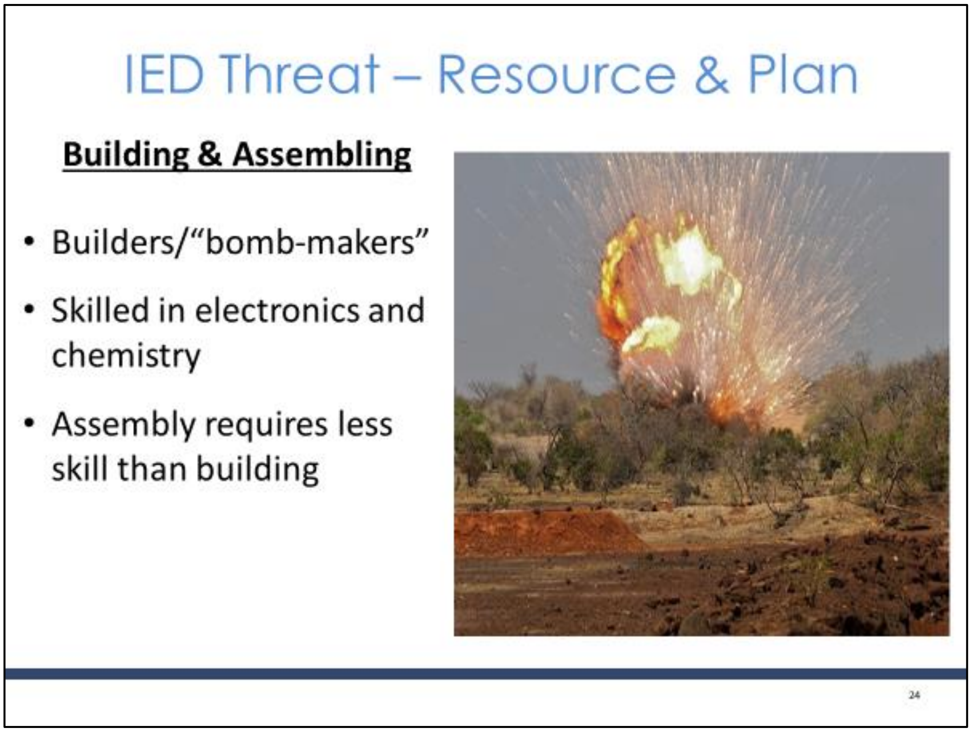
This chart provides a comprehensive explanation of the requirements for an IED event by an armed group and the methods they employ to obtain these resources. On the left side of the chart, we observe an extensive logistics trail necessary to resource an IED, encompassing more than just the components of the device itself. On the right side, we see that armed groups utilise a combination of legal and illegal means to acquire the resources mentioned on the left. The components involved in an IED event include:

- Vehicles, drivers, and emplacers: Required for transportation and positioning of the IED
- Reconnaissance/surveillance expertise: Skilled individuals responsible for gathering peacekeeping-intelligence and conducting surveillance
- Experts: Building, assembling, training, recruiting, and transporting personnel with specialised knowledge and skills
- Intelligence, safe houses, and storage for materials: Facilities and resources to store essential materials and maintain secrecy

Here are how these components are obtained:

- Funding: Acquiring financial resources through legal or illegal channels to support the IED event
- Stealing and gathering: Illicit acquisition of necessary resources through theft or collection
- Soliciting or coercing police, military, government, or other groups: Utilising various methods, such as persuasion or coercion, to obtain resources from these entities
- This chart highlights the multifaceted nature of resourcing an IED event and the diverse strategies employed by terrorist organisations to secure the required components

Slide 24



IED Threat – Resource & Plan

Building & Assembling

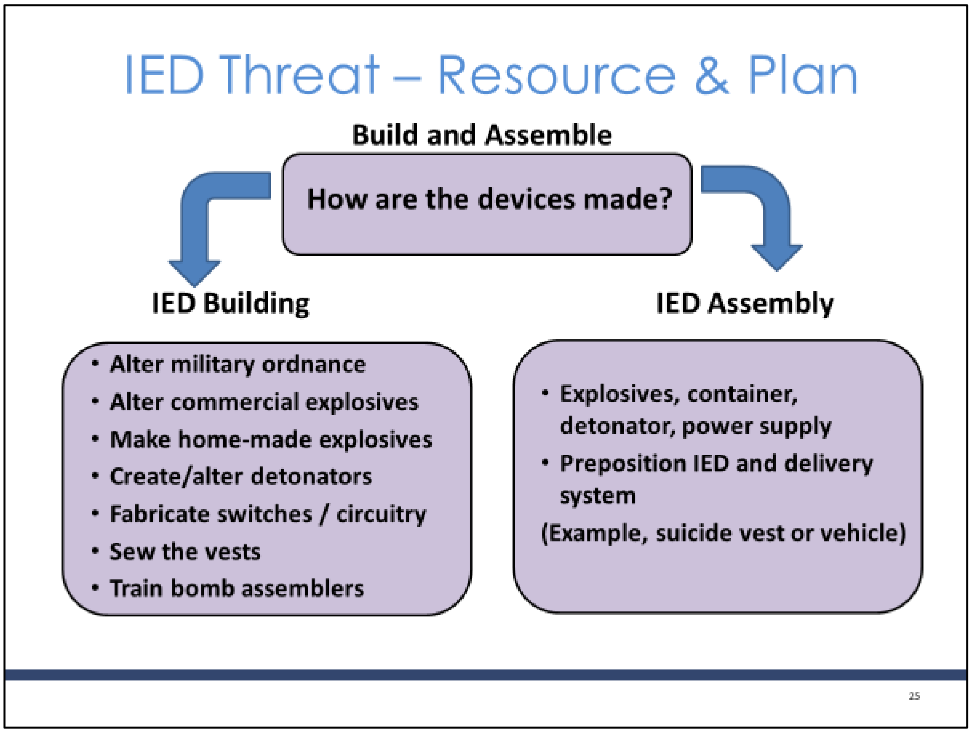
- Builders/“bomb-makers”
- Skilled in electronics and chemistry
- Assembly requires less skill than building

24

The process of building an IED involves creating specific components through various techniques. This includes modifying electronic key fobs to serve as detonators, incorporating accelerators to enhance explosive powder, constructing vests to carry dynamite sticks, or redesigning vehicles to conceal artillery shells within the trunk and back seat. Individuals involved in this phase are often referred to as bomb makers, possessing advanced skills and potentially educational backgrounds in areas like chemistry or electrical engineering, surpassing the abilities of mere assemblers.

Assembling an IED involves bringing together the different components to a specific location and connecting them. In some cases, this assembly may occur in close proximity to the intended target and possibly be carried out by the same person who emplaces and detonates the device. Those involved in the assembly process may receive basic training in simple mechanics, such as connecting wires to establish the electric circuit, attaching power source batteries, or programming a radio dial tone with the initiation code. However, it is common for more skilled individuals to remain in safer areas away from the target, as assembly duties expose them to the risk of encountering friendly forces, making them vulnerable.

Slide 25



IED Threat – Resource & Plan

Build and Assemble

How are the devices made?

IED Building

- Alter military ordnance
- Alter commercial explosives
- Make home-made explosives
- Create/alter detonators
- Fabricate switches / circuitry
- Sew the vests
- Train bomb assemblers

IED Assembly

- Explosives, container, detonator, power supply
- Preposition IED and delivery system

(Example, suicide vest or vehicle)

The armed group's proficiency in building a bomb/IED is of utmost importance, particularly as the complexity of the devices increases. It is noteworthy that the IED building list on the left side of the chart represents more advanced skills compared to the assembly list on the right. Building a functional device requires the expertise of a true specialist, while minimal training is sufficient for the assembly process. When facing an IED threat in your area of operations, it becomes crucial to have a comprehensive understanding of how these devices are constructed. This knowledge enables UN units/forces to recognise early indicators during community interactions and information gathering. IED building involves several advanced skills and techniques, including:

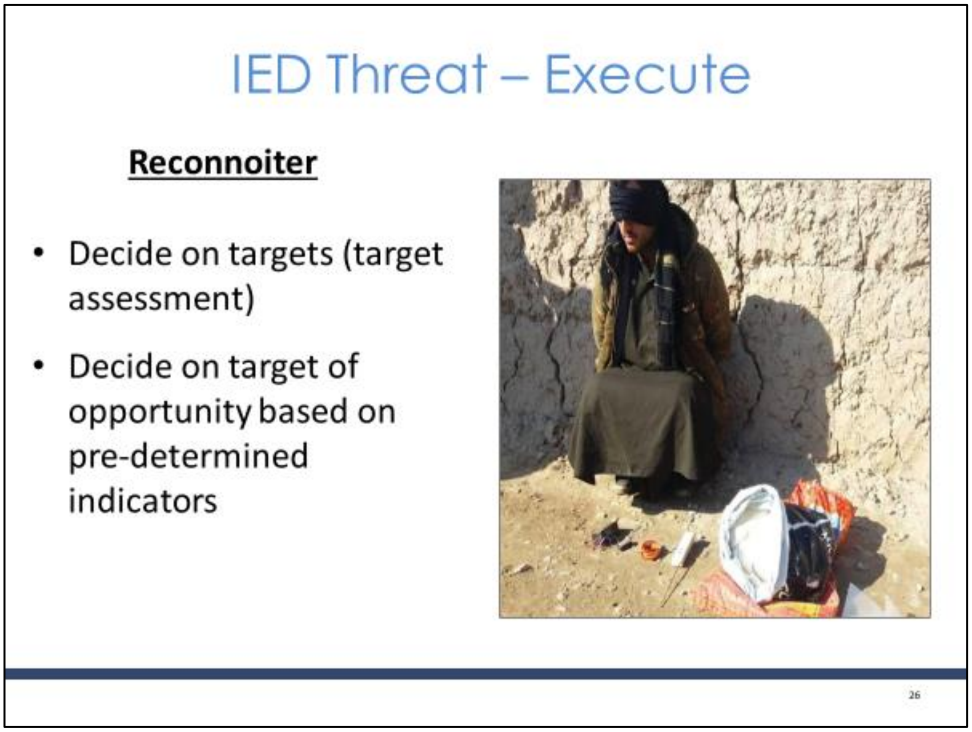
- Modifying military ordinance: Adapting military explosives or devices
- Modifying commercial explosives: Altering commercially available explosive
- Manufacturing homemade explosives: Creating explosive materials using commonly available ingredients
- Creating/altering detonators: Fabricating or modifying mechanisms used to initiate the explosive reaction
- Fabricating switches/circuitry: Constructing electrical components and circuitry
- Sewing vests: Crafting and assembling vests that can hold explosives
- Training bomb assemblers: Providing instruction to individuals

On the other hand, IED assembly involves the basic elements required for the device:

- Explosives, container, detonator, power supply: Gathering the necessary components for the explosive device, including the explosives themselves, a suitable container, the detonator, and a power supply
- Prepositioning IED and delivery system: Positioning the IED in a predetermined location and selecting an appropriate delivery system, such as a suicide vest or a vehicle

By understanding the intricacies of IED construction, UN units can better detect and respond to potential threats, enhancing overall situational awareness and safety within the community.

Slide 26



IED Threat – Execute

Reconnoiter

- Decide on targets (target assessment)
- Decide on target of opportunity based on pre-determined indicators

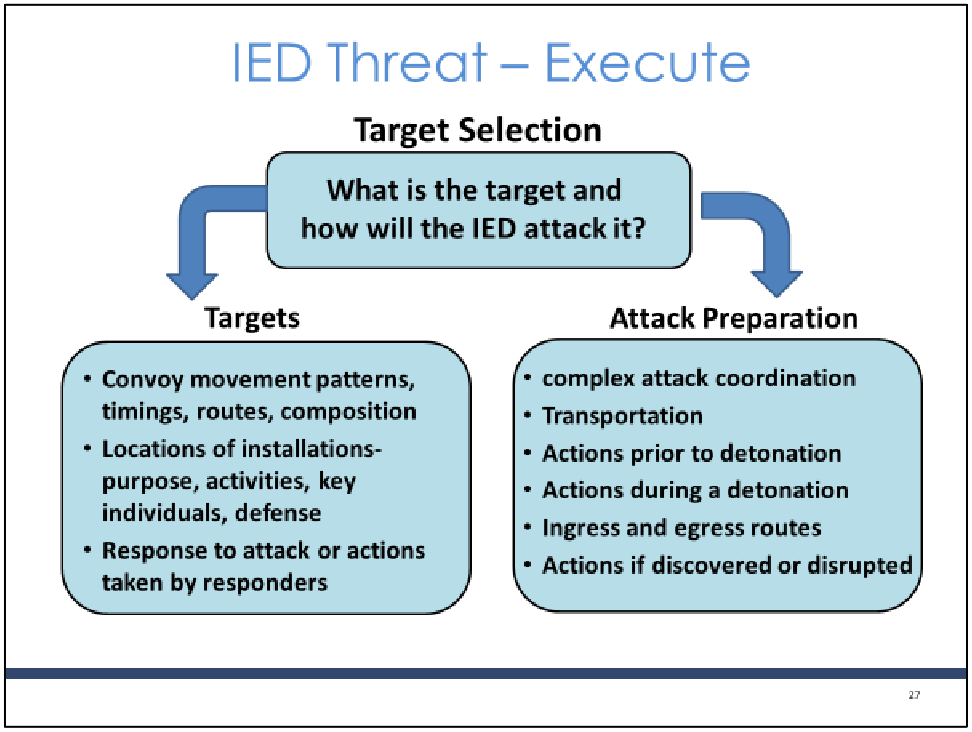
26

Armed groups possess the flexibility to choose specific targets at any point during the IED threat model. These targets can vary in nature, ranging from static or mobile, military or nonmilitary, and may include groups, installations, or individuals. The group conducts their reconnaissance and performs their own version of target assessment, which can lead to changes in their target selection. If they have the necessary resources, they may also alter the type of IED they intend to use.

In certain situations, armed groups may consider targets of opportunity, particularly if they are limited in personnel or lack advanced skills. This shift in targets can create conflicting indicators regarding their actual objectives. However, if they conduct any form of rehearsal or training, observable indicators and signatures can help elucidate their decision-making process. Rehearsals and training sessions can range from elaborate mock-ups or driving courses to simpler activities such as discussions between the bomb maker and the emplacer in a room.

These observable indicators and rehearsals provide valuable insights for friendly forces, enabling them to better understand the group’s intentions and adapt their countermeasures accordingly. By identifying and analysing these indicators and signatures, security forces can gain clarity on the enemy's target selection process and take appropriate measures to prevent or respond to potential threats.

Slide 27



IED Threat – Execute

Target Selection

What is the target and how will the IED attack it?

Targets

- Convoy movement patterns, timings, routes, composition
- Locations of installations- purpose, activities, key individuals, defense
- Response to attack or actions taken by responders

Attack Preparation

- complex attack coordination
- Transportation
- Actions prior to detonation
- Actions during a detonation
- Ingress and egress routes
- Actions if discovered or disrupted

27

IEDs are typically constructed with a specific target in mind, and understanding the target can provide insights into the characteristics of the device and vice versa. Targets can be classified into broad categories such as mobile targets (convoys), static targets (military bases), or high-value individuals (VIPs or first responders). The rationale behind why an armed group would choose to target first responders may vary and could be influenced by factors such as disrupting emergency response efforts, instilling fear and chaos, or retaliating against specific individuals or organisations.

On the right side of the chart, you will also find considerations that the armed group must consider when selecting a site for the attack. Understanding the terrain surrounding your location can offer valuable insights into the preparations. It allows you to anticipate their approach and departure routes, evaluate whether the terrain favours an IED attack against a mobile target, and identify potential vulnerabilities or gaps in your force protection plans that may make certain areas more susceptible to an IED attack. Targets can encompass various elements, including:

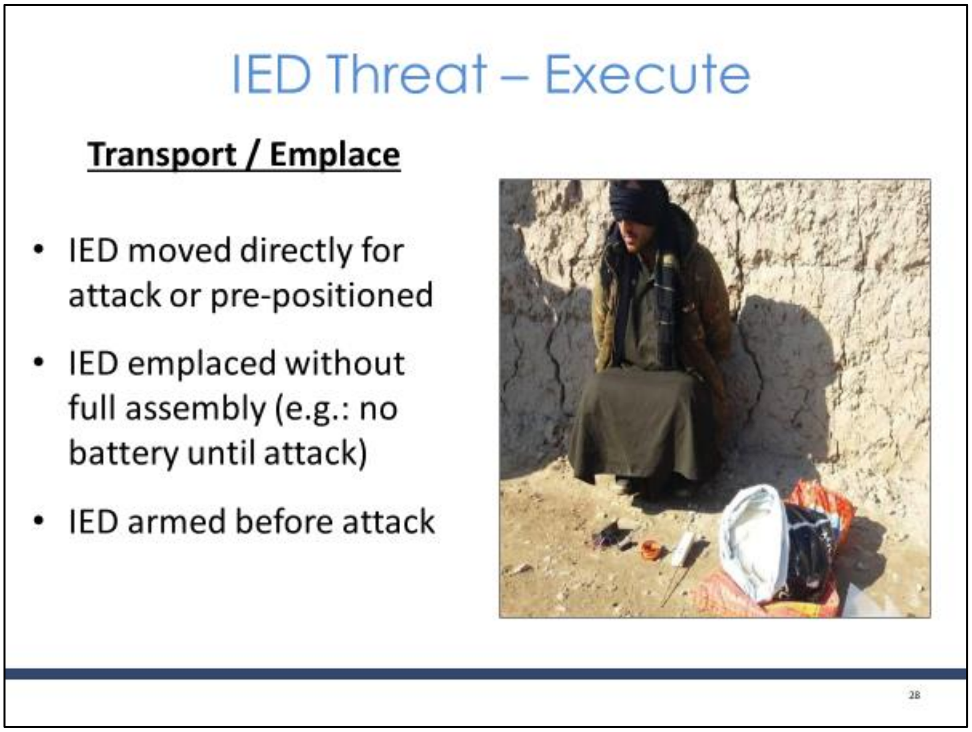
- Convoy movement patterns, timings, routes, and composition: Understanding the characteristics and organisation of convoy operations
- Locations of installations: Identifying the pose, activities, key individuals, and defence capabilities of various installations
- Response to attack or actions taken by responders: Analysing the behaviour and protocols of responders in the event of an attack

Attack preparations may involve:

- Complex attack coordination: Planning and organising multiple elements of the attack to maximize effectiveness
- Transportation: Arranging suitable means of transportation for personnel and materials
- Actions prior to detonation: Preparatory steps taken leading up to the detonation
- Actions during a detonation: Coordination of actions and potential secondary objectives during the explosion
- Ingress and egress routes: Identifying the entry and exit routes utilise by attackers
- Actions if discovered or disrupted: Contingency plans in case of discovery or interference during the operation

By understanding these considerations, friendly forces can enhance their situational awareness, anticipate potential attack scenarios, and implement appropriate countermeasures to mitigate the threat posed by IED attacks.

Slide 28



IED Threat – Execute

Transport / Emplace

- IED moved directly for attack or pre-positioned
- IED emplaced without full assembly (e.g.: no battery until attack)
- IED armed before attack

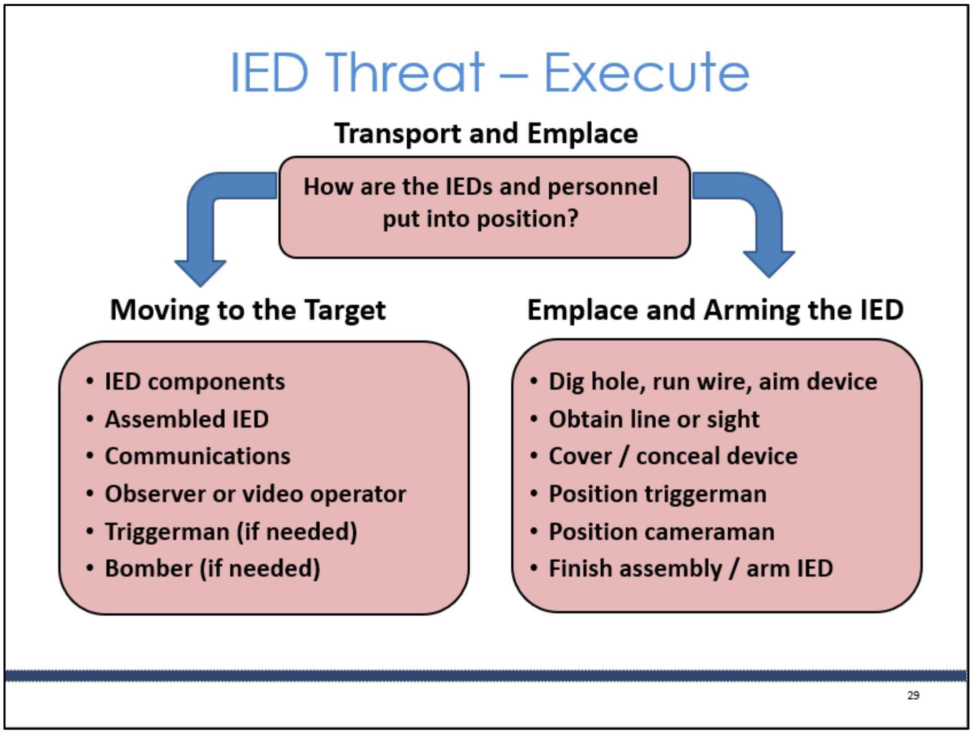
28

The process of deploying an IED involves strategically positioning or directly moving it to the target area. Once the target is selected and reconnaissance provides the armed group with information about the target's layout and security measures, the armed group can proceed to move and set up the IED for detonation. It's important to note that the IED may already be constructed, but the final assembly may vary depending on the specific type of IED, target, and intended location for detonation.

Emplacing the device entails carefully placing it in its final position, arming it, and maintaining surveillance over it. Depending on the nature of the device, concealing the IED, having a triggerman or an observer nearby might be necessary. In certain cases, gaining access to the target might involve a suicide bomber as part of the emplacement process. Arming the device for detonation is another crucial step in the emplacement process.

Throughout both the transportation and emplacement stages, the enemy's movement of the device and personnel provides opportunities for observation and enables the implementation of various counter-explosive ordnance (C-EO) measures to thwart their efforts.

Slide 29



IED Threat – Execute

Transport and Emplace

How are the IEDs and personnel put into position?

Moving to the Target

- IED components
- Assembled IED
- Communications
- Observer or video operator
- Triggerman (if needed)
- Bomber (if needed)

Emplace and Arming the IED

- Dig hole, run wire, aim device
- Obtain line or sight
- Cover / conceal device
- Position triggerman
- Position cameraman
- Finish assembly / arm IED

29

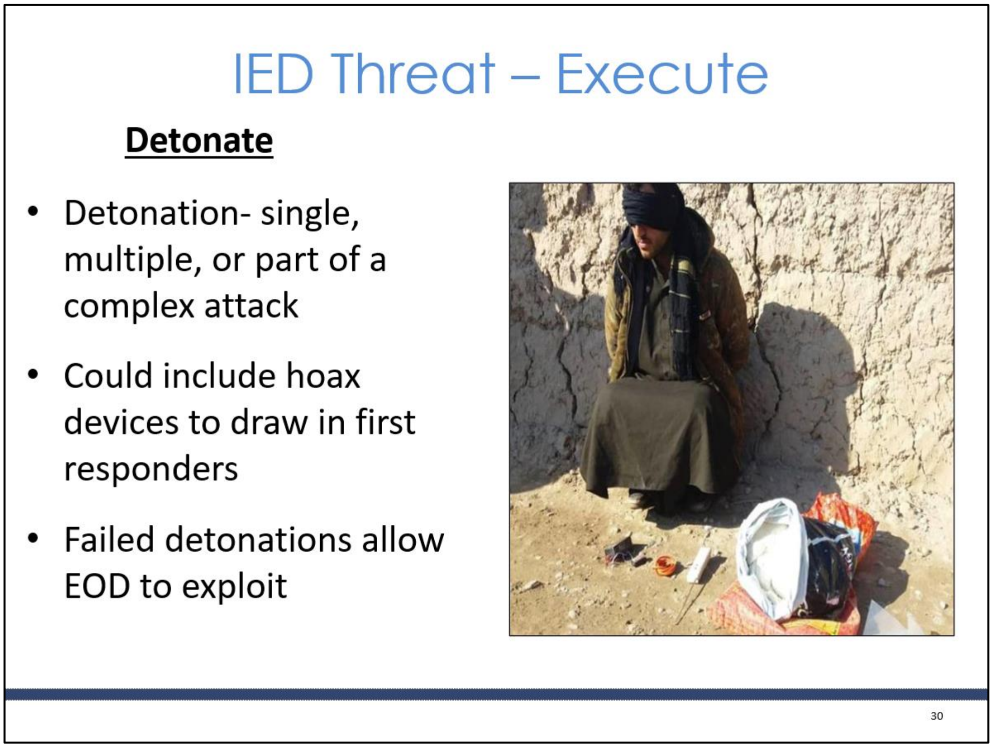
Approaching an IED detonation event, time becomes a critical factor in effectively identifying indicators and taking appropriate action. Therefore, it is crucial to detect these indicators as early as possible. The subsequent stage of the process involves the armed group physically transporting the IED to the intended attack site and carefully emplacing it, whether it be buried in the ground or arranged in a specific configuration. However, this poses significant risks for the group, as engaging in such activities may attract attention and raise suspicion.

Furthermore, as the indicators become increasingly conspicuous, the armed group would be compelled to carry out these activities during periods of reduced visibility, such as when there are fewer people around or under the cover of darkness. Moving toward the target may involve transporting various components of the IED, including both its assembled form as well as communication equipment, an observer or video operator, and a triggerman if necessary.

The process of emplacing and arming the IED encompasses several steps, such as digging a hole, running wires, and precisely aiming the device. Acquiring an unobstructed line of sight is crucial, while efforts to cover and conceal the device aim to minimise its visibility. Additionally, strategic placement of the triggerman and cameraman is necessary, followed by the final assembly and arming of the IED.

By refining your awareness of these indicators and their progression, you can better identify potential threats and respond effectively to mitigate the risks.

Slide 30



IED Threat – Execute

Detonate

- Detonation- single, multiple, or part of a complex attack
- Could include hoax devices to draw in first responders
- Failed detonations allow EOD to exploit

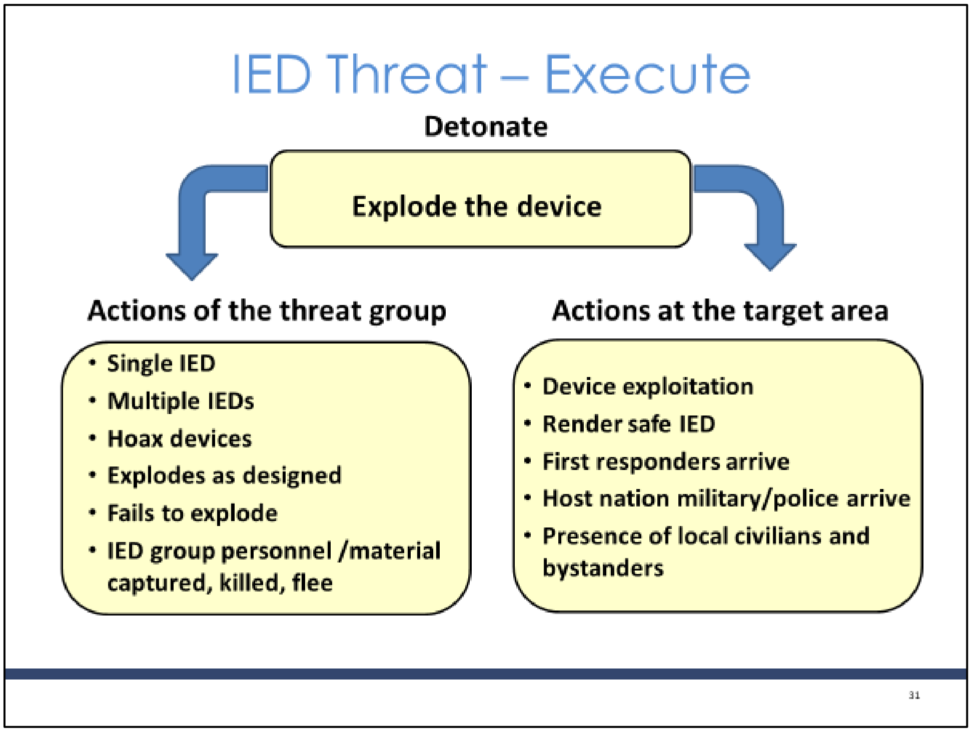
30

Armed groups aim to detonate the device, and these detonations can take various forms, including single explosions, multiple explosions, or being part of complex ambush attacks. In some cases, armed groups may employ dummy devices, known as "finds," either to observe the responses of potential targets or to lure them into a larger, coordinated, or multiple IED attack.

During a detonation event, individuals involved may attempt to escape into the surrounding crowd as part of their plan or due to the failure of the device to explode correctly. Meanwhile, people in the vicinity may be moving towards or away from the blast site, further complicating efforts to manage the aftermath and minimise the impact of the explosion.

While an explosion is one possible outcome, another scenario may involve the device failing to detonate fully or not at all. In such cases, C-EO render-safe elements can be deployed to neutralise the bomb while C-EO forensics specialists gather technical and forensic data for analysis. From an peacekeeping-intelligence perspective, an IED attack underscores the importance of ongoing peacekeeping-intelligence support, which focuses on predicting the capabilities and intentions of armed groups through the analysis of individual events within the broader context of the overall conflict.

Slide 31



IED Threat – Execute

Detonate

Explode the device

Actions of the threat group

- Single IED
- Multiple IEDs
- Hoax devices
- Explodes as designed
- Fails to explode
- IED group personnel /material captured, killed, flee

Actions at the target area

- Device exploitation
- Render safe IED
- First responders arrive
- Host nation military/police arrive
- Presence of local civilians and bystanders

31

At this stage of the process, the failure to identify early indicators necessitates a response to a potentially catastrophic detonation event. Although the occurrence of a detonation is always undesirable, it presents an opportunity that must not be wasted.

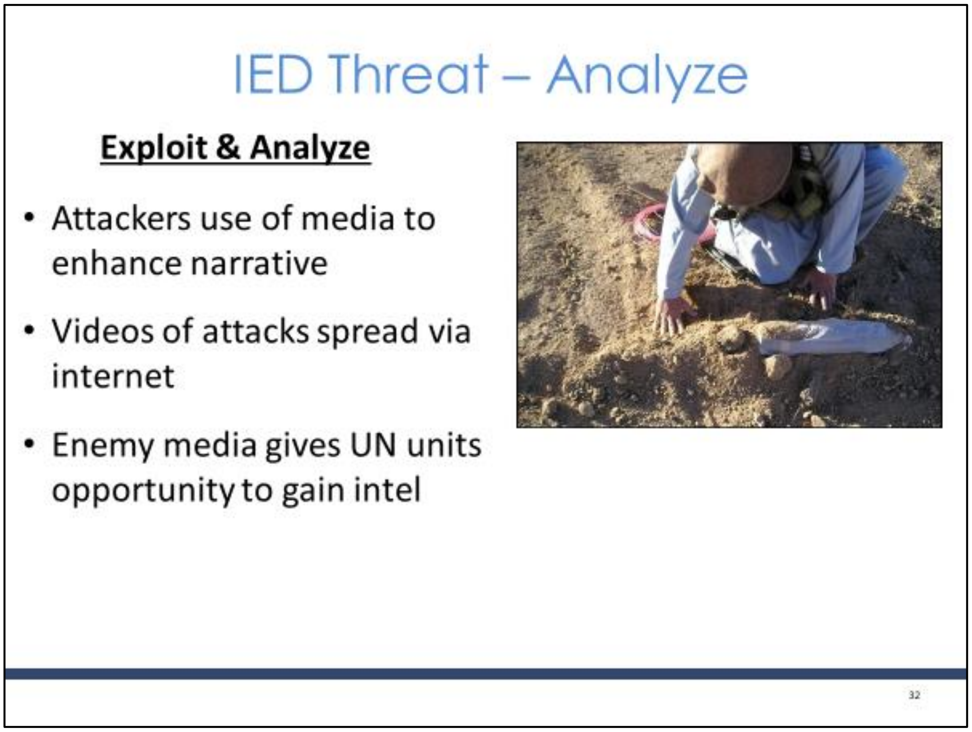
Lessons learned from such events, including device exploitation carried out by Explosive Ordnance Disposal (EOD) units, should be leveraged to enhance our understanding of IEDs. For instance, evidence collection can provide valuable insights into the materials used for constructing the device, as well as the methods of emplacement and resource acquisition. These new data points can enable UN units and forces to detect indicators earlier, prior to the occurrence of the next IED attack.

The actions of the armed group, attackers, or threat may manifest in various ways, such as the deployment of a single IED, multiple IEDs, or the use of hoax devices. These devices can either explode as intended or fail to detonate altogether. Additionally, encounters with the armed group may result in the capture, elimination, or flight of personnel associated with the IED operations.

At the target area, several actions may unfold in response to the detonation event. These actions include device exploitation, where experts examine and analyse the IED for peacekeeping-intelligence purposes. Efforts to render the IED safe are undertaken by specialised personnel. First responders, including emergency services, arrive at the scene to provide immediate assistance. The presence of local civilians and bystanders further adds to the complexity of the situation, requiring considerations for their safety and well-being.

By effectively executing these actions and capitalizing on the lessons learned, friendly forces can improve their overall understanding of IEDs, enhance their response capabilities, and ultimately strive to prevent future IED attacks.

Slide 32



IED Threat – Analyze

Exploit & Analyze

- Attackers use of media to enhance narrative
- Videos of attacks spread via internet
- Enemy media gives UN units opportunity to gain intel

32

Armed groups utilise various communication channels, including local and international media, to disseminate images and information about IED events, promoting their vision and amplifying the impact of this weapon. Although not essential for conducting an IED attack, this constant dissemination significantly enhances the secondary and tertiary effects. A proficient armed group can meticulously capture every stage of the IED threat model on video, from bomb construction to training and reconnaissance, as well as the explosion itself and the response of friendly forces.

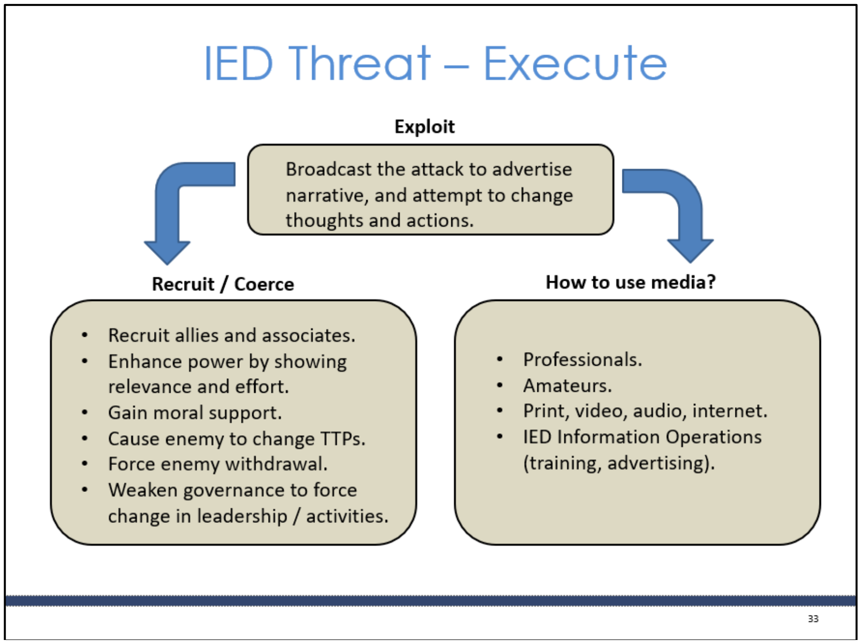
Such videos serve multiple purposes:

- They serve as alleged evidence of the armed group's capability to carry out attacks
- They portray the armed group as an attractive organisation to join, offering resources like money, weapons, IEDs, personnel, and related capabilities
- They allow the armed group to propagate its abilities, instil fear, or elicit sympathy from the population
- They serve as a training tool for the armed group to improve their IED threat, including the construction of more sophisticated devices

Armed groups distribute these videos directly through their own media engagements or indirectly via the Internet. While the armed groups utilise these recordings for their own purposes, they can serve as valuable sources of information about their techniques, leadership, capabilities, and limitations. The video documentation can establish links between the IED group and other elements, aiding in the identification and degradation of the network and its devices by counter-explosive ordnance (C-EO) operations. Access to these recordings also provides an effective means of training UN units and UN forces.

In summary, armed groups leverage communication platforms to disseminate videos showcasing their IED activities, which not only serve their propaganda objectives but also offer valuable insights for understanding, countering, and training against the IED threat.

Slide 33



IED Threat – Execute

Exploit

Broadcast the attack to advertise narrative, and attempt to change thoughts and actions.

Recruit / Coerce

- Recruit allies and associates.
- Enhance power by showing relevance and effort.
- Gain moral support.
- Cause enemy to change TTPs.
- Force enemy withdrawal.
- Weaken governance to force change in leadership / activities.

How to use media?

- Professionals.
- Amateurs.
- Print, video, audio, internet.
- IED Information Operations (training, advertising).

33

As friendly UN units attempt to seize the opportunity to exploit a detonation event, armed groups also capitalize on their meticulously planned and resource-intensive IED attacks to maximize their impact. One common tactic employed by these groups is recording the event, using it as a powerful tool to shape and control a specific narrative.

While this propaganda can further their objectives, it also serves as a valuable source for the UN to analyse and comprehend the group's goals and strategies. It is crucial for the UN to remain vigilant and watch for individuals who may be nearby, recording these attacks. The purposes for armed groups to exploit IED attacks through media dissemination can encompass the following objectives:

- Recruiting allies or associates to expand the armed group's network
- Enhancing the power and influence of the armed group by showcasing their successful attacks
- Garnering moral and local support by evoking emotions and sympathy from the population
- Attempting to influence the tactics, techniques, and procedures (TTPs) employed by international organisations such as the UN
- Endeavoring to force UN withdrawal or impact the morale of international forces operating in the area
- Undermining governance structures and destabilizing the local environment

Armed groups employ various media outlets to leverage their attacks, including:

- Professional media outlets that possess the resources and reach to amplify the armed group's message
- Amateur outlets that may consist of individuals or smaller organisations disseminating content independently
- Social media platforms that offer a wide and instantaneous audience
- Different media formats such as print, video, audio, and internet content cater to different preferences and maximize exposure
- The recorded events may also serve as training aids and manuals for the armed group, supporting their information operations and enabling adjustments to their training, advertising, and techniques and procedures

In summary, armed groups exploit IED attacks by utilising media to shape narratives and achieve various objectives. The UN can leverage this propaganda for analysis, gaining insights into the enemy's motives and strategies. It is essential to remain attentive to individuals recording attacks, as it can provide valuable peacekeeping-intelligence.

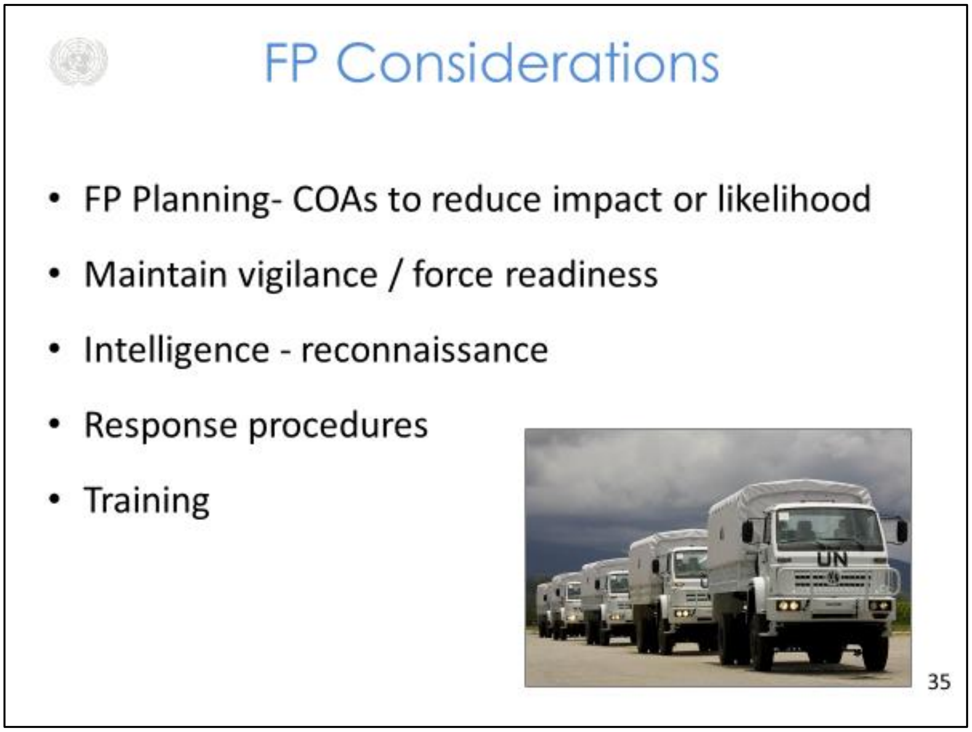
Slide 34

Force Protection Considerations

34

In this upcoming section of the instruction, we will analyse the topic of Force Protection and the potential threats posed by using Improvised Explosive Devices (IEDs) as instruments of attack.

Slide 35



FP Considerations

- FP Planning- COAs to reduce impact or likelihood
- Maintain vigilance / force readiness
- Intelligence - reconnaissance
- Response procedures
- Training

35

Effective planning and thorough rehearsals are crucial in preparing for all operations. It is essential to conduct comprehensive training sessions that cover the procedures for identifying threats, mitigating risks, detecting IEDs, and responding to IED attacks. Additionally, maintaining a rapid response capability in case of IED attacks is paramount, and regularly rehearsing response procedures reinforces operational readiness.

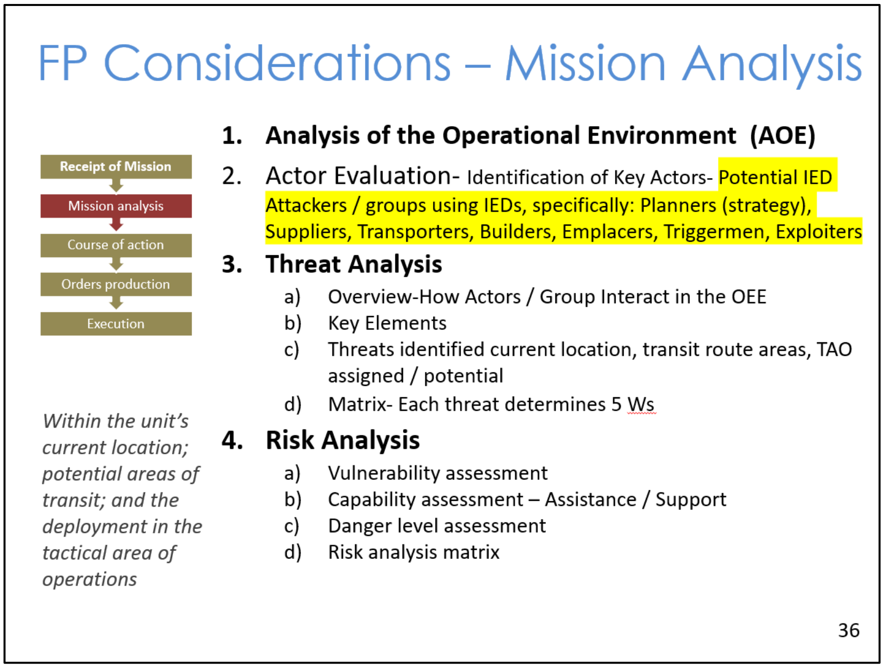
Actions taken during operations should be consistently reinforced at every opportunity. By incorporating fundamental principles into all aspects of preparation, we can enhance the success of operations and effectively mitigate explosive threats. The following key areas should be given due attention:

- Force Protection Planning: Develop courses of action (CoAs) aimed at reducing the impact or likelihood of IED attacks
- Vigilance and Force Readiness: Maintain a state of constant vigilance and ensure force readiness by actively monitoring any suspicious or out-of-the-ordinary behaviour, as well as indicators linked to IEDs
- Intelligence and Reconnaissance: Prioritise gathering peacekeeping-intelligence and conducting thorough reconnaissance to gather critical information on potential threats and their characteristics
- Response Procedures: Establish clear and well-defined procedures for responding to IED attacks, ensuring that personnel are trained

- Training: Dedicate training resources to educate and familiarize staff and commanders with a threat-based approach to Force Protection planning. This includes identifying threats, conducting risk analyses, and implementing effective courses of action to mitigate risks, specifically in an IED environment

By emphasising these aspects throughout the training material, we can provide valuable insights into enhancing Force Protection planning and creating a strong counter to IED threats.

Slide 36



FP Considerations – Mission Analysis

Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Within the unit's current location; potential areas of transit; and the deployment in the tactical area of operations

1. **Analysis of the Operational Environment (AOE)**
2. Actor Evaluation- Identification of Key Actors- Potential IED Attackers / groups using IEDs, specifically: Planners (strategy), Suppliers, Transporters, Builders, Emplacers, Triggermen, Exploiters
3. **Threat Analysis**
   a) Overview-How Actors / Group Interact in the OEE
   b) Key Elements
   c) Threats identified current location, transit route areas, TAO assigned / potential
   d) Matrix- Each threat determines 5 Ws
4. **Risk Analysis**
   a) Vulnerability assessment
   b) Capability assessment – Assistance / Support
   c) Danger level assessment
   d) Risk analysis matrix

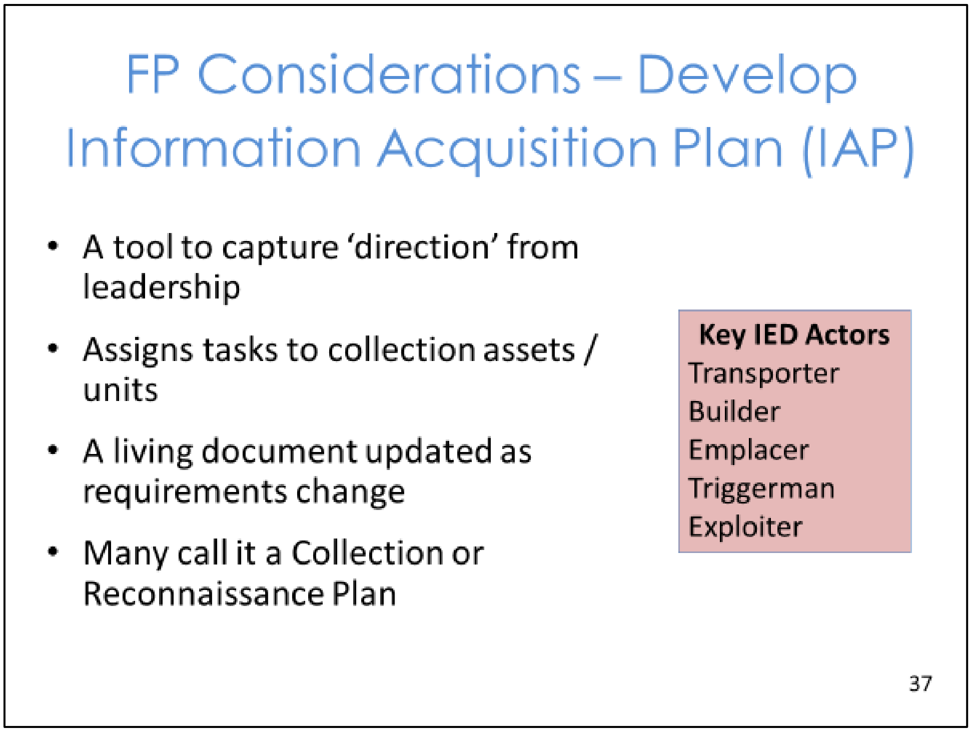
36

The commander's and staff's understanding of the operational environment and potential threats relies heavily on comprehensive mission analyses, the AOE, and evaluations of key actors to facilitate the identification of armed groups that possess an IED network. These groups typically consist of planners, suppliers, transporters, builders, triggermen, and exploiters. Conducting thorough threat analyses allows the units to assess risks, identify actions to mitigate IED threats, and minimise the potential and consequences of an attack or event.

Mitigating IED threats involves a coordinated approach at the strategic, operational, and tactical levels. All UN units share the collective responsibility of increasing force protection by gathering and exchanging vital information about IED threats. Therefore, assessment and planning processes should integrate expertise in explosive threat mitigation whenever necessary. This information contributes to more accurate assessments, guides capability requirements, and facilitates informed decision-making to mitigate the impact of IEDs on both the UN Mission and the civilian population.

Like other peacekeeping-intelligence products, IED threat assessments require continuous reviews to stay abreast of developments in tactical, operational, and strategic situations. Regularly reassessing and updating these assessments ensures that they remain current and reflect the evolving threat landscape.

Slide 37



FP Considerations – Develop Information Acquisition Plan (IAP)

- A tool to capture 'direction' from leadership
- Assigns tasks to collection assets / units
- A living document updated as requirements change
- Many call it a Collection or Reconnaissance Plan

Key IED Actors
Transporter
Builder
Emplacer
Triggerman
Exploiter

37

Develop an enhanced Information Acquisition Plan (IAP) for Disrupting IED Networks

Objective: The primary goal of this Information Acquisition Plan (IAP) is to gather crucial peacekeeping-intelligence on key IED network actors, including the Transporter, Builder, Emplacer, Triggerman, and Exploiter. By effectively collecting information and indicators related to these actors, we aim to disrupt the network's operations at various stages of the threat chain.

Leadership Engagement: Establish a process to capture clear direction and objectives from leadership regarding the desired outcomes of the IED network disruption efforts. Regular communication with leadership will ensure alignment and updated guidance as requirements evolve.

Task Assignment: Assign specific tasks to dedicated collection assets or units to acquire information on the identified key IED network actors. Each asset/unit will be responsible for gathering peacekeeping-intelligence related to a specific actor using appropriate methods and resources.

Living Document: Maintain a living document that serves as the central repository. This document will be continuously updated to reflect changes in requirements, progress, and emerging information needs. Regular reviews will ensure its relevance and effectiveness throughout the disruption process.

Cell Organisation: Recognise that each function within the IED network may be organised into one or more cells, with participants often unaware of other cells' existence. Develop strategies to identify and track these cells, aiming to uncover the broader network structure and interconnections.

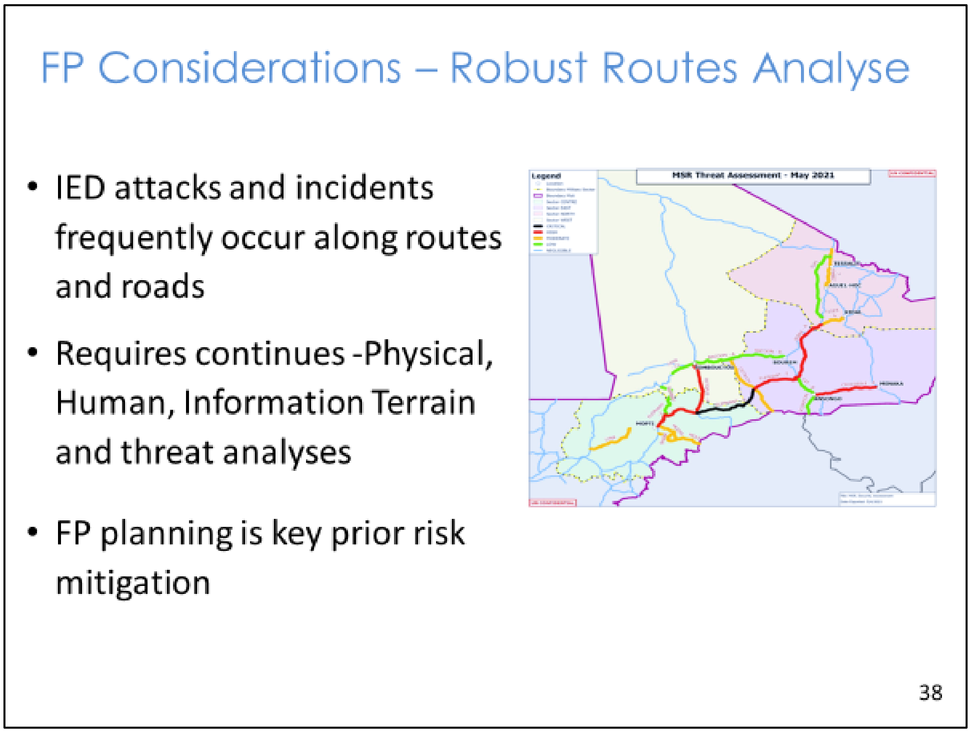
Disruption Opportunities: Identify opportunities at each stage of the threat’s chain to disrupt the network’s operations directly or indirectly. Direct interventions from the Host nation or the UN Mission may involve blocking access to funding, materials, or personnel involved in bomb-making activities. Indirect interventions involve gathering valuable information from critical and noncritical functions within the network, allowing for the identification, tracking, and exploitation of vulnerabilities that impede potential attacks.

Detection and Tracking: Implement comprehensive mechanisms to detect and track the IED network. Focus on identifying characteristics such as theft or unauthorised acquisition of precursor chemicals, which may provide insights into the network's structure, sustainability, and modus operandi. Combine peacekeeping-intelligence from multiple sources to paint a comprehensive picture of the network's activities.

Collaboration and Integration: Promote collaboration and information sharing among relevant agencies and stakeholders involved in countering IED networks. Foster partnerships to leverage expertise, resources, and insights to enhance the effectiveness of information acquisition efforts. Regularly integrate and analyse acquired peacekeeping-intelligence to generate actionable insights.

By implementing this Enhanced Information Acquisition Plan (IAP) focused on the IED network, we aim to gather critical peacekeeping-intelligence on key IED network actors and disrupt their operations. Through ongoing adaptation and collaboration, we can enhance our understanding of the network's structure and vulnerabilities, ultimately impairing its ability to carry out potential attacks.

Slide 38



FP Considerations – Robust Routes Analyse

- IED attacks and incidents frequently occur along routes and roads
- Requires continues -Physical, Human, Information Terrain and threat analyses
- FP planning is key prior risk mitigation

Legend
MSR Threat Assessment - May 2021
38

An enhanced IED Route Analysis and Risk Mitigation is required to mitigate risks associated with IED threats. Given that IED attacks and incidents frequently occur along routes and roads, it is crucial to capture relevant details and employ pattern analysis techniques. This approach will assist Force Protection (FP) planners in developing predictive analyses, which, in turn, aid in the formulation of risk-mitigating Courses of Action (CoAs). To support these efforts, we have developed a map tool that incorporates route coding and risk threshold indicators.

Route Analysis: Thoroughly analyse historical data on IED attacks and incidents, specifically focusing on their locations along routes and roads. Identify patterns, including common attack zones, preferred target areas, and modus operandi employed by threat actors. This analysis will provide insights into high-risk areas and potential attack patterns.

Predictive Analysis: Utilise the findings from route analysis and historical data to develop predictive analyses. By identifying trends and patterns, forecast potential areas and times at higher risk for future IED attacks. This proactive approach enables FP planners to allocate resources more effectively and implement targeted risk mitigation measures.

Risk Mitigation Courses of Action (CoAs): Leveraging the predictive analyses, working collaboratively with FP planners to develop risk mitigation CoAs. These CoAs should address identified high-risk areas and propose appropriate measures to reduce the vulnerability of routes and roads to IED attacks. Consider physical barriers, increased security presence, surveillance technologies, peacekeeping-intelligence-driven operations, and community engagement as potential components of the CoAs.

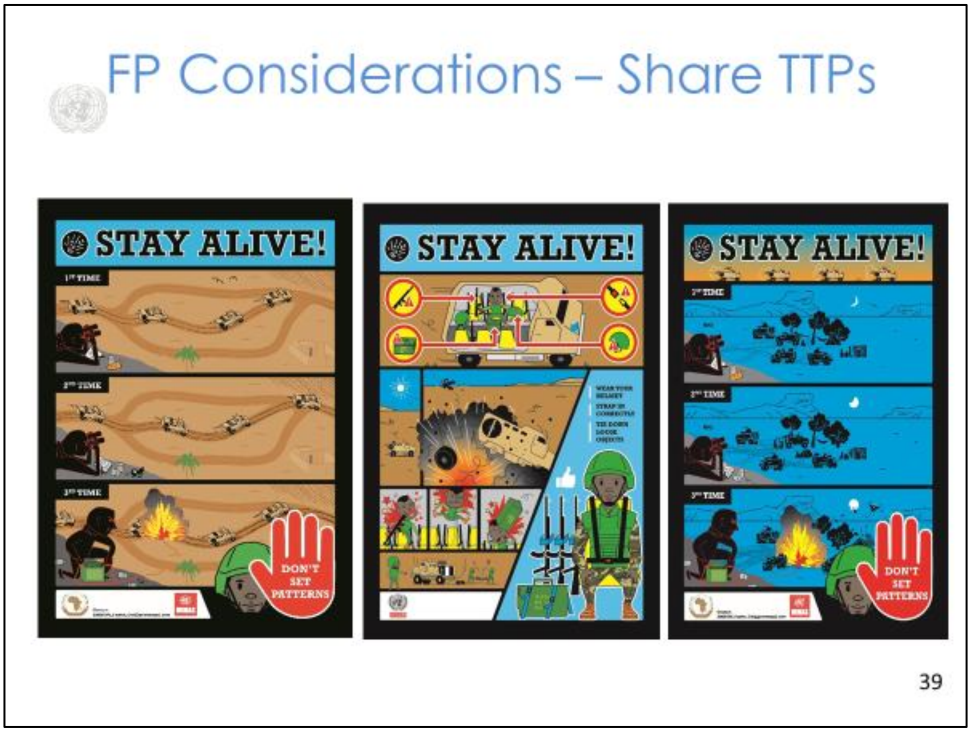
Route Coding Map Tool: Introduce a user-friendly map tool designed to aid in the route coding process. This tool will allow for the systematic categorization of routes based on their vulnerability to IED attacks. Establish clear criteria for coding routes, considering factors such as historical attack data, geographical features, local demographics, and peacekeeping-intelligence reports. The map tool should visually represent the coded routes, providing FP planners with a clear understanding of the threat landscape.

Risk Threshold Indicators: Implement risk threshold indicators within the map tool to provide FP planners with an immediate assessment of the level of risk associated with each coded route. These indicators can be colour-coded or categorized based on severity levels. They will assist planners in prioritizing resource allocation and risk mitigation efforts, focusing on routes that exceed predetermined risk thresholds.

Continuous Evaluation and Adaptation: Regularly assess and update the map tool, route coding, and risk threshold indicators based on new information, emerging threats, and changes in the operational environment. Maintain an iterative approach to ensure the tool remains relevant and accurate over time.

By employing this enhanced approach to route analysis and risk mitigation, we can effectively anticipate and address the threat of IED attacks along routes and roads. The combination of predictive analyses, risk mitigation CoAs, and the map tool with route coding and risk threshold indicators will provide FP planners with valuable insights to make informed decisions and allocate resources efficiently, thereby enhancing overall force protection measures.

Slide 39



FP Considerations – Share TTPs

39

Effective information sharing on IED threats is crucial within UN missions to mitigate risks and ensure the safety of all components. This slide exemplifies a document shared among all components to aid in the mitigation of IED threats. In addition to sharing tactics, techniques, and procedures (TTPs), information sharing and coordination regarding IEDs within UN missions should be actively supported by all components. Establishing an peacekeeping-intelligence cell (for example, JMAC) responsible for enhancing situational awareness is essential to facilitate effective coordination and support to site-exploitation operations and information/intelligence requests.

Information Sharing and Coordination: Promote the importance of sharing information on IED threats with the UN Mission. Encourage all components to actively contribute to and utilise the shared document, ensuring that relevant information and updates regarding IED threats are disseminated promptly. Foster a culture of cooperation and collaboration among components, emphasising the collective responsibility to mitigate IED risks.

Intelligence Cell: Establish an peacekeeping-intelligence cell dedicated to enhancing situational awareness for all forces involved in operations. This cell should serve as the central hub for coordinating peacekeeping-intelligence support to site-exploitation operations and responding to requests for information/intelligence related to IED threats. Their role is critical in ensuring that relevant peacekeeping-intelligence reaches the right personnel in a timely manner.

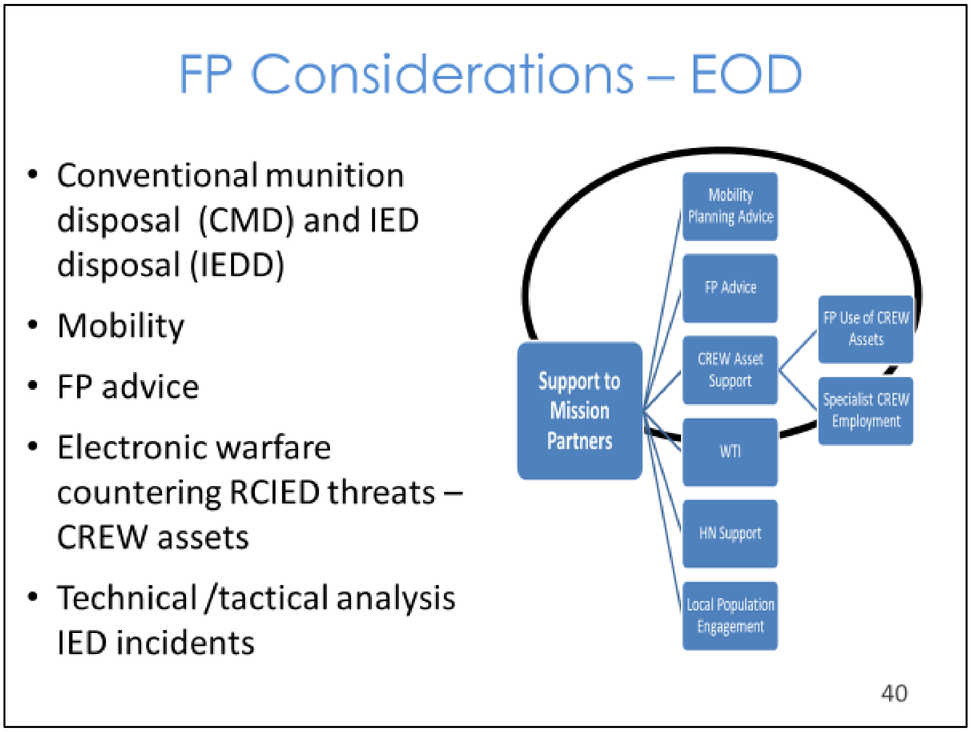
Prioritisation of Collection Assets: Ensure that mission leadership and commanders prioritise the allocation of peacekeeping-intelligence, surveillance, and reconnaissance assets to support the counter-IED / C-EO campaign. These assets should be assigned based on the specific needs and priorities identified by mission leadership. Persistent surveillance capabilities are particularly crucial for supporting focused reconnaissance response forces, post-incident exploitation, and the collection of geospatial information to support planning and ongoing operations.

Coordination with T/PCCs: Emphasise the need for coordination among Troop/Police Contributing Countries (T/PCCs) regarding IED counter capabilities. Encourage the sharing of peacekeeping-intelligence, surveillance, weapon technical peacekeeping-intelligence, search, and explosive ordnance disposal (EOD) expertise and capabilities. Mutual trust, respect, and coordination among T/PCCs will enhance the effectiveness of IED threat mitigation efforts.

Mission Partners as Knowledge Sources: Recognise that mission partners also serve as valuable sources of knowledge on IED threats and TTPs. Encourage open communication and information sharing with mission partners, leveraging their experiences and expertise to enhance overall situational awareness and response capabilities.

By enhancing information sharing and coordination within UN missions, we can strengthen the collective ability to mitigate IED threats effectively. Through the establishment of an peacekeeping-intelligence cell, prioritisation of collection assets, coordination with T/PCCs, and leveraging mission partner knowledge, we can improve situational awareness and develop robust counter-IED capabilities. Ultimately, these efforts contribute to successful peace support operations built on mutual trust, respect, and the shared commitment to mitigating IED risks.

Slide 40



FP Considerations – EOD

- Conventional munition disposal (CMD) and IED disposal (IEDD)
- Mobility
- FP advice
- Electronic warfare countering RCIED threats – CREW assets
- Technical /tactical analysis IED incidents

Support to Mission Partners

Mobility Planning Advice

FP Advice

CREW Asset Support

WTI

HN Support

Local Population Engagement

FP Use of CREW Assets

Specialist CREW Employment

40

The Military Explosive Ordnance Disposal (EOD) unit plays a crucial role in providing support to UN tactical police and military units. As an essential component of a UN force, EOD units are primarily responsible for countering explosive ordnance threats during operations. The term EOD encompasses various capabilities, including Conventional Munition Disposal (CMD) and Improvised Explosive Device Disposal (IEDD). CMD focuses on eliminating and removing IED components from an area.

EOD units serve as operational enablers, contributing to the goals of Freedom of Movement (FoM) and Force Protection (FP). These units are consistently in high demand, and there is typically a shortage of adequately trained personnel. Moreover, the nature of their work exposes them to significant risks. Consequently, EOD units are usually under the direct control of the formation headquarters, and their tasks are prioritised accordingly.

In addition to their primary role in countering explosive threats, EOD units may also be assigned other operations such as search, force protection, disposal, and component recording and recovery. This comprehensive approach effectively mitigates explosive ordnance threats in support of Force Protection (FP) and Protection of Civilians (PoC).

EOD units can be organised in separate ways. Either they can be combined with other arms or capabilities within a composite unit, where the same unit possesses both EOD and search capabilities, or they can be organised into separate units and brought together for specific operations or tasks. Regardless of the organisational structure, it is common for EOD and search assets to be deployed together.

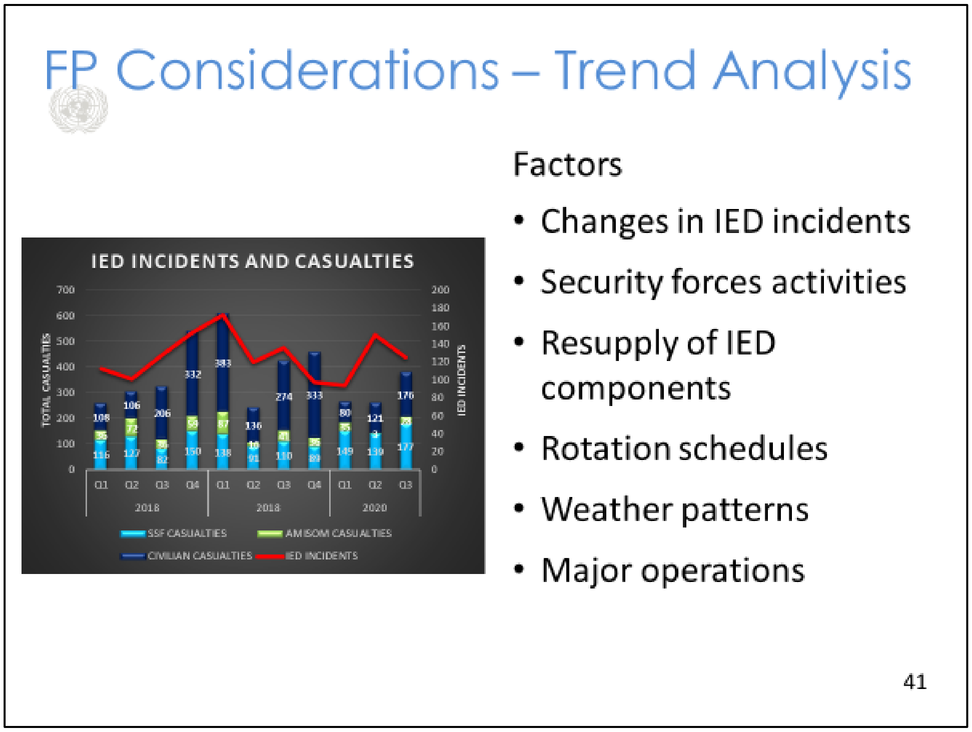
Electronic Warfare (EW): Electronic warfare refers to the use of electromagnetic spectrum to detect, deceive, or deny enemy forces the effective use of electronic systems. In the context of countering Radio-Controlled Improvised Explosive Device (RCIED) threats, EW involves the application of electronic techniques to disrupt or neutralise the radio signals used to remotely control explosive devices.

RCIED Threats: RCIEDs are improvised explosive devices that are remotely controlled using radio signals. These threats pose a significant risk to military forces, law enforcement agencies, and civilians, as they can be detonated from a safe distance by the perpetrators. Countering RCIED threats involves employing various measures to detect, locate, and neutralise these devices.

CREW Assets: CREW stands for Counter Radio-Controlled Improvised Explosive Device Electronic Warfare. CREW assets are specialised electronic warfare systems and equipment designed to detect and counter RCIED threats. These assets include jammers, signal detectors, signal peacekeeping-intelligence systems, and other electronic countermeasures. CREW assets are used to disrupt or disable the radio signals that RCIEDs rely on for their remote control, preventing the detonation of these devices.

Technical/Tactical Analysis of IED Incidents: Technical analysis of IED incidents involves examining the components, construction, and design of improvised explosive devices. This analysis aims to gather information about the type of explosives used, the triggering mechanism employed, and any unique features or modifications that could provide insights into the perpetrators' capabilities or intentions. Technical analysis helps in understanding the characteristics and potential dangers associated with specific IEDs, which can aid in developing effective countermeasures.

Slide 41



FP Considerations – Trend Analysis

Factors

- Changes in IED incidents
- Security forces activities
- Resupply of IED components
- Rotation schedules
- Weather patterns
- Major operations

41

Pattern the analysis of IED incidents: It is important to consider various factors that can provide valuable insights into the patterns and dynamics of these attacks. Some of the factors to include in the analysis are:

Pattern Analysis: Examining patterns in IED incidents can reveal valuable information about the tactics, techniques, and procedures (TTPs) employed by the perpetrators. This analysis may involve identifying similarities in target selection, attack methods, or timing of the incidents. Comparing IED incidents to major events, UN and host nation operations, and other relevant factors can help identify potential connections or correlations.

Security Forces Activities: Analysing IED incidents in relation to security forces activities can provide insights into the impact of specific operations or countermeasures on the frequency or intensity of attacks. Changes in the level of security presence, military operations, or police law enforcement activities may influence the behaviour of adversaries and impact the occurrence of IED incidents.

Resupply of IED Components: Understanding the resupply of IED components is crucial in analysing the sustainability and capabilities of the perpetrators. Monitoring the availability and acquisition of materials such as explosives, detonators, and other necessary components can help identify potential sources and supply chains. Disrupting or interdicting the resupply process can significantly impact the effectiveness of IED attacks.

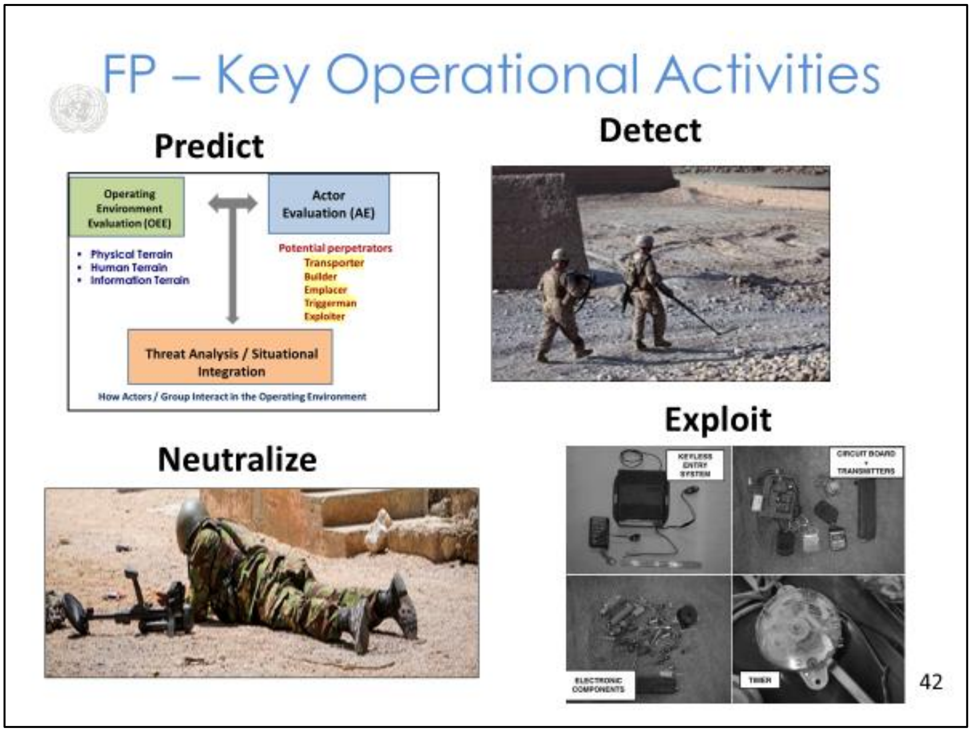
Rotation Schedules: Analysing rotation schedules of UN military and police units or security forces operating in a particular area can provide insights into the vulnerability and adaptation patterns of the adversaries. Changes in the timing of IED incidents may be correlated with the arrival or departure of specific units, as perpetrators may exploit the transition periods to carry out attacks or adjust their tactics accordingly.

Weather Patterns: Considering weather patterns is essential as they can impact the operational environment and affect the perpetrators' ability to conduct IED attacks. Adverse weather conditions, such as heavy rain, snowstorms, or extreme heat, may influence the frequency or effectiveness of attacks. For example, certain weather conditions may hinder the planting or detonation of IEDs, leading to fluctuations in the incident rate.

Major Operations: Analysing IED incidents in relation to major police or military operations can provide insights into the tactics and strategies employed by adversaries during intense conflict situations. Examining how the occurrence of IED incidents changes during or after major operations can help identify trends, adjust tactics, and develop effective countermeasures.

By incorporating these factors into the analysis of IED incidents, security forces and counter-IED / C-EO teams can gain a comprehensive understanding of the threat landscape, enabling them to adapt their strategies, allocate resources effectively, and enhance the overall effectiveness of their operations.

Slide 42



FP – Key Operational Activities

Predict

Operating Environment Evaluation (OEE)

- Physical Terrain
- Human Terrain
- Information Terrain

Actor Evaluation (AE)

Potential perpetrators
Transporter
Builder
Emplacer
Triggerman
Exploiter

Threat Analysis / Situational Integration

How Actors / Group Interact in the Operating Environment

Detect

Exploit

KEYLESS ENTRY SYSTEM
CIRCUIT BOARD + TRANSMITTERS
ELECTRONIC COMPONENTS
TIMER

Neutralize

42

To better understand Counter-IED (C-IED) / Counter Explosive Ordnance (C-EO) operations, it is important to address key activities that contribute to a comprehensive understanding of the operational IED environment.

Predict: The predictive aspect of C-IED / C-EO involves conducting analytical actions to maintain a comprehensive understanding of the operational IED environment, such as the Analyses of the Operation Environment. This includes analysing various factors to forecast IED operations, such as the attacker's cell structures, systems, networks, training, equipment, infrastructure, tactics, techniques & procedures (TTPs), support mechanisms (e.g., IED materiel), and other actions. By predicting IED operations, we can gain a more concise understanding of the threat landscape and better prepare for potential attacks.

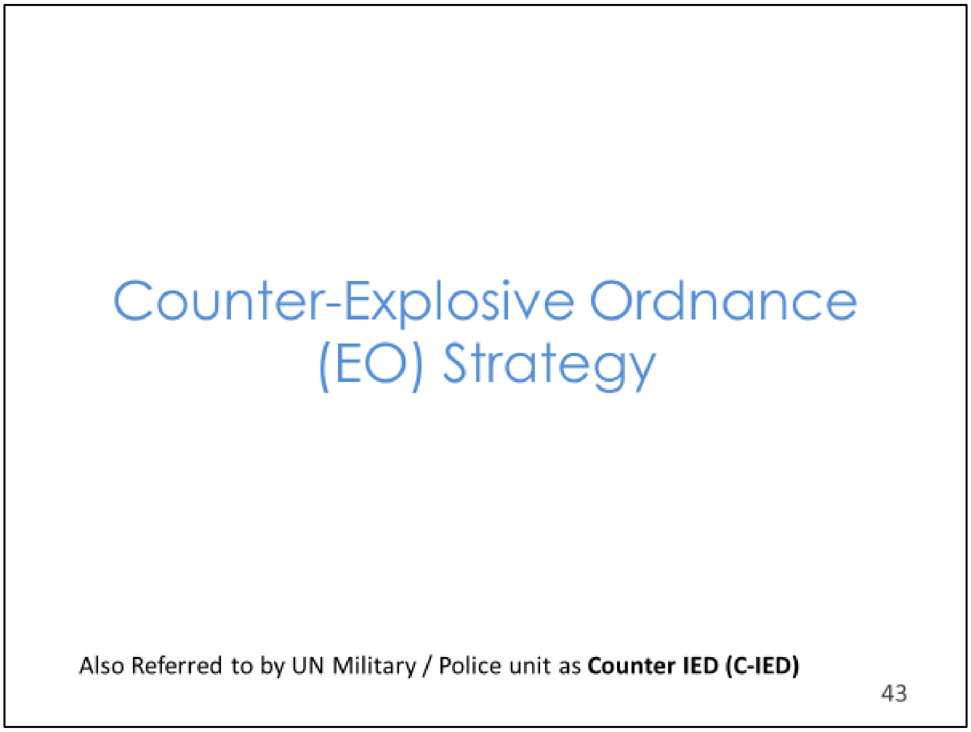
Neutralise/Dispose: To prevent uncontrolled detonation, IEDs must be disposed of safely through deliberate detonation, disruption, or neutralization. The neutralisation and disposal of IEDs are crucial to ensure the safety of peacekeepers and the local populace. This involves employing specialised techniques and equipment to render the explosive device harmless while minimising the risk to personnel and infrastructure.

Detect: The detection phase occurs after an IED has been emplaced and involves activities designed to identify and locate various elements related to the threat. This includes personnel involved in IED activities, explosive devices (including their component parts), equipment used in the emplacement process, caches of IED components, and weapons associated with the threat. Detection efforts involve employing a range of technical and tactical means, such as surveillance, peacekeeping-intelligence gathering, and search operations, to identify and locate IED-related elements and networks.

Exploit: Exploitation is the process of recording and analysing events and associated physical materials related to IED incidents. The objective of exploitation is to gain a deeper understanding of the aggressor's methods of operation, relationships, and the capabilities of the devices used. Exploitation can occur at any stage within the IED system, and it is crucial to conduct it as early as possible. For example, the recovery and exploitation of IED components provides valuable information about the bombmaker's abilities and serves as a starting point to trace the aggressor's supply chain.

By addressing these key activities in C-EO, the UN and its partners can enhance their understanding of the IED threat environment, improve their ability to predict and prevent attacks, effectively neutralise or dispose of IEDs, detect IED-related elements, and exploit gathered information to disrupt and dismantle IED networks more effectively.

Slide 43



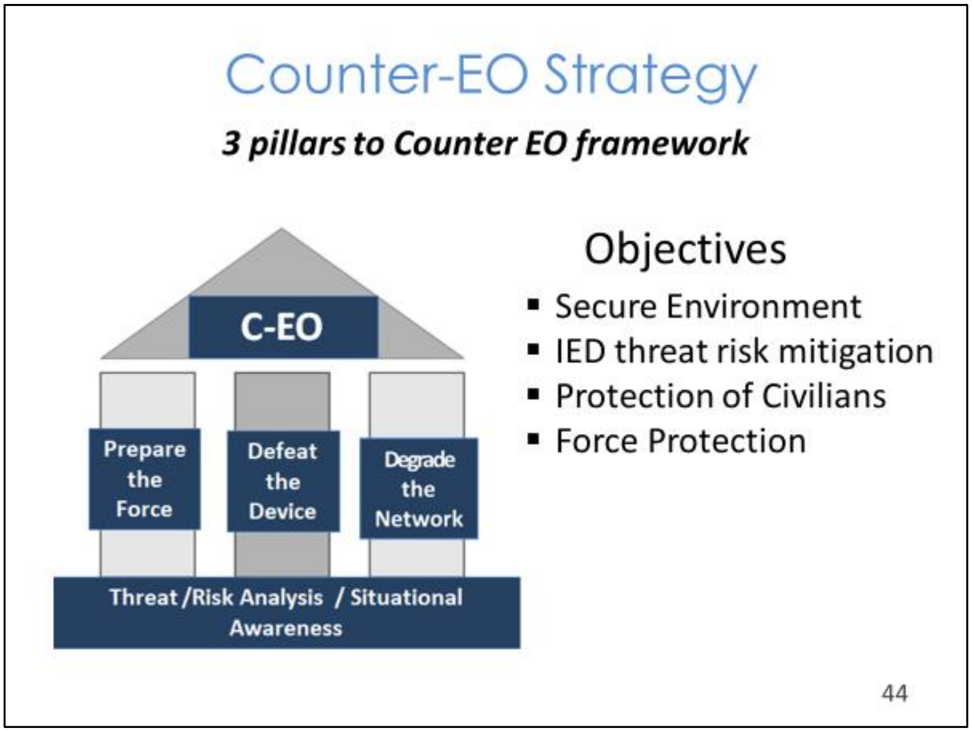
Counter-Explosive Ordnance (EO) Strategy

Also Referred to by UN Military / Police unit as **Counter IED (C-IED)**

43

Transition slide.

Slide 44



Counter-EO Strategy

3 pillars to Counter EO framework

C-EO

Prepare the Force

Defeat the Device

Degrade the Network

Threat /Risk Analysis / Situational Awareness

Objectives

- Secure Environment
- IED threat risk mitigation
- Protection of Civilians
- Force Protection

44

To conclude this lesson, it is essential to highlight the holistic UN strategy aimed at mitigating the risks posed by IED threats. The UN Secretary General recognise "Better protection against IEDs" as one of the critical necessities aligning with the UN mandate of peacekeeping and creating a secure environment for UN military and police units, as well as civilians. The objectives set for IED risk mitigation in UN missions include:

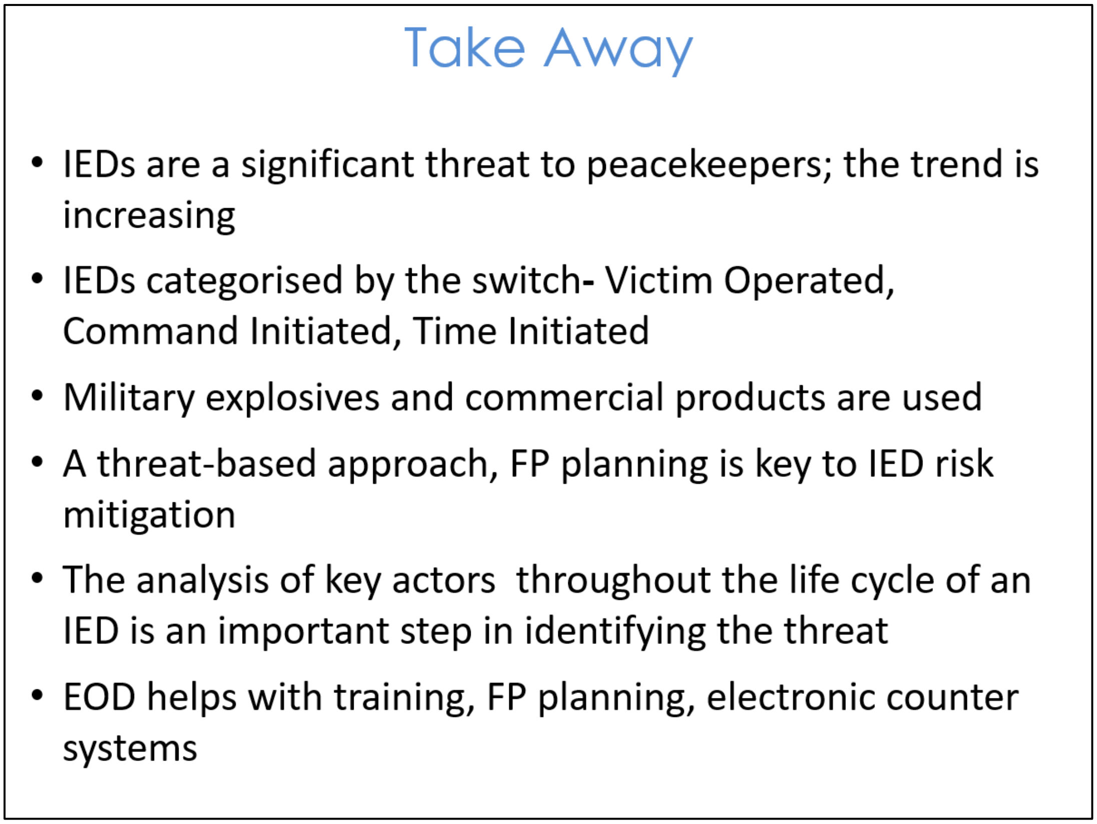
- Secure Environment: Ensuring a safe and secure environment for all UN components, interlocutors, and stakeholders to operate freely and without restrictions on their actions and movement
- IED Threat Risk Mitigation: Reducing casualties by mitigating the risk posed by IED threats. This involves implementing measures to detect, neutralise, and prevent IED attacks, thereby minimising their impact
- Protection of Civilians: Safeguarding the welfare and well-being of civilian populations in conflict-affected areas by countering IED threats. This includes measures to prevent harm to civilians and minimise the disruption caused by IED attacks
- Force Protection: Enhancing the protection of UN military and police units involved in peacekeeping missions. This encompasses implementing strategies and measures to reduce the vulnerability of UN personnel to IED attacks and ensure their safety and effectiveness in fulfilling their mission

The strategic term used by the UN for this approach is Counter EO (C-EO). C-EO refers to collective efforts aimed at defeating the IED system and reducing the impact or likelihood of IED attacks. It recognises that an IED is part of a broader system that includes actors, processes, and equipment involved in its deployment as a weapon. The C-EO doctrine consists of three pillars:

- Train the Force: This pillar focuses on training and preparing UN units by building capabilities in areas such as peacekeeping-intelligence, situational awareness, threat analysis, identification, actions/drills, force protection planning, local outreach, and best practice
- Defeat the Device: This pillar emphasises activities to improve freedom of movement and mission accomplishment by reducing the effects of IEDs. It includes search activities, IED disposal and countermeasures (IEDD and CMD activities), and support for minimising the threat of IEDs
- Degrade the Network: This pillar involves peacekeeping-intelligence gathering, establishing partnerships, evidence collection, and exploitation to disrupt and reduce the capabilities of IED networks. It also includes proactive activities to prevent and pre-empt IED attacks

In UN missions, the term IED-TM is used to refer to the comprehensive approach that focuses on the physical, procedural, and/or training aspects related to countering IED threats. Additionally, the term Counter IED (C-IED) is commonly used in the UN lexicon to denote activities related to countering IED threats.

Slide 45



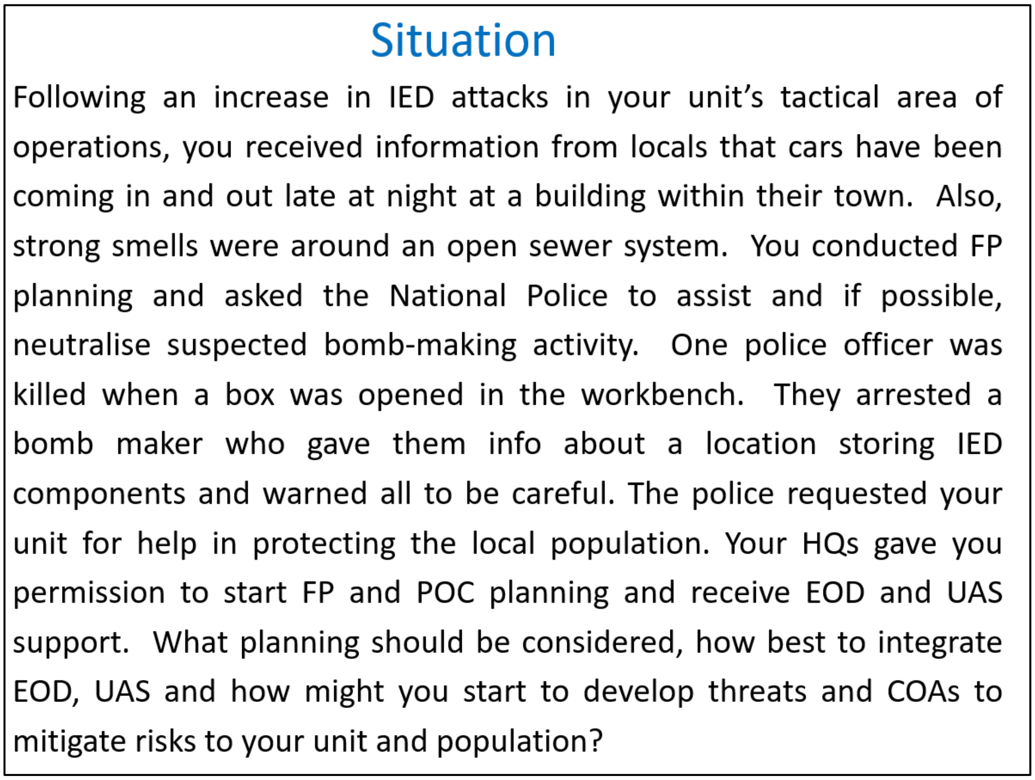
Take Away

- IEDs are a significant threat to peacekeepers; the trend is increasing
- IEDs categorised by the switch- Victim Operated, Command Initiated, Time Initiated
- Military explosives and commercial products are used
- A threat-based approach, FP planning is key to IED risk mitigation
- The analysis of key actors throughout the life cycle of an IED is an important step in identifying the threat
- EOD helps with training, FP planning, electronic counter systems

Summary

- IEDs pose a significant threat to peacekeepers, and the trend of such attacks is increasing
- IEDs can be categorized based on the switch type: Victim Operated, Command Initiated, or Time Initiated. Understanding these categories helps in identifying the potential methods of activation and the associated risks
- Both military explosives and commercial products are utilised in the construction of IEDs, highlighting the diverse sources of materials that IED networks can access
- Implementing a threat-based approach and incorporating force protection (FP) planning are crucial elements in mitigating the risks associated with IEDs
- Analysing key actors involved throughout the life cycle of an IED is an important step in identifying the threat landscape
- EOD (Explosive Ordnance Disposal) plays a crucial role in various aspects, including training, FP planning, and the deployment of electronic counter systems

LA Slide 46



Situation

Following an increase in IED attacks in your unit's tactical area of operations, you received information from locals that cars have been coming in and out late at night at a building within their town. Also, strong smells were around an open sewer system. You conducted FP planning and asked the National Police to assist and if possible, neutralise suspected bomb-making activity. One police officer was killed when a box was opened in the workbench. They arrested a bomb maker who gave them info about a location storing IED components and warned all to be careful. The police requested your unit for help in protecting the local population. Your HQs gave you permission to start FP and POC planning and receive EOD and UAS support. What planning should be considered, how best to integrate EOD, UAS and how might you start to develop threats and COAs to mitigate risks to your unit and population?

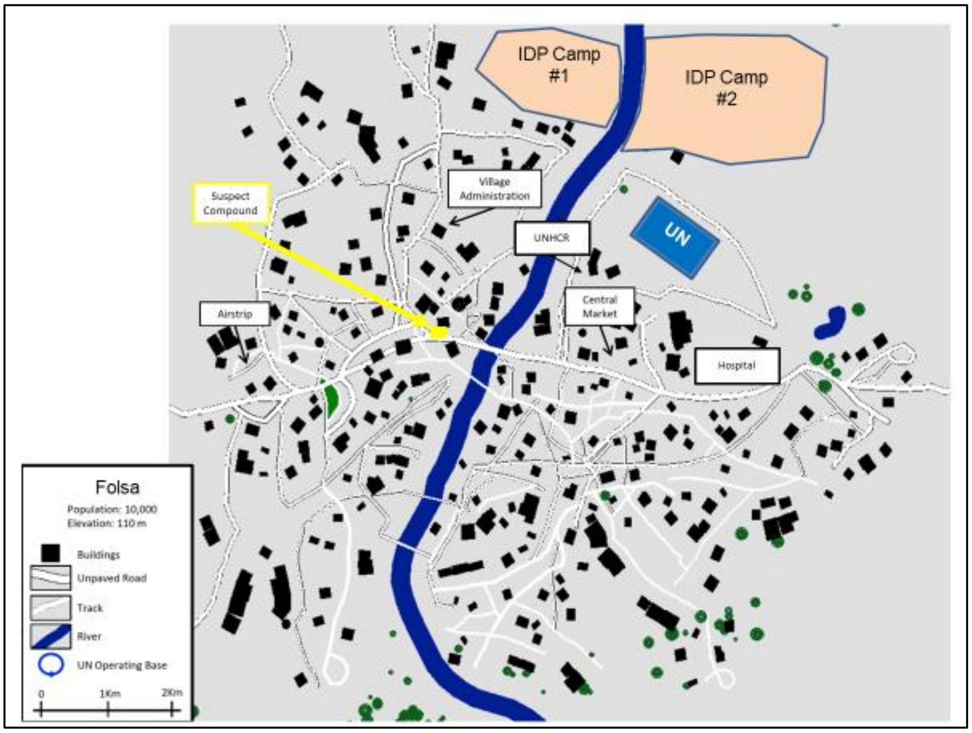
RESOURCES Projector to show slides or print and handout; 1 flip chart, markers

TIME Total: approx 30 minutes

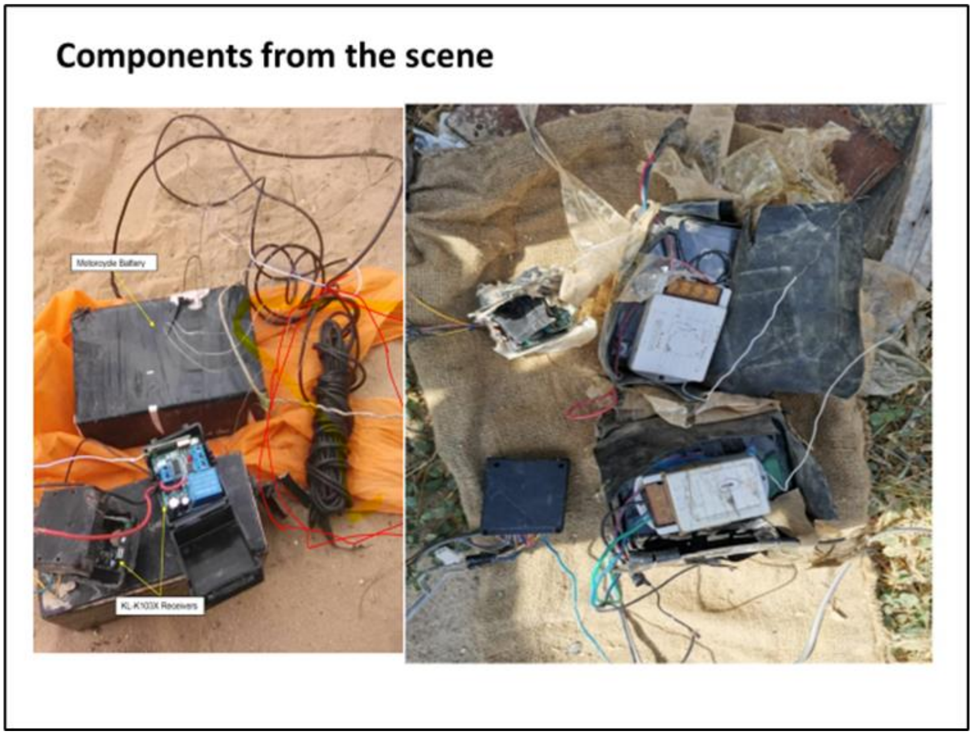
Present the situation and backup slides. Break out into subgroups; present the situation and back up slides. Have groups discuss and write down their planning considerations for future operations. Have them return to the plenary and discuss their planning considerations, threats, and possible mitigating measures.

Also, ask how the unit might have planned better for FP prior to the detonation in the first building location.

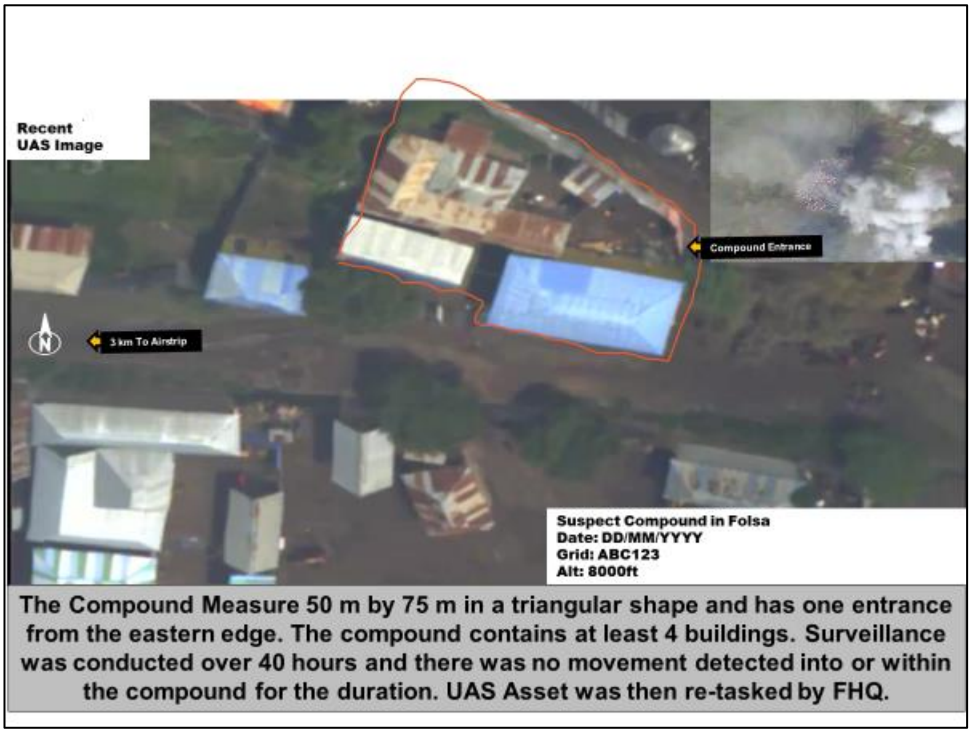
LA Slide 47



LA Slide 48


Components from the scene

LA Slide49



Suspect Compound in Folsa
Date: DD/MM/YYYY
Grid: ABC123
Alt: 8000ft

The Compound Measure 50 m by 75 m in a triangular shape and has one entrance from the eastern edge. The compound contains at least 4 buildings. Surveillance was conducted over 40 hours and there was no movement detected into or within the compound for the duration. UAS Asset was then re-tasked by FHQ.

Instructor notes to help facilitate - The situation should generate the following discussion points:

Resources: Identify units or assets that can assist, such as cordon teams, civil-military assets, EP (Explosive Protection) teams, EOD (Explosive Ordnance Disposal), IEDD (Improvised Explosive Device Disposal) assets, engineers search teams, additional UN police and military police, and explosive detection dogs. Discuss their roles and responsibilities in the operation.

Engaging Local Population Leadership: Explore strategies to engage with local population leaders to direct civilians away from blast areas. This includes understanding cultural sensitivities and effective communication methods to ensure their cooperation and safety.

Aerial Photos and Blast Area Identification: Discuss the significance of obtaining aerial photos of the compound and the surrounding area. Identify the blast area and establish safe zones to coordinate operations effectively.

Assets for Civilian Engagement and Liaison: Identify assets required to support civilian engagement and liaison, ensuring effective communication and understanding between UN personnel and the local population.

Incident Control Point (ICP) Establishment: Highlight the importance of setting up a well-defined Incident Control Point to manage operations efficiently and ensure effective coordination among all involved parties.

Community Engagement: Emphasize the importance of briefing EOD personnel and involving higher HQs in community engagement efforts to build trust and gather critical information.

Outer and Inner Cordon Establishment: Discuss the need for both outer and inner cordons to secure the area and prevent unauthorized access.

IED Threat Awareness: Reinforce the IED 5 C's (Confirm, Clear, Cordon, Control, Call) to all personnel, emphasizing their role in IED threat awareness and response.

Actions on IED Discovery: Develop procedures for different scenarios, such as finding an IED during a search operation or on the cordon. Ensure personnel are adequately trained to respond appropriately.

MEDEVAC/CASEVAC Plan and Civil Unrest Considerations: Formulate a comprehensive MEDEVAC/CASEVAC plan that considers the potential for civil unrest in the area. Discuss coordination with local medical facilities and evacuation routes.

Fire Service Support: Determine if fire service support is necessary and ensure it is requested if needed to enhance emergency response capabilities.

Traffic Control Points (TCPs): Define the setup and operation of TCPs to inspect vehicles for potential IED components or transporting IEDs, ensuring thorough security measures.

VBIEDs (Vehicle-Borne IEDs): Discuss the specific challenges and response protocols related to VBIEDs, considering their potential impact on the operation.

Heightened Base Security Defences: Review and strengthen base security defence considering the operation, ensuring the safety of personnel and assets.

Command, Control, and Communication: Establish clear procedures for command, control, and communication with HSSF (Hostile Environment Security Forces) and other supporting units to maintain operational effectiveness.

By addressing these discussion points, the team can better prepare for the operation, mitigate risks, and respond effectively to any potential threats.

Lesson 1.7

Introduction to Cyber Threats

The Lesson

Starting the Lesson

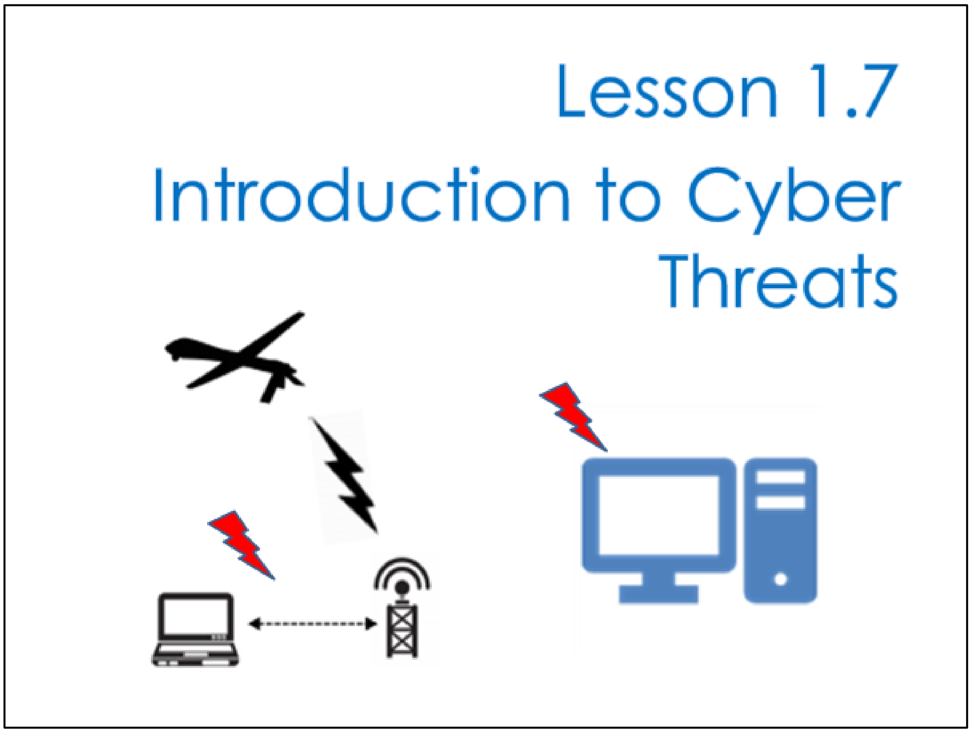
Overview

For an interactive start to this lesson, engage participants to seek their understanding of what they consider "Cyber Threats". Why they think it is important for UN units operating in a PKO environment to understand potential impacts on the UN Missions. Ask the group if they have any experiences with Cyber-attacks personally or professionally.

Member States have expressed concern over cyber threats and support UNDPO's efforts for the promotion of inter-agency cooperation and collaboration on information and cybersecurity-related matters. The UN's primary objective is to optimise information security within the UN Missions. This objective is pursued through the continuous and collective assessment of the UN system's exposure to internal and external cyber threats, to reduce risks to UN Missions and other UN organisations, particularly at the operational and tactical levels. In this training material, our aim is to familiarise the participants on the rise in cyber-attacks and the impact on tactical operations.

Strategic References: 6th review of the UN Global Counter-Terrorism Strategy A/RES/72/284; UN Security Council Resolution 2341 (2017); UN Security Council Resolution 2370 (2017); and Security Council text S/2015/939 (Madrid guiding principles)

Slide 1



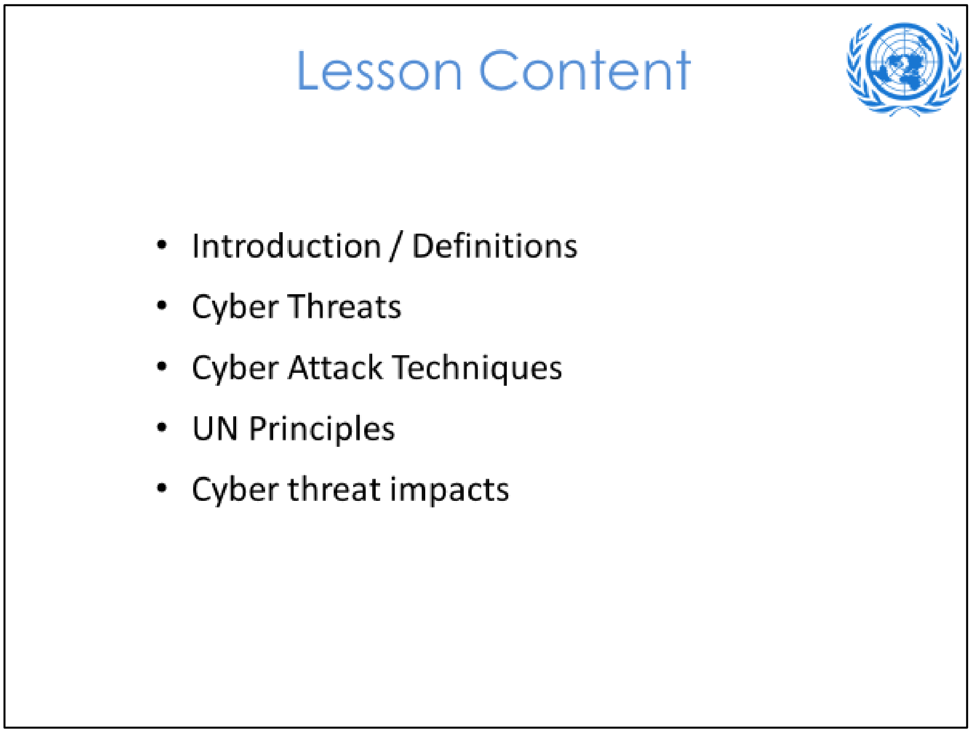
Lesson 1.7

Introduction to Cyber Threats

Welcome to this lesson, designed to enhance your understanding of the conceptual framework surrounding cyber threats. We will delve into the intricacies of cyber threats, aiming to familiarize you with their various aspects and implications.

Our primary objective is to equip you with a basic understanding of the conceptual framework that underpins cyber threats. By the end of this lesson, you will possess the knowledge necessary to navigate the landscape of cybersecurity effectively.

Slide 2



Lesson Content

- Introduction / Definitions
- Cyber Threats
- Cyber Attack Techniques
- UN Principles
- Cyber threat impacts

In this lesson, we will cover the following important topics related to cybersecurity:

Cyber Threats: We will explore the various threats faced both during missions and in day-to-day operations. Understanding these threats is crucial as they directly impact us. We will discuss how these threats can compromise our security, compromise sensitive information, or disrupt critical systems. It is essential to be aware of these threats to mitigate and respond to them effectively.

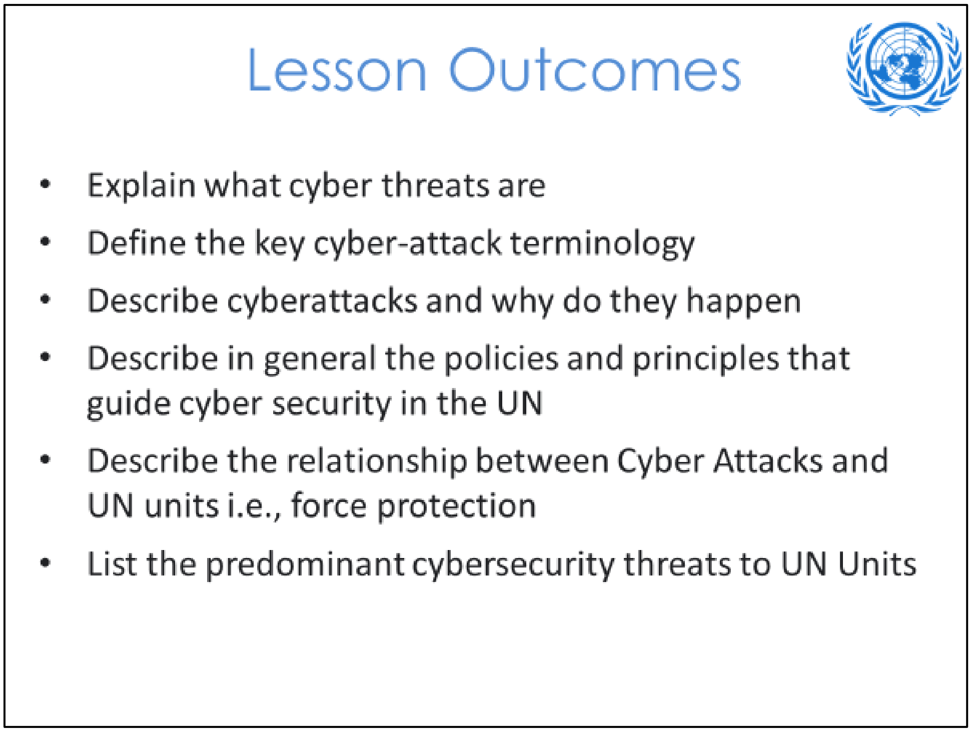
Cyber Attack Techniques: We will delve into the diverse range of techniques employed by cyber attackers. This can include the use of malicious software, viruses, and social engineering tactics like baiting on social media. These techniques have evolved and refined over time, making us all susceptible to attacks. By learning about these techniques, we can better recognise and defend against them, enhancing our overall cybersecurity posture.

UN Principles: We will examine the UN principles that underpin efforts to mitigate cyber risks. These principles provide a framework for promoting responsible behaviour, cooperation, and accountability in cyberspace. Understanding these principles is crucial for aligning our actions with international norms and best practices, ensuring a secure and stable digital environment.

Cyber Effects: We will analyse the specific threats faced by the Unit and its personnel while on missions. Cyber-attacks can have significant consequences, ranging from compromising sensitive information and disrupting operations to endangering the safety and well-being of individuals. By understanding these effects, we can implement appropriate measures to protect ourselves and mitigate potential risks.

By comprehensively covering these topics, we aim to enhance your knowledge and awareness of cybersecurity issues, equipping you with the tools and understanding necessary to effectively navigate the evolving cyber landscape.

Slide 3



Lesson Outcomes

- Explain what cyber threats are
- Define the key cyber-attack terminology
- Describe cyberattacks and why do they happen
- Describe in general the policies and principles that guide cyber security in the UN
- Describe the relationship between Cyber Attacks and UN units i.e., force protection
- List the predominant cybersecurity threats to UN Units

Here are the improved learning outcomes for this lesson:

Understand Cyber Threats: Gain a clear understanding of what cyber threats entail, including the types of risks and potential consequences they pose to individuals and organisations. Develop the ability to identify and assess different cyber threats.

Define Key Cyber Attack Terminology: Define and familiarise yourself with essential terminology related to cyber-attacks. This includes terms such as malware, phishing, social engineering, ransomware, and other common attack techniques. By understanding these terms, you will be better equipped to discuss and address cyber threats effectively.

Explore the Nature of Cyber Attacks: Explore the motivations and underlying reasons behind cyber-attacks. Gain insights into why cyber-attacks occur and the potential impact they can have on individuals, operations, organisations, and critical infrastructure. Develop an awareness of the evolving nature of cyber-attacks and the importance of proactive defence.

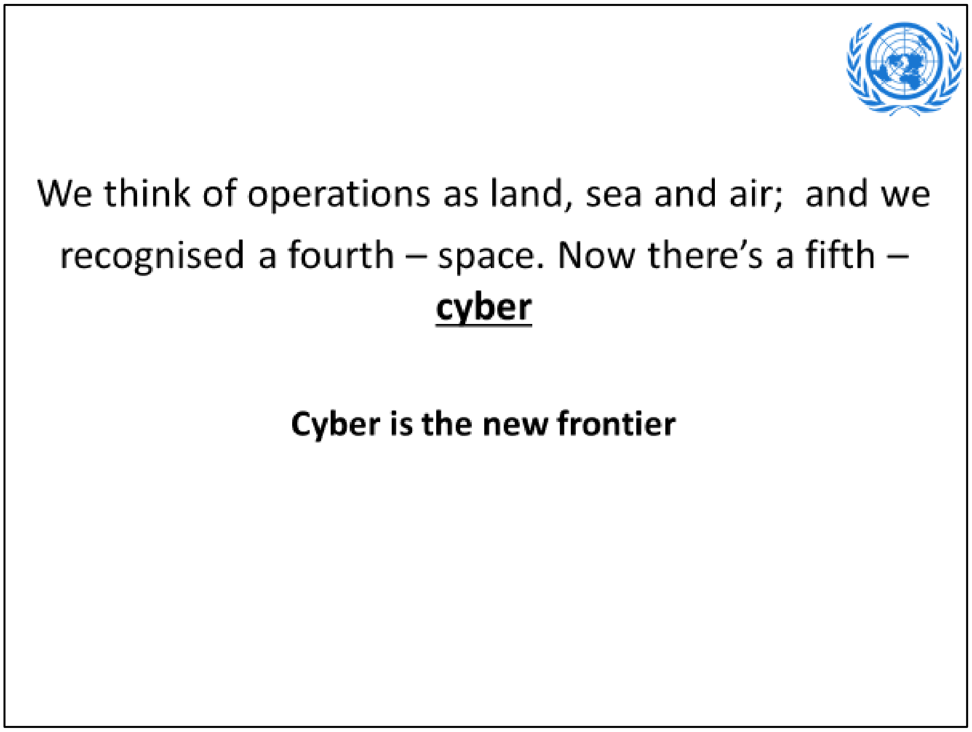
Understand UN Cybersecurity Policies and Principles: Gain a comprehensive overview of the policies and principles that guide cybersecurity within the United Nations. Explore the UN's approach to cybersecurity, its emphasis on international cooperation, and the promotion of responsible behaviour in cyberspace. Understand how these policies support effective cybersecurity practices.

Recognise the Relationship between Cyber Attacks and UN Units: Understand the specific implications of cyber-attacks on UN units, including the impact on force protection and mission success. Gain insights into the unique challenges faced by UN personnel and units in maintaining cybersecurity while carrying out their mandates.

Identify Predominant Cybersecurity Threats to UN Units: Identify and familiarise yourself with the predominant cybersecurity threats faced by UN units. This includes an overview of common attack vectors, such as spear-phishing, supply chain attacks, network intrusions, and insider threats. Develop an understanding of the specific vulnerabilities and risks that UN units may encounter.

By achieving these learning outcomes, you will be equipped with a solid foundation in cybersecurity concepts, UN policies, and the specific challenges faced by UN units in safeguarding their operations against cyber threats.

Slide 4



We think of operations as land, sea and air; and we recognised a fourth – space. Now there's a fifth – **cyber**

Cyber is the new frontier

As we traditionally think of operations encompassing land, sea, air, and space, we now recognise a fifth domain: cyber. Cyber has emerged as the new frontier and has become the weapon of choice in contemporary warfare and conflicts.

This slide serves as a reminder of how we should approach cyber warfare, acknowledging the significant threat it poses and emphasising the collective efforts we must internalize. Relying solely on firewalls and external defence is no longer sufficient. We each bear a personal responsibility to actively contribute to the security of our UN units and forces.

Understanding the gravity of the cyber threat landscape and its potential impact is crucial. By recognising that cyber-attacks can target critical infrastructure, compromise sensitive information, and disrupt operations, we appreciate the need for proactive measures. We must prioritise cybersecurity as an integral part of our operational readiness.

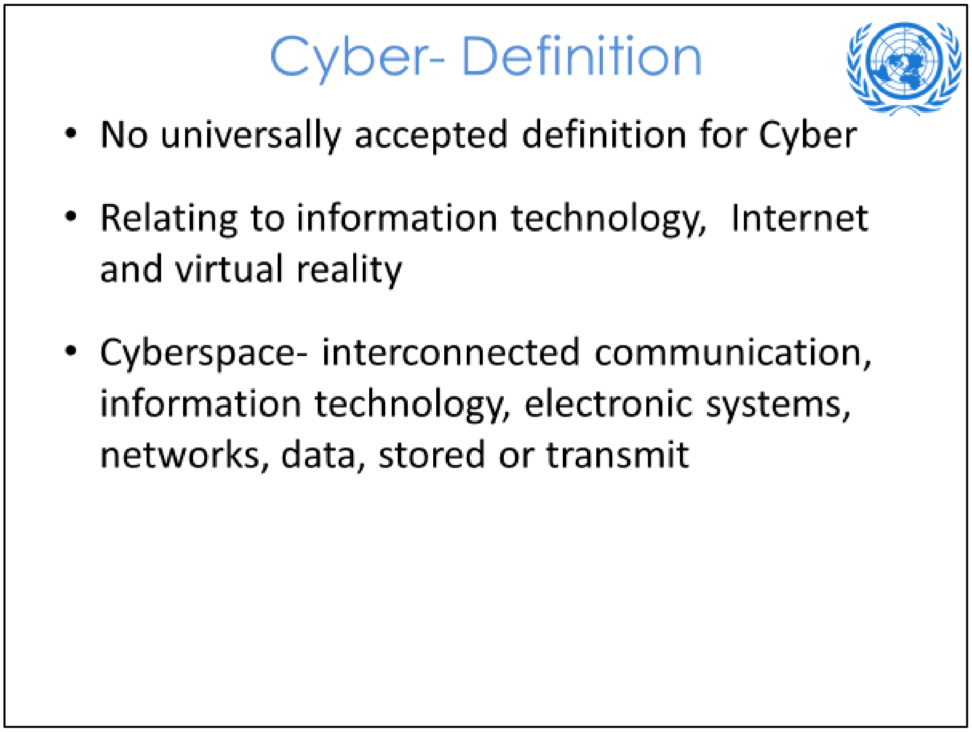
By embracing this mindset and actively engaging in cybersecurity efforts, we fortify our collective defence and contribute to a safer operating environment in the face of evolving cyber threats.

Slide 5

Definitions

To ensure a shared understanding throughout this lesson, it is vital that we establish a common vocabulary and comprehension of the key definitions and terminology that will be used. The following slides will present an explanation of the specific terms and definitions that are integral to this training material. By familiarizing ourselves with these terms, we can effectively communicate and engage with the content covered in this lesson.

Slide 6



Cyber- Definition

- No universally accepted definition for Cyber
- Relating to information technology, Internet and virtual reality
- Cyberspace- interconnected communication, information technology, electronic systems, networks, data, stored or transmit

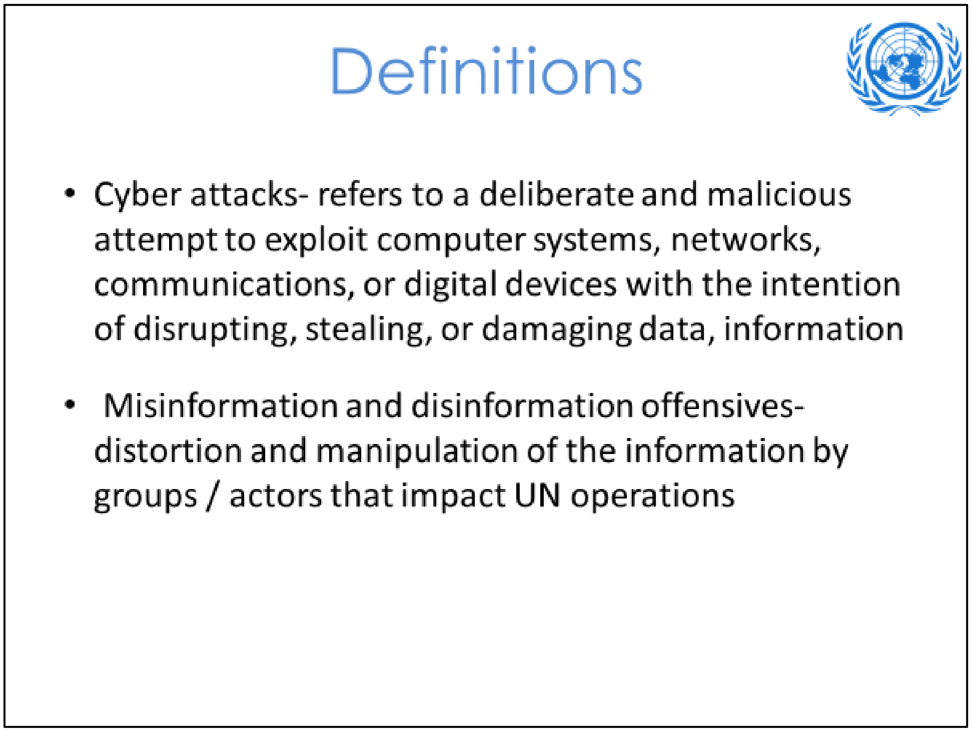
While there are no universally accepted definitions for terms like "Cyber," we will establish specific definitions for the purpose of this training material.

Cyber: In the context of this training material, "Cyber" refers to the realm associated with information technology, the Internet, and virtual reality. It encompasses the interconnected systems, networks, and technologies that facilitate communication, data processing, and information exchange.

Cyberspace: We define "Cyberspace" as the global environment that encompasses interconnected communication systems, information technology infrastructure, electronic systems, networks, and the data they process, store, or transmit. It includes both interconnected networks and isolated systems, collectively forming a virtual domain.

By using these definitions, we can establish a common understanding of the terms used throughout this lesson, enabling effective communication and comprehension of the topics covered.

Slide 7



Definitions

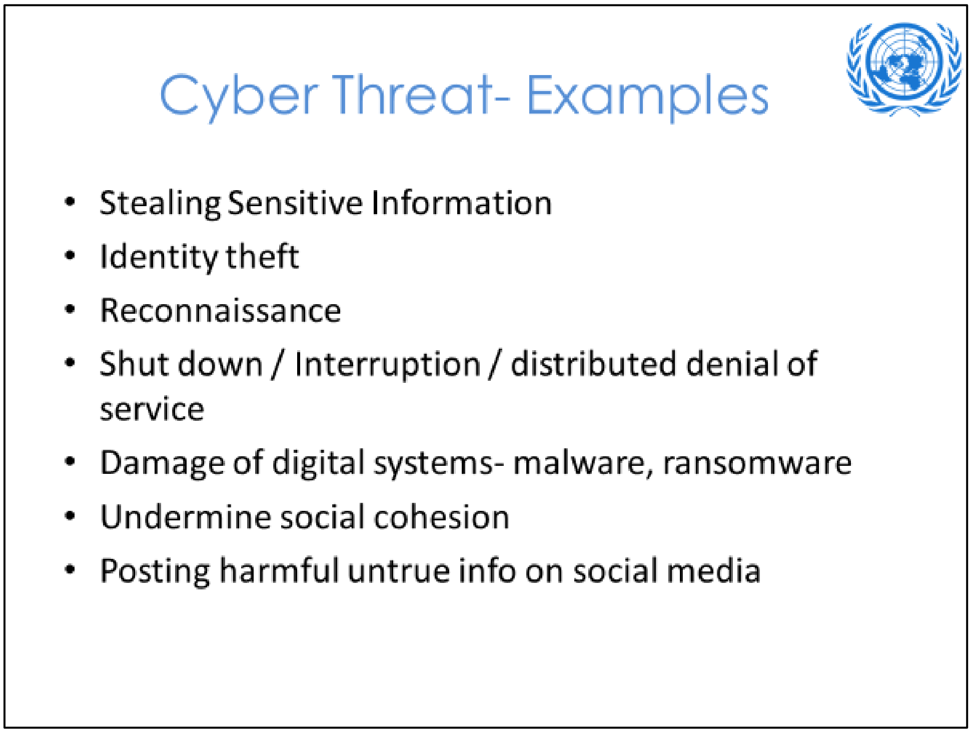
- Cyber attacks- refers to a deliberate and malicious attempt to exploit computer systems, networks, communications, or digital devices with the intention of disrupting, stealing, or damaging data, information
- Misinformation and disinformation offensives- distortion and manipulation of the information by groups / actors that impact UN operations

A cyber-attack refers to a deliberate and malicious attempt to exploit computer systems, networks, communications, or digital devices with the intention of disrupting, stealing, or damaging data or information. Cyber-attacks are typically carried out by groups/actors using various techniques and tools to exploit vulnerabilities in systems or take advantage of human error.

The consequences of a cyber-attack can range from financial losses and reputational damage to the compromise of personal or sensitive data, disruption of critical infrastructure, or even threats to operational security.

Cyber-attacks encompass misinformation and disinformation offensives. These offensives involve deliberate distortion and manipulation of information by malicious groups/actors, aiming to disrupt an operation and undermine the effective implementation of the mandate.

Slide 8



Cyber Threat- Examples

- Stealing Sensitive Information
- Identity theft
- Reconnaissance
- Shut down / Interruption / distributed denial of service
- Damage of digital systems- malware, ransomware
- Undermine social cohesion
- Posting harmful untrue info on social media

Here are examples of cyber-attacks:

Theft of Sensitive Information: Unauthorised acquisition or exfiltration of confidential data, such as personal, financial, or proprietary information, with the intent to exploit it for malicious purposes.

Identity Theft: The fraudulent acquisition and use of someone's personal information, such as their name, social security number, or financial credentials, to impersonate them or commit fraudulent activities.

Reconnaissance: The process of gathering information about a target system or organisation to identify vulnerabilities, weaknesses, or potential entry points for a cyber-attack.

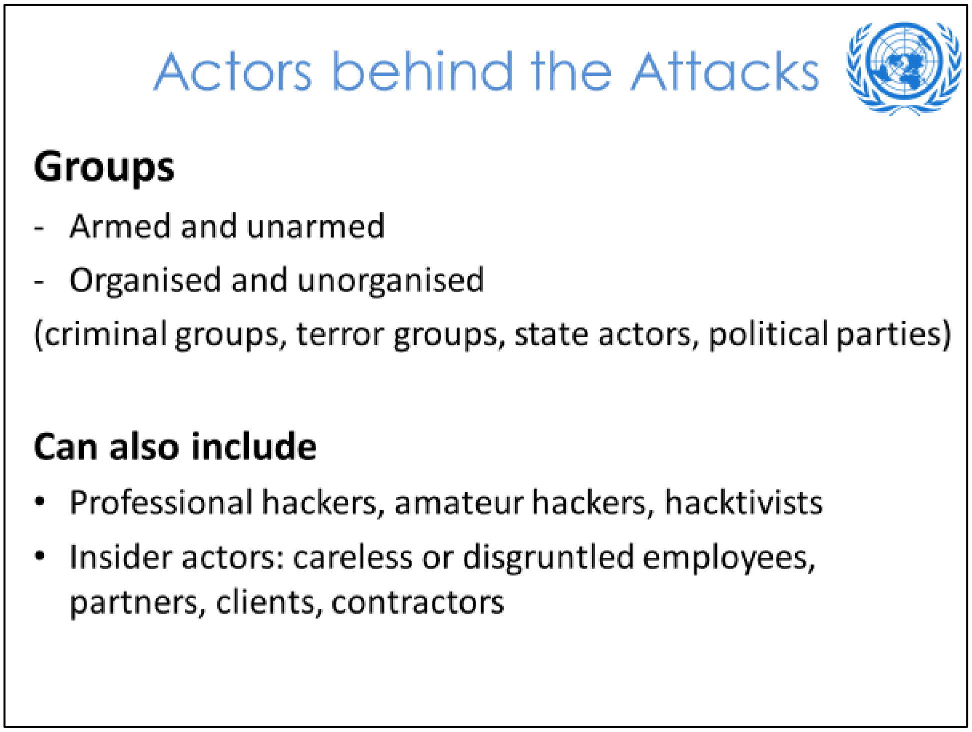
Disruption and Distributed Denial of Service (DDoS): Coordinated efforts to overwhelm a target system, network, or website with a flood of illegitimate traffic, rendering it unresponsive or unavailable to legitimate users.

Damage to Digital Systems: The deliberate use of malicious software, such as malware or ransomware, to compromise or impair the functionality, integrity, or availability of digital systems, networks, or data.

Undermining Social Cohesion: Manipulating or disseminating false information, rumours, or divisive content on social media platforms to exploit existing social or political divisions, incite unrest or erode trust within communities.

Spreading Harmful False Information on social media: Intentionally posting and sharing misinformation, disinformation, or harmful content on social media platforms to deceive or manipulate individuals/organisations, provoke fear or panic, or tarnish reputations.

Slide 9



Actors behind the Attacks

Groups

- Armed and unarmed
- Organised and unorganised

(criminal groups, terror groups, state actors, political parties)

Can also include

- Professional hackers, amateur hackers, hacktivists
- Insider actors: careless or disgruntled employees, partners, clients, contractors

This slide provides an overview of the various actors that constitute the most prominent threats in the realm of cyber-attacks. Understanding these actors is crucial in developing effective strategies to combat cyber threats and protect sensitive information.

The actors can be broadly categorised into different groups, considering their characteristics and affiliations. These groups encompass armed and unarmed actors, as well as organised and unorganised entities. Among them, we find criminal groups, terror groups, state actors, and even certain political parties. These entities possess varying degrees of sophistication and resources, each posing unique challenges.

Additionally, we must consider the involvement of unique actors who play significant roles in cyber threats. Professional hackers, often possessing advanced technical skills and knowledge, engage in cybercriminal activities for personal gain or on behalf of others. On the other hand, amateur hackers, while less experienced, can still pose a threat to organisations and individuals through their malicious actions.

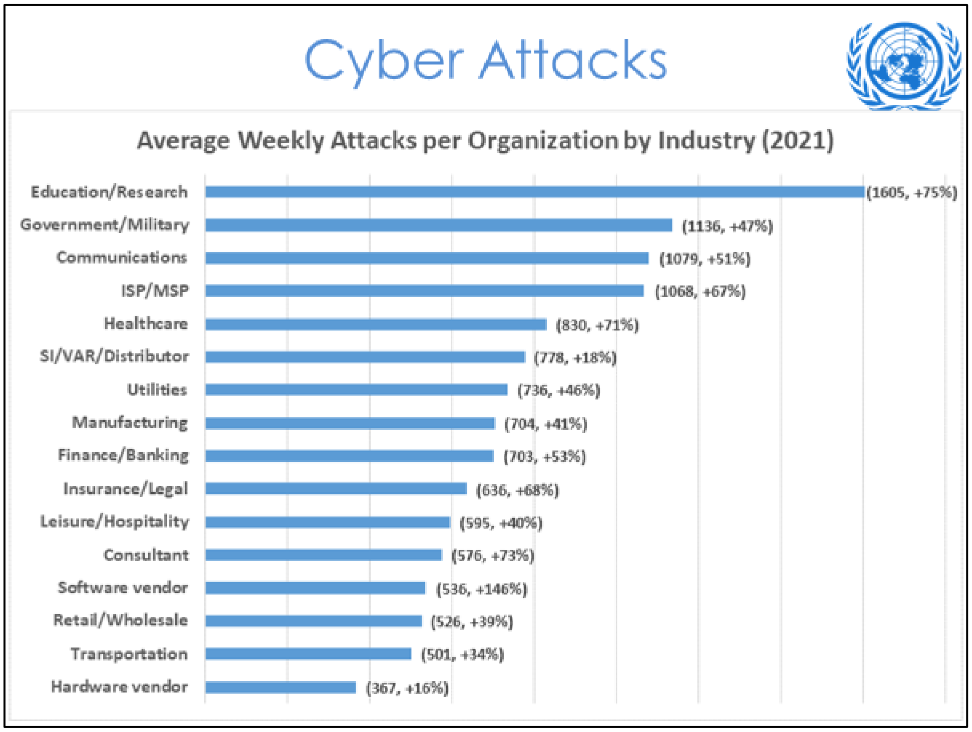
Another category of actors is hacktivists, individuals who support groups who employ hacking techniques to further their social or political causes. Hacktivism often involves targeting organisations or systems that the hacktivists perceive as morally or politically problematic.

Furthermore, insider actors pose a distinct challenge in cybersecurity. These insiders can be classified into two main types: careless or disgruntled employees, partners, clients, and contractors. Shockingly, insiders account for a significant portion, approximately 60%, of cyberattacks. Their familiarity with an organisation's systems and access privileges makes them difficult to detect. Insiders, whether accidentally or deliberately, have the potential to expose or assist in exposing confidential information, intellectual property, and financial resources. They possess insider knowledge of an organisation's sensitive data and can exploit this knowledge for personal gain or to cause harm.

Detecting and preventing insider threats requires a combination of technical measures and organisational policies. It is crucial for organisations to implement strict access controls, conduct thorough background checks, and establish robust monitoring systems to mitigate the risks associated with insider threats.

In summary, this slide provides an overview of the diverse actors involved in cyber threats. By recognising the different groups, including criminal organisations, state actors, and hacktivists, as well as the specific challenges posed by insider actors, organisations can develop comprehensive FP strategies to reduce risks to their operations and resources.

Slide 10



Cyber Attacks

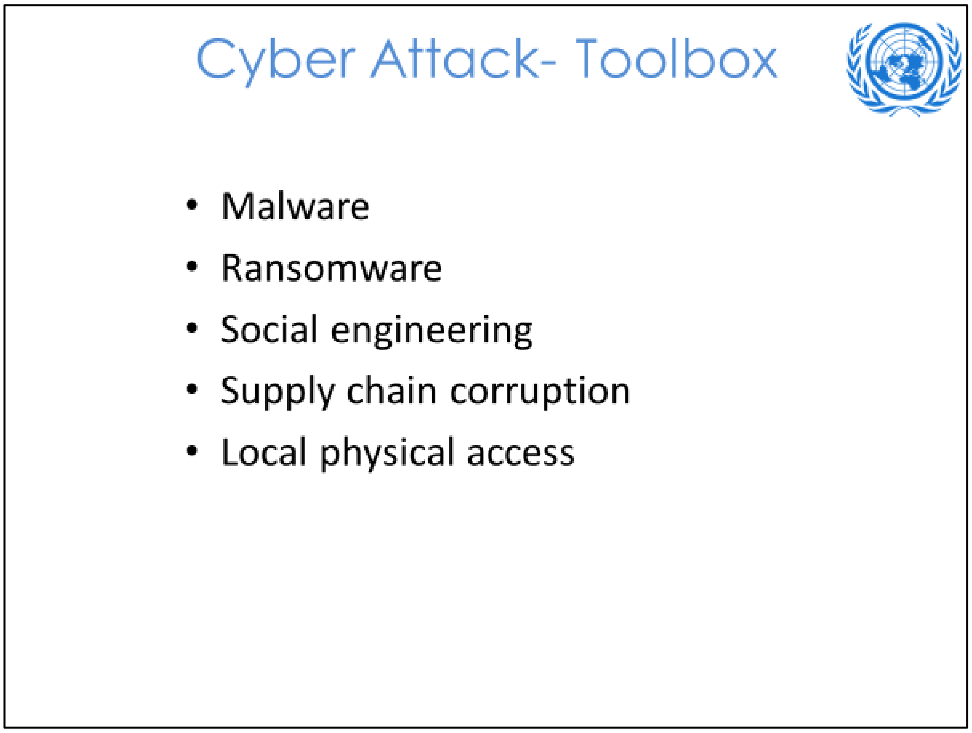
Average Weekly Attacks per Organization by Industry (2021)

It is evident that cyber-attacks have experienced a substantial increase, with reports indicating a steady annual growth. In light of this alarming trend, it is imperative for UN missions to recognise themselves as desirable targets and take proactive measures to mitigate the risks.

The rise in cyber-attacks poses a significant risk to the operations, security, and integrity of UN missions. These attacks can result in consequences, such as compromised sensitive information, disrupted communications and operations, financial loss, and reputational damage. Therefore, it is essential for UN missions to adopt a robust protective stance to safeguard their critical systems and data.

To address this growing threat, UN missions should prioritise efforts to enhance their cybersecurity and FP posture. This entails implementing comprehensive risk mitigation measures.

Slide 11



Cyber Attack- Toolbox

- Malware
- Ransomware
- Social engineering
- Supply chain corruption
- Local physical access

Within the realm of cyber-attacks, a diverse range of techniques form what can be referred to as a "cyber toolbox." It is important to note that the technical aspects of these attacks often undergo daily mutations, reflecting the ever-evolving nature of cyber threats. This cyber toolbox encompasses various methods, including, but not limited to:

Malware: This term encompasses a broad range of malicious software designed to infiltrate and compromise computer systems. Examples include viruses, worms, trojans, and spyware, each with its own unique functionality and potential for harm.

Ransomware: This particular type of malware has gained significant prominence in recent years. Ransomware encrypts files on a victim's system and demands a ransom in exchange for the decryption key. It can have devastating effects on individuals, organisations, and even critical infrastructure systems.

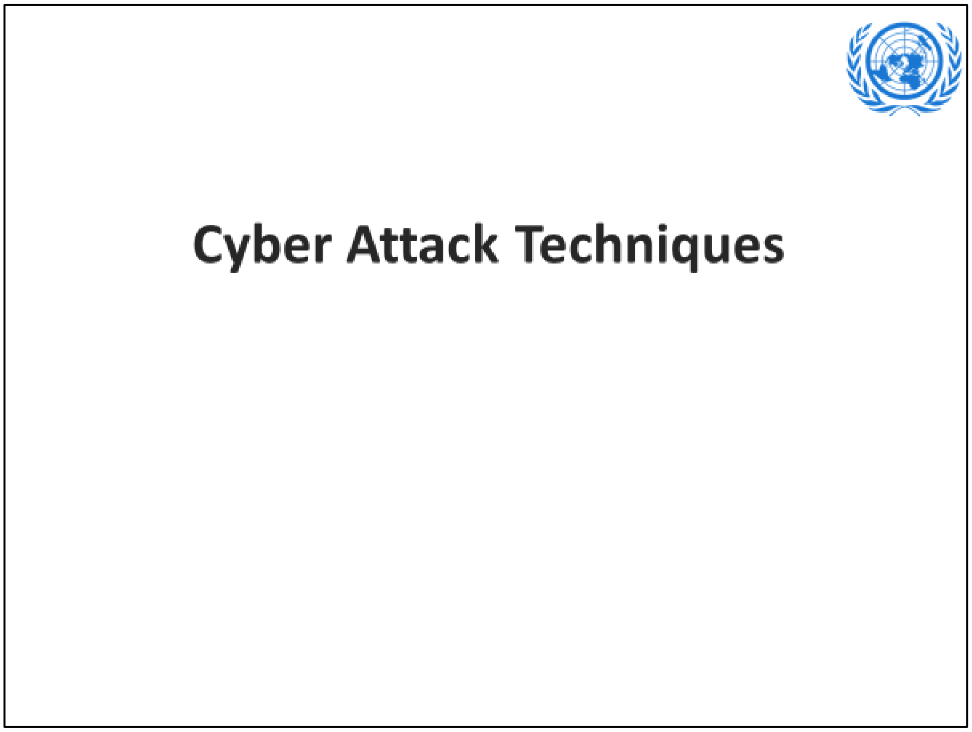
Social engineering: This technique exploits human psychology and manipulation to deceive individuals and gain unauthorised access to systems or sensitive information. Common social engineering tactics include phishing, where attackers impersonate legitimate entities to trick victims into revealing personal or confidential data.

Supply chain corruption: Cyber attackers may target the supply chain of organisations, compromising the integrity of software or hardware components. By infiltrating the supply chain, attackers can introduce vulnerabilities, backdoors, or malicious code into the systems used by their intended targets.

Local physical access: This form of attack occurs when an adversary gains physical access to a device, network, or infrastructure. It allows the attacker to bypass certain security measures and directly manipulate or compromise the targeted system.

These are just a few examples of the tools in the cyber attacker's arsenal. It is important to recognise that cyber threats constantly evolve, and new techniques may emerge over time. Therefore, organisations must remain vigilant and implement comprehensive security measures to protect themselves against these various forms of cyber-attacks.

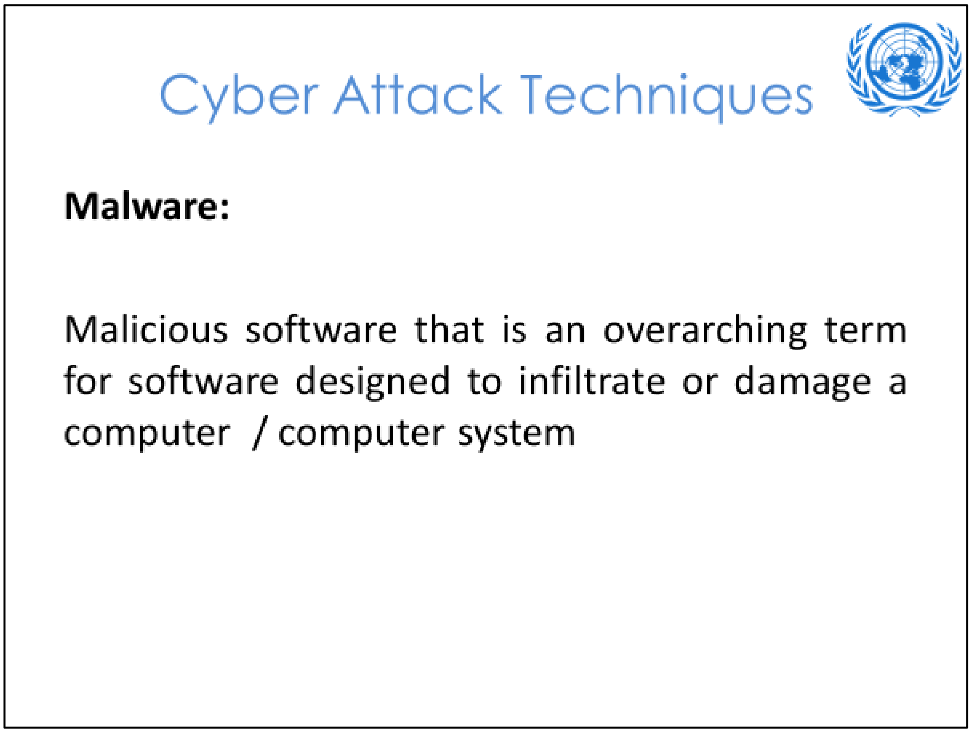
Slide 12



Cyber Attack Techniques

Let's delve deeply into the various facets of cyber threats. This training will provide a thorough understanding of the most common cyber threats, as well as the potential ramifications they may have on the operational effectiveness of these units.

Slide 13



Cyber Attack Techniques

Malware:

Malicious software that is an overarching term for software designed to infiltrate or damage a computer / computer system

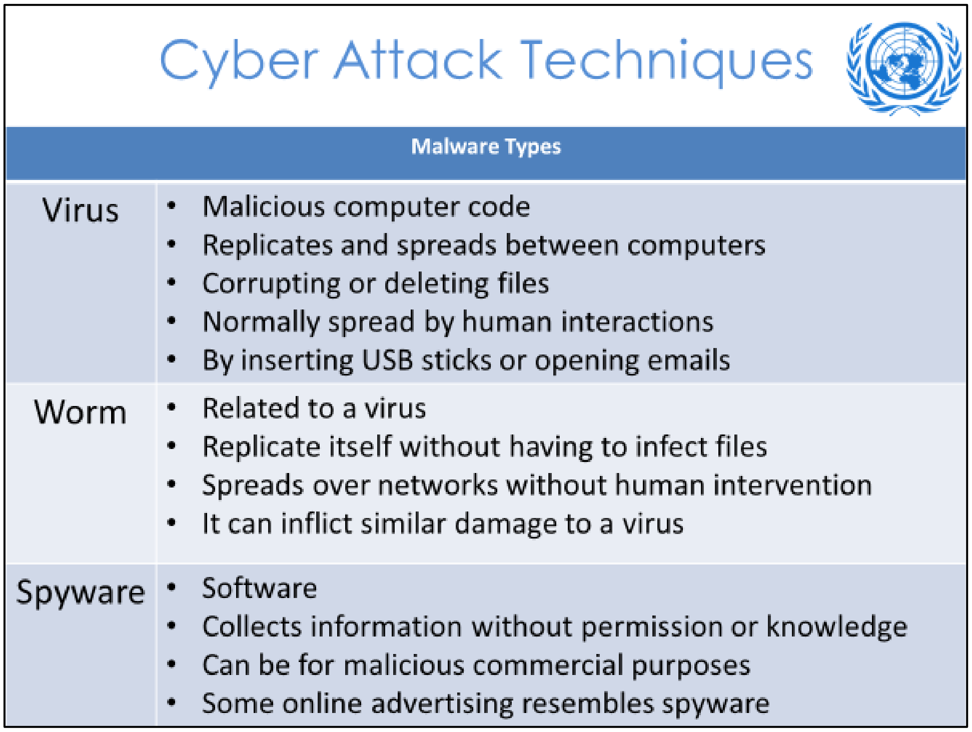
Malware, short for malicious software, encompasses various software designed to infiltrate or harm computers. It serves multiple purposes, including:

- Keystroke logging: This type of malware records a user's keystrokes, compromising sensitive data such as passwords and credit card details
- Monitoring online activity: Malware can monitor and track users' online behaviour, including eavesdropping on voice and video communications and determining the geolocation of smartphones, tablets, and other personal electronic devices
- Exploiting social networking applications: Malicious software leverages social networking platforms to support social engineering attacks, tricking users into divulging confidential information
- Privilege escalation: Malware gains access to a system and escalates the attacker's level of control, potentially acquiring administrator privileges for complete control over the compromised system
- Denial of service: Some malware aims to overload systems by flooding them with requests, rendering them unresponsive or unavailable to legitimate users

- Botnet recruitment: Malware can turn a target system into a part of a botnet, allowing the attacker to launch distributed denial-of-service attacks using the compromised system, often utilising the user's contacts or email address book

Malware types have traditionally targeted computers, communication systems, and computer networks. However, the increasing popularity and sophistication of smartphones, tablets, and other internet-enabled devices. Moreover, some malware combines attributes into "blended threats," making them challenging to detect and remove.

Slide 14



Cyber Attack Techniques

Malware Types	
Virus	• Malicious computer code • Replicates and spreads between computers • Corrupting or deleting files • Normally spread by human interactions • By inserting USB sticks or opening emails
Worm	• Related to a virus • Replicate itself without having to infect files • Spreads over networks without human intervention • It can inflict similar damage to a virus
Spyware	• Software • Collects information without permission or knowledge • Can be for malicious commercial purposes • Some online advertising resembles spyware

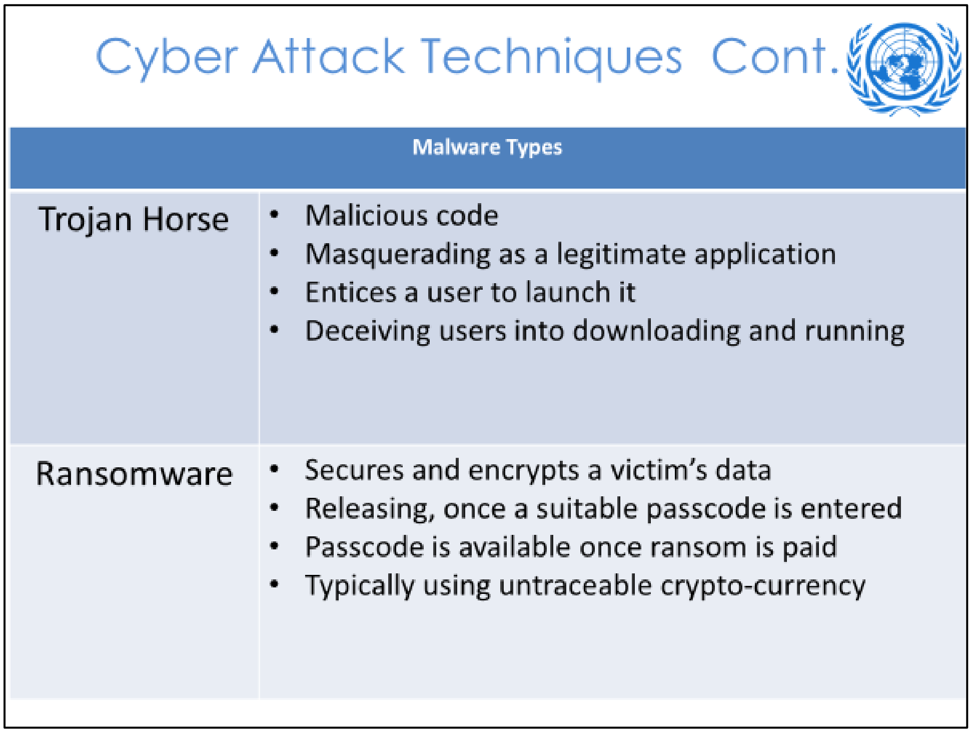
Malware attack techniques:

- Virus: A virus is a type of malicious computer code capable of replicating itself and spreading from one computer to another. Once it infects a machine, it can corrupt or delete files. Viruses are typically transmitted through human interactions, such as inserting infected USB sticks or opening malicious emails

- Worm: Similar to a virus, a worm is self-replicating, but it can spread across networks without relying on infecting files on the host machine. Worms propagate from one computer to another automatically without requiring human intervention. Once a worm infiltrates a computer, it can cause similar damage to that of a virus

- Spyware: Spyware refers to software that covertly collects information on a computer without the user's permission or knowledge, transmitting it back to the entity behind it. This collected data can be exploited for malicious commercial purposes. Some forms of online advertising may resemble spyware in their intrusive nature

Slide 15



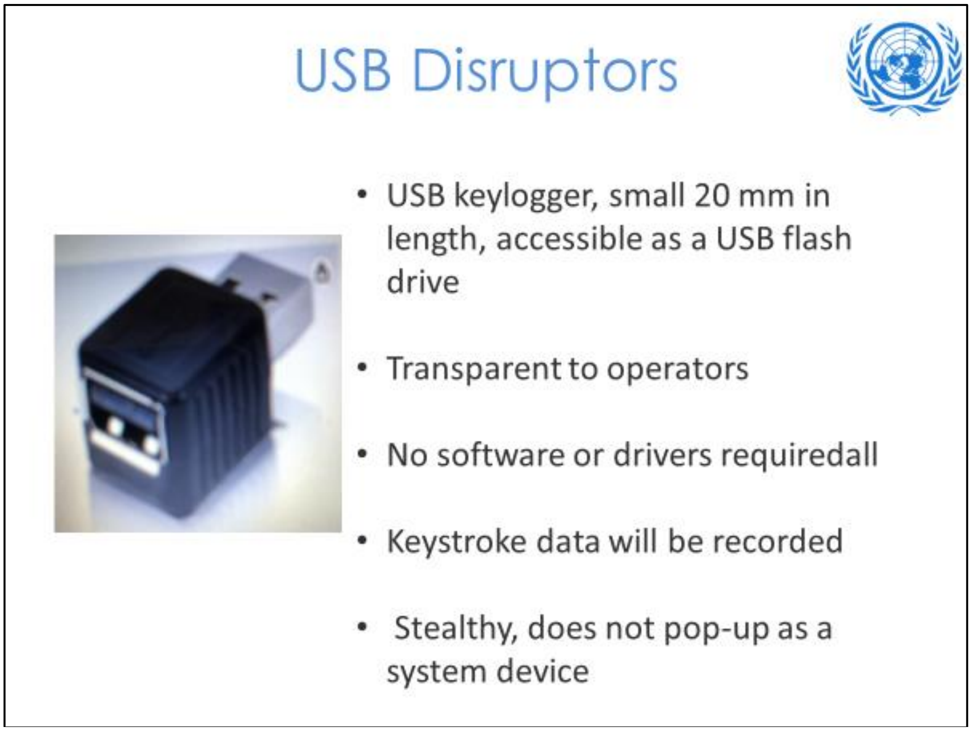
Cyber Attack Techniques Cont.

Malware Types	
Trojan Horse	• Malicious code • Masquerading as a legitimate application • Entices a user to launch it • Deceiving users into downloading and running
Ransomware	• Secures and encrypts a victim's data • Releasing, once a suitable passcode is entered • Passcode is available once ransom is paid • Typically using untraceable crypto-currency

Malware attack techniques continued:

- Trojan Horse: A trojan horse, commonly referred to as a "trojan," disguises malicious code as a legitimate and harmless application. It tricks users into launching it, allowing the payload to execute its malicious activities. Unlike viruses or worms, trojans do not replicate themselves. Instead, they rely on deceiving users into downloading and running them, often leading to the installation of a rootkit, which grants unauthorised access to the compromised system
- Ransomware: Ransomware employs encryption to lock and secure a victim's data within an information technology system. The data remains inaccessible until a specific passcode, known only to the attacker, is entered. To obtain the passcode, the victim is typically required to pay a significant ransom, often demanded in untraceable cryptocurrency. Only upon payment, the attacker may provide the passcode to decrypt and release the victim's data

Slide 16



USB Disruptors

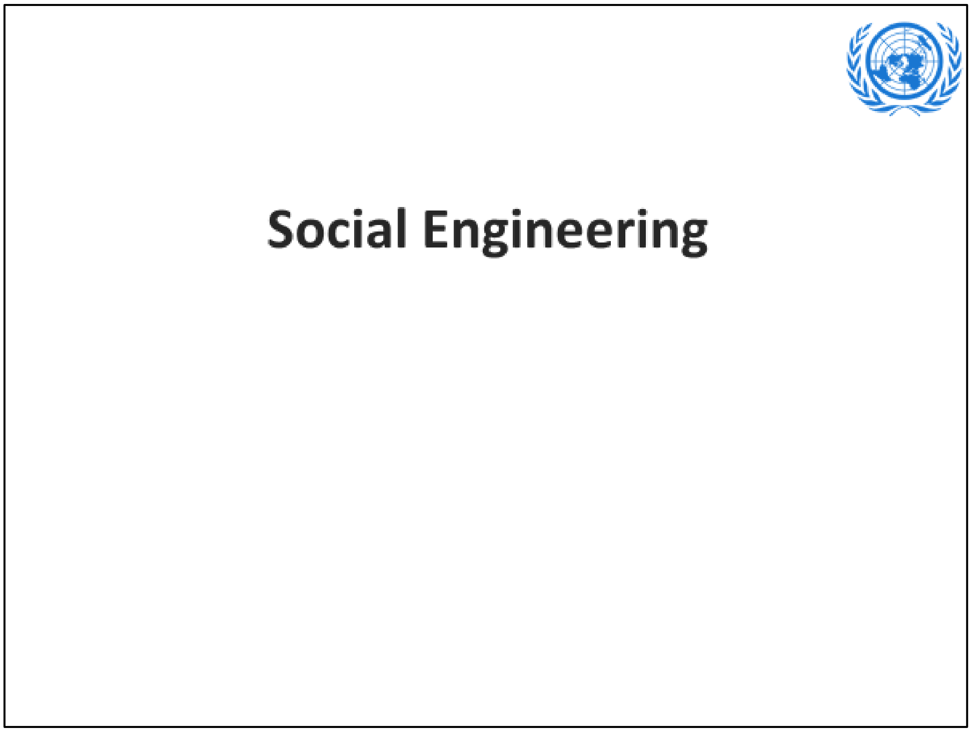
- USB keylogger, small 20 mm in length, accessible as a USB flash drive
- Transparent to operators
- No software or drivers requiredall
- Keystroke data will be recorded
- Stealthy, does not pop-up as a system device

It's important to stay vigilant and aware of potential threats. Seen here is an ultra-small USB keylogger available for under 50 US dollars. With a length of only 0.8" (20 mm), it functions as a USB flash drive and requires no software or drivers. It supports various keyboard layouts, making it versatile and easy to use.

The compact size makes it advantageous for surveillance, security, and forensic applications. Installing it is a breeze - simply plug it between the USB keyboard and port, and it will automatically start recording all typed data to its internal flash disk.

To retrieve recorded data, switch to flash drive mode by pressing a specific 3-key combination. The captured data is stored in a file called LOG.TXT and is formatted to resemble the keystrokes on the screen.

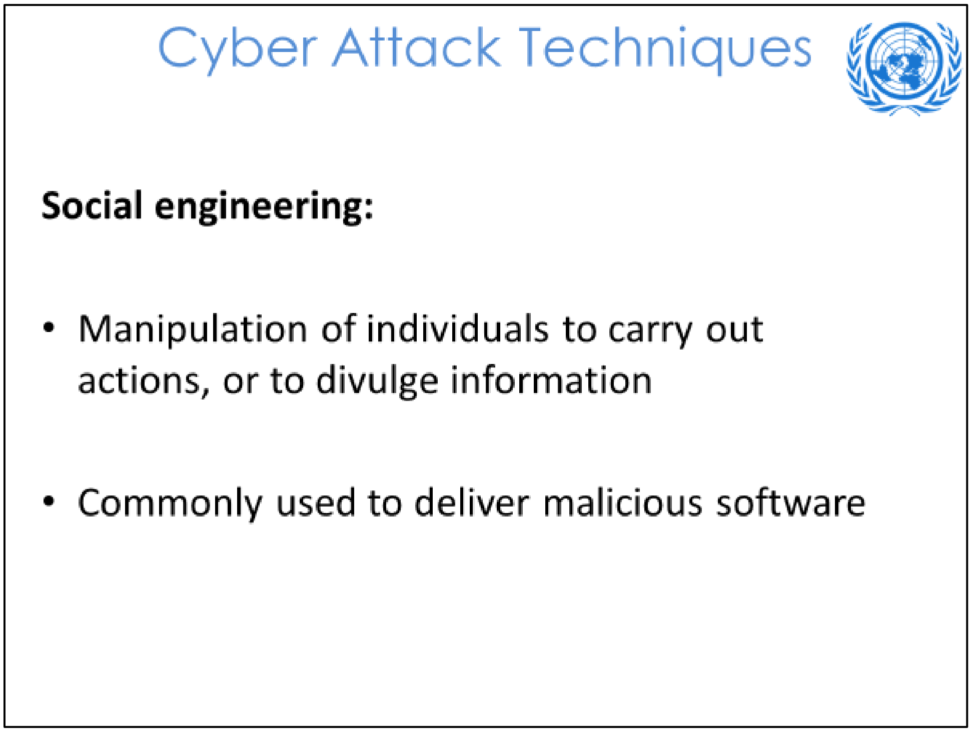
Slide 17



Social Engineering

Let’s now conduct an exploration of the concept of social engineering. These concepts will encompass a detailed examination of various social engineering techniques and their potential implications for the security and operational integrity of these units.

Slide 18



Cyber Attack Techniques

Social engineering:

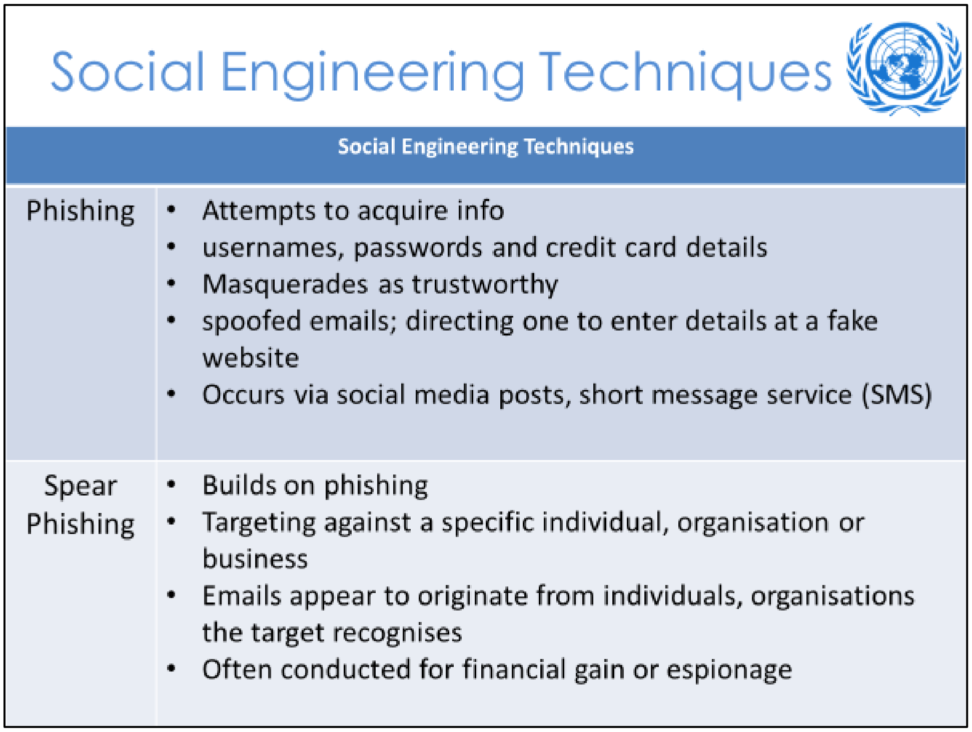
- Manipulation of individuals to carry out actions, or to divulge information
- Commonly used to deliver malicious software

Social Engineering Techniques.

Social engineering involves manipulating individuals to perform specific actions or disclose information, often for the purpose of delivering malicious software to targeted systems. The information obtained through social engineering is frequently utilised to facilitate cyberattacks. As adversaries gain a deeper understanding of an individual's online behaviour and interactions, the threat to that individual intensifies.

Attackers/groups employing social engineering techniques typically conduct extensive research on their targets to increase their chances of success. They seek out organisational charts, contact details, and email addresses and leverage social media platforms to enhance their knowledge about the intended victim. Armed with this information, attackers can make use of personal references to build trust and confidence, thereby increasing the likelihood of the victim complying with their requests. It is important to be aware of social engineering tactics and remain vigilant.

Slide 19



Social Engineering Techniques

Social Engineering Techniques	
Phishing	• Attempts to acquire info • usernames, passwords and credit card details • Masquerades as trustworthy • spoofed emails; directing one to enter details at a fake website • Occurs via social media posts, short message service (SMS)
Spear Phishing	• Builds on phishing • Targeting against a specific individual, organisation or business • Emails appear to originate from individuals, organisations the target recognises • Often conducted for financial gain or espionage

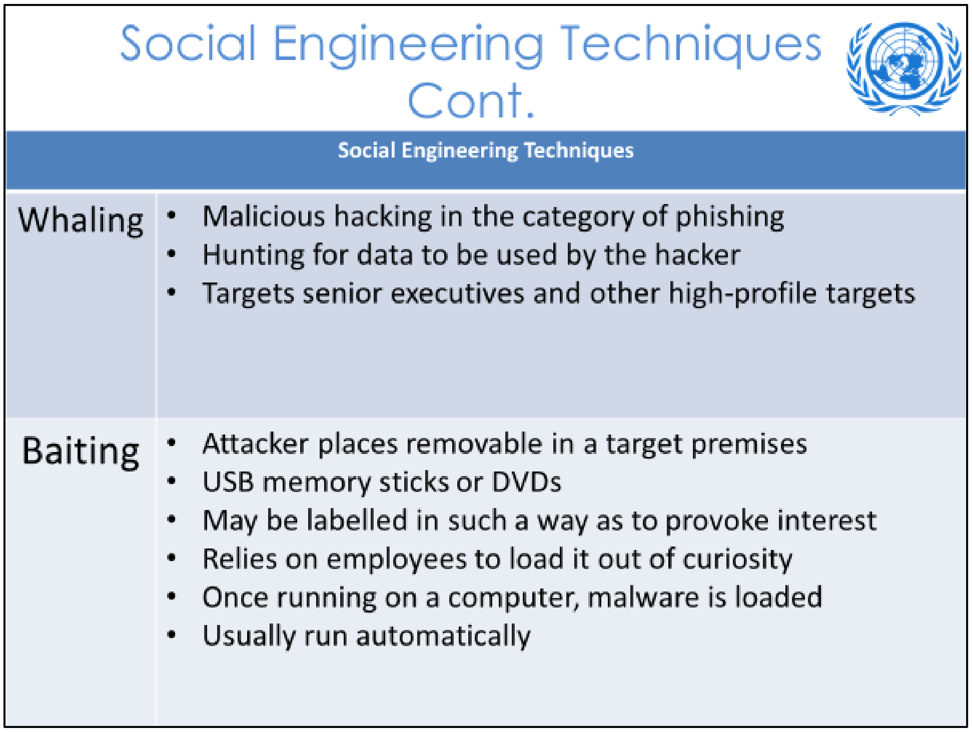
Social Engineering Techniques.

- Phishing: Phishing is a method used to deceive individuals into revealing sensitive information such as usernames, passwords, and credit card details. It involves impersonating a trustworthy entity online, often through spoofed emails or directing users to fake websites that closely resemble legitimate ones. Phishing attacks can also occur through social media posts, SMS messages, and instant messaging services

- Spear Phishing: Spear phishing is an advanced form of phishing that specifically targets a particular individual, organisation, or business. The emails used in spear phishing attempts often contain personalized details or appear to originate from familiar individuals or organisations to enhance their credibility. Unlike random hackers, spear phishing attacks are typically carried out for financial gain or espionage purposes

These social engineering techniques exploit human psychology and trust to trick individuals into disclosing confidential information. It is crucial to exercise caution, verify the authenticity of communications, and stay informed about these tactics to protect oneself from falling victim to such attacks.

Slide 20



Social Engineering Techniques Cont.

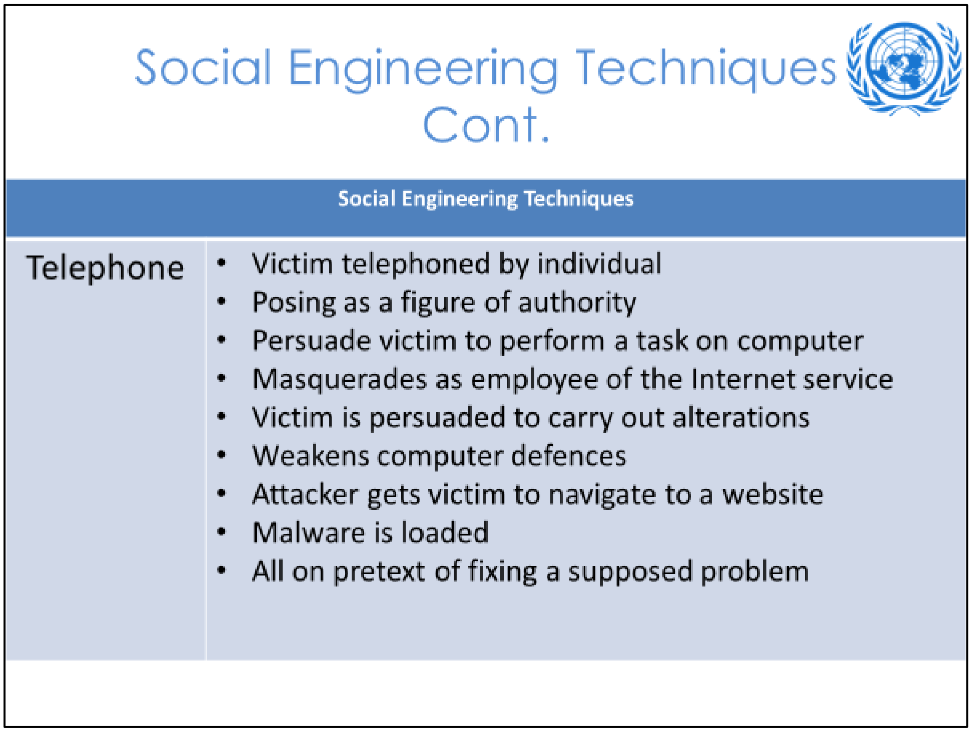
Social Engineering Techniques	
Whaling	• Malicious hacking in the category of phishing • Hunting for data to be used by the hacker • Targets senior executives and other high-profile targets
Baiting	• Attacker places removable in a target premises • USB memory sticks or DVDs • May be labelled in such a way as to provoke interest • Relies on employees to load it out of curiosity • Once running on a computer, malware is loaded • Usually run automatically

Social Engineering Techniques.

- Whaling: Whaling is a form of malicious hacking that falls under the broader category of phishing. It specifically targets senior leaders and other high-profile individuals within an organisation, aiming to obtain data that can be exploited for targeted phishing attacks

- Baiting: Baiting involves the placement of removable media, such as USB memory sticks or DVDs, within a targeted premises. These media may be labelled in a way that piques curiosity or is left unmarked. The technique relies on employees of the targeted organisation picking up the media and loading it onto their computers out of curiosity. Once executed, the payload on the media (such as malware enabling remote access) typically activates automatically. Surprisingly, this technique has proven to be highly effective

Slide 21



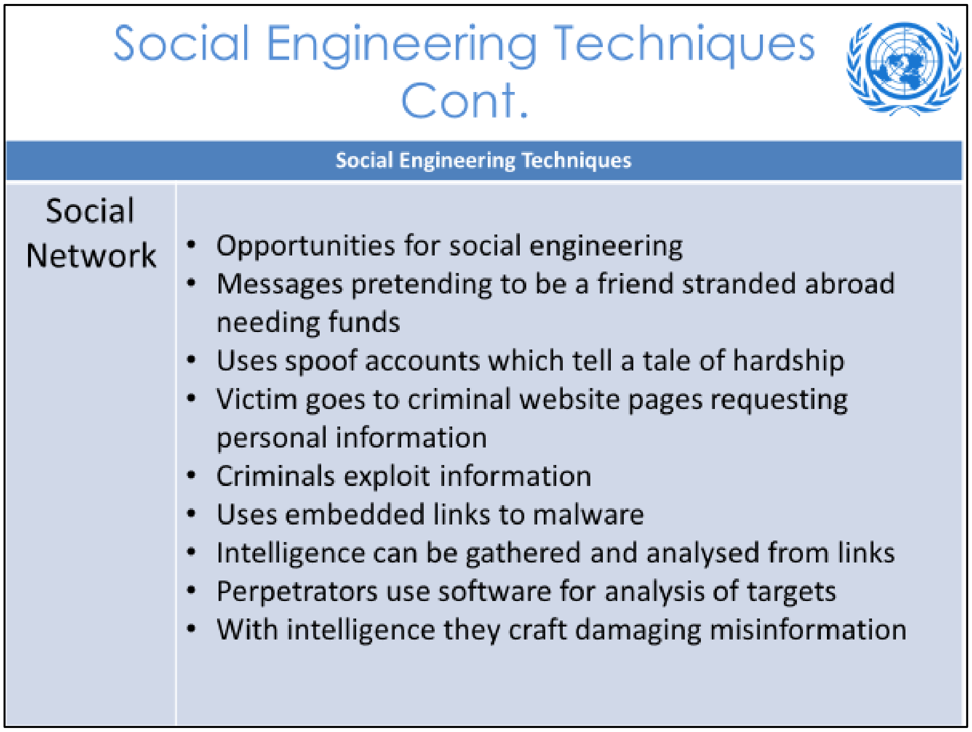
Social Engineering Techniques Cont.

Social Engineering Techniques	
Telephone	• Victim telephoned by individual • Posing as a figure of authority • Persuade victim to perform a task on computer • Masquerades as employee of the Internet service • Victim is persuaded to carry out alterations • Weakens computer defences • Attacker gets victim to navigate to a website • Malware is loaded • All on pretext of fixing a supposed problem

Social Engineering Techniques.

Telephone Scam: A fraudulent scheme occurs when someone impersonates an authoritative figure to contact victims via telephone, aiming to convince them to engage in certain activities. Frequently, criminals pretend to be employees from the victim's Internet service provider or Microsoft, fabricating issues with the victim's computer. Through various tactics, the scammers can manipulate the victim into making changes to their computer settings that compromise its security, visiting a website that grants remote access, downloading malware under the false pretence of resolving a supposed problem, obtaining virus protection, or divulging personal and financial information.

Slide 22



Social Engineering Techniques Cont.

Social Engineering Techniques	
Social Network	• Opportunities for social engineering • Messages pretending to be a friend stranded abroad needing funds • Uses spoof accounts which tell a tale of hardship • Victim goes to criminal website pages requesting personal information • Criminals exploit information • Uses embedded links to malware • Intelligence can be gathered and analysed from links • Perpetrators use software for analysis of targets • With intelligence they craft damaging misinformation

Social Engineering Tactics via Social Networks:

- Opportunities for Social Engineering: Social networks provide fertile ground for social engineering attacks, enabling malicious individuals to exploit human vulnerabilities for their gain

- Impersonation of a Friend in Need: A common tactic involves sending messages that feign a friend stranded abroad, desperately seeking financial assistance. This ruse aims to deceive the victim into providing funds willingly

- Utilisation of Spoof Accounts and Tales of Hardship: Malicious actors employ spoof accounts to further deceive their targets. These fake profiles narrate stories of adversity, tugging at the victim's emotions and creating a sense of urgency

- Exploiting Victims on Criminal Group Websites: Victims are directed to criminal websites that masquerade as legitimate platforms, tricking them into divulging personal information willingly. This allows criminals to gain unauthorised access to sensitive data

- Information Exploitation: Armed with the obtained personal information, groups exploit it for their own malicious purposes. This can include identity theft, financial fraud, or other forms of illicit activities

- Malware via Embedded Links: Social engineering attacks often leverage embedded links within messages or posts. Clicking on these links may lead unsuspecting victims to unwittingly download malware, compromising their devices and privacy

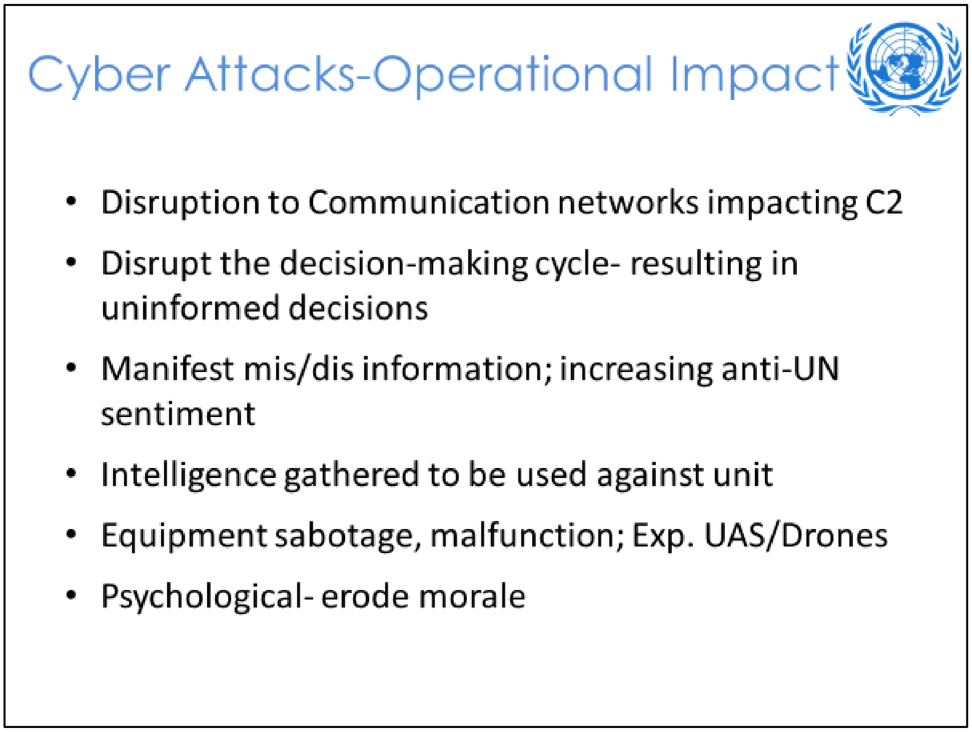
- Intelligence Gathering and Analysis: Perpetrators gather and analyse intelligence from the links victims interact with. This information provides valuable insights into the targets' preferences, behaviours, and vulnerabilities.

- Target Analysis through Software: Groups employ specialised software tools to analyse the collected peacekeeping-intelligence, allowing them to identify patterns, exploit weaknesses, and tailor their manipulative tactics accordingly

- Crafting Damaging Misinformation: Armed with the peacekeeping-intelligence gleaned from their analysis, malicious groups craft and disseminate damaging misinformation. This misinformation aims to deceive and manipulate victims, leading them to make harmful decisions or take detrimental actions

It is crucial for individuals to exercise caution, verify the authenticity of messages, and maintain a healthy scepticism to mitigate the risks associated with social engineering attacks on social networks.

Slide 23



Cyber Attacks-Operational Impact

- Disruption to Communication networks impacting C2
- Disrupt the decision-making cycle- resulting in uninformed decisions
- Manifest mis/dis information; increasing anti-UN sentiment
- Intelligence gathered to be used against unit
- Equipment sabotage, malfunction; Exp. UAS/Drones
- Psychological- erode morale

While the impact of cyber-attacks on critical infrastructure and civilian systems is well-documented, the potential repercussions on tactical military units should not be underestimated. The vulnerabilities of tactical UN units to cyber-attacks and the subsequent implications for police and military operations could include the following:

Tactical military units are heavily reliant on advanced technologies, communication networks, and data systems to ensure swift and coordinated operations. However, these strengths also make them vulnerable to cyber-attacks. The consequences of such attacks could be far-reaching, affecting the performance, command and control, situational awareness, and overall effectiveness of tactical units conducting operations.

Disrupted Communication and Coordination:
Cyber-attacks targeting communication networks can sever vital lines of communication between units, leading to chaos, confusion, and delayed response times. Without reliable communication, the coordination and synchronization of operations become compromised, jeopardizing the success of mission objectives.

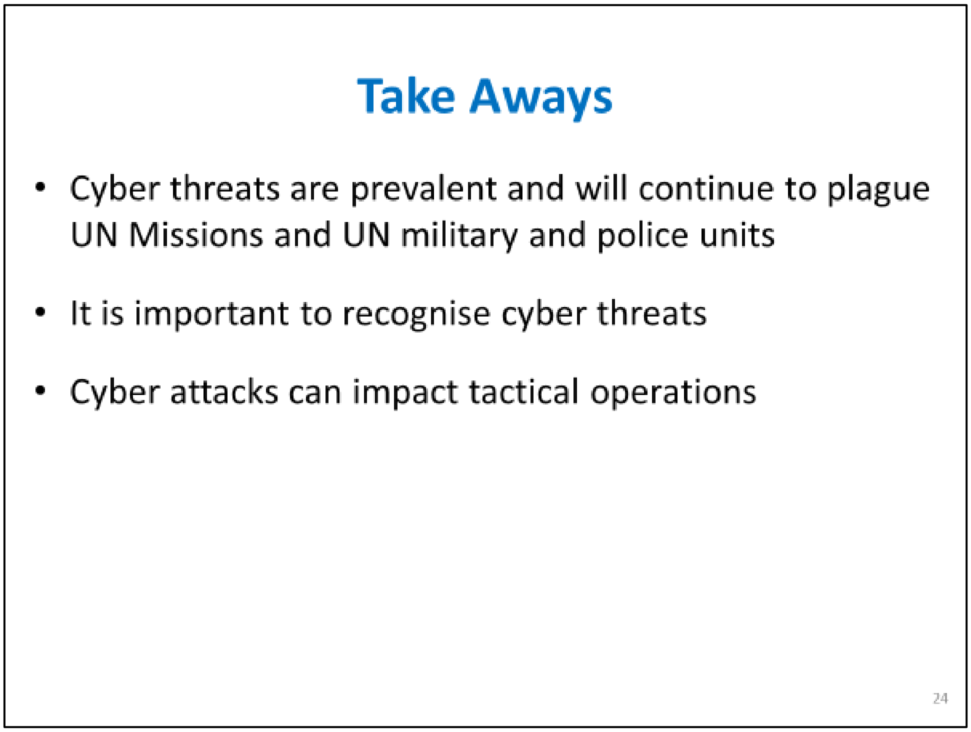
Manipulated Data and Misinformation:
By infiltrating data systems, cyber attackers can manipulate or forge critical information, leading to incorrect decision-making by military and law enforcement leadership. Inaccurate peacekeeping-intelligence, false orders, or misleading situational awareness can hamper the effectiveness of tactical units, potentially resulting in compromised operations or even putting lives at risk.

Equipment and Systems Sabotage:
Cyber-attacks targeting military equipment and systems can render them inoperable or even cause them to malfunction. Tactical units heavily rely on technology-driven assets such as drones, surveillance systems, or weapon systems. Compromising these assets could significantly hinder their ability to gather peacekeeping-intelligence, execute precision strikes, or maintain operational superiority.

Psychological Impacts:
Beyond the immediate operational consequences, cyber-attacks against tactical military and police units can have psychological and strategic impacts. The loss of trust in digital systems and vulnerabilities exposed by such attacks could erode morale within the ranks and undermine confidence in the effectiveness of future operations. Moreover, successful cyber-attacks against tactical units may embolden adversaries and potentially tip the balance of our PKO or deter successes in the peacekeeping mandate.

Conclusion:
The potential impact of cyber-attacks on tactical police and military units is a matter of concern for the UN Mission. Recognising the vulnerabilities inherent in their reliance on technology, it is crucial to bolster cybersecurity measures and invest in robust defence mechanisms. Strengthening resilience against cyber threats, enhancing training and awareness, and fostering collaboration between military, police units, and cybersecurity experts are essential to mitigate the risks posed by these attacks. Additionally, unit commanders need to monitor issues and analyse these threats to determine if they impact their current or future tactical operations. If the attack does impede or impact negatively, commanders are required to mitigate the risks that impact the operation. Options might include adjusting the plan, delaying, or cancelling the tactical operation. In module 3, we will go into more detail about the operational framework.

Slide 24



Take Aways

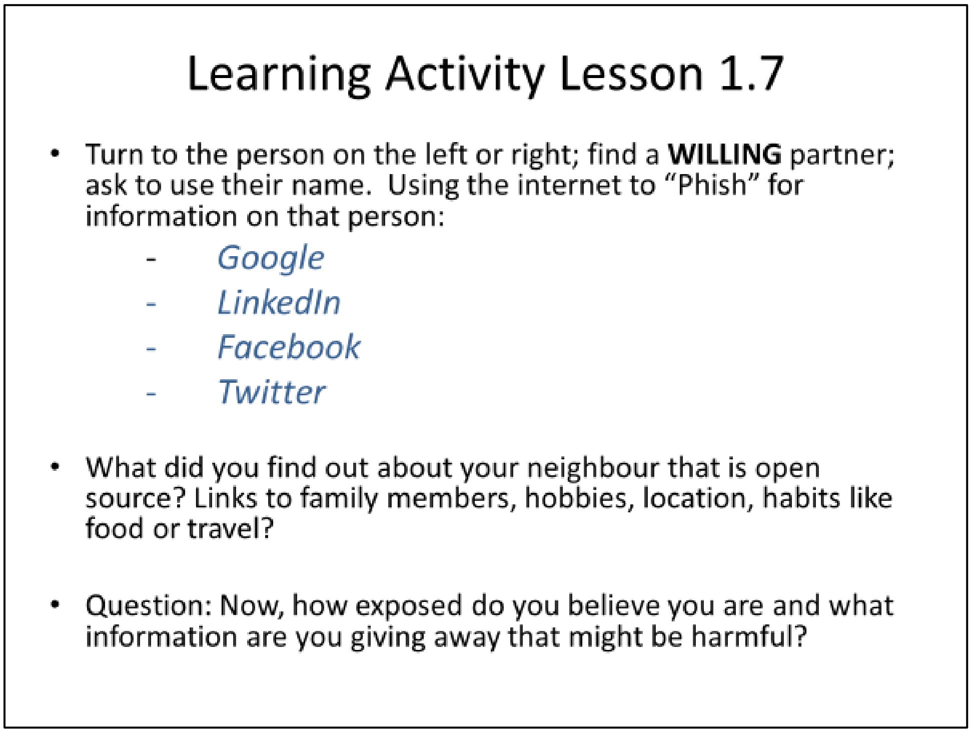
- Cyber threats are prevalent and will continue to plague UN Missions and UN military and police units
- It is important to recognise cyber threats
- Cyber attacks can impact tactical operations

24

Summary

- Cyber threats are pervasive and will persistently pose challenges to UN Missions, UN military, and police units. These threats demand ongoing attention and proactive measures to safeguard against potential attacks and impacts to PKO
- Identifying Cyber Threats and mitigating the risks is of paramount importance. By acknowledging their presence, organisations can better prepare and allocate resources to enhance their cybersecurity and FP
- Cyber-attacks have the potential to significantly disrupt tactical operations. These malicious threats can compromise communication systems, compromise sensitive information, and undermine the effectiveness of military and police units
- By acknowledging the persistent nature of cyber threats, prioritizing their recognition, and understanding their potential impact on operational activities, UN entities can better protect against potential cyber-attacks

Learning Activity Lesson 1.7



Learning Activity Lesson 1.7

- Turn to the person on the left or right; find a **WILLING** partner; ask to use their name. Using the internet to "Phish" for information on that person:
  - *Google*
  - *LinkedIn*
  - *Facebook*
  - *Twitter*
- What did you find out about your neighbour that is open source? Links to family members, hobbies, location, habits like food or travel?
- Question: Now, how exposed do you believe you are and what information are you giving away that might be harmful?

Lesson 1.8

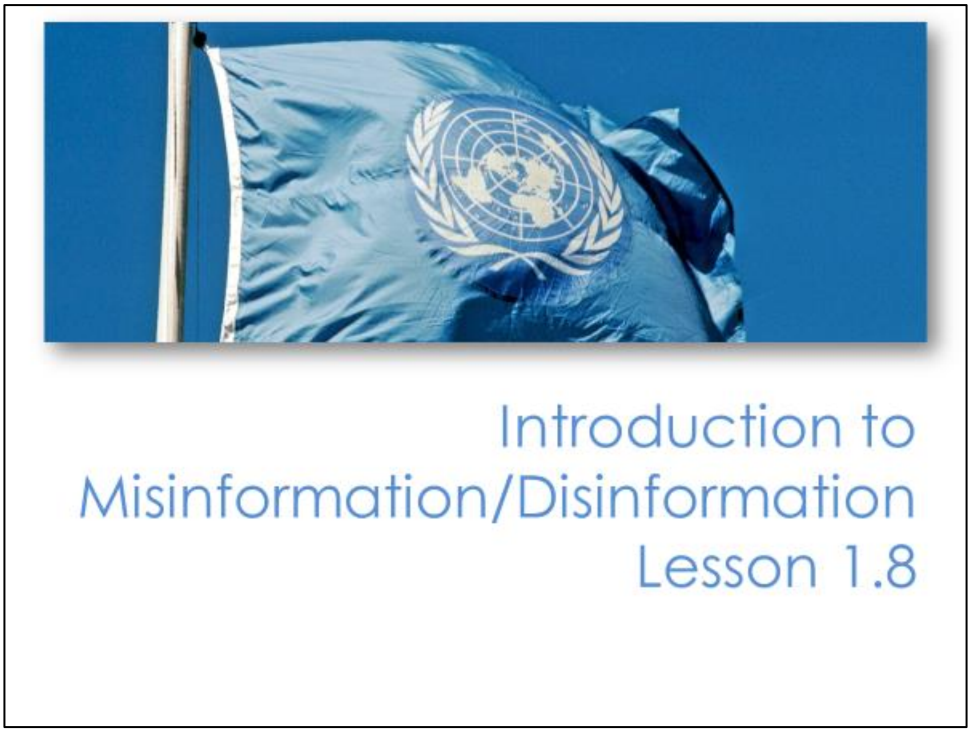
Mis/Dis Information Introduction

The Lesson

Starting the Lesson

To start off this Lesson with an engaging approach, begin by inquiring whether the participants possess any knowledge pertaining to Mis/Disinformation within the context of operating in a UN peacekeeping mission. Encourage them to share any personal experiences related to incidents or operational impacts resulting from Mis/Disinformation encountered during their involvement in a UN Mission.

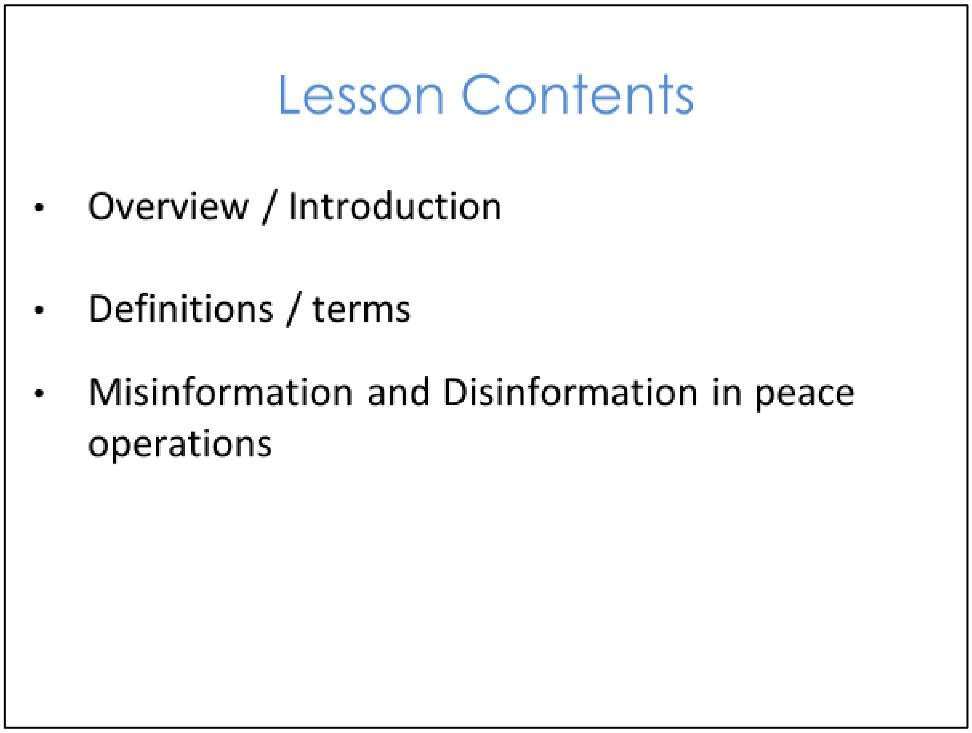
Slide 1



Introduction to
Misinformation/Disinformation
Lesson 1.8

Misinformation and disinformation (Mis/Disinformation) offences are classified as cyber-attacks. This lesson aims to provide an overview of Mis/Disinformation and its impact on the United Nations Peacekeeping Operational environment. Through examples, we will delve into its role in shaping public opinion, manipulating narratives, and eroding trust. Additionally, we will explore the dissemination methods and tools employed by malicious groups to spread Mis/Disinformation. By the end of this lesson, you will have developed a fundamental understanding of Mis/Disinformation. It is essential to acknowledge that UN units operate in collaboration with other United Nations mission components, agencies, and stakeholders to manage information and counter cyber-attacks targeting the UN effectively.

Slide 2



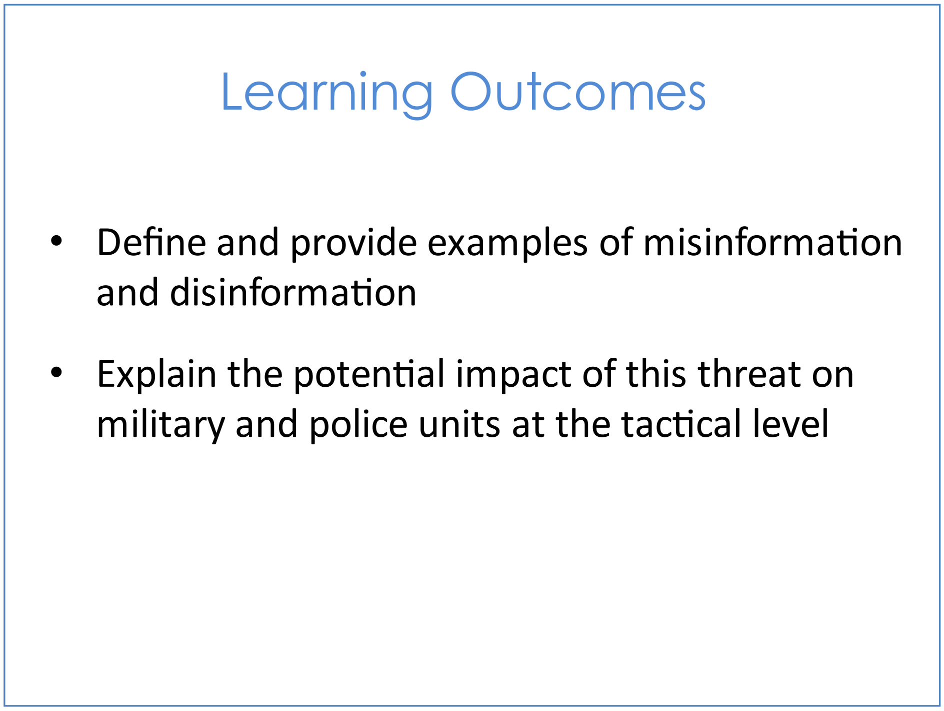
Lesson Contents

- Overview / Introduction
- Definitions / terms
- Misinformation and Disinformation in peace operations

Here are the subject areas we will be covering:

- Overview / Introduction
- Definitions / terms
- Misinformation and Disinformation in Peace Operations

Slide 3



Learning Outcomes

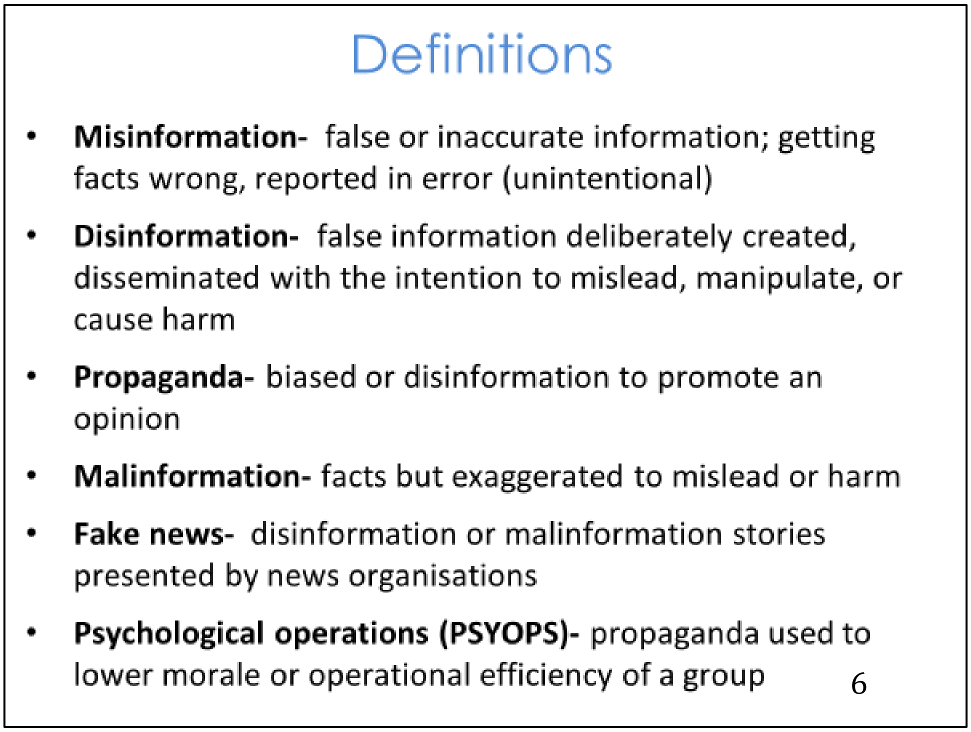
- Define and provide examples of misinformation and disinformation
- Explain the potential impact of this threat on military and police units at the tactical level

By the conclusion of this lesson, our objective is for you to have a basic understanding of the significance of Mis/Disinformation within a UNPKO environment. You will be equipped to address the following questions:

- Define and provide examples of misinformation and Disinformation.
- Explain the potential impact of this threat on military and police units at the tactical level.

Through comprehensive discussions and relevant examples, we will delve into the nature of misinformation and Disinformation, enabling you to distinguish between the two and comprehend their implications. Furthermore, we will explore how these deceptive tactics can disrupt and undermine the effectiveness of a UN Mission, specifically in relation to military and police units operating on the ground.

Slide 4



Definitions

- **Misinformation-** false or inaccurate information; getting facts wrong, reported in error (unintentional)
- **Disinformation-** false information deliberately created, disseminated with the intention to mislead, manipulate, or cause harm
- **Propaganda-** biased or disinformation to promote an opinion
- **Malinformation-** facts but exaggerated to mislead or harm
- **Fake news-** disinformation or malinformation stories presented by news organisations
- **Psychological operations (PSYOPS)-** propaganda used to lower morale or operational efficiency of a group

6

Let's take a moment to explore key definitions in the realm of mis/disinformation. It is crucial for missions to have a thorough understanding of the "information ecosystem" and the key actors operating within their specific context. This includes how local communities access and interpret information, the sources they trust, the narratives that resonate with them, and the necessary measures to address misinformation or Disinformation effectively.

To navigate this landscape, it is vital to map the actors involved, particularly on social media platforms, and their connections to political and/or security actors at the local, regional, or international levels.

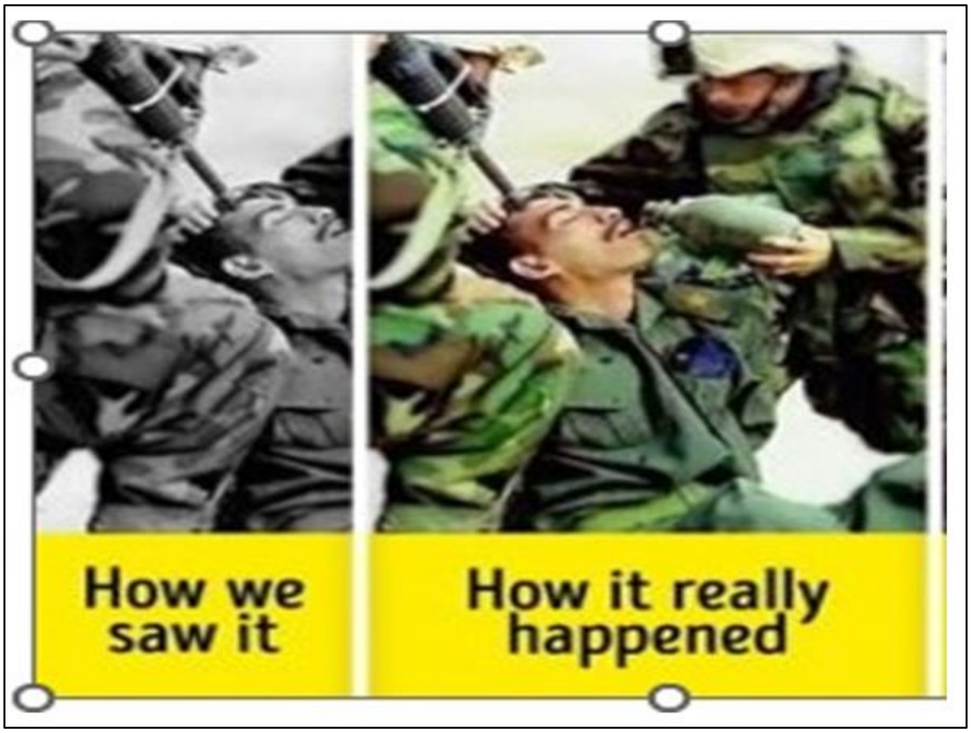
Here are the key definitions:

- Misinformation: False or inaccurate information resulting from unintentional errors in reporting where facts are incorrect.
- Disinformation: False information deliberately created and disseminated with the intention to mislead, guide, manipulate, or cause harm.
- Propaganda: Biased or misleading information, often with a specific agenda, used to promote a particular cause or influence public opinion.

- Malinformation: Information rooted in truth or facts but presented in an exaggerated manner to mislead or cause harm.
- Fake news: Disinformation or Malinformation stories presented by news organisations, typically designed to mislead or manipulate public perception.
- Psychological operations (PSYOPS): Propaganda tactics employed to lower morale or disrupt the operational efficiency of a specific group.

Understanding these definitions will provide a solid foundation for comprehending the nuances of mis/disinformation and its various manifestations in the information landscape.

Slide 5

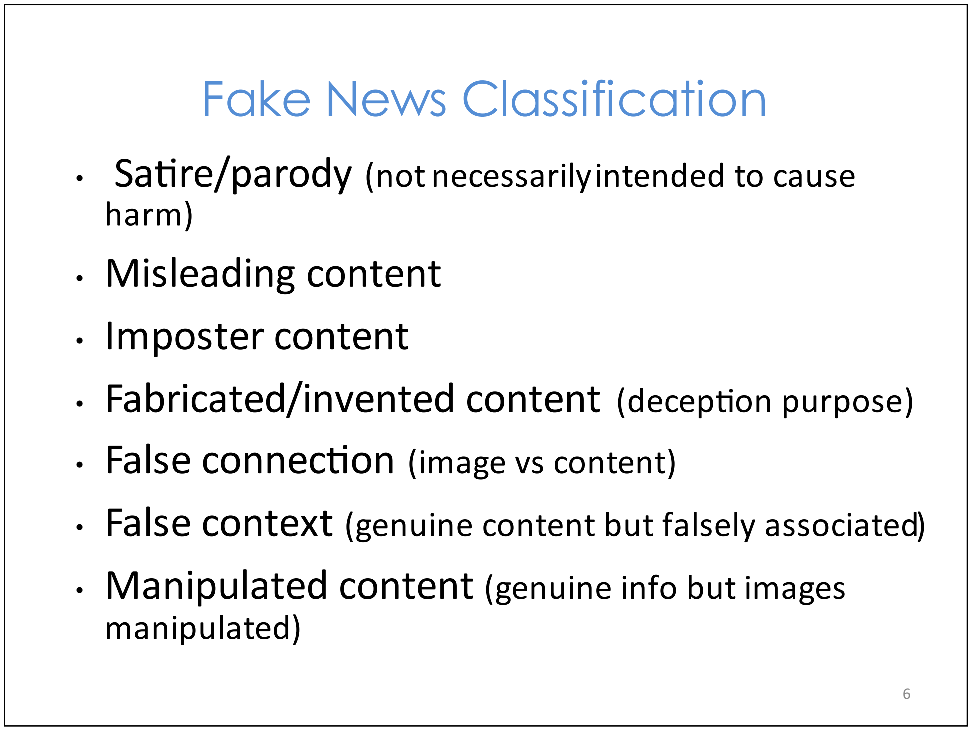


Mis/disinformation has a profound and escalating impact on UN peacekeeping operations. It shapes the perceptions of local, regional, and international actors and audiences, disrupts the implementation of mandates, and jeopardises the safety and security of peacekeepers and the communities they serve. To illustrate this, let's consider an example of how a photo can be manipulated or cropped to convey a particular message.

On the left side of the slide, you can see how the photo was presented in the local press, intentionally emphasising a negative viewpoint. The angled weapon in the image suggests the possibility of a peacekeeper pointing a firearm at an individual, fostering a negative perception. However, on the right side of the slide, we reveal the unedited photo, which provides a different context. It shows humanitarian aid being provided in the form of water to an individual in need, illustrating a positive and compassionate action.

This example highlights how mis/disinformation can be propagated through the manipulation of visuals to promote specific narratives or biases. It underscores the importance of critically analysing information and images in order to counteract the potentially harmful effects of mis/Disinformation in UN peacekeeping missions.

Slide 6



Fake News Classification

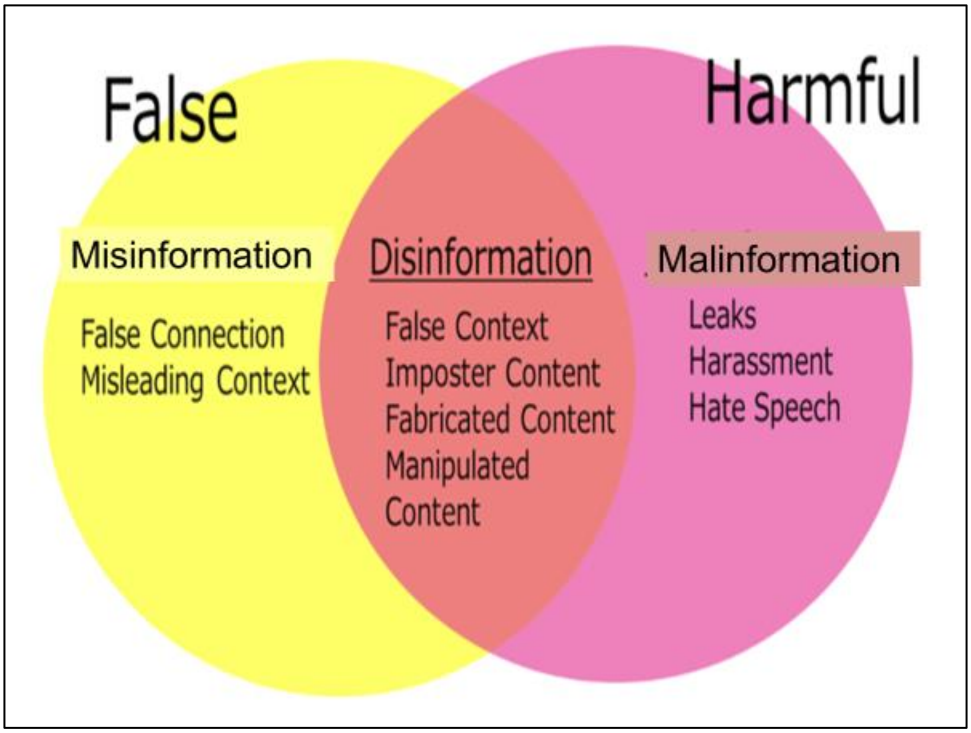
- Satire/parody (not necessarily intended to cause harm)
- Misleading content
- Imposter content
- Fabricated/invented content (deception purpose)
- False connection (image vs content)
- False context (genuine content but falsely associated)
- Manipulated content (genuine info but images manipulated)

6

Fake News Classifications:

- Satire or Parody: Content created for comedic or satirical purposes, not necessarily intended to cause harm.
- Misleading Content: Deceptive use of information with the intent to incriminate or mislead someone.
- Imposter Content: Genuine sources are replaced or impersonated, leading to deceptive information.
- Fabricated Content: Content generated specifically to deceive or mislead others.
- False Connection: Images or visuals that are falsely associated with content, creating a misleading impression.
- False Context: Genuine content that is shared with false or inaccurate information, distorting its intended meaning.
- Manipulated Content: Genuine information or images that have been intentionally altered or manipulated to deceive others.

Slide 7



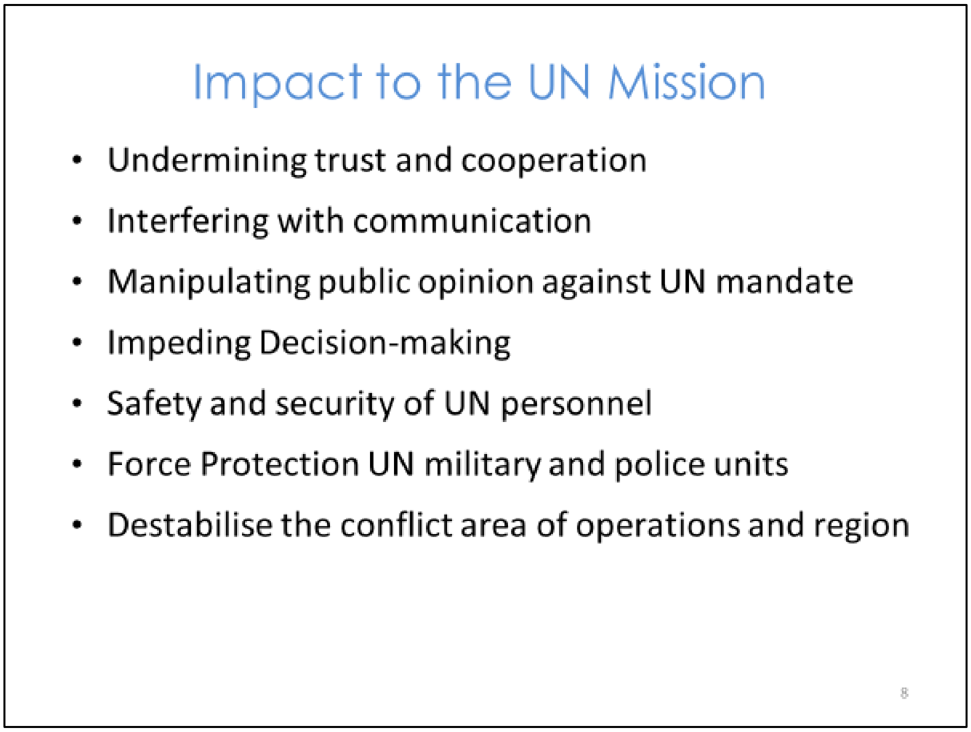
This diagram illustrates the interconnection of Mis/Disinformation and the nuanced aspects of intent. While misinformation and Disinformation are often used interchangeably and are only one word apart, it is crucial to recognise the significant distinction between these two terms: intent.

Intent serves as the differentiating factor between these closely related words. Misinformation refers to false or inaccurate information that is shared unintentionally, often stemming from errors or lack of verification. On the other hand, Disinformation involves the deliberate creation and dissemination of false information with the intention to deceive, mislead, or manipulate others.

Understanding the role of intent helps us navigate the complex landscape of Mis/Disinformation, enabling us to discern between unintentional errors and intentional deception. By recognising this critical distinction, we can develop a more comprehensive awareness of the motivations and potential harm associated with Mis/Disinformation.

Note on the far-right side of the slide, and it is important to highlight that malinformation can be considered the worst form of Disinformation.

Slide 8



Impact to the UN Mission

- Undermining trust and cooperation
- Interfering with communication
- Manipulating public opinion against UN mandate
- Impeding Decision-making
- Safety and security of UN personnel
- Force Protection UN military and police units
- Destabilise the conflict area of operations and region

8

Misinformation and disinformation attacks can have significant implications on the tactical military and police units of the United Nations operating in the field during peacekeeping operations. Some of the key implications include:

Undermining trust and cooperation: Mis/disinformation erodes trust between peacekeeping forces and local communities, hindering cooperation and making it more challenging to fulfil mission objectives.

Interfering with communication: False information can disrupt communication channels and hinder the effective exchange of critical information among UN units, impacting coordination and decision-making processes.

Manipulating public opinion against UN mandate: Mis/disinformation campaigns can manipulate public opinion, creating a negative perception of the UN mission's objectives and undermining support from local populations.

Impeding decision-making: Mis/disinformation can cloud the decision-making process by introducing false or misleading information, leading to suboptimal choices and impeding effective mission execution.

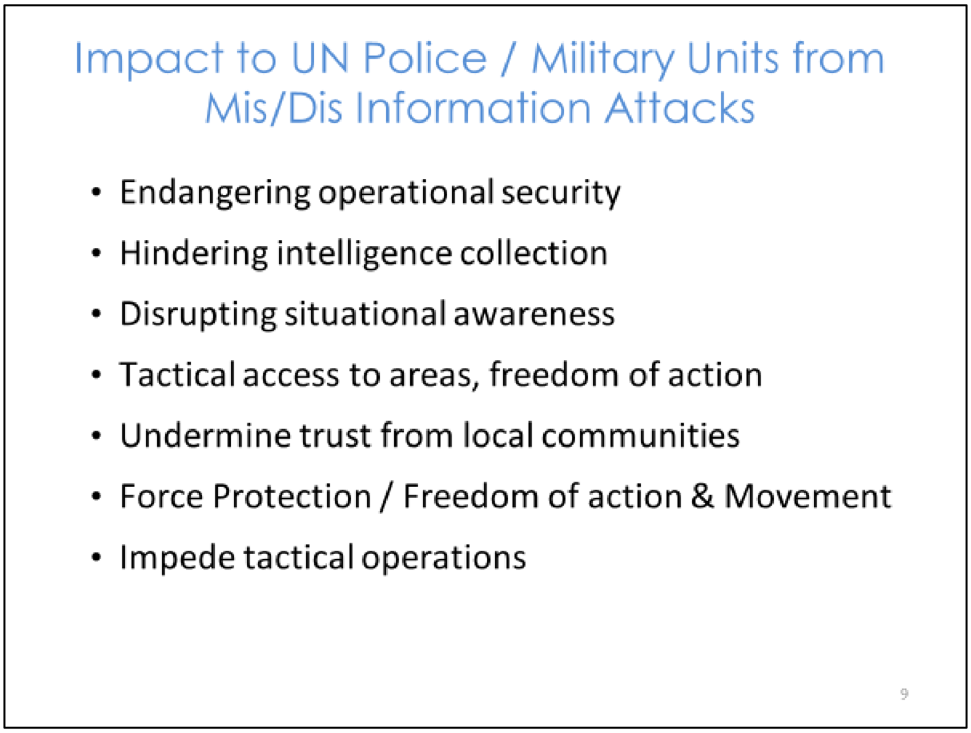
Safety and security of UN personnel: Mis/disinformation can directly impact the safety and security of UN personnel by spreading false threats, inciting violence, or revealing operational details to hostile entities.

Force protection of UN military and police units: False information can specifically target UN military and police units, but the broader impact of these attacks often extends beyond direct concerns. These attacks can jeopardise the freedom of action of UN units or hinder the successful execution of their mission and tasks. This can manifest as constraints on their operational capabilities compromised situational awareness, or increased risks in carrying out their duties effectively. It is essential to recognise the potential implications of mis/disinformation attacks on the overall force protection and operational effectiveness of UN military and police units in order to implement appropriate risk mitigation measures and safeguards.

Destabilizing the conflict area and region: Mis/disinformation offences / campaigns can exacerbate tensions, escalate conflicts, and contribute to the destabilisation of not only the conflict area but also the wider region.

Recognising these implications is crucial for UN military and police units to effectively address and counter the challenges posed by mis/Disinformation during peacekeeping operations.

Slide 9



Impact to UN Police / Military Units from Mis/Dis Information Attacks

- Endangering operational security
- Hindering intelligence collection
- Disrupting situational awareness
- Tactical access to areas, freedom of action
- Undermine trust from local communities
- Force Protection / Freedom of action & Movement
- Impede tactical operations

9

Misinformation and disinformation attacks can have specific implications for the United Nations tactical military and police units operating in the field during a peacekeeping operation. Here's a refined focus on how these attacks can impact their tasks and operations:

Endangering Operational Security: Misinformation and Disinformation can compromise the operational security of UN tactical units. False information about troop movements, planned operations or vulnerabilities can be used by hostile actors to exploit weaknesses, ambush patrols, or undermine the element of surprise. It can also jeopardise the safety of UN personnel, compromising the success of their missions.

Hindering peacekeeping-intelligence Collection: Tactical units heavily rely on accurate peacekeeping-intelligence to make informed decisions and execute operations effectively. Misinformation campaigns can manipulate local populations, making it difficult for UN units to gather reliable information. False narratives or deliberate misdirection can lead to unreliable sources, reducing the effectiveness of peacekeeping-intelligence-gathering efforts.

Disrupting Situational Awareness: Misinformation and Disinformation can distort the understanding of the operational environment. UN tactical units need accurate and up-to-date situational awareness to assess threats, determine the status of conflicting parties and understand local dynamics. False information can lead to misinterpretation of the situation, hindering effective decision-making and operational planning.

Undermining Trust with Local Communities: Tactical units' success often depends on the trust and cooperation of local communities. Misinformation and disinformation campaigns can erode trust, making it challenging to build relationships and gain vital information from the local population. It can also fuel hostility towards the UN presence, hindering community engagement efforts and potentially leading to a hostile environment for peacekeeping personnel.

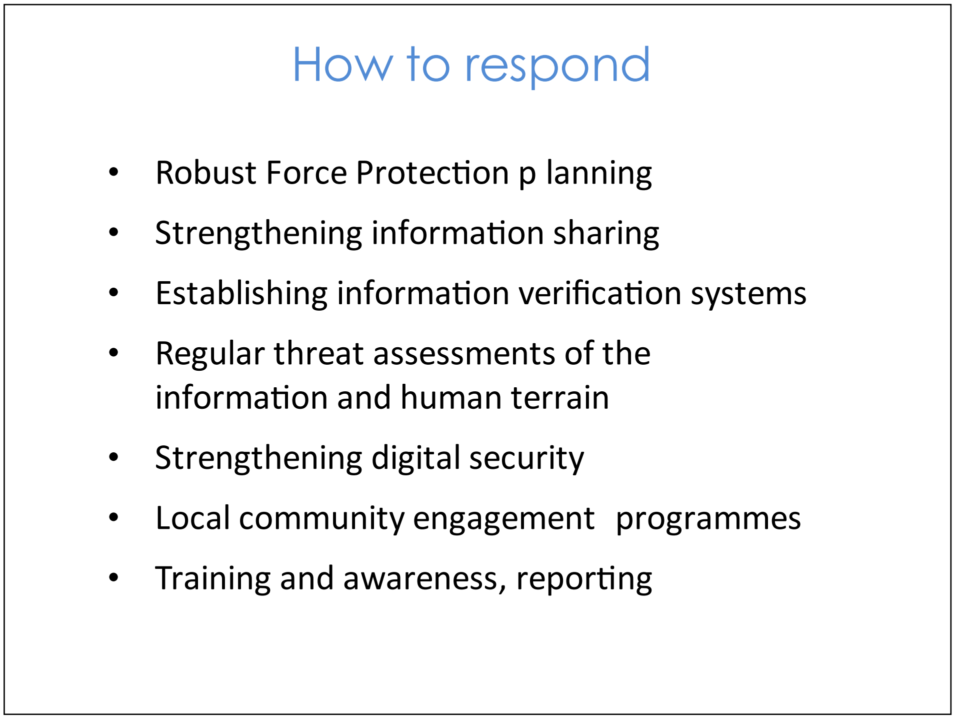
Manipulating Conflict Dynamics: Disinformation campaigns can exploit existing divisions and grievances within conflict-affected communities. They can propagate false narratives, incite violence or deepen mistrust among different factions. These manipulations can escalate tensions and complicate the peacekeeping mission's objectives by fuelling conflicts rather than resolving them.

Force Protection: Mis/Disinformation can pose a threat to the safety and security of UN military and police personnel. False information about potential attacks, ambushes or improvised explosive devices (IEDs) can lead to units being unprepared or taking unnecessary risks. It can also compromise operational security by revealing sensitive information, such as troop movements or operational plans, to hostile actors. This can increase the vulnerability of UN peacekeeping forces and jeopardise the FP planning force and implement inaccurate mitigating courses of action.

Freedom of Action & Movement: UN peacekeeping forces rely on their freedom of action and movement to effectively carry out their mandate. Mis/Disinformation can hinder their ability to operate freely by spreading rumours or false narratives that create fear, confusion or suspicion among local populations. This can result in restricted access to critical areas, limited cooperation from local communities or even hostility towards UN forces. Such constraints can impede the ability of peacekeeping units to establish a secure environment, conduct patrols, engage with communities and effectively implement their mission objectives.

Impede Tactical Operations: Tactical operations require accurate and timely information to plan and execute missions successfully. Mis/Disinformation can disrupt these operations by misleading UN military and police units about the intentions, capabilities or locations of hostile forces or armed groups. False reports about the presence or absence of armed elements, misleading peacekeeping-intelligence, or fabricated threats can lead to poor decision-making, misguided deployments, or compromised operational effectiveness. This can result in unnecessary risks to personnel and equipment, reduce situational awareness and the potential failure to achieve the mission objectives.

Slide 10



How to respond

- Robust Force Protection p lanning
- Strengthening information sharing
- Establishing information verification systems
- Regular threat assessments of the information and human terrain
- Strengthening digital security
- Local community engagement programmes
- Training and awareness, reporting

To mitigate the impact of misinformation and disinformation attacks, UN tactical military and police units should consider the following measures:

Strengthening Information Sharing: Enhance collaboration and information-sharing mechanisms among UN units, local authorities, and peacekeeping-intelligence partners. Establish channels for sharing verified information and analysis, enabling the rapid dissemination of accurate peacekeeping-intelligence to improve situational awareness.

Establishing Robust Information Verification: Implement rigorous processes to verify the credibility of information sources. Training UN personnel in media literacy and critical analysis can enable them to discern accurate information from misinformation. Establish partnerships with local media outlets and engage with trusted local sources to verify information on the ground.

Conducting Regular Threat Assessments: Regularly assess the threat landscape to identify emerging disinformation tactics and their potential impact on tactical operations. Analyse trends and patterns in misinformation campaigns, adapting strategies and tactics accordingly to stay ahead of the disinformation curve.

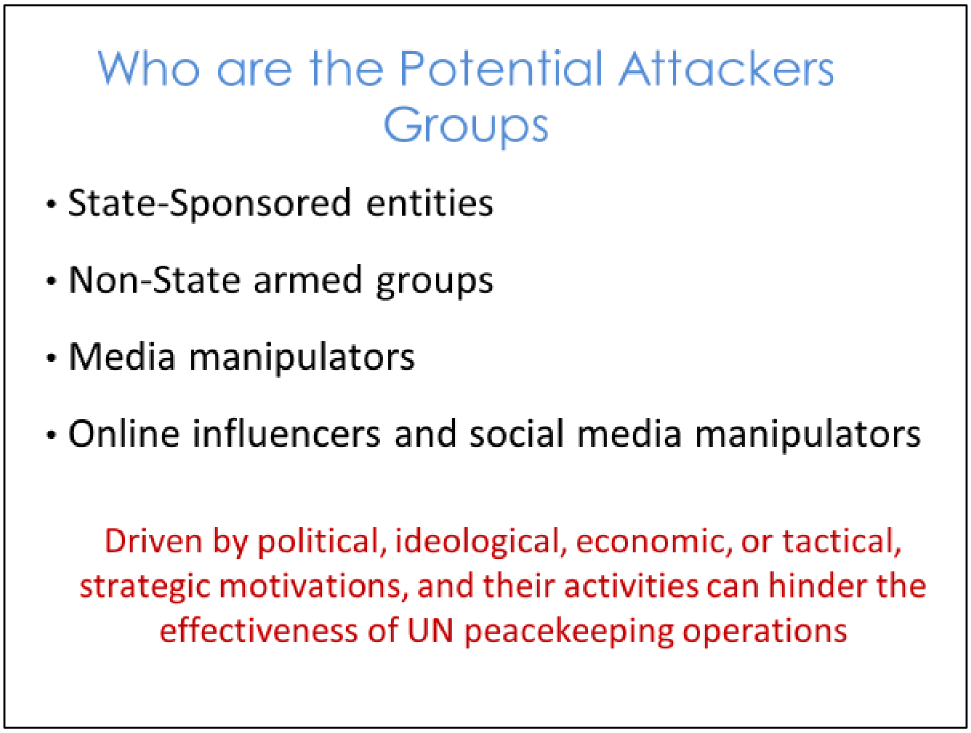
Strengthening Digital Security: Enhance cybersecurity measures to protect sensitive information and communication channels from infiltration or manipulation. Implement encryption, multi-factor authentication, and other security measures to prevent unauthorised access and mitigate the risk of disinformation attacks targeting UN communication networks.

Engaging with Local Communities: Foster relationships with local communities through community policing initiatives, outreach programmes, and public information campaigns. By actively engaging and building trust, UN units can counteract misinformation narratives, address grievances, and foster collaboration with the local population.

Training and Awareness: Provide specialised training to UN tactical units on recognising and countering misinformation and disinformation tactics. Enhance their digital literacy and critical thinking skills to navigate the information landscape effectively. This will enable personnel to identify potential threats, assess the credibility of information and respond appropriately.

By implementing these measures, UN tactical military and police units can better adapt to the challenges posed by misinformation and Disinformation, enhance their operational effectiveness and contribute to the overall success of the peacekeeping mission.

Slide 11



Who are the Potential Attackers Groups

- State-Sponsored entities
- Non-State armed groups
- Media manipulators
- Online influencers and social media manipulators

Driven by political, ideological, economic, or tactical, strategic motivations, and their activities can hinder the effectiveness of UN peacekeeping operations

Potential actors or groups that may engage in using misinformation and Disinformation against United Nations peacekeeping missions include:

State-Sponsored Entities: Governments or state actors seeking to protect their interests or maintain control over a conflict or region, may deploy misinformation and disinformation campaigns to discredit UN peacekeeping operations.

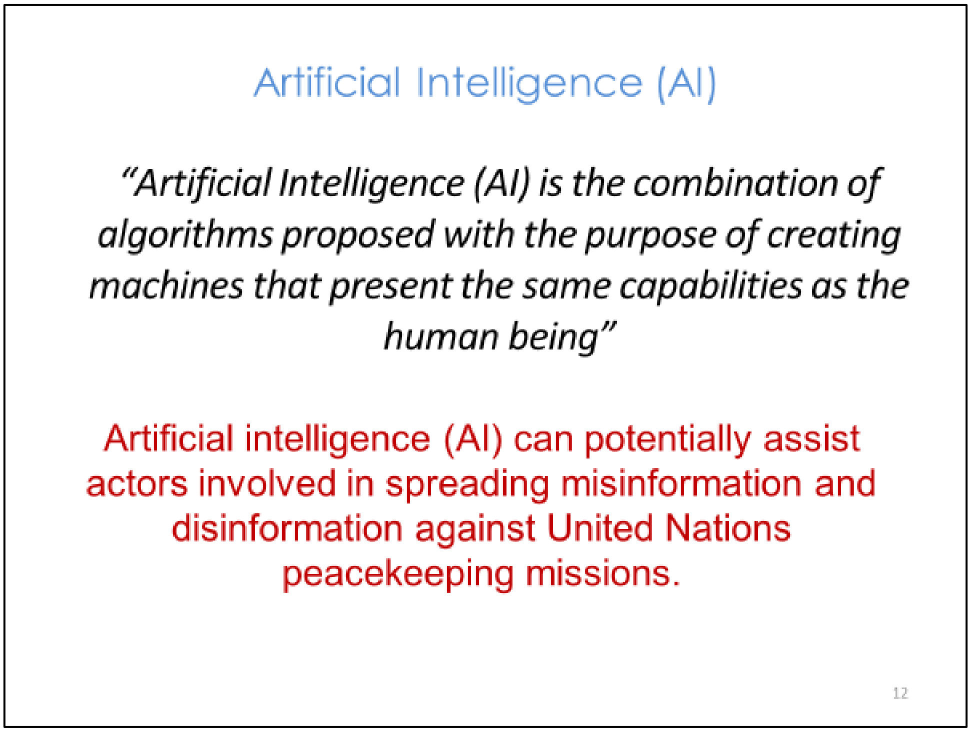
Non-State Armed Groups: Rebel factions, extremist organisations or armed militias with a vested interest in challenging international interventions or preserving their power may spread false information to undermine the credibility of UN peacekeeping missions.

Media Manipulators: Certain media outlets or individuals with specific agendas or biases might manipulate information or create false narratives to shape public opinion, create divisions or generate controversy surrounding UN peacekeeping operations.

Online Influencers and Social Media Manipulators: Through social media platforms, online influencers or the use of automated bots, actors or groups with anti-UN motives can rapidly spread misinformation and Disinformation, aiming to manipulate public discourse and undermine trust in peacekeeping efforts.

These actors may be driven by political, ideological, economic or strategic motivations, and their activities can hinder the effectiveness of UN peacekeeping missions. It is crucial for individuals to critically assess information, rely on verified news sources and remain vigilant against the influence of misinformation and Disinformation.

Slide 12



Artificial Intelligence (AI)

"Artificial Intelligence (AI) is the combination of algorithms proposed with the purpose of creating machines that present the same capabilities as the human being"

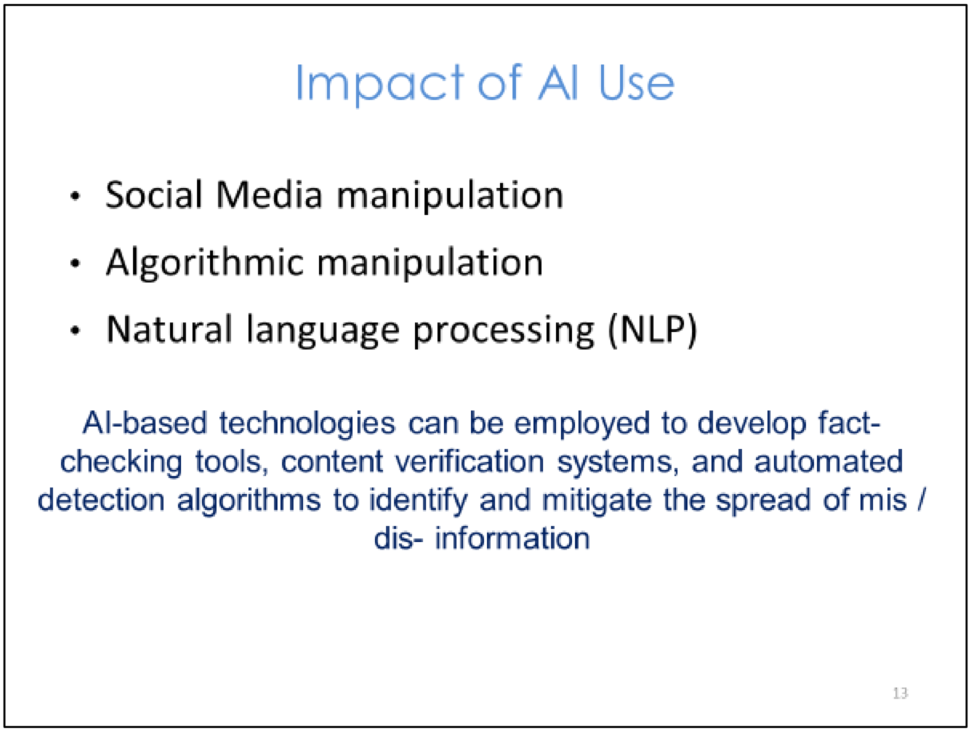
Artificial intelligence (AI) can potentially assist actors involved in spreading misinformation and disinformation against United Nations peacekeeping missions.

12

AI can potentially assist actors involved in spreading misinformation and Disinformation against United Nations peacekeeping missions. Here are a few ways AI might be used:

Automated Content Generation: AI-powered tools can generate large volumes of false information or misleading narratives. These tools can create fake news articles, fabricated images or even deepfake videos that appear authentic, making it challenging for users to discern fact from fiction.

Slide 13



Impact of AI Use

- Social Media manipulation
- Algorithmic manipulation
- Natural language processing (NLP)

AI-based technologies can be employed to develop fact-checking tools, content verification systems, and automated detection algorithms to identify and mitigate the spread of mis / dis- information

13

Impacts can include:

Social Media Manipulation: AI algorithms can be used to create and operate networks of social media bots that disseminate and amplify false information. These bots can generate likes, shares and comments to create an illusion of widespread support for a particular narrative, thereby increasing its visibility and influence.

Algorithmic Manipulation: AI algorithms can be deployed to manipulate online platforms' recommendation systems, search results or trending algorithms. By exploiting these algorithms, actors can ensure that false or misleading content reaches a wider audience, increasing its impact and potential to sow confusion.

NLP: AI-powered NLP models can be trained to generate coherent, persuasive and contextually relevant false narratives. These models can mimic human-like writing styles, making it more difficult to identify automated disinformation campaigns.

It is important to note that while AI can be used to amplify misinformation and Disinformation, it can also play a crucial role in detecting and combating these issues. AI-based technologies can be employed to develop fact-checking tools, content verification systems, and automated detection algorithms to identify and mitigate the spread of false information.

Slide 14

Partners who can help

CTBTO
UNDESA
UNDPA
Food and Agriculture Organization of the United Nations
IAEA
ILO
IOM
International Trade Centre
ITU
United Nations Human Rights
UN WOMEN
UNAIDS
UNITED NATIONS UNCTAD
UN environment
UNESCO
UNFPA
UN HABITAT
UNHCR
unicef
UNIDO
UNISDR
unitar
UNODC
UNOPS
WFP World Food Programme
World Health Organization
WIPO
WORLD METEOROLOGICAL ORGANIZATION

In today's fast-paced digital landscape, addressing misinformation and Disinformation is of paramount importance for United Nations peacekeeping missions. Thankfully, several organisations have risen to the occasion, dedicating their efforts to combating false narratives and safeguarding the integrity of these crucial operations. Within the list of potential partners, three organisations are highlighted in black on this slide (where are the black highlights on the slide?), which I will discuss.

United Nations Communications Group (UNCG):
The UNCG plays a pivotal role in coordinating and strengthening communications efforts across various UN entities. Through its strategic guidance and support, the UNCG helps peacekeeping missions develop effective communication strategies to counter misinformation and Disinformation. By promoting accurate information dissemination and engaging with local communities, the UNCG contributes to building trust and countering false narratives that may hinder peacekeeping operations.

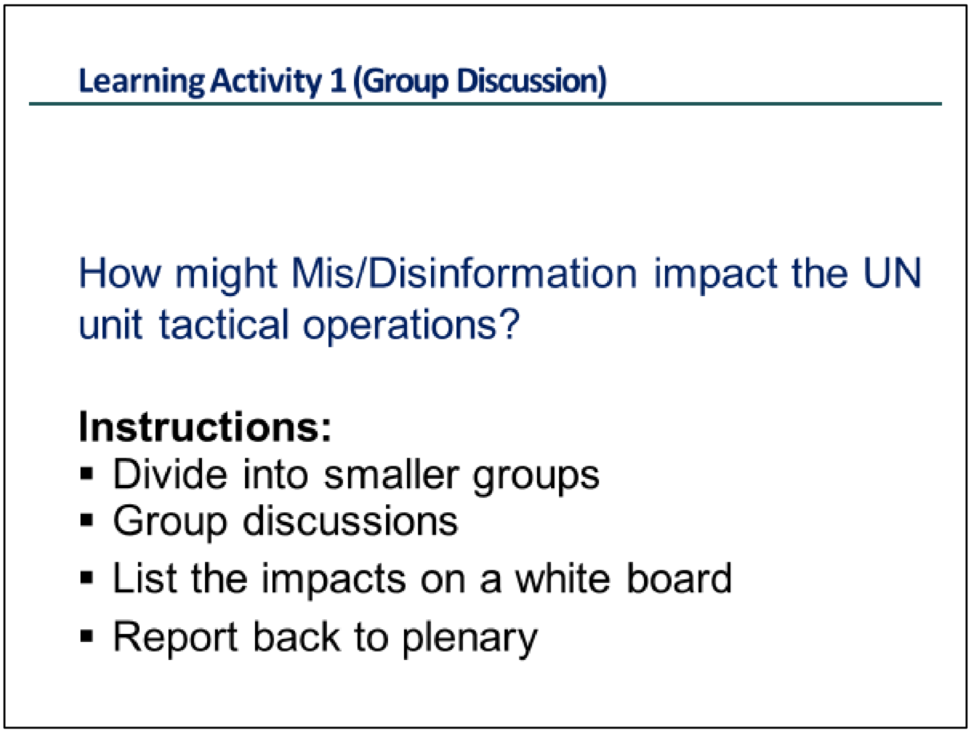
United Nations Educational, Scientific and Cultural Organisation (UNESCO):
UNESCO plays a crucial role in promoting media literacy and supporting independent journalism worldwide. Through its programme and initiatives, UNESCO strengthens media and information literacy skills among local populations, empowering them to critically assess and navigate the information landscape.

By fostering media literacy, UNESCO equips communities with the tools necessary to identify and combat misinformation and Disinformation, thus contributing to the overall resilience of UN peacekeeping missions.

International Fact-Checking Network (IFCN):
The IFCN is a global network of fact-checkers dedicated to promoting accuracy in public discourse. Its member organisations rigorously fact-check information and debunk falsehoods across various topics and regions. By collaborating with the IFCN, UN peacekeeping missions can access reliable information and leverage the expertise of fact-checkers to counter misinformation and Disinformation effectively.

Conclusion:
Misinformation and disinformation attacks pose significant challenges to United Nations peacekeeping missions. However, through the concerted efforts of organisations on this slide, strides are being made to help mitigate the risks. By promoting accurate information, enhancing media literacy, and leveraging technological advancements, these organisations contribute to the resilience and effectiveness of UN peacekeeping operations.

Slide 15



Learning Activity 1 (Group Discussion)

How might Mis/Disinformation impact the UN unit tactical operations?

Instructions:

- Divide into smaller groups
- Group discussions
- List the impacts on a white board
- Report back to plenary

To foster engaging discussions about the effects of Mis/Disinformation at the tactical operational level, follow these steps:

Group Formation: Divide the class into small groups, ensuring an equal distribution of students in each group.

Materials: Provide flip charts or large sheets of paper and markers to each group for note-taking and brainstorming.

Discussion Prompt: Introduce the topic by asking the students to list the effects of Mis/Disinformation at the tactical operational level. Encourage them to consider the potential impacts on various aspects of unit operations.

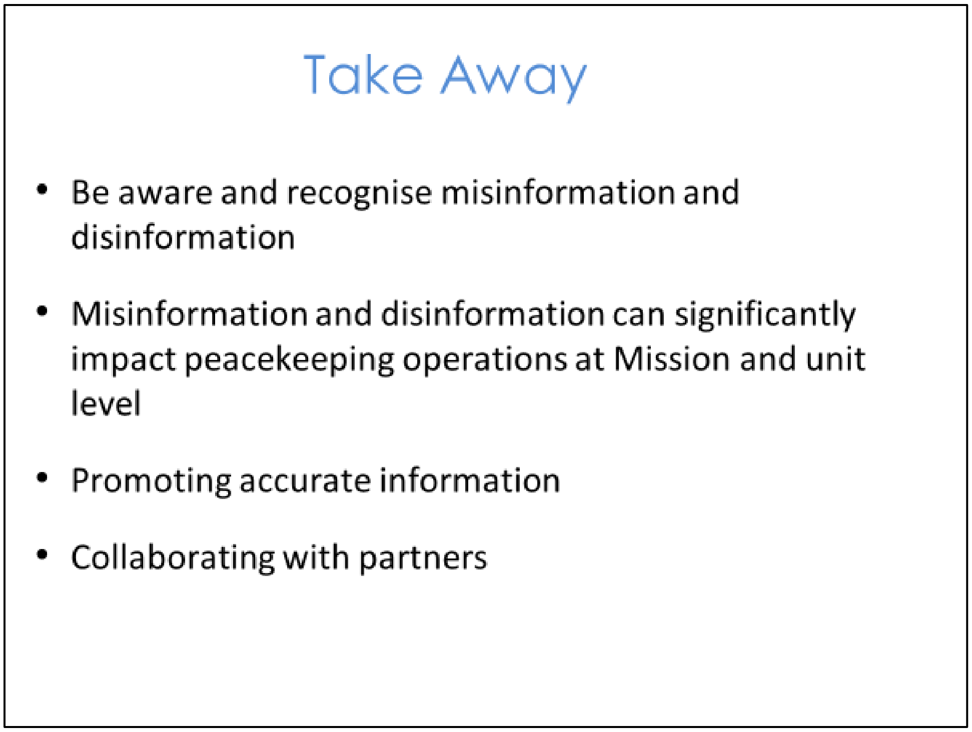
Group Brainstorming: Allocate sufficient time for each group to brainstorm and list the effects of Mis/Disinformation. Encourage them to think critically and consider both immediate and long-term consequences.

Presentation: Request one representative from each group to present their group's list of effects. This allows for a diverse range of perspectives and ideas to be shared with the class.

Guided Conversation: Guide the conversation during the presentations by asking follow-up questions to deepen the understanding of each effect listed. Encourage students to provide examples or scenarios to illustrate the impact of Mis/Disinformation on mobility, credibility, TOB security engagement with local populations, demonstrations against the UN, and attacks against UN facilities and personnel.

By following this approach, students will actively participate in group discussions, share their insights, and collectively explore the multifaceted effects of Mis/Disinformation at the tactical operational level. The guided conversation will enable a deeper understanding of the topic and encourage critical thinking among the students.

Slide 16



Take Away

- Be aware and recognise misinformation and disinformation
- Misinformation and disinformation can significantly impact peacekeeping operations at Mission and unit level
- Promoting accurate information
- Collaborating with partners

Summary

- Enhancing awareness and recognition: Strengthening the ability of peacekeeping personnel to identify misinformation and disinformation through training and tools.
- Understanding the significant impact: Recognising the negative effects of false narratives on UN missions and UN units, emphasising the need for FP planning and risk mitigation measures
- Promoting accurate information dissemination: Prioritising the transparent and timely sharing of verified information with relevant stakeholders to combat the influence of false narratives.
- Collaborating with partners: Engaging with various stakeholders, such as local authorities, international organisations, media outlets, and civil society groups, to leverage their expertise and resources in countering misinformation and disinformation

Module 1

Conceptual Framework

At the conclusion of Module 1, a few concluding points are worth noting:

- A range of policies, manuals, guidelines, philosophies, and principles have been developed over time to create an understanding of UNFORPRO in UN Peacekeeping Missions.

- Nevertheless, the implementation and execution of the UN Mission's FP strategy is never straightforward and clear and adjusts due to the UNPKO environment. A flexible attitude within the conceptual framework is needed.

- All personnel must have a general understanding of FP and the threat-based approach to the analysis of the peacekeeping environment.

- When planning an FP strategy, it must be based on threats and risk analysis. The PKO environment is lethal and has spoilers that focus efforts to disrupt mandate objectives. The conceptual framework will now provide a baseline to help build on the operational framework for planning FP courses of action to mitigate the risks posed by threats to our units. We will go into more detail in Module 3

Module 2

Legal Framework for United Nations Force Protection

Aim

This module conveys to key aspects of the legal framework underlying UN Peacekeepers' force protection efforts.

Relevance

Module 2 empowers UN peacekeepers with confidence to effectively protect themselves, other UN personnel and installations by providing them an understanding on when and how they may use defensive force and peacekeeping intelligence for purposes of protection.

Learning Objectives for the Module

- Understand when and how uniformed personnel may use force to protect themselves or other mission personnel against attacks of a military or non-military nature
- Know the UN legal framework for the collection of peacekeeping intelligence related to force protection
- Legal framework supports our FP operations

Overview

Module 2 provides an overview on when defensive force can be employed by military and police components (authority to use force) and how such force may be employed against threats of a military or non-military nature (limits on the use of force). The Module also sets out the UN's legal framework for peacekeeping intelligence, as relevant to force protection.

Symbols Legend Reminder

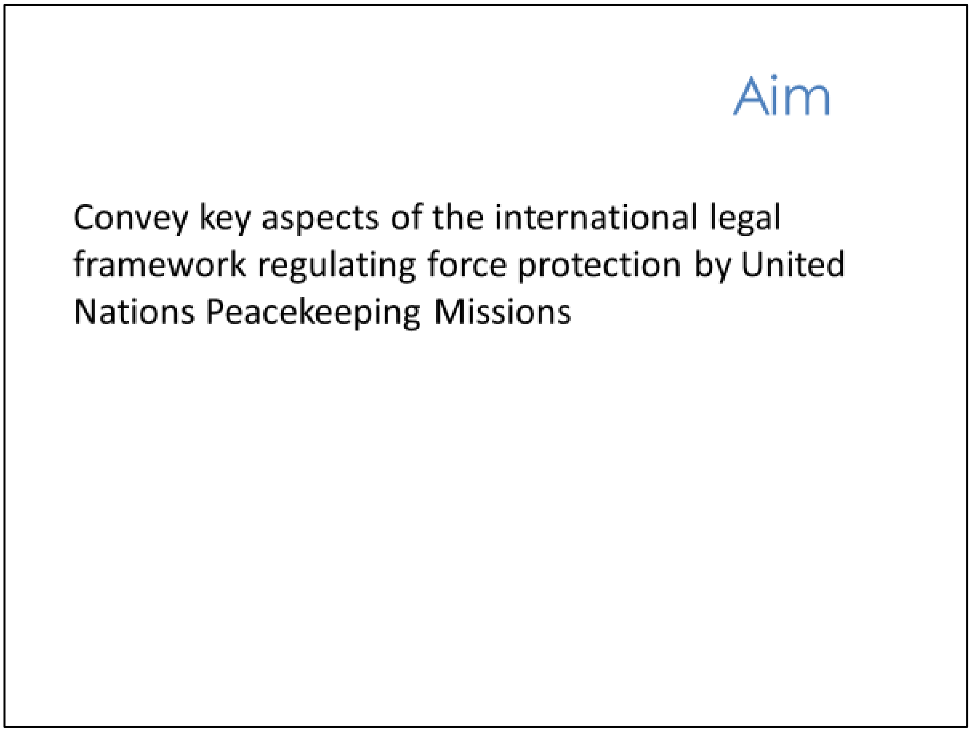
💡	Interactive presentations or small exercises to engage the participants
🎞	Suggested film segment to illustrate the content
☞	Note to the instructor to highlight aspects of the materials or point towards additional materials

Slide 1

Lesson 2

Legal Framework for
United Nations Force Protection

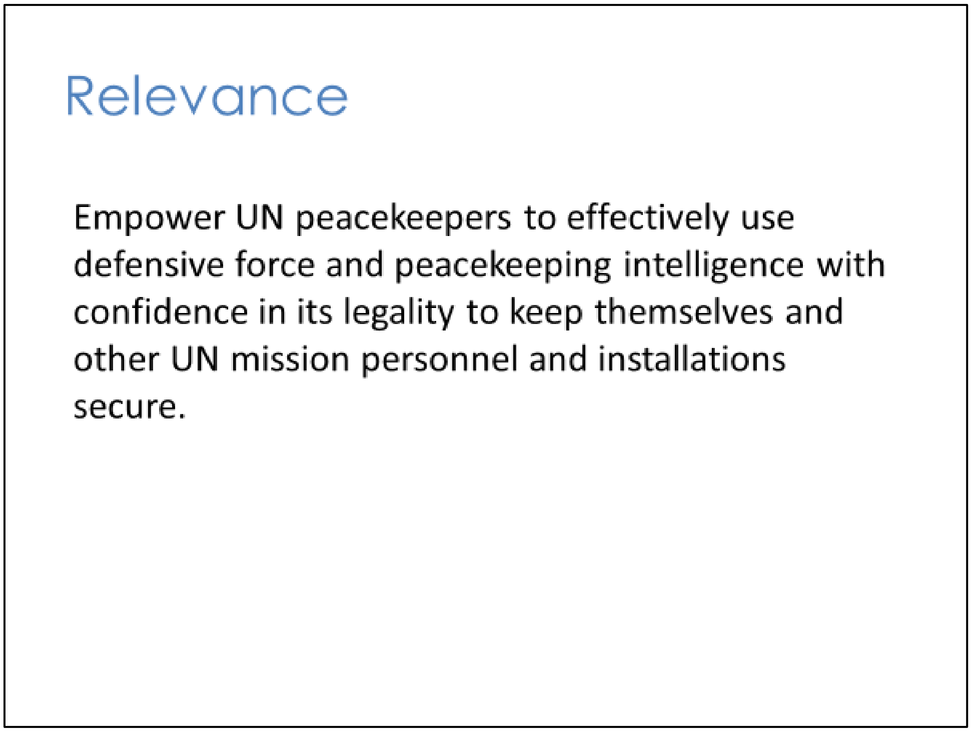
Slide 2



Aim

Convey key aspects of the international legal framework regulating force protection by United Nations Peacekeeping Missions

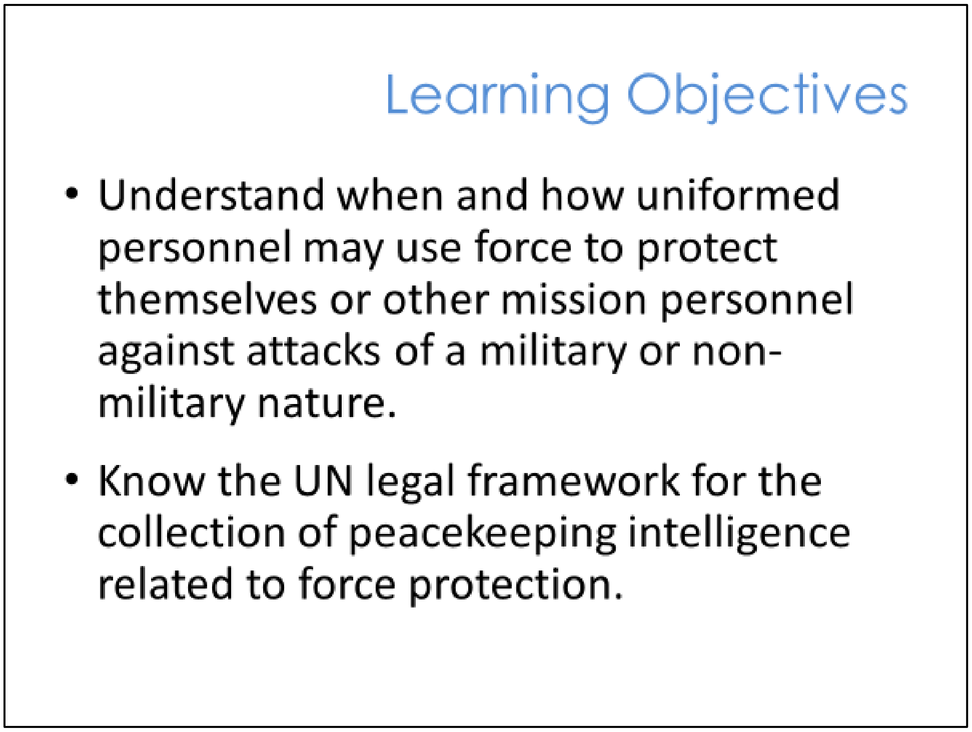
Slide 3



Relevance

Empower UN peacekeepers to effectively use defensive force and peacekeeping intelligence with confidence in its legality to keep themselves and other UN mission personnel and installations secure.

Slide 4

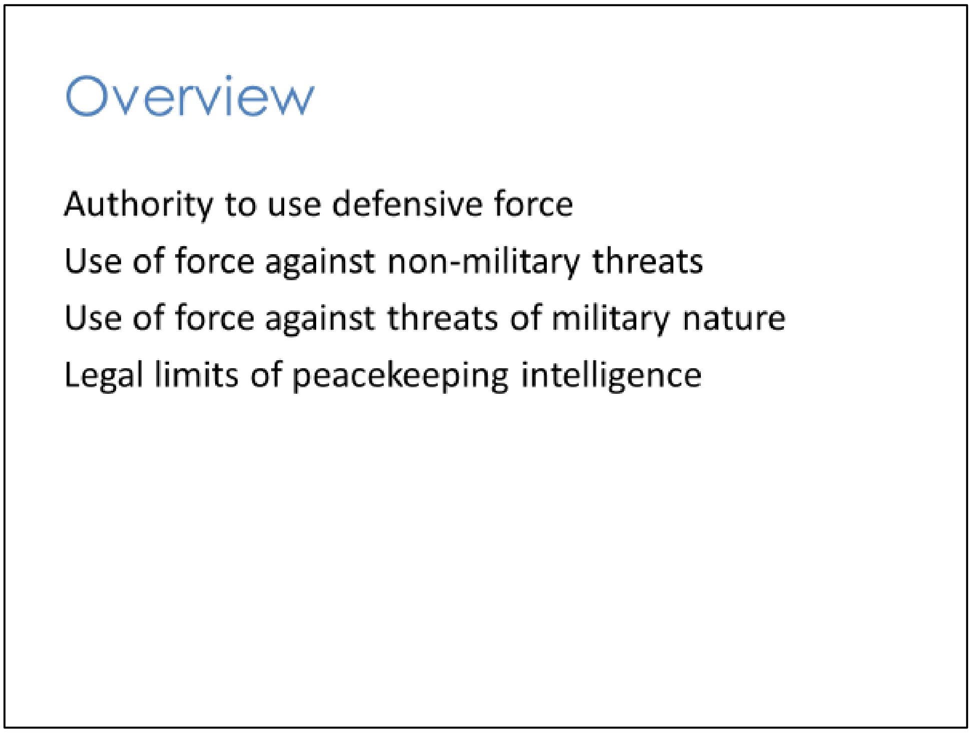


Learning Objectives

- Understand when and how uniformed personnel may use force to protect themselves or other mission personnel against attacks of a military or non-military nature.
- Know the UN legal framework for the collection of peacekeeping intelligence related to force protection.

Here are the learning objectives for this lesson.

Slide 5



Overview

Authority to use defensive force

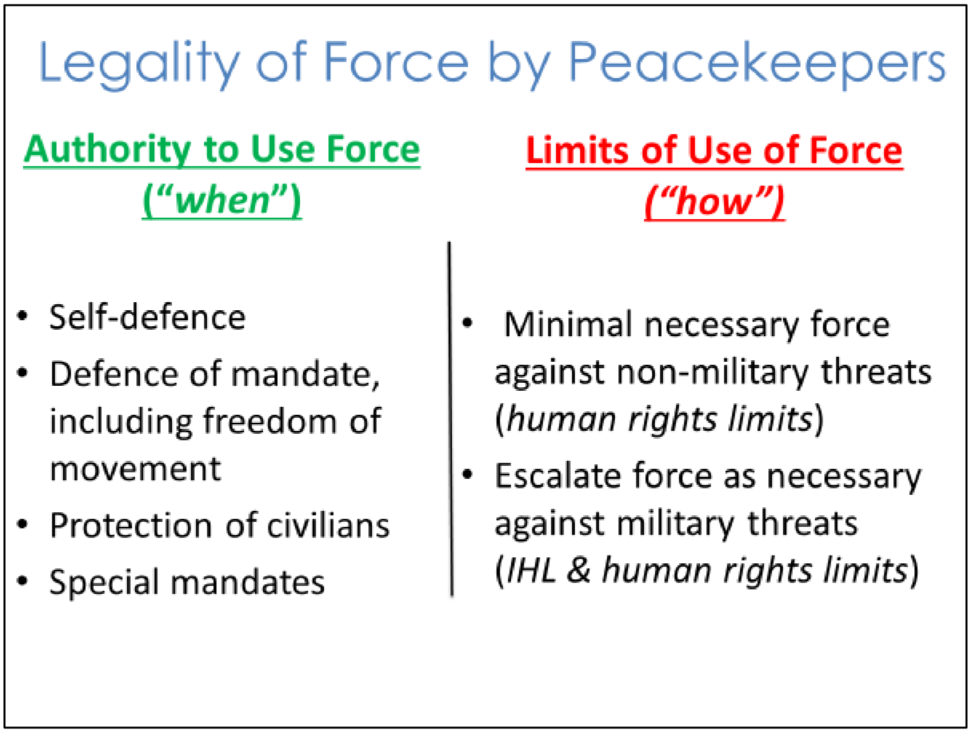
Use of force against non-military threats

Use of force against threats of military nature

Legal limits of peacekeeping intelligence

Here is the overview or contents of this lesson.

Slide 6:



Legality of Force by Peacekeepers

Authority to Use Force (*"when"*)

- Self-defence
- Defence of mandate, including freedom of movement
- Protection of civilians
- Special mandates

Limits of Use of Force (*"how"*)

- Minimal necessary force against non-military threats (*human rights limits*)
- Escalate force as necessary against military threats (*IHL & human rights limits*)

Key message: Missions are always authorised to use force in self-defence. They must use the minimal force necessary to counter non-military threats but may escalate force as necessary to defend themselves against military threats.

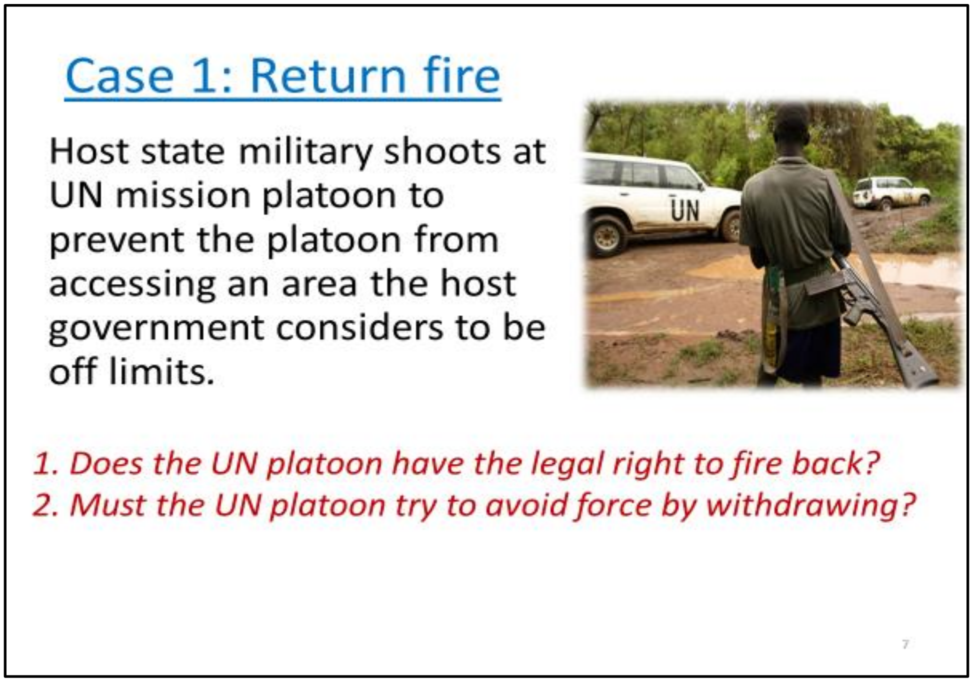
The mission's Rules of Engagement (ROE, for the UN military) and Directive on the Use of Force (DUF, for UN police) are set out when the mission has the authority to use force. Peacekeeping missions always have the authority to use force in self-defence. The use of force beyond self-defence depends on the mandate. Multidimensional missions are usually authorised to use force in defence of the mandate, including for purposes of asserting their freedom of movement. Furthermore, they are regularly mandated to use all necessary means to protect civilians against physical violence. In some cases, the mandate may further expand the authority to use force. Some mandates have given missions authority to use force to neutralise armed groups in support of the host state.

ROE and DUF also establish limits on the use of force. Under their DUFs, UN Police must always use force within the limits of international law enforcement and human rights standards.

The ROE for the military component also restrains the use of force to the minimum necessary level. Against threats of a non-military nature, the minimum use of force necessary to defend against the threat effectively and safely may be used. The limits on the use of force are similar to what law enforcement officials are allowed to use when defending themselves or others against an unlawful attack.

However, the UN military may engage in combat-level military force where necessary to effectively defend themselves, other UN personnel or UN installations against an unlawful attack of a military nature. In such situations, military peacekeepers are bound notably by the rules of IHL on the conduct of hostilities, although human rights continue to apply as well.

Slide 7:



Case 1: Return fire

Host state military shoots at UN mission platoon to prevent the platoon from accessing an area the host government considers to be off limits.

1. Does the UN platoon have the legal right to fire back?
2. Must the UN platoon try to avoid force by withdrawing?

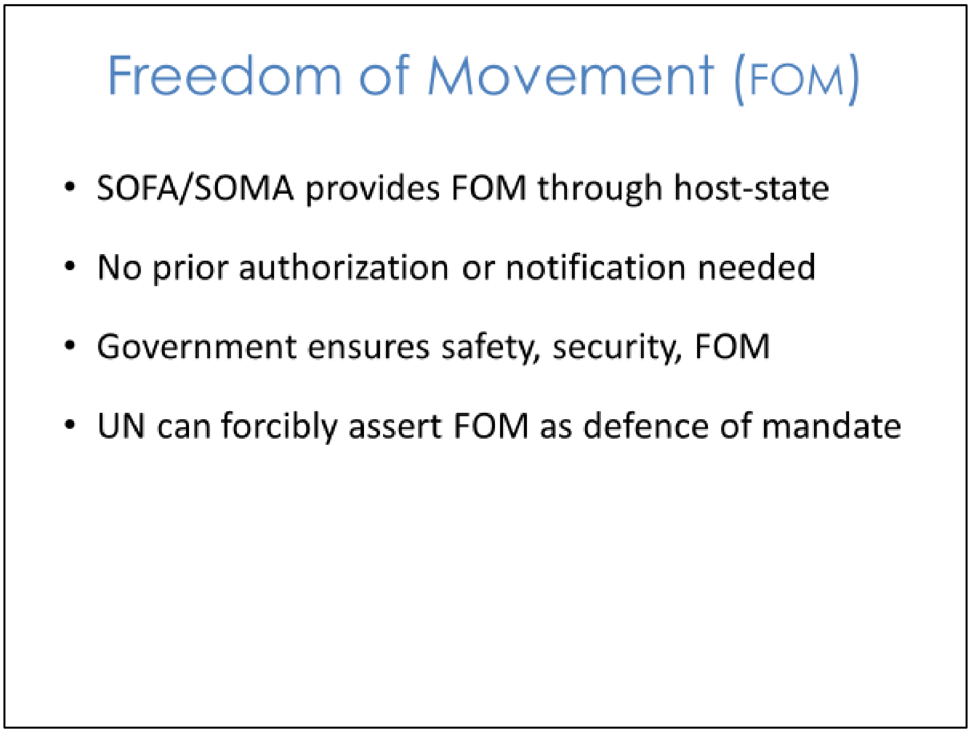
7

For this and the other cases in this module, ask participants to discuss in small groups or in plenary how they would respond to each question. For the debriefing on case 1, you can use slides 8 and 9. The following issues should emerge from the case discussion:

- *The host state military impedes the freedom of movement throughout the country, which is guaranteed under the SOFA/SOMA. Missions do not have to seek prior authorisation before moving around the country, as this would undermine their capacity to effectively conduct observation and other tasks in the mission area. Under its defence of mandate authority to use force, the mission may use force to gain access to the area concerned.*
- *Furthermore, the mission is subject to an unlawful attack (based on an unlawful denial of freedom of movement). The platoon may exercise its rights to self-defence, including by using firearms to defend themselves against an attack that may cause death or serious injuries among the platoon members.*

- *While operational considerations may make it prudent to withdraw from the area, legally, the mission has a right to stand its ground and thereby assert its freedom of movement. It does not have to avoid the use of defensive force by withdrawing from the area.*

Slide 8:



Freedom of Movement (FOM)

- SOFA/SOMA provides FOM through host-state
- No prior authorization or notification needed
- Government ensures safety, security, FOM
- UN can forcibly assert FOM as defence of mandate

Key message: UN mission personnel enjoy freedom of movement throughout the mission area, and the mission may use force to assert its freedom of movement.

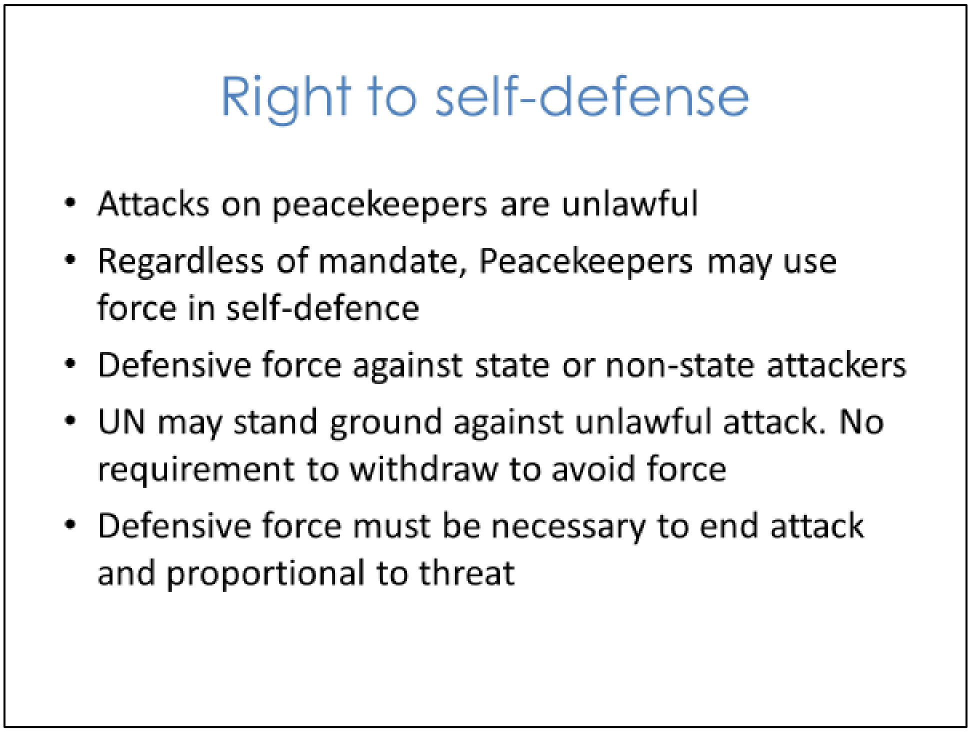
Status of Force Agreements/Status of Mission Agreements (SOFAs/SOMAs) provide that peace operations enjoy freedom of movement throughout the territory of the host state. Such freedom is essential for implementing mission mandates.

While the language slightly varies between SOFAs/SOMAs, the UN will not accept requirements of prior authorisation or notification for its own movements. However, there may be reasonable exceptions, e.g., for movements by UN aircraft for air traffic control purposes.

In many situations, armed groups pose the greatest threats to the mission's freedom of movement. The SOFA/SOMA legally requires the host state authorities to ensure safety, security, and freedom of movement, notably by clearing illegal roadblocks and checkpoints.

The mission may also assert freedom of movement under its authority to use force in defence of the mandate. This legal authority exists regardless of whether armed groups or government officials deny freedom of movement. But as noted above, it is a different question whether the mission will make the decision to use that authority to use force, especially against state officials, which will have considerable political and operational implications.

Slide 9:



Right to self-defense

- Attacks on peacekeepers are unlawful
- Regardless of mandate, Peacekeepers may use force in self-defence
- Defensive force against state or non-state attackers
- UN may stand ground against unlawful attack. No requirement to withdraw to avoid force
- Defensive force must be necessary to end attack and proportional to threat

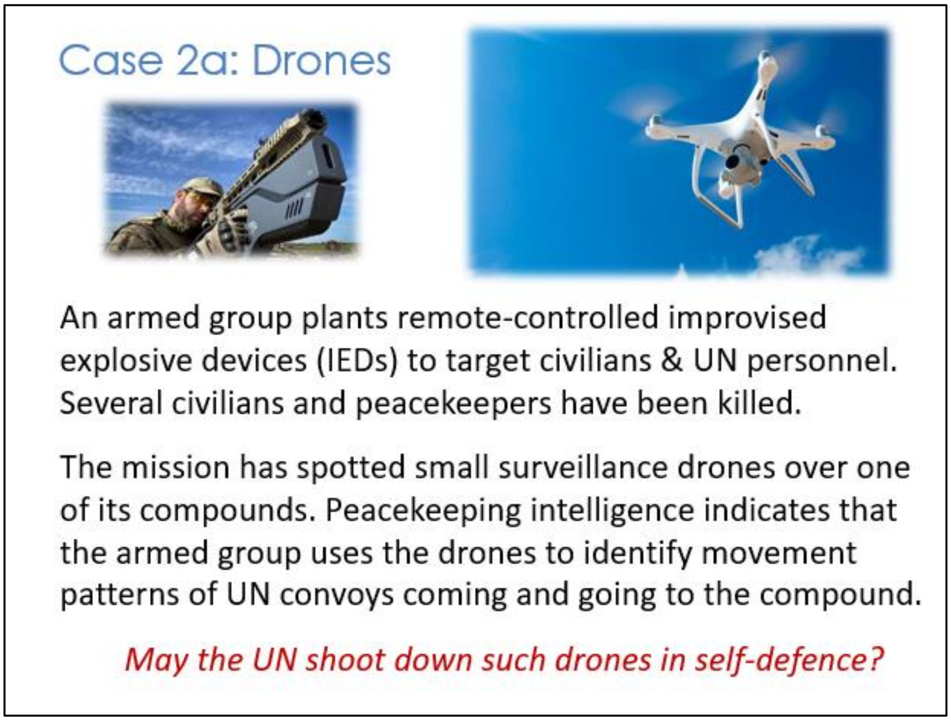
Key message: UN peacekeepers may use necessary force in self-defence against unlawful attacks by state or non-state actors.

Peacekeepers enjoy special protection under international law, based on the 1994 Convention on the Safety of United Nations and Associated Personnel. Attacks on peacekeepers, regardless of whether they are military, police, or civilians, will therefore generally be illegal under international law.

Regardless of the mandate of the peacekeeping missions, peacekeepers have the right to use force in self-defence against attacks by state or non-state actors. Even missions with an overall limited mandate – for instance, a United Nations ceasefire observer mission – enjoy that right of self-defence.

In defending itself, the UN may use the force necessary to defend itself effectively and safely against the attack. The level of defence must also not be out of proportion to the threat. There is no requirement to withdraw to avoid the use of force, especially since the UN enjoys the right of freedom of movement across the mission area.

Slide 10:



Case 2a: Drones

An armed group plants remote-controlled improvised explosive devices (IEDs) to target civilians & UN personnel. Several civilians and peacekeepers have been killed.

The mission has spotted small surveillance drones over one of its compounds. Peacekeeping intelligence indicates that the armed group uses the drones to identify movement patterns of UN convoys coming and going to the compound.

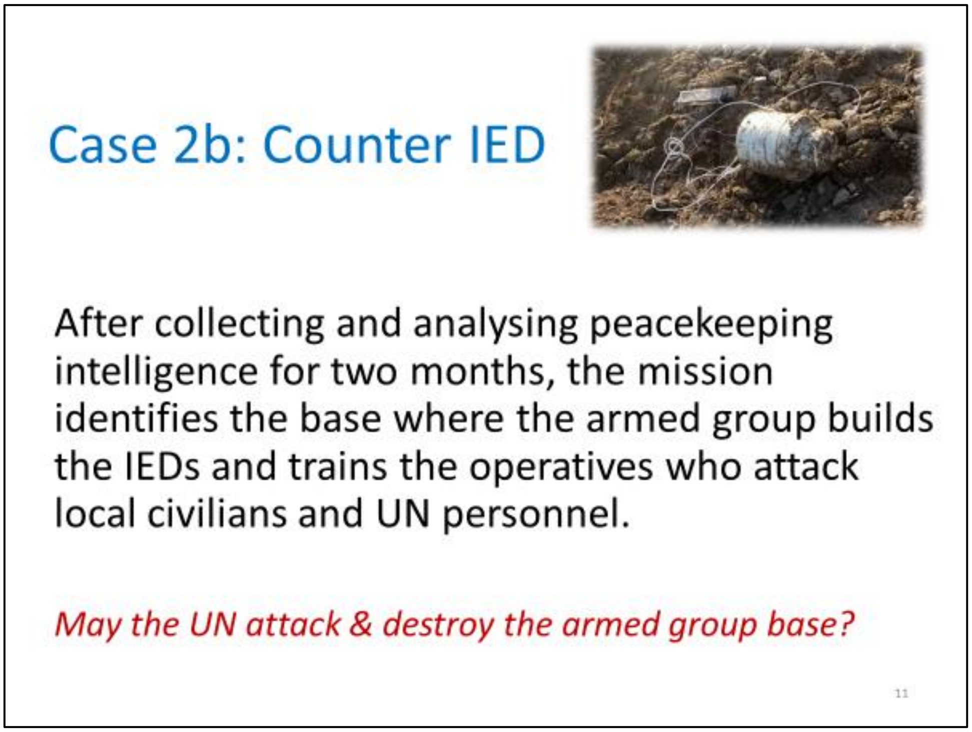
May the UN shoot down such drones in self-defence?

Participants should discuss this case in plenary – or, if time permits, in small groups. Slide 12 can be used to facilitate the debriefing.

Key points to emphasise for case 2a:

- *Even though the drones are unarmed, there are indications that their operation in the vicinity of UN compounds forms an integral part of recurrent military-level IED attacks on the UN.*
- *The exercise of the right to self-defence by peacekeepers against military attacks does not require a currently ongoing or imminent attack (see also next case). Given that the UN is already subject to recurrent attacks and the threat is latent, proactive defensive military action can be taken to prevent further IED attacks. In particular, the peacekeepers may shoot down the drones.*

Slide 11:



Case 2b: Counter IED

After collecting and analysing peacekeeping intelligence for two months, the mission identifies the base where the armed group builds the IEDs and trains the operatives who attack local civilians and UN personnel.

May the UN attack & destroy the armed group base?

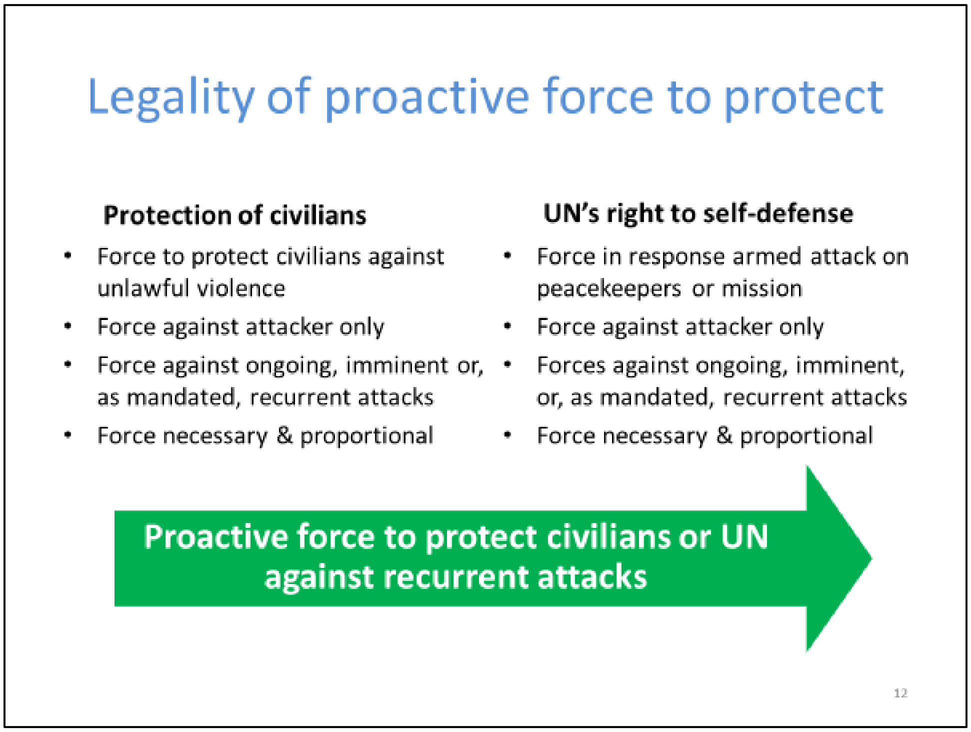
11

Participants should discuss this case in plenary – or, if time permits, in small groups. Slide 12 can be used to facilitate the debriefing.

Key points to emphasise for case 2b:

- *Use of force within the ROE is permitted*
- *The exercise of the right to self-defence by peacekeepers against attacks does not require a currently ongoing attack. Also, the POC framework here is important. Given that the UN and civilians have been targeted and are already subject to recurrent attacks and the threat is latent, proactive military action can be taken to prevent further IED attacks.*
- *In planning, it might be suggested to incorporate HSSF and or special police forces from the host state to do the targeting and arresting, etc.; EOD teams should also be incorporated for risk mitigation and forensics.*

Slide 12:



Legality of proactive force to protect

Protection of civilians

- Force to protect civilians against unlawful violence
- Force against attacker only
- Force against ongoing, imminent or, as mandated, recurrent attacks
- Force necessary & proportional

UN's right to self-defense

- Force in response armed attack on peacekeepers or mission
- Force against attacker only
- Forces against ongoing, imminent, or, as mandated, recurrent attacks
- Force necessary & proportional

Proactive force to protect civilians or UN against recurrent attacks

12

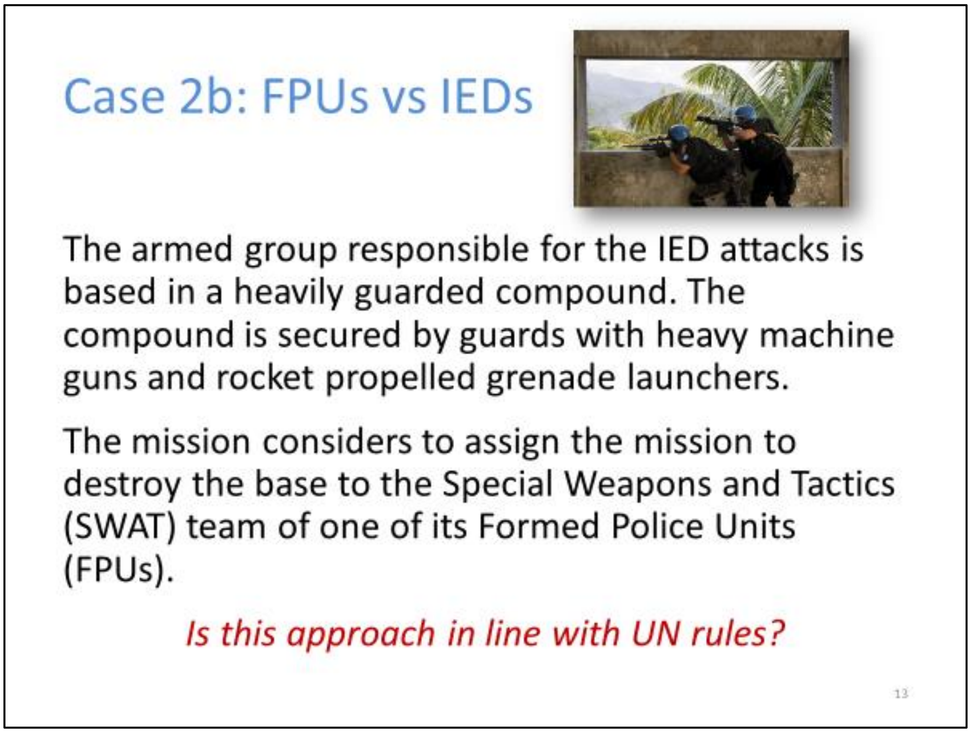
Key message: UN missions may use proactive defensive force to neutralise the source of recurrent attacks against civilians or UN personnel.

Contemporary protection of civilians mandates tasks the United Nations to protect civilians against violent attacks. Earlier mandate restrictions for such attacks to be imminent are now often removed. This means that the mission is allowed to take proactive measures to neutralise the attackers before they strike (including through lethal force, to the extent necessary and proportional). In practice, armed groups that attack the UN are often also carrying out attacks on civilians, so proactive force against them can be justified on that basis.

Regarding the right to self-defence proper, peacekeepers may defend themselves if attacked or about to be attacked. But where peacekeepers have been subject to recurrent attacks of a military nature, they do not have to wait until they are struck again before taking proactive defence measures. They may use proactive force against the authors of the attacks, including lethal force to the extent necessary and proportional. In some missions, such as MINUSMA, the mandate specifically authorises force to counter recurrent attacks. In other missions, the military can rely on the defence of mandate authority to take proactive action. In particular, force is permitted to secure the freedom of movement of the mission and its personnel. Attacks by armed groups (in particular IEDs) effectively deny freedom of movement.

It should be noted that such force in reaction to recurrent attacks is different from so-called "preventive self-defence" before any attack is about to occur. Instead, the peacekeepers defend themselves after attacks have already occurred, in a situation of recurrent attacks. They would also use force at the tactical level against elements of those armed groups that actually attack them and not engage in a general counterinsurgency/counter-terrorism campaign.

Slide 13:



Case 2b: FPUs vs IEDs

The armed group responsible for the IED attacks is based in a heavily guarded compound. The compound is secured by guards with heavy machine guns and rocket propelled grenade launchers.

The mission considers to assign the mission to destroy the base to the Special Weapons and Tactics (SWAT) team of one of its Formed Police Units (FPUs).

Is this approach in line with UN rules?

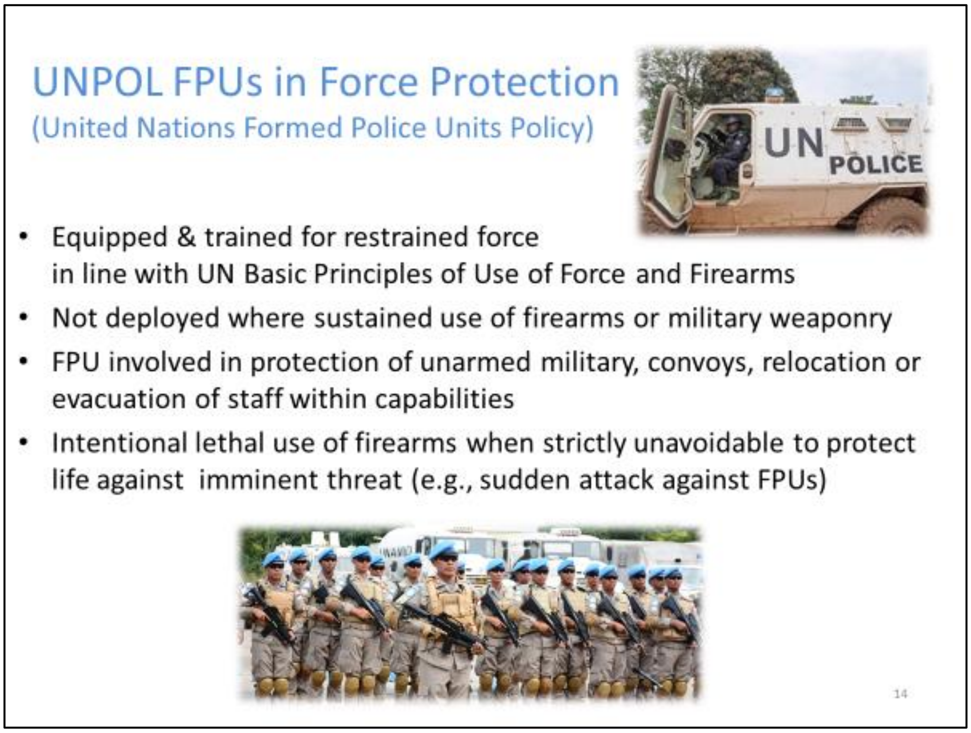
13

Participants should discuss this case in plenary or in small groups. Slides 12 and 14 can be used to facilitate the debriefing on case 2b.

Key points to emphasise for case 2b:

- *To defend themselves and civilians against recurrent IED attacks, the UN mission may take proactive defensive action to neutralise the armed group responsible for the IED attacks and destroy the base where it fabricates the IEDs. As noted above, such proactive defensive force in the face of recurrent attacks is permissible under most mandates.*
- *However, UN rules prohibit the use of the FPU SWAT team for this particular operation. It should be carried out by the UN military instead. The planned, proactive defensive force is directed against a military threat, given that the armed group has shown itself capable of carrying out complex, military-level IED attacks and is also armed with military-grade weapons such as heavy machine guns and RPGs.*
- *As further discussed in slide 14, UN rules do not allow the use of FPUs in planned operations as that would require the "sustained use of firearms or military weaponry."*

Slide 14:



UNPOL FPUs in Force Protection

(United Nations Formed Police Units Policy)

- Equipped & trained for restrained force in line with UN Basic Principles of Use of Force and Firearms
- Not deployed where sustained use of firearms or military weaponry
- FPU involved in protection of unarmed military, convoys, relocation or evacuation of staff within capabilities
- Intentional lethal use of firearms when strictly unavoidable to protect life against imminent threat (e.g., sudden attack against FPUs)

14

Key message: UN Formed Police Units must not be used in operations against military threats. But they may use lethal force to defend themselves against imminent or ongoing attacks threatening their life.

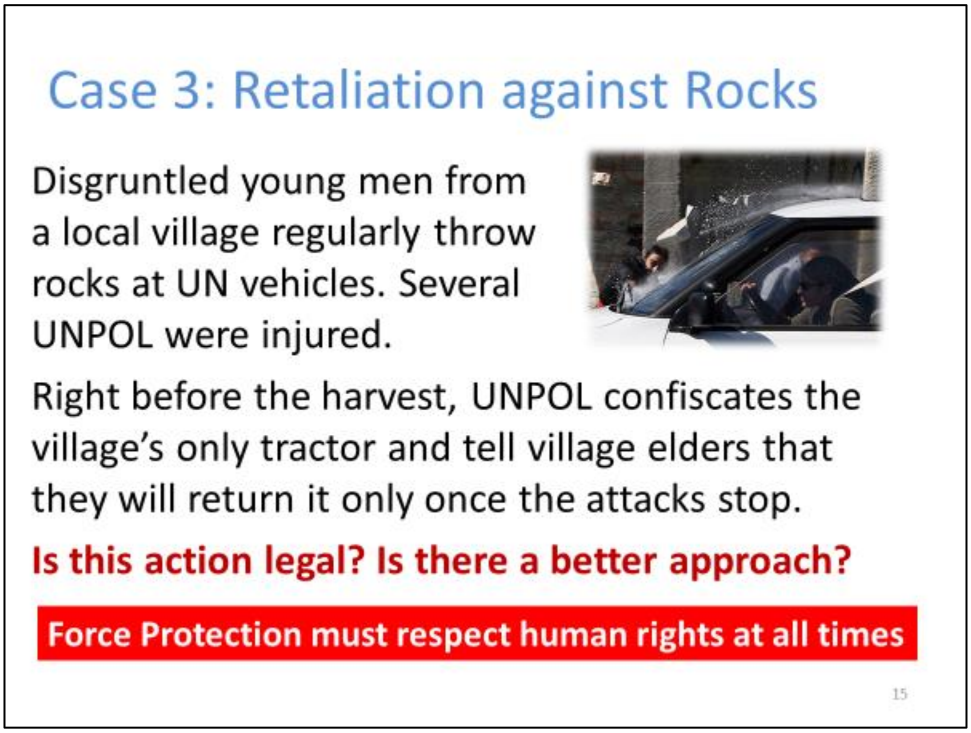
Formed police units may be robustly armed for a police unit, including assault rifles and armoured personnel carriers. However, they do not have the equipment, training, or directives to counter military-level threats.

Instead, they are meant to counter non-military threats. FPU's directives on the use of force will be aligned with the restrained force principles set out by the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

FPU can carry out some armed operations of a defensive nature, where they protect, for instance, unarmed military observers, individual police officers, mission civilians, or UN convoys against non-military threats such as criminal gangs or bandits. However, they may not be assigned to planned protection operations, where they would be likely to encounter militarily organised groups or other threats of a military nature.

The limitations on the involvement of FPUs in planned operations do not preclude FPUs from defending themselves (either alone or alongside the UN military) with lethal force against sudden attacks that carry the risk of death or serious injury – regardless of whether such attacks are of a military or non-military nature. For instance, if an FPU patrol is attacked by an organised armed group, the FPU can respond with the lethal force at their disposal (while calling for backup by the UN military). Similarly, if a UN compound is subject to a military attack, FPU may use their firearms to defend the compound (jointly with their UN military colleagues) in the exercise of the right to self-defence.

Slide 15:



Case 3: Retaliation against Rocks

Disgruntled young men from a local village regularly throw rocks at UN vehicles. Several UNPOL were injured.

Right before the harvest, UNPOL confiscates the village's only tractor and tell village elders that they will return it only once the attacks stop.

Is this action legal? Is there a better approach?

Force Protection must respect human rights at all times

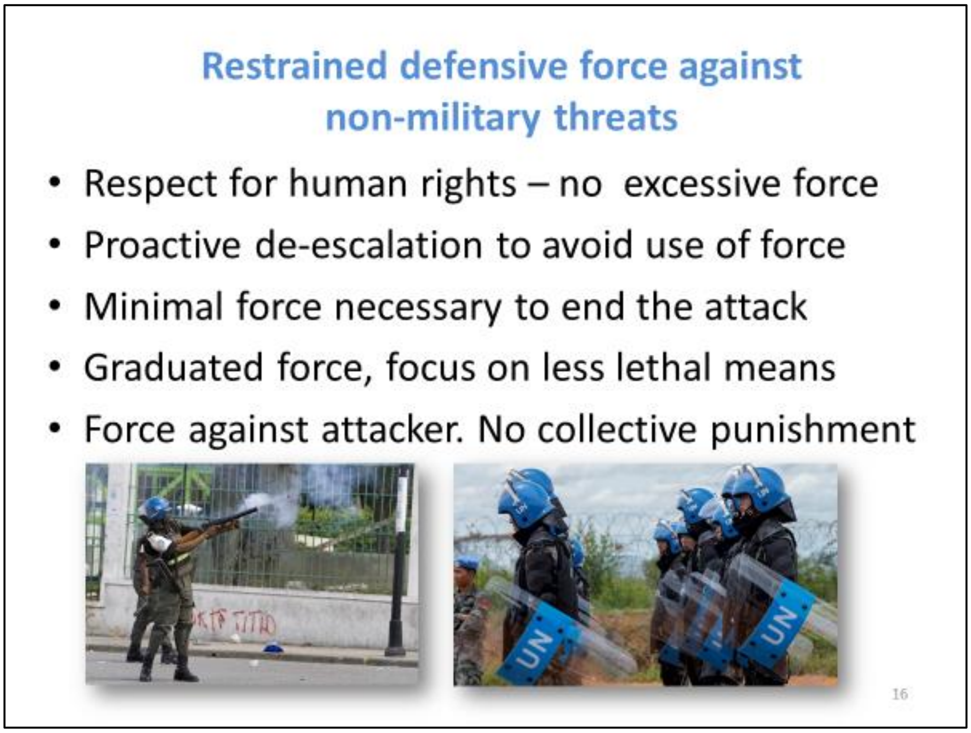
15

Participants should discuss case 3 in plenary or small groups. Slide 16 can be used to facilitate the debriefing on case 2b. Key points to emphasise :

- *UNPOL is subject to unlawful attacks of a non-military nature and may use defensive force in response. For instance, UNPOL could pursue and apprehend the young men throwing rocks, temporarily detain them and then hand them over to the authorities for criminal investigation and prosecution (details of the legal requirements for apprehension, detention, and handover will be discussed later in this module)*
- *However, any force protection measures must be in line with international human rights law. Human rights prohibit collective punishments and reprisals. For this reason, UNPOL is not allowed to take measures that would harm the entire village and its harvest in response to the unlawful attacks of only some of the villagers.*
- *The UN should notify the host state police and demand that they investigate and prosecute the perpetrators in line with the host state's SOFA/SOMA commitments to protect the UN mission.*

- *Appropriate UN interlocutors (e.g., civil affairs or the head of the UN mission in the sector) should also seek a dialogue with the village elders and convince them to use their moral authority to make the young men stop their attacks.*

Slide 16:



Restrained defensive force against non-military threats

- Respect for human rights – no excessive force
- Proactive de-escalation to avoid use of force
- Minimal force necessary to end the attack
- Graduated force, focus on less lethal means
- Force against attacker. No collective punishment

16

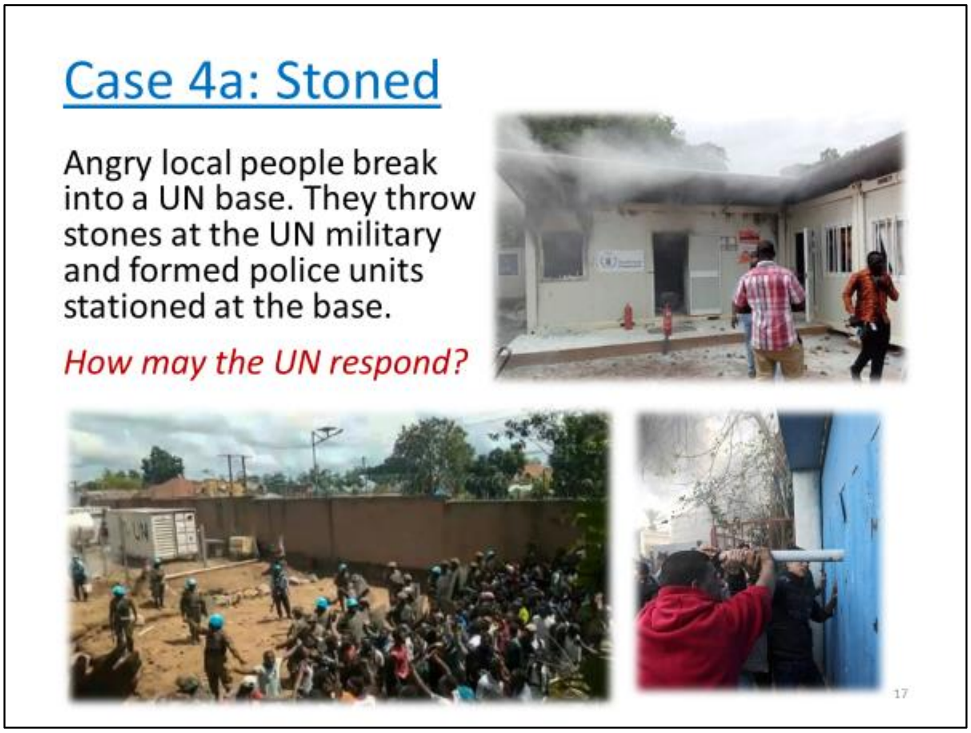
Key message: When responding to threats of a non-military nature, the UN must respect the limits on the use of force established by international human rights law and must not use excessive force.

If possible, non-forcible, de-escalatory measures should be used to end attacks against the United Nations. For instance, if UNPOL is subject to sporadic attacks from within a crowd (e.g., bottles thrown), the UN should consider how the situation can be de-escalated. For instance, a dialogue with the assembly organisers resulted in a direct (peaceful) intervention with the violent elements among the protesters.

Where force becomes necessary, the minimum level of force to defend against a threat effectively and safely may be used. As far as possible, bodily force or less-lethal weapons should be used, with the use of firearms reserved for exceptional types of non-military threats (see below). However, this does not mean that the type of force must be the same as that of the attackers. Self-defence does not require an "equality of arms" as long as the defensive force is not completely disproportional to the threat. For instance, if UNPOL is being attacked by an unarmed crowd throwing fists, they may still be permitted to defend themselves with batons if that is necessary to protect themselves effectively and safely.

As noted above, defensive force must always be directed against the attacker and not collectively against an entire community or group. For instance, if there are attacks from within a crowd, the defensive force should be directed against the attackers rather than against the crowd as a whole (e.g., through targeted apprehensions). However, where necessary to address more generalise violence, less lethal weapons with a broad area effect can be used (e.g., tear gas), even if some non-violent members of a crowd are also unintentionally affected despite all reasonable precautions taken to spare them.

Slide 17:



Case 4a: Stoned

Angry local people break into a UN base. They throw stones at the UN military and formed police units stationed at the base.

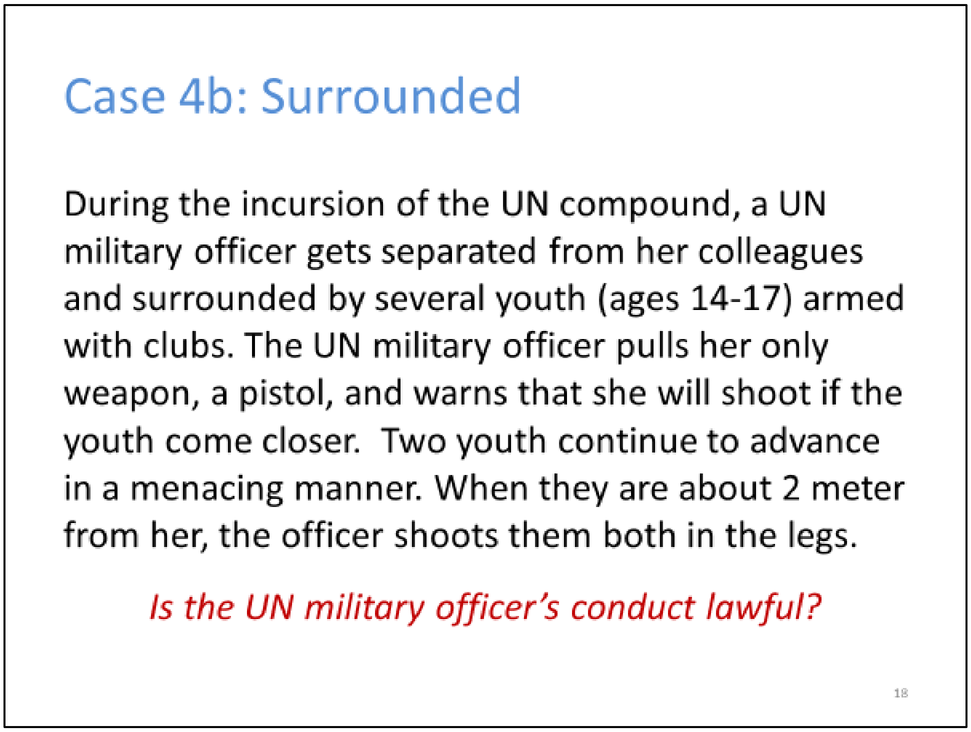
How may the UN respond?

17

Participants should discuss this case in plenary or in small groups. Slide 16 can be used to facilitate the debriefing on case 4a. Key points to emphasise :

- *Formed police units should be leading the defence against this attack of a non-military nature. They should use the less lethal weapons at their disposal to effectively end the throwing of rocks and push the intruders out of the UN compound. The safety of the UN personnel in the confined space must be considered when deciding, for instance, whether a baton charge is appropriate or the use of tear gas.*
- *Exceptionally, if the former police unit on its own cannot effectively and safely defend itself and other UN personnel, the UN military can participate in the defensive effort. But the UN military should use the same type of restrained force – in particular by resorting to less lethal weapons and not their firearms – to respond to the threat.*

Slide 18:



Case 4b: Surrounded

During the incursion of the UN compound, a UN military officer gets separated from her colleagues and surrounded by several youth (ages 14-17) armed with clubs. The UN military officer pulls her only weapon, a pistol, and warns that she will shoot if the youth come closer. Two youth continue to advance in a menacing manner. When they are about 2 meter from her, the officer shoots them both in the legs.

Is the UN military officer's conduct lawful?

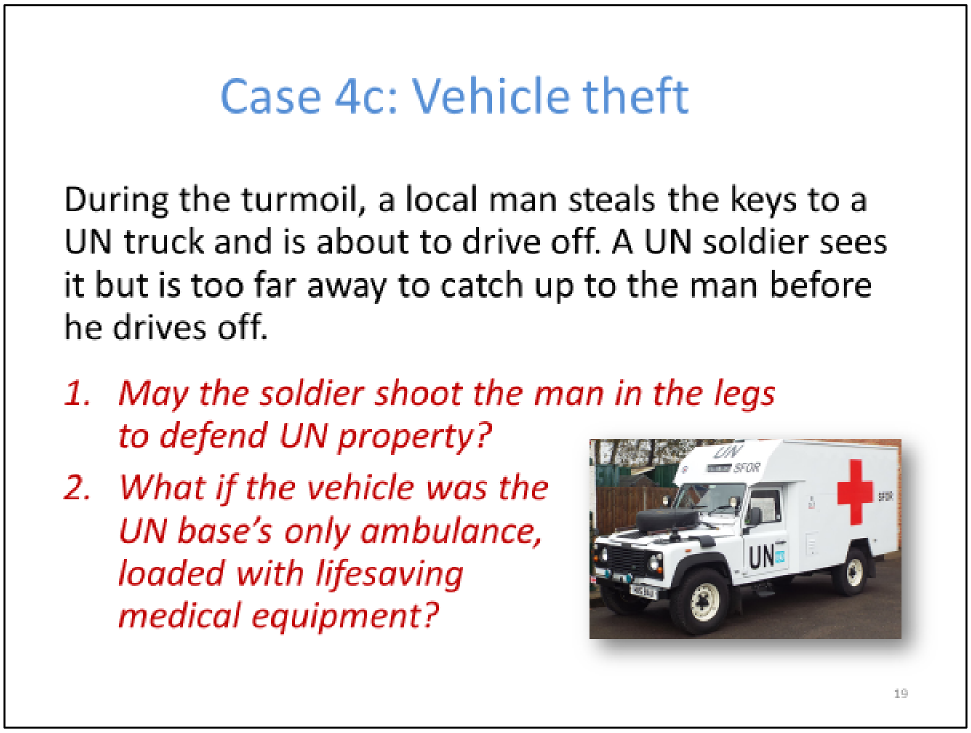
18

Participants should discuss this case in plenary – or, if time permits, in small groups. Slide 16 can be used to facilitate the debriefing on cases 4b and 4c.

Key points to emphasise for case 4b:

- *Even in response to attacks of a non-military nature, like this attack by youth armed with clubs, the exceptional use of firearms is permissible in self-defence against an imminent threat of death or serious injury.*
- *The UN military officer is facing a threat of serious injury or worse. Despite her verbal warning, the youth advanced almost into striking range so that shooting them in the legs to incapacitate them and stop their advance was necessary and proportional to defend herself effectively and safely against their attack.*

Slide 19



Case 4c: Vehicle theft

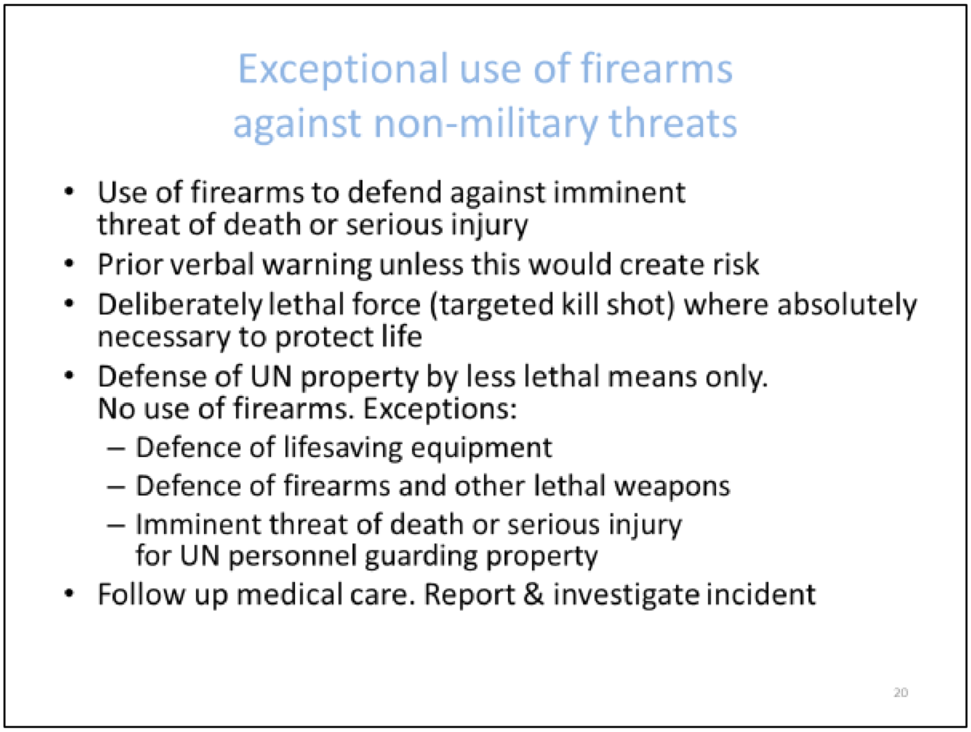
During the turmoil, a local man steals the keys to a UN truck and is about to drive off. A UN soldier sees it but is too far away to catch up to the man before he drives off.

1. *May the soldier shoot the man in the legs to defend UN property?*
2. *What if the vehicle was the UN base's only ambulance, loaded with lifesaving medical equipment?*

Discuss the case in plenary or in groups, using slide 20 for the debriefing. Key points to emphasise for case 4c:

- *Firearms may not be used solely for the purpose of protecting UN property, even if the unlawful attack is directed against a valuable piece of UN property, like a truck.*
- *During the incursion, UN uniformed personnel could have been ordered to guard vehicles and other valuable equipment. If such UN personnel had then been attacked to get to the vehicles, they could have used all necessary force to protect their own life and health, including firearms where necessary, to defend themselves against a threat of death or serious injury.*
- *Another exception from the prohibition of using firearms solely to protect property applies to lifesaving property because losing such property creates a threat to life. If the vehicle was an ambulance loaded with medical equipment, the UN soldier could shoot the man to incapacitate him and thereby prevent the theft of the ambulance.*

Slide 20:



Exceptional use of firearms against non-military threats

- Use of firearms to defend against imminent threat of death or serious injury
- Prior verbal warning unless this would create risk
- Deliberately lethal force (targeted kill shot) where absolutely necessary to protect life
- Defense of UN property by less lethal means only. No use of firearms. Exceptions:
  – Defence of lifesaving equipment
  – Defence of firearms and other lethal weapons
  – Imminent threat of death or serious injury for UN personnel guarding property
- Follow up medical care. Report & investigate incident

20

Key message: In self-defence against a non-military threat, firearms may only be used where necessary to defend against an imminent threat of death or serious injury.

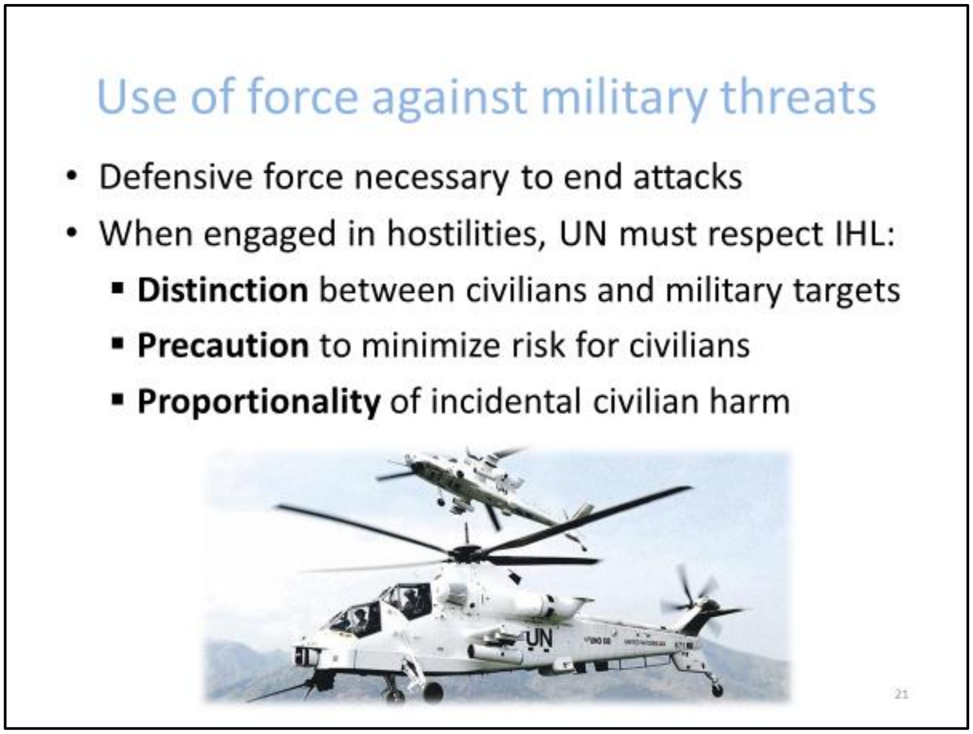
Prior to any use of firearms, UN uniformed personnel must give a verbal warning (not a warning shot!). No prior warning is necessary if the threat is so imminent that losing time by issuing a warning first would place the person under attack at serious risk (for instance, during a sudden attack where there are only split seconds to react in self-defence).

In principle, firearms should be aimed to incapacitate the attacker by targeting the legs or abdomen. However, deliberately lethal force (e.g., a targeted headshot) is permissible where absolutely necessary to protect life against an imminent threat. Examples: An UNPOL sniper shoots and kills a hostage taker who is threatening to imminently kill hostages. A suicide bomber is about to detonate her bomb unless instantly neutralised with a headshot.

UN property must be defended by less lethal means such as tear gas. As noted above (case 4c), an exception applies where the use of firearms is the only means to defend lifesaving property. Another exception applies where firearms or other lethal weapons are about to be stolen (because then the armed attacker poses a serious risk to life).

UN personnel guarding UN property maintain their own right to self-defence. If they are attacked in a manner that places their life or health at serious risk, they may use firearms to the extent necessary for their self-defence.

Slide 21:



Use of force against military threats

- Defensive force necessary to end attacks
- When engaged in hostilities, UN must respect IHL:
  - **Distinction** between civilians and military targets
  - **Precaution** to minimize risk for civilians
  - **Proportionality** of incidental civilian harm

Key message: Defensive force against military threats may be more intensive and use the full range of means at the disposal of the UN military. However, it is still subject to the general limits imposed by international humanitarian and human rights limits for military hostilities.

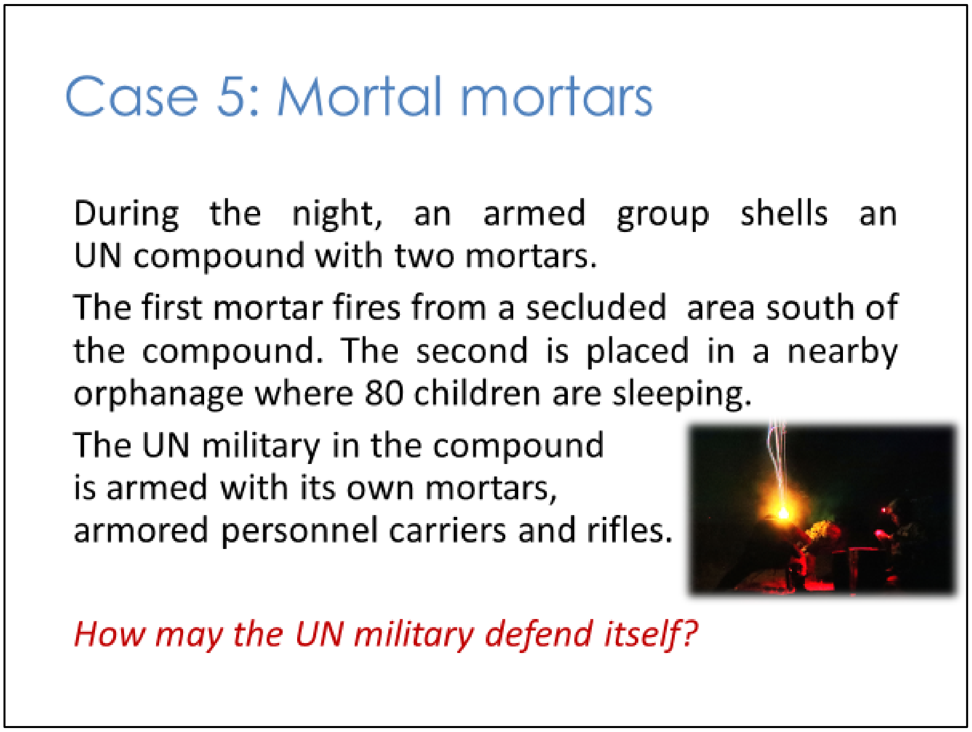
In principle, United Nations peacekeepers aim to use as little force as possible so as not to become a party to the conflict, not escalate the situation or create unnecessary threats to the civilian population. However, the UN military may escalate its use of force to the full range of its military capabilities to the extent necessary to defend UN personnel or installations against military attacks (and also to protect civilians). Example: The UN military fires rockets from an attack helicopter (see photo) at an armed group advancing against a UN compound because this level of force is necessary to effectively stop this military attack.

The use of military force must be in line with international humanitarian and human rights law standards applicable to military hostilities, including the basic IHL principles of:

- **Distinction** between civilians and combatants and between civilian objects and military targets. Operations must only be directed against military objects. Indiscriminate attacks that do not distinguish between civilians and combatants are prohibited.

- **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 minimise, incidental loss of civilian life, injury to civilians and damage to civilian objects
- **Proportionality**: Loss of life and damage to property incidental to attacks must not be excessive in relation to 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 in relation to the military advantage gained. Proportionality, in the sense used by IHL, is not an issue if the target is purely military and no civilians or civilian objects are nearby.

Slide 22:



Case 5: Mortal mortars

During the night, an armed group shells an UN compound with two mortars.

The first mortar fires from a secluded area south of the compound. The second is placed in a nearby orphanage where 80 children are sleeping.

The UN military in the compound is armed with its own mortars, armored personnel carriers and rifles.

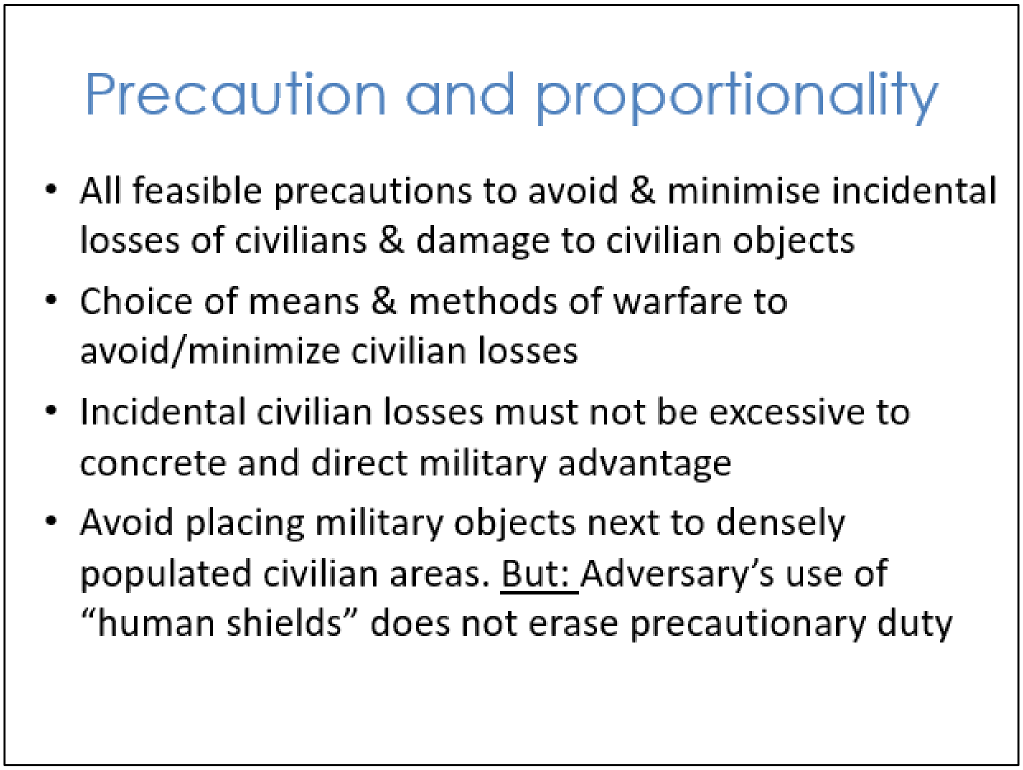
How may the UN military defend itself?

A plenary or group discussion should bring out the following key points related to precaution and proportionality (Slide 23 can be used for the debriefing):

- *The UN can defend itself against the attack from the secluded area south of the compound by firing back with its own mortars*
- *The second mortar has been placed by the armed group in a densely populated civilian area (the orphanage), in clear violation of international humanitarian law.*
- *Notwithstanding the armed group's illegal conduct, the United Nations must still take precautions to minimise incidental civilian losses in its response and not cause disproportional civilian harm. In particular, shelling the armed group position may lead to disproportional civilian losses among the children. Depending on the exact circumstances of the situation, a more appropriate defensive action might be to lead an infantry assault to destroy the second mortar.*

- *The case indicates a potential serious planning error on the part of the United Nations because its compound is near a densely populated area. United Nations peacekeeping bases should always be constructed away from civilian objects, and guarantees should be sought from the host state that no such civilian objects are later built next to UN peacekeeping bases.*

Slide 23:



Precaution and proportionality

- All feasible precautions to avoid & minimise incidental losses of civilians & damage to civilian objects
- Choice of means & methods of warfare to avoid/minimize civilian losses
- Incidental civilian losses must not be excessive to concrete and direct military advantage
- Avoid placing military objects next to densely populated civilian areas. But: Adversary's use of "human shields" does not erase precautionary duty

Key message: The Secretary-General's Bulletin on the Observance by United Nations Forces of International Humanitarian Law (1999) commits the United Nations to respect the requirements of precaution and proportionality.

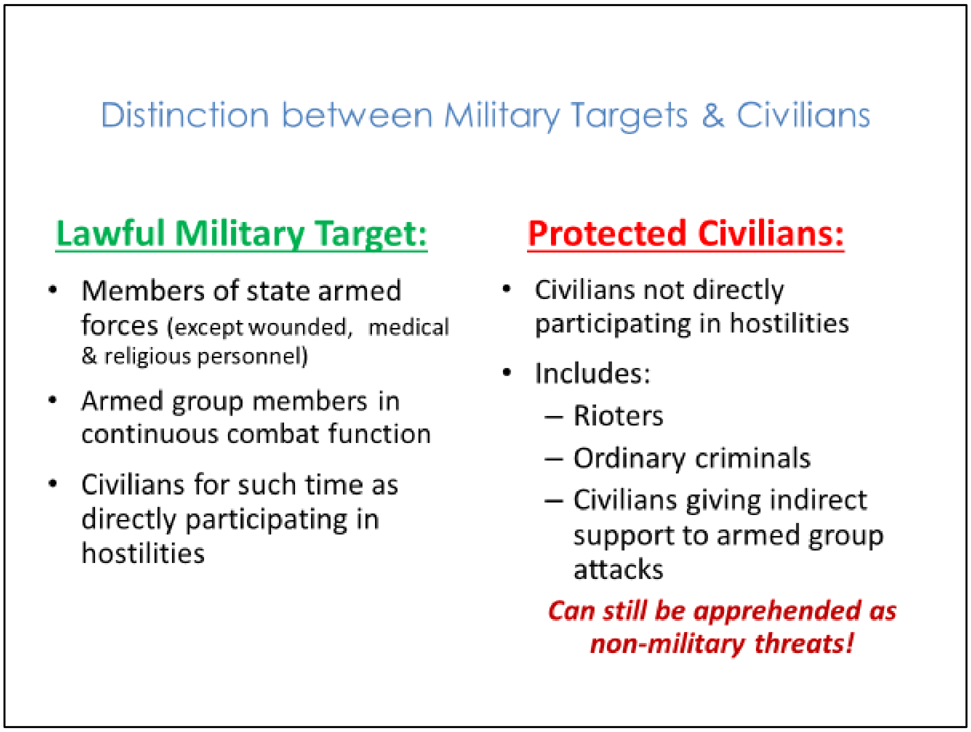
The Bulletin stipulates that:

The United Nations force shall take all feasible precautions to avoid, and in any event to minimise, incidental loss of civilian life, injury to civilians or damage to civilian peoples.

In its area of operation, the United Nations force shall avoid, to the extent feasible, locating military objectives within or near densely populated areas and take all necessary precautions to protect the civilian population, individual civilians and civilian objects against the dangers resulting from military operations.

The United Nations force is prohibited from launching operations that may be expected to cause incidental loss of life among the civilian population or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated.

Slide 24:



Distinction between Military Targets & Civilians

Lawful Military Target:

- Members of state armed forces (except wounded, medical & religious personnel)
- Armed group members in continuous combat function
- Civilians for such time as directly participating in hostilities

Protected Civilians:

- Civilians not directly participating in hostilities
- Includes:
  - Rioters
  - Ordinary criminals
  - Civilians giving indirect support to armed group attacks

Can still be apprehended as non-military threats!

Key message: According to the Secretary-General's Bulletin on the Observance of IHL, the United Nations force shall make a clear distinction at all times between civilians and combatants and between civilian objects and military objectives. Military operations shall be directed only against combatants and military objectives. Attacks on civilians or civilian objects are prohibited. However, non-military threats can still be subject to defensive force, in particular their apprehension (capture).

In the exercise of its right to self-defence, the United Nations military may lawfully use military force against attacks by:

- members of state armed forces
- armed group members in a continuous combat function (individuals whose continuous function it is to take a direct part in hostilities)
- civilians for such time as they take a direct part in hostilities.

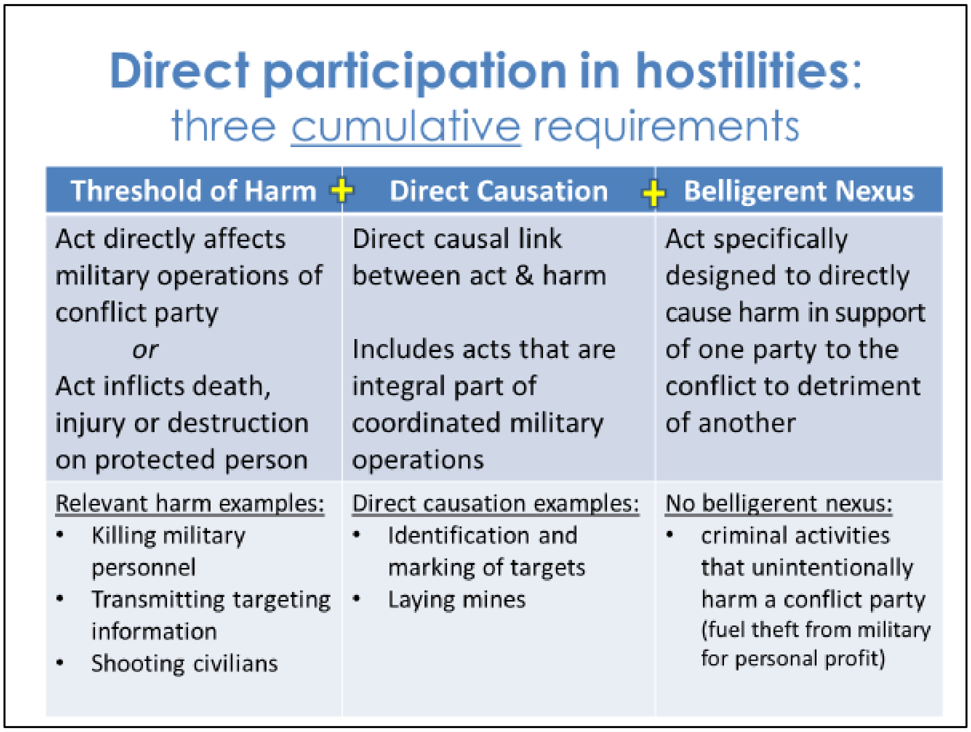
Civilians not directly participating in hostilities are protected persons under IHL and not lawful military targets. Among such protected civilians may still be individuals who engage in violence or criminal conduct against the United Nations, including:

- Civilian rioters
- Bandits and other ordinary criminal

- Civilians giving indirect support to armed group attacks (discussed in greater detail below)

United Nations personnel may still defend themselves against such persons, but only within the limits of self-defence against non-military threats discussed above (slides 16-20). In particular, the mission can apprehend and temporarily detain such individuals with a view to handing them over to the host state authorities for prosecution.

Slide 25:



Direct participation in hostilities:
three cumulative requirements

Threshold of Harm +	Direct Causation +	Belligerent Nexus
Act directly affects military operations of conflict party *or* Act inflicts death, injury or destruction on protected person	Direct causal link between act & harm Includes acts that are integral part of coordinated military operations	Act specifically designed to directly cause harm in support of one party to the conflict to detriment of another
Relevant harm examples: • Killing military personnel • Transmitting targeting information • Shooting civilians	Direct causation examples: • Identification and marking of targets • Laying mines	No belligerent nexus: • criminal activities that unintentionally harm a conflict party (fuel theft from military for personal profit)

Key message: Whether a civilian is directly participating in hostilities is determined by whether the civilian's acts fulfil three cumulative requirements: (i) threshold of harm, (ii) direct causation, (iii) belligerent nexus.

The International Committee of the Red Cross (ICRC) has developed authoritative guidance setting out three cumulative requirements to determine whether a civilian is directly participating in conflict (whether as a continuous combat function or only for a particular time in a specific operation):

Threshold of harm: The act in question must either directly or adversely affect the military operations of one of the conflict parties (examples: killing soldiers or transmitting information to target them). Or it must inflict death, injury, or destruction on a protected person (shooting civilians, destroying civilian property).

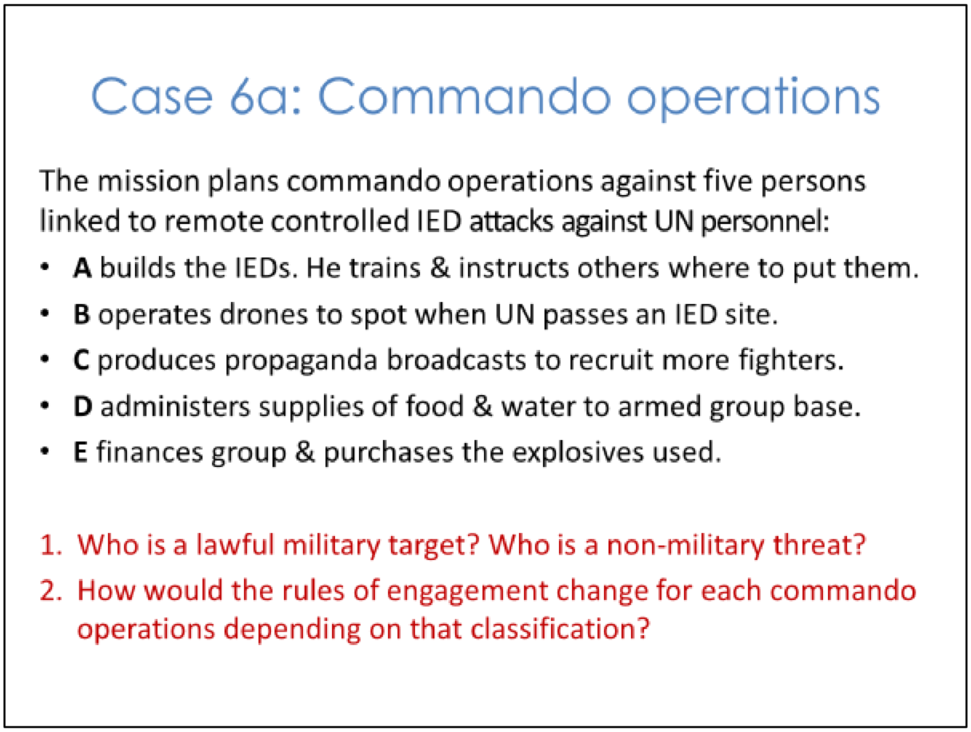
Direct causation: There must be a direct causal link between the act and the harm likely to result (the harm must be brought about in one causal step), for instance, laying a mine, on which a soldier then steps. An act which is an integral part of a coordinated military operation leading to harm will suffice, for instance, identifying and marking a target that is then attacked.

It is critical to distinguish between mere war-sustaining activities (indirect participation) and acts that cross the line into the conduct of hostilities. War-sustaining activities falling short of conduct of hostilities include the production/shipping of military equipment or political, economic or media activities supporting the general war effort, which does not directly bring about the materialisation of harm.

Belligerent nexus: The act must be specifically designed to directly cause the required harm in support of one party to the conflict to the detriment of another. Activities that do not form part of the conduct of hostilities, including violent criminal activities, do not have the required nexus, even if they unintentionally impede military activity. Example: armed bandits rob a convoy delivering fuel and food to one of the conflict parties with the intent to sell their loot on the black market (so not specifically to harm a conflict party).

Individual self-defence or defence of others against IHL violations also lacks a belligerent nexus. Example: Villagers shoot and kill soldiers who are trying to loot their property. By the mere act of defending themselves, they do not become lawful military targets.

Slide 26:



Case 6a: Commando operations

The mission plans commando operations against five persons linked to remote controlled IED attacks against UN personnel:

- **A** builds the IEDs. He trains & instructs others where to put them.
- **B** operates drones to spot when UN passes an IED site.
- **C** produces propaganda broadcasts to recruit more fighters.
- **D** administers supplies of food & water to armed group base.
- **E** finances group & purchases the explosives used.

1. Who is a lawful military target? Who is a non-military threat?
2. How would the rules of engagement change for each commando operations depending on that classification?

Discuss the case in plenary or through group discussions. A debriefing can be based on slides 25 and 27 and should bring out the following key points:

- *Not everyone who somehow contributes to the IED attacks against the UN and civilians is a military target. Instead, it needs to be carefully assessed whether any of the five persons directly participate in hostilities based on the three cumulative requirements set out in slide 25. The permissible rules of engagement will change depending on who is a lawful military target and who is not*

<u>Lethal force against a lawful military target</u>

- *Normally, persons involved in the production of weapons (e.g., workers in a munitions factory) are not direct participants in conflict. However, in this case, A, the IED builder, forms an integral part of an integrated military-level operation since he not only builds the bombs but also instructs others on how to carry out concrete operations. A is, therefore, a lawful military target.*
- *The drone spotter B is also a lawful military target. Persons can be direct participants in hostilities without using force themselves. The identification and marking of targets, in particular, is a form of direct participation.*

- *Commando operations targeting A and B can foresee their immediate engagement with lethal force. Only if A or B clearly indicates their will to surrender or can be safely captured (e.g., if the commando operation finds them unarmed and easy to capture) must they be apprehended. Once apprehended, they must be treated humanely, detained only temporarily and then handed over to the host state authorities for prosecution.*

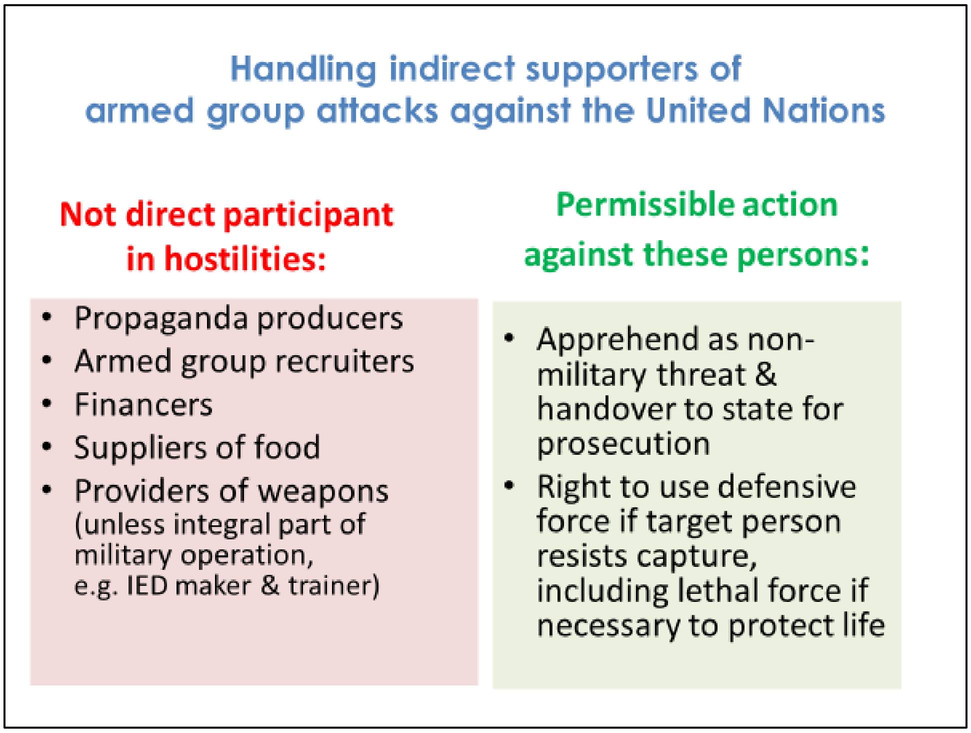
Focus on apprehension (capture) of non-military threats:

- *C poses a threat to civilians and to the mission because C's work leads to the recruitment of more fighters. Such conduct would normally also be criminal under host state laws. However, the production of propaganda and recruitment materials is not a form of direct participation, so C must not be engaged in a manner as if C was a military target.*
- *D is not a military target either, even if D's supplies to the armed group are essential to operate their base. Depending on the circumstances, such conduct may be criminal under host state law.*
- *Financing an armed group (case E) or purchasing weapons for the group is typically also criminal behaviour, but not direct participation in hostilities.*
- *The mission may treat all three persons as non-military threats. Under its self-defence and protection of civilians mandates, it may launch commando operations aimed at capturing (apprehending) them with a view to temporarily detaining them and then handing them over to the host state for prosecution. If any of them resist in a way that places UN personnel or civilians at risk of death or serious injury (e.g., by shooting at the UN commando), the UN personnel may exercise defensive lethal force and fire back.*

In a nutshell, the permissible rules of engagement for the five commando operations are:

- *Military target (cases A and B): Lethal force is immediately permissible unless surrender or safe capture*
- *Non-military threat (cases C, D and E): Focus on capture, lethal force where necessary in self-defence*

Slide 27:

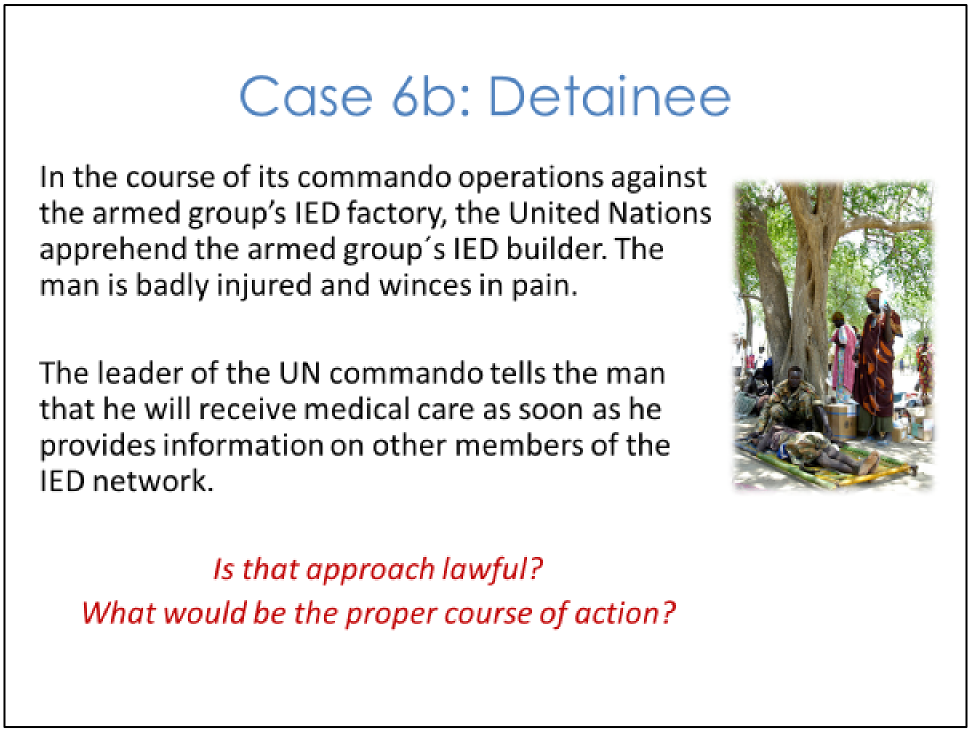


Handling indirect supporters of
armed group attacks against the United Nations

Not direct participant in hostilities:	Permissible action against these persons:
• Propaganda producers • Armed group recruiters • Financers • Suppliers of food • Providers of weapons (unless integral part of military operation, e.g. IED maker & trainer)	• Apprehend as non-military threat & handover to state for prosecution • Right to use defensive force if target person resists capture, including lethal force if necessary to protect life

Persons who support armed group attacks only indirectly are not lawful military targets. But they may still be captured with a view to having them prosecuted by host-state authorities. Self-defence may be exercised if they resist capture.

Slide 28:



Case 6b: Detainee

In the course of its commando operations against the armed group's IED factory, the United Nations apprehend the armed group´s IED builder. The man is badly injured and winces in pain.

The leader of the UN commando tells the man that he will receive medical care as soon as he provides information on other members of the IED network.

Is that approach lawful?

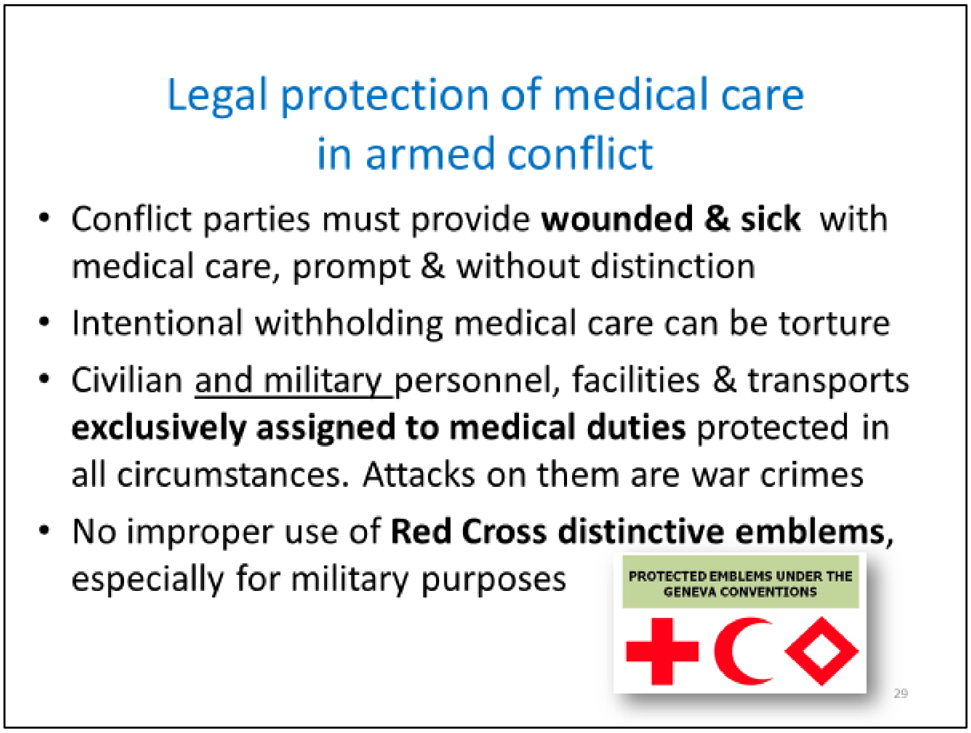
What would be the proper course of action?

Discuss case 6b in plenary or through group discussions. A debriefing can be based on slide 29 and should bring out the following key points:

- *One of the fundamental principles of IHL is to promptly and without distinction provide the wounded and sick with medical care. By withholding medical care, the UN commando leader fails to respect IHL.*
- *The omission prolongs the detainee's severe suffering in an attempt to extract information. Taking place in a situation of military hostilities involving the UN, this amounts to the war crime of torture, which is defined in international criminal law as "the intentional infliction of severe pain or suffering, whether physical or mental, upon a person in custody or under the control of the accused." The UN leader would have to be prosecuted for that war crime*
- *The proper course of action would require following the United Nations Standard Operating Procedures on Handling of Detention in Peace Operations. After safely establishing control over the IED builder and having him searched, the man should be administered first aid and then brought to a UN medical facility for further treatment (see the following slides for a discussion of the procedure)*

- *After receiving the necessary medical treatment and before being handed over to state authorities, the IED Builder can still be questioned but must not be forced to respond to questions.*

Slide 29:



Legal protection of medical care in armed conflict

- Conflict parties must provide **wounded & sick** with medical care, prompt & without distinction
- Intentional withholding medical care can be torture
- Civilian and military personnel, facilities & transports **exclusively assigned to medical duties** protected in all circumstances. Attacks on them are war crimes
- No improper use of **Red Cross distinctive emblems,** especially for military purposes

PROTECTED EMBLEMS UNDER THE GENEVA CONVENTIONS

29

Key message: Medical care in armed conflict enjoys special protection that the United Nations must also respect.

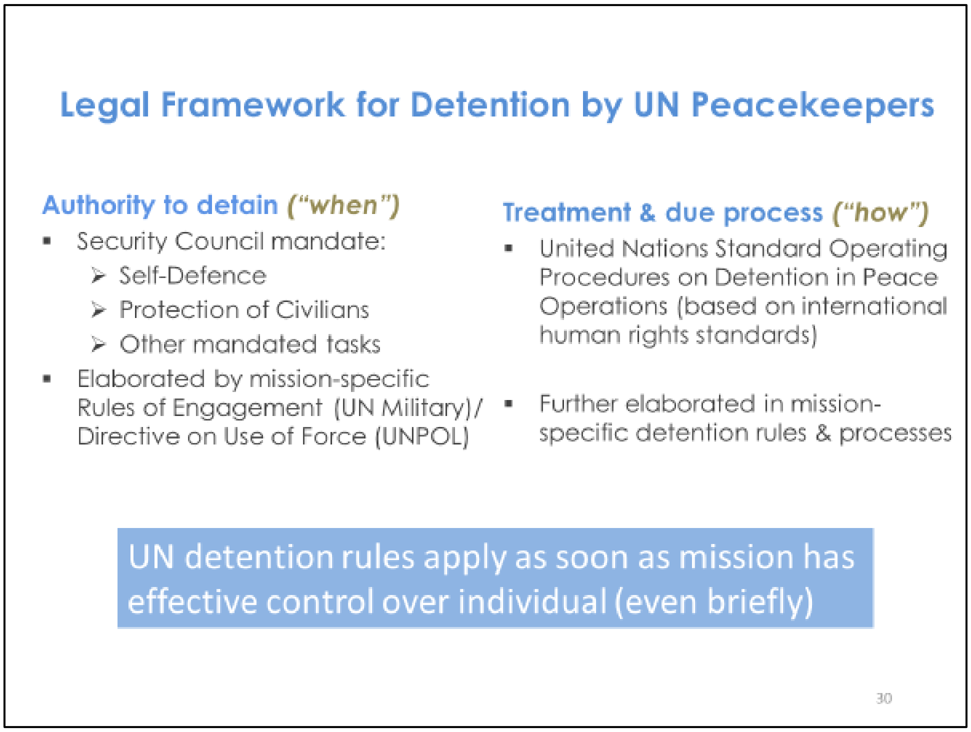
The Secretary-General's Bulletin on IHL stipulates:
"Members of the armed forces and other persons in the power of the United Nations force who are wounded or sick shall be respected and protected in all circumstances. They shall be treated humanely and receive the medical care and attention required by their condition without adverse distinction. Only urgent medical reasons will authorise priority in the order of treatment to be administered."

As noted above, intentionally withholding medical care to inflict severe suffering can amount to the war crime of torture.

Civilian and military personnel, facilities, and transports exclusively assigned to medical duties are protected in all circumstances. Attacks on them are war crimes. Conflict parties can still detain injured soldiers of the adversary that fall into their hands (e.g., when they capture an area containing a military hospital), but they then assume a responsibility to provide those soldiers with continued medical care.

It is prohibited to improperly use the Red Cross' distinctive emblems, especially for military purposes. The photo shows the different emblems that may be used depending on the cultural and religious context where the conflict takes place.

Slide 30:



Legal Framework for Detention by UN Peacekeepers

Authority to detain ***("when")***

- Security Council mandate:
  - Self-Defence
  - Protection of Civilians
  - Other mandated tasks
- Elaborated by mission-specific Rules of Engagement (UN Military)/ Directive on Use of Force (UNPOL)

Treatment & due process ***("how")***

- United Nations Standard Operating Procedures on Detention in Peace Operations (based on international human rights standards)
- Further elaborated in mission-specific detention rules & processes

UN detention rules apply as soon as mission has effective control over individual (even briefly)

30

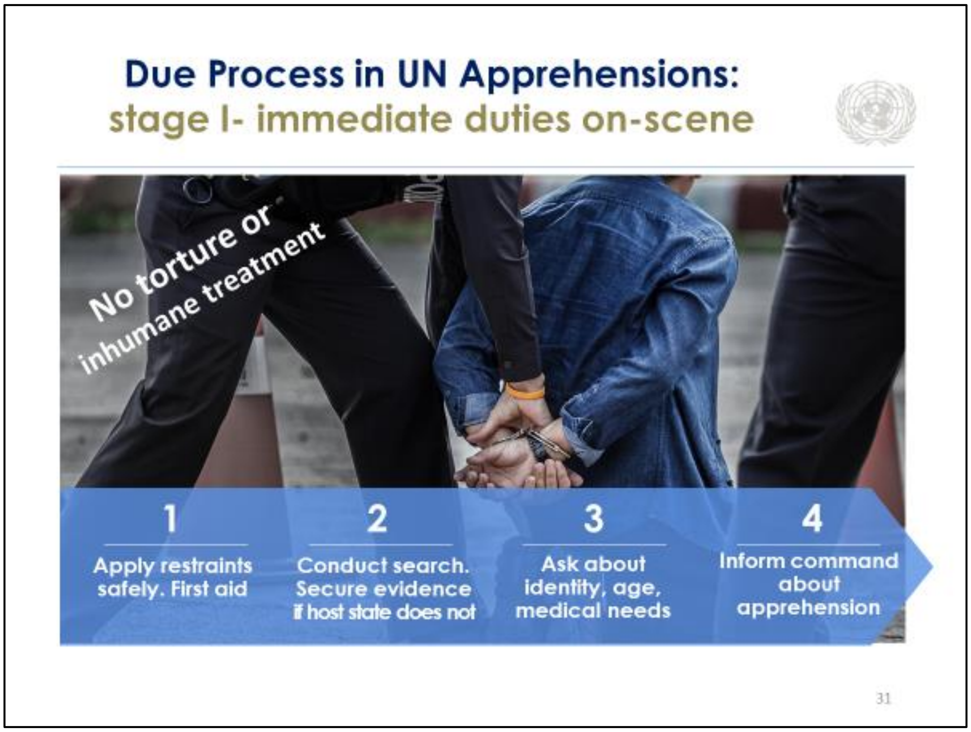
Key Message: Under its self-defence and PoC mandates, UN peacekeepers may apprehend and detain persons under its self-defence. As soon as they establish effective control, detainees must be treated in line with international standards of humane treatment and due process.

UN peacekeepers' apprehension power flows from its mandates on self-defence, defence of the mission, protection of civilians and other mandated tasks (e.g., support to host authorities to establish rule of law). Rules of Engagement (for the UN military) and Directive on the Use of Force (for UNPOL) elaborate the details.

Once they establish effective control over an individual, the mission's detention procedures must be followed. These will be based on the United Nations Standard Operation Procedures on Detention in Peace Operations, which are, in turn, based on international human rights standards.

These UN detention rules apply once the UN has the target persons under its effective control, even for very short periods. In particular, UN detention rules apply even if some host state military or police officers may accompany UNPOL during operations as long as UN personnel effectively control the apprehension operation. Compliance with the UN detention rules cannot be evaded by introducing evasive concepts like "temporary holding" or the like.

Slide 31:



Due Process in UN Apprehensions:
stage I- immediate duties on-scene

No torture or inhumane treatment

1 Apply restraints safely. First aid

2 Conduct search. Secure evidence if host state does not

3 Ask about identity, age, medical needs

4 Inform command about apprehension

31

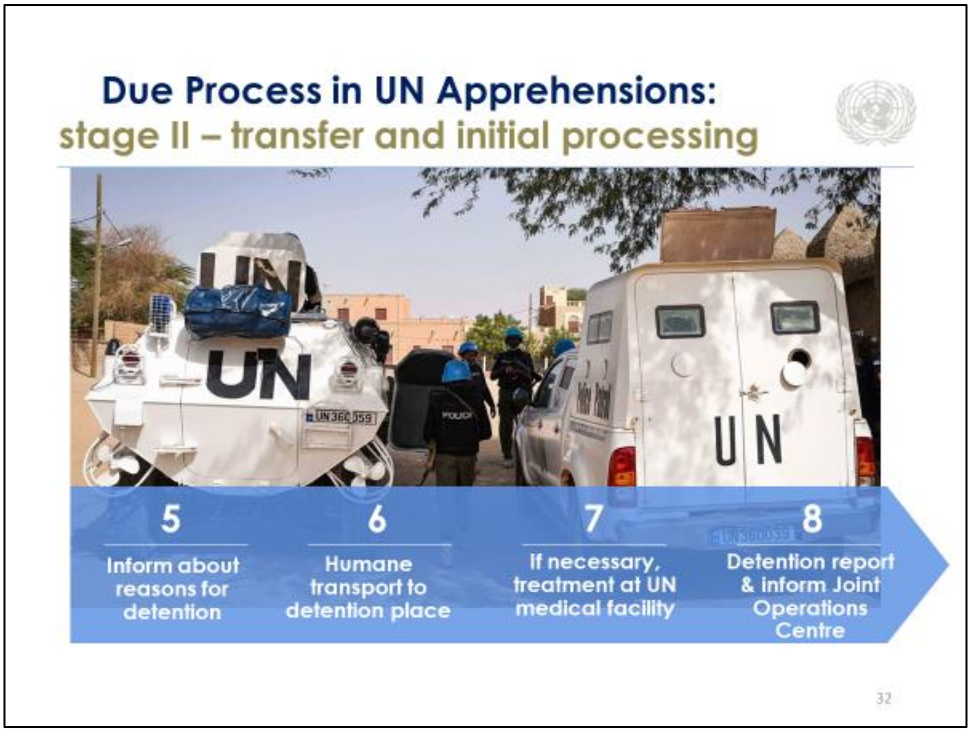
Key Message: UN personnel must secure the situation and cover urgent medical needs as a matter of initial priority.

When apprehending an individual, UN personnel must

- If necessary, apply handcuffs to prevent the detained person from escaping or from harming him/herself or others in a manner that ensures due consideration to the safety of both the detaining unit and the detainee
- Conduct an initial search of the detained person (unless the apprehended individual is presumed to be a child) and seize weapons and other items which may be used to cause harm to persons (including the detained person him/herself) or damage to property, as well as mobile phones
- Provide first aid as needed or call for an ambulance if necessary
- If the host state is unable or unwilling to secure physical evidence, conduct a site survey at the place of apprehension in order to collect any relevant items that might be useful as evidence in any future criminal proceedings

- Ask the detained person for his/her identity, age and whether he/she needs any medical treatment, including for any injuries that he/she may have suffered in the course of his/her detention
- Immediately inform the Unit Commander of the apprehension, including whether the apprehended person is presumed to be a child (because then special rules apply)

Slide 32:



Due Process in UN Apprehensions: stage II – transfer and initial processing

5 Inform about reasons for detention

6 Humane transport to detention place

7 If necessary, treatment at UN medical facility

8 Detention report & inform Joint Operations Centre

32

Key message: Apprehended persons must be informed about the reasons for their detention, receive necessary medical care and be transported in a humane manner to the place of detention.

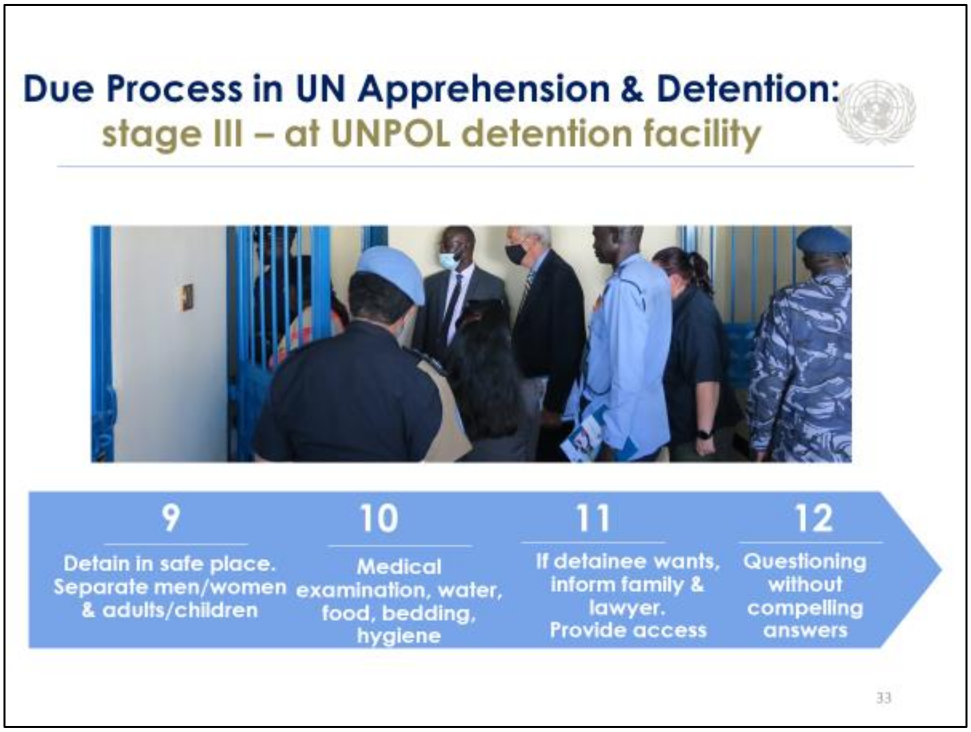
Unless their commander decides that the apprehended individual should be immediately released, the apprehending unit must:

- Inform the detained person of the reasons for the detention and upcoming transfer to a United Nations place of detention;
- Organise the transport of the detained person as quickly as possible to a designated place of detention. The transportation shall always be carried out humanely and in a manner that ensures due consideration for the safety of both United Nations personnel and the detainee (appropriate UN vehicles can and should be used);
- Organise the transport of any items seized from the detained person and any evidence collected at the scene to the same designated place of detention;

- If the detained person is seriously injured or sick and needs medical treatment that cannot be provided at the designated place of detention, immediately organise his/her transport to a designated United Nations medical facility.

- The command must immediately notify the Joint Operations Centre or other designated office about the apprehension and whether to continue to detain the persons concerned.

Slide 33:



Due Process in UN Apprehension & Detention:
stage III – at UNPOL detention facility

9
Detain in safe place. Separate men/women & adults/children

10
Medical examination, water, food, bedding, hygiene

11
If detainee wants, inform family & lawyer. Provide access

12
Questioning without compelling answers

33

Key message: At the UN detention facility, the responsible commander must ensure due process and humane treatment of detainees.

UN personnel at the UN detention facility must:

- Ensure that a medical examination is conducted as soon as possible by qualified United Nations medical personnel. A detained person who is seriously ill or seriously injured and/or who needs medical treatment that cannot be provided at the designated place of detention must be transferred to a designated United Nations medical facility as soon as possible.

- Register the detained person by completing the relevant forms and transmit the information to the mission’s Detention Focal Point through the Joint Operations Centre for recording purposes.

- Take possession of items seized from the detained person and those items collected at the scene at the time of his/her apprehension, and ensure that they are tagged for identification and recording purposes, registered using the relevant forms, and safely stored.

- Supervise a further search of the detained person. Seize any additional items found on the detained person in the course of the search, ensure that they are tagged for identification and recording purposes and register and store them.

- Authorise the destruction of dangerous items to avoid the risk of harm to persons or damage to property.

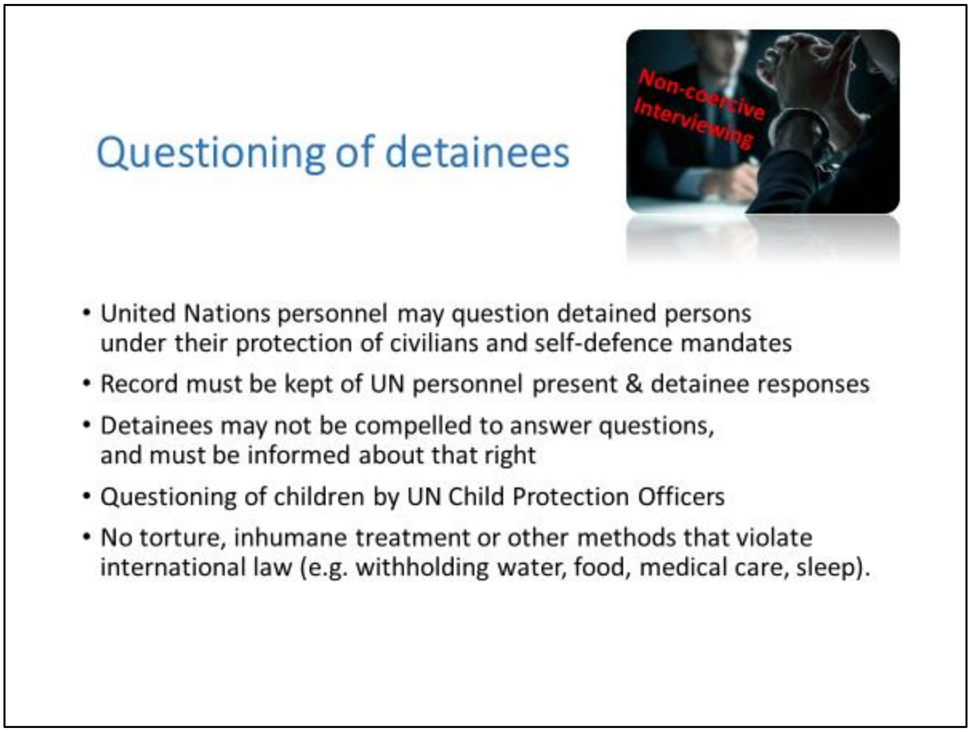
- Ensure that detainees are kept safely and treated humanely and receive water, food, bedding, and hygiene items as elaborated by the SOPs on Detention.

- Different categories of detainees must be kept apart for their own protection, especially to prevent sexual violence among detainees. Neither women and men nor adults and children may be detained together. Dangerous and ordinary detainees must be kept apart.

- Ask the detained person if he/she wishes a family member, a lawyer or another person designated by him/her to be informed of his/her detention.

- Without prejudice to the host State's responsibility to conduct criminal investigations, conduct preliminary questioning of the detainee (while informing him/her of his right, does not respond to questions that may incriminate him herself).

Slide 34:


Non-coercive
Interviewing

Questioning of detainees

- United Nations personnel may question detained persons under their protection of civilians and self-defence mandates
- Record must be kept of UN personnel present & detainee responses
- Detainees may not be compelled to answer questions, and must be informed about that right
- Questioning of children by UN Child Protection Officers
- No torture, inhumane treatment or other methods that violate international law (e.g. withholding water, food, medical care, sleep).

Key message: The UN may question detainees to obtain information for purposes of force protection or protection of civilians but using non-coercive methods only.

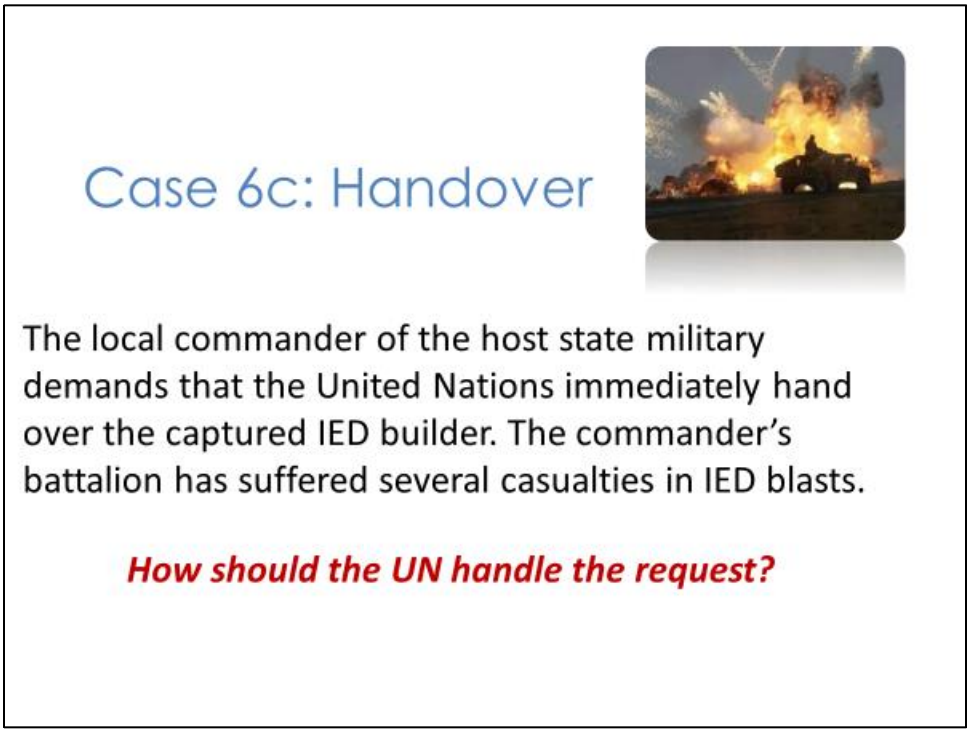
While this is not explicitly mentioned in the DPO Detention SOPs, the UN may question detained persons in pursuance of their protection of civilian and self-defence mandates. A record of all questioning conducted must be kept, including who was present and what responses were provided.

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

As a matter of policy, the United Nations uses and promotes techniques of non-coercive interviewing, which have been successfully used in law enforcement and peacekeeping-intelligence work of many advanced national law enforcement agencies. The details are summarised in the UNPOL/OHCHR/UNODC on Non-coercive Interviewing.

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

Slide 35:



Case 6c: Handover

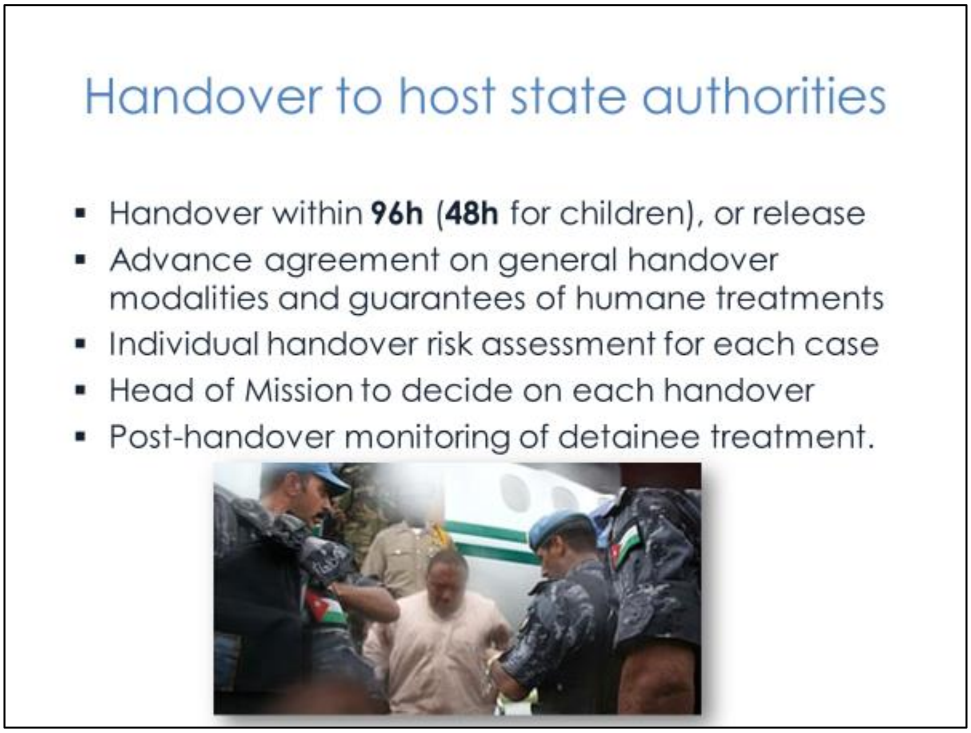
The local commander of the host state military demands that the United Nations immediately hand over the captured IED builder. The commander's battalion has suffered several casualties in IED blasts.

How should the UN handle the request?

Discuss case 6c in plenary or through group discussions. A debriefing can be based on slides 34 and 35 and should bring out the following key points:

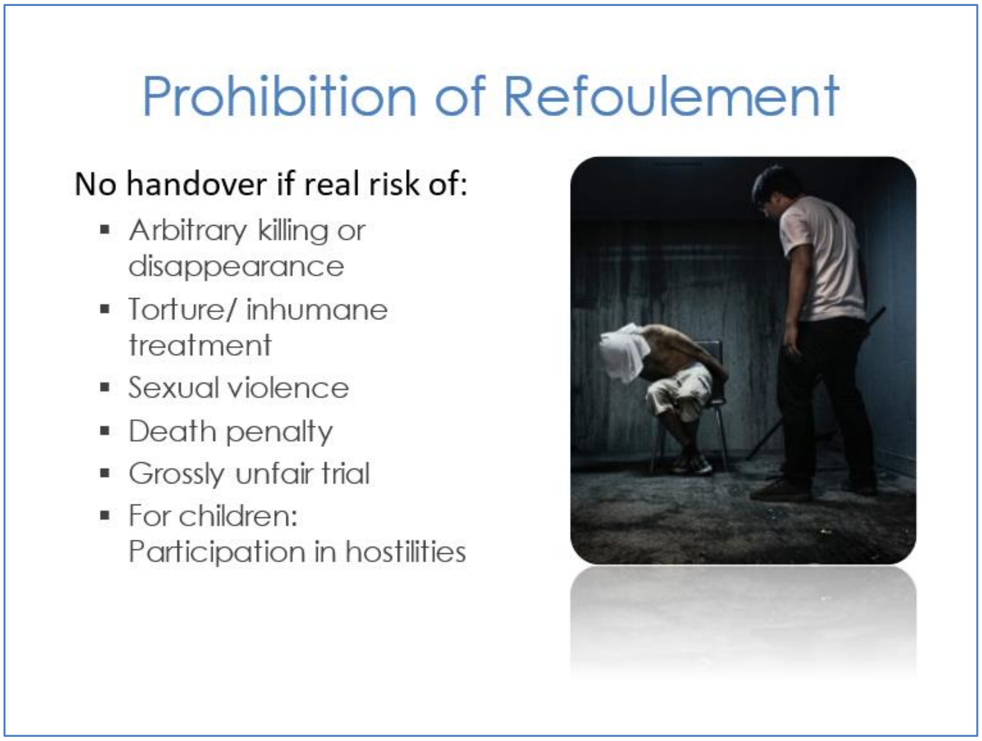
- *The United Nations will seek to hand over the IED builder to national authorities for his criminal investigation and prosecution. However, in line with the principle of non-refoulement, any risks of the IED builder suffering serious human rights violations after handover have to be assessed first.*
- *The IED builder can only be handed over after a prior risk assessment is conducted. Given that the IEDs caused casualties among the very battalion requesting his handover, the risk of the IED builder suffering unlawful reprisals must be seriously considered (considering also whether any such reprisals occurred in the past). In this situation, it may be more prudent to hand the person over to other host state authorities (e.g., the national police)*

Slides 36 & 37:



Handover to host state authorities

- Handover within **96h** (**48h** for children), or release
- Advance agreement on general handover modalities and guarantees of humane treatments
- Individual handover risk assessment for each case
- Head of Mission to decide on each handover
- Post-handover monitoring of detainee treatment.



Prohibition of Refoulement

No handover if real risk of:

- Arbitrary killing or disappearance
- Torture/ inhumane treatment
- Sexual violence
- Death penalty
- Grossly unfair trial
- For children: Participation in hostilities

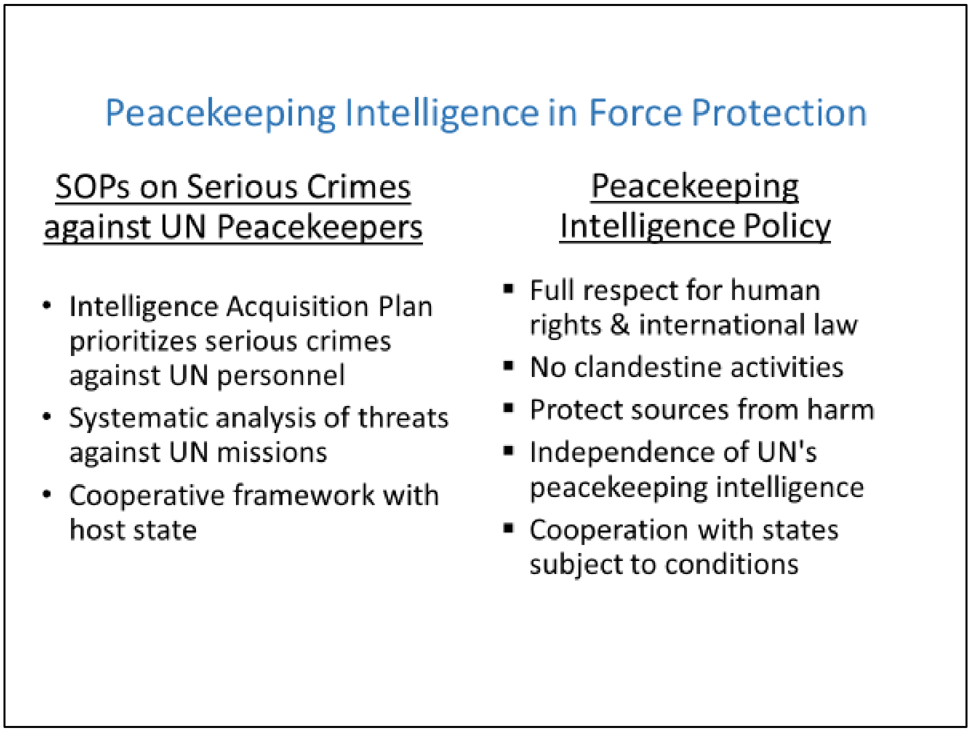
Key message: Handover must take place within 96 hours (48 hours for children). Otherwise, the person must be released. Handover of detained persons to the host-state authority is possible only if there is a host-state warrant and guarantees that the person would not be persecuted, tortured, ill-treated, disappeared, subjected to the death penalty, or summarily executed.

The mission must conduct a handover risk assessment for each individual case (to be led by the human rights component) and subsequent monitoring of the fate of persons who were handed over. A handover will take place at a location agreed by the mission and the Government. General modalities for handover, accompanied by assurances of humane treatment, should be agreed upon with the host state before an individual case occurs. The head of mission is responsible for all decisions on individual handovers.

After the person is handed over, the mission will still monitor the person's treatment, and the Head of Mission has to intervene if the person is subjected to serious human rights violations, including the death penalty.

If the host-state authorities fail to agree to a handover, to provide the required guarantees, or if a real risk of grave violations after the handover remains, the mission will release the person.

Slide 38:



Peacekeeping Intelligence in Force Protection

SOPs on Serious Crimes against UN Peacekeepers

- Intelligence Acquisition Plan prioritizes serious crimes against UN personnel
- Systematic analysis of threats against UN missions
- Cooperative framework with host state

Peacekeeping Intelligence Policy

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

Key message: Force protection is a priority for peacekeeping intelligence, which has to be conducted in line with international law and the UN's specific rules.

According to the Standard Operating Procedures on Serious Crimes against UN Peacekeepers, the mission's peacekeeping-intelligence Acquisition Plan must prioritise the prevention and response to serious crimes against UN personnel, including through systematic threat analysis and appropriate peacekeeping-intelligence cooperation with host state authorities.

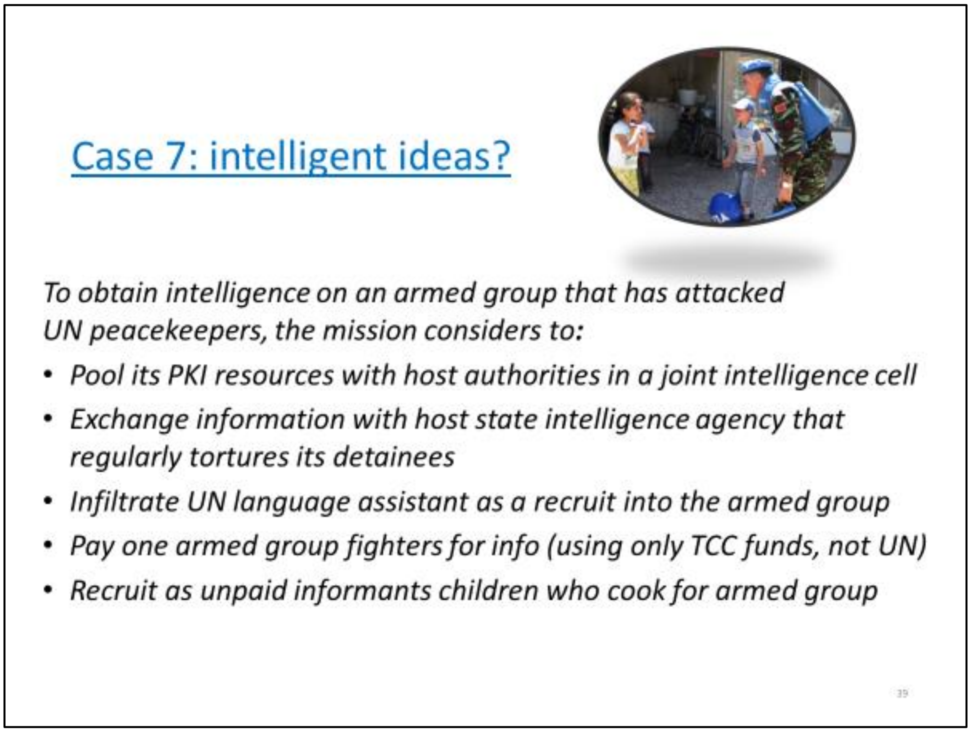
However, gathering and sharing United Nations Peacekeeping Intelligence is subject to legal limits. Some limits follow directly from international human rights law. Others are established by the Peacekeeping Intelligence Policy to protect the independence and impartiality of UN missions. Even though they are established through a UN policy, they are nevertheless binding on all UN personnel.

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 peacekeeping-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 personnel must never break into a government building or hack into a database of a non-governmental organisation to obtain information.

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

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 peacekeeping-intelligence arm of the host government or third states. Information may be shared with other state authorities but is subject to human rights safeguards.

Slide 39:



Case 7: intelligent ideas?

To obtain intelligence on an armed group that has attacked UN peacekeepers, the mission considers to:

- *Pool its PKI resources with host authorities in a joint intelligence cell*
- *Exchange information with host state intelligence agency that regularly tortures its detainees*
- *Infiltrate UN language assistant as a recruit into the armed group*
- *Pay one armed group fighters for info (using only TCC funds, not UN)*
- *Recruit as unpaid informants children who cook for armed group*

39

Discuss case 7 in plenary or groups. You can use slides 38 & 40 for the debriefing. The discussions should highlight the following key points:

a. *The mission may share peacekeeping-intelligence with national peacekeeping-intelligence agencies, subject to compliance with human rights law and the related HRDDP. However, its PKI activities must remain independent, and the mission must, therefore, not pool its PKI resources with the host authorities into a joint peacekeeping-intelligence cell.*

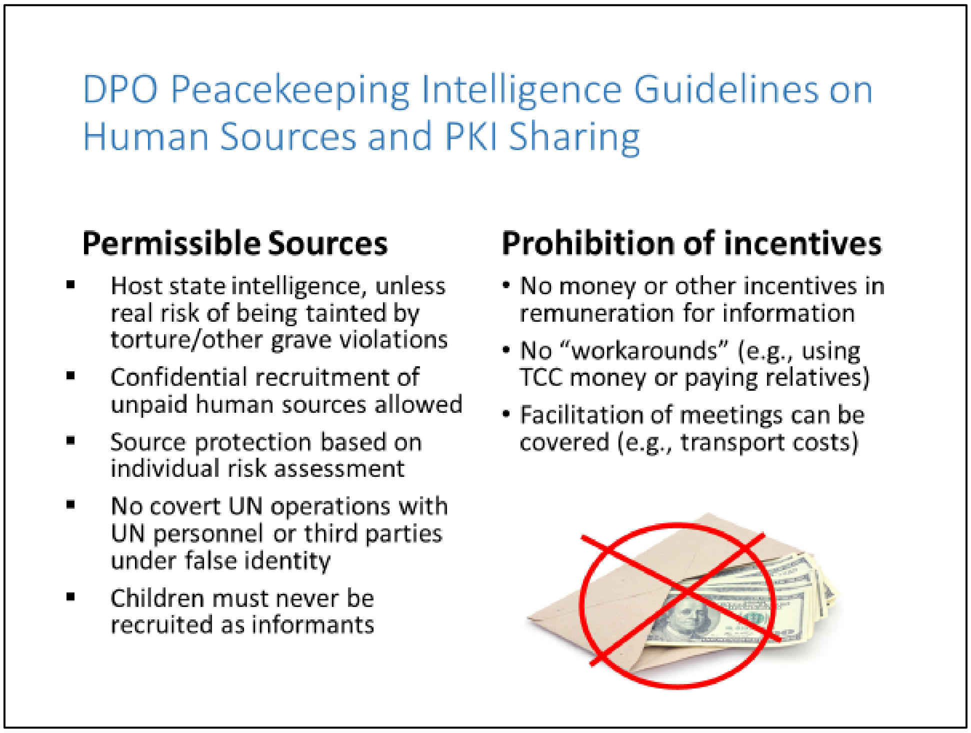
b. *The UN must not become complicit to torture, including by soliciting information if there is a reasonable risk that it will derive from torture (plus, torture-generated information is regularly unreliable). For this reason, the UN Guidelines on Sharing Peacekeeping Intelligence prohibit the mission from accepting or soliciting peacekeeping-intelligence where there is a real risk that it was obtained by way of torture or other grave violations of international human rights or humanitarian law.*

c. *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.*

d. *The UN Guidelines on Human Sources in Peacekeeping Intelligence prohibit payments or other incentives as remuneration for peacekeeping intelligence. This prohibition must not be circumvented by using TCC national funds rather than UN funds.*

e. *In line with the UN Guidelines on Human Sources in Peacekeeping Intelligence, the mission must never recruit or otherwise develop children as sources of peacekeeping-intelligence (even as unpaid informers) 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 40:



DPO Peacekeeping Intelligence Guidelines on Human Sources and PKI Sharing

Permissible Sources

- Host state intelligence, unless real risk of being tainted by torture/other grave violations
- Confidential recruitment of unpaid human sources allowed
- Source protection based on individual risk assessment
- No covert UN operations with UN personnel or third parties under false identity
- Children must never be recruited as informants

Prohibition of incentives

- No money or other incentives in remuneration for information
- No "workarounds" (e.g., using TCC money or paying relatives)
- Facilitation of meetings can be covered (e.g., transport costs)

Key message: The UN is prohibited from collecting peacekeeping intelligence by providing payments, recruiting child informants, running covert operations under false identities, or accepting intelligence obtained through torture.

The UN can accept peacekeeping-intelligence from third parties. However, UN policy stipulates that if there is a real risk that certain intelligence from third parties (e.g., host state intelligence agencies) has been obtained by way of torture or other grave violations of international human rights or humanitarian law, missions must neither accept nor solicit such intelligence.

The UN can confidentially recruit human sources and must ensure to keep their identity confidential. However, the UN will not use its own personnel or third parties in covert operations, where persons operate under an assumed or false identity. Neither will the UN recruit children as informants.

The DPO Guidelines on Information from Human Sources for Peacekeeping Intelligence stipulate that no amount of money will be paid, nor gifts offered, to human sources or their relatives in remuneration for information. It is strictly forbidden to trade something that the source wants for information. However, logistical expenses (e.g., a reasonable lump sum to cover the source's transport costs) to facilitate meetings and debriefings with a source are not considered prohibited incentives.

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

Slide 41:

Lesson Take Aways

- Mission can use necessary and proportional force in self-defence against ongoing or recurrent attacks
- Defensive force to respect human rights (non-military threats) or IHL & human rights law (military threats)
- Peacekeeping intelligence prioritizes protection of mission, but has clear legal & policy limits

Summary

Key takeaways regarding the Legal Framework for Force Protection include:

- **The Mission can use necessary and proportional force in self-defence against ongoing or recurrent attacks**
- **Defensive force must always respect human rights (in relation to non-military threats) or IHL & human rights law (in relation to military threats)**
- **Peacekeeping intelligence prioritizes protection of mission but has clear legal & UN policy limits.**

Module 2

Legal Framework

Take away from Module 2 include:

- International and national humanitarian legal frameworks impact and guide peacekeepers in the field
- Bodies of international law provide special protection for peacekeepers and those members of communities that are most vulnerable: women, children, refugees
- Peacekeepers do not have impunity from laws and are held accountable for unlawful activities
- The mission can use necessary and proportional force in self-defence against ongoing or recurrent attacks
- Defensive actions must always respect human rights
- Peacekeeping intelligence prioritises protection of civilians and UN units.

Module 3

Operational Framework

Module 3 at a Glance

Aim

The module does not aim to create or train participants on a decision-making process for UN peacekeeping; and does not discuss particular doctrines, which may vary between troop / police contributing countries. Rather, the module offers tactical planning considerations that commanders and their staff might apply to their own decision-making processes as per their national doctrine.

Learning Objectives

The learning objectives for Module 3 are based on the goal of being able to apply the main aspects of the first two modules into practise:

- Know how to translate conceptual and legal frameworks into appropriate action at the tactical level
- Identify tools that may provide guidance to help plan FP in a UN PKO environment

Overview

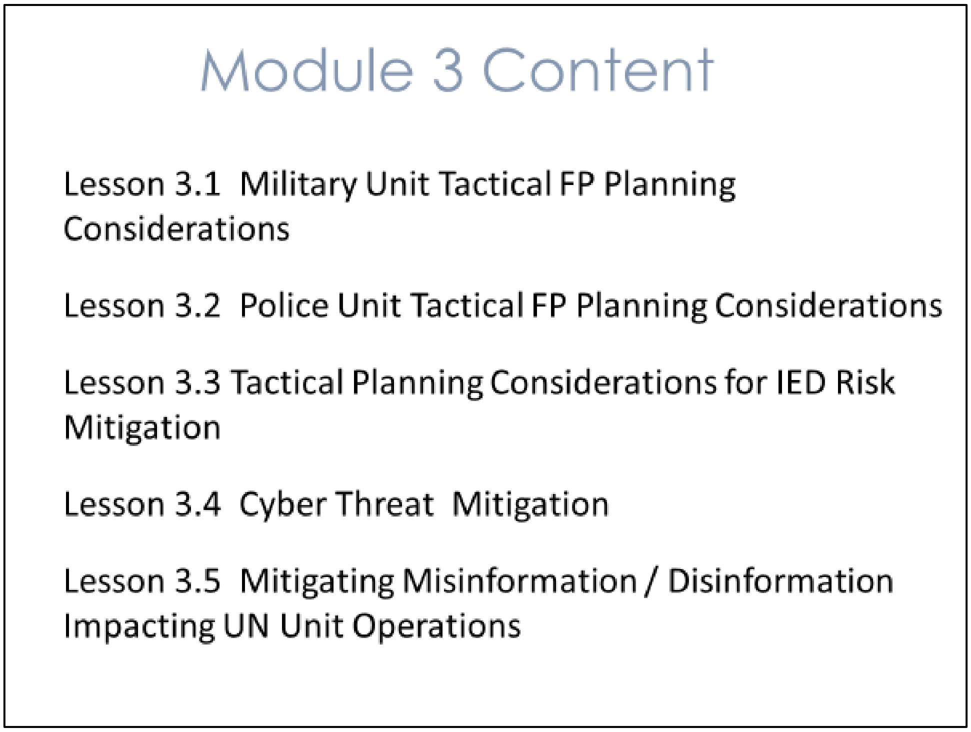
Module 3 provides a systematic approach to apply unique tactical planning considerations for FP, tasks that support the FP strategy, the employment of and coordination with specialised units, and counter IED.

While this module focuses on the tactical level, the overview you received in modules 1 and 2 provide the strategic and conceptional concepts that help in the transition into this module. The module focuses on the "how" and provides guidance to help in the approach to planning for FP in a UN PKO.

Slide 1

Module 3 Operational Framework for UNFORPRO

Slide 2



Module 3 Content

Lesson 3.1 Military Unit Tactical FP Planning Considerations

Lesson 3.2 Police Unit Tactical FP Planning Considerations

Lesson 3.3 Tactical Planning Considerations for IED Risk Mitigation

Lesson 3.4 Cyber Threat Mitigation

Lesson 3.5 Mitigating Misinformation / Disinformation Impacting UN Unit Operations

Welcome to Module 3, where we will delve into the crucial topic of conducting FP tactical planning in a United Nations Peacekeeping Operations (UN PKO) environment. Our main objective is to equip unit staff and their leaders with the necessary tools and considerations for effective FP planning. We will introduce a range of techniques and tools that can assist unit staff and leaders in their FP planning endeavours. These tools will facilitate the process of developing actionable risk mitigation plans, ensuring successful unit operations.

Throughout this module, we will explore the following key areas:

- Lesson 3.1 Military Unit Tactical FP Planning Considerations
- Lesson 3.2 Police Unit Tactical FP Planning Considerations
- Lesson 3.3 Tactical Planning Considerations for IED Risk Mitigation
- Lesson 3.4 Cyber Threat Mitigation
- Lesson 3.5 Mitigating Misinformation / Disinformation Impacting UN Unit Operations

By the end of Module 3, you will have gained a comprehensive understanding of FP tactical planning in a UN PKO environment. Equipped with the necessary tools and considerations, you will be better prepared to navigate the complexities of peacekeeping operations and contribute to the overall success of your unit.

Lesson 3.1

Force Protection Planning Considerations (Military)

Starting the Lesson *Ask / inquire from the participants about the concept of FP (Force Protection) and explore how military units might conduct FP planning, highlighting its distinctions from POC planning. Delve into the importance of adopting a mindset that surpasses the traditional attack-defend approach to operations. In the current peacekeeping landscape, United Nations (UN) forces face significant risks and are specifically subjected to attacks. While the use of violence against UN peacekeeping is increasing; reports from the Department of Peacekeeping Operations (DPO) indicate an escalating trend of peacekeepers themselves becoming the targets.*

☞ ***Note to instructor:***

In this lesson, we will explore how commanders and their staff can effectively integrate Peacekeeping Operations (PKO) Force Protection (FP) considerations into their own military decision-making process. Rather than imposing a rigid process, the aim is to highlight the importance of incorporating FP into decision-making.

Given the comprehensive nature of this lesson, it is expected to span several hours. To facilitate engagement and learning, the lesson can be divided into distinct sections, allowing for breaks and practical exercises to be incorporated based on the instructor's discretion. It is recommended to structure instructional blocks of 30 to 45 minutes, considering the skill level of the students.

Within the Department of Peace Operations (DPO), there are documents that outline FP as measures designed to mitigate risks to UN personnel, facilities, equipment, materials, operations, and activities, encompassing both threats and natural hazards. However, this particular lesson will focus specifically on tactical operational threats and attacks against UN military and police units.

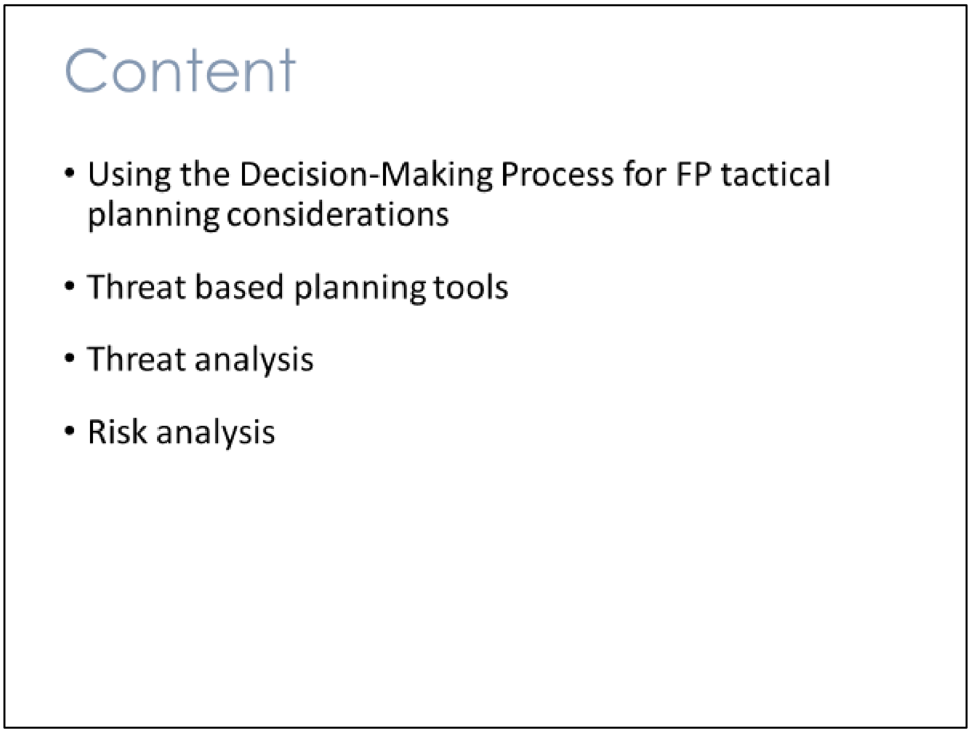
Slide 3

Lesson 3.1 Military Unit Tactical Planning Considerations for Force Protect (FP)

In today's peacekeeping environment, proactive force protection planning is essential due to the diverse and often ambiguous threat patterns. Collaboration between the military component, UN departments, offices, and mission components is crucial for analysing threats and mitigating risks to UN forces. This lesson will provide guidance, considerations, and tools to aid in tactical force protection planning. It is important to note that force protection is an integral part of all military operations, both static and mobile.

☞***Note to Instructor***: *This lesson does not aim to impose a specific UN decision-making process or doctrine, as these may vary among troop or police-contributing countries. Instead, it offers planning tools, guidance and considerations for commanders and their staff that can be aligned with their own national doctrine and decision-making processes.*

Slide 4



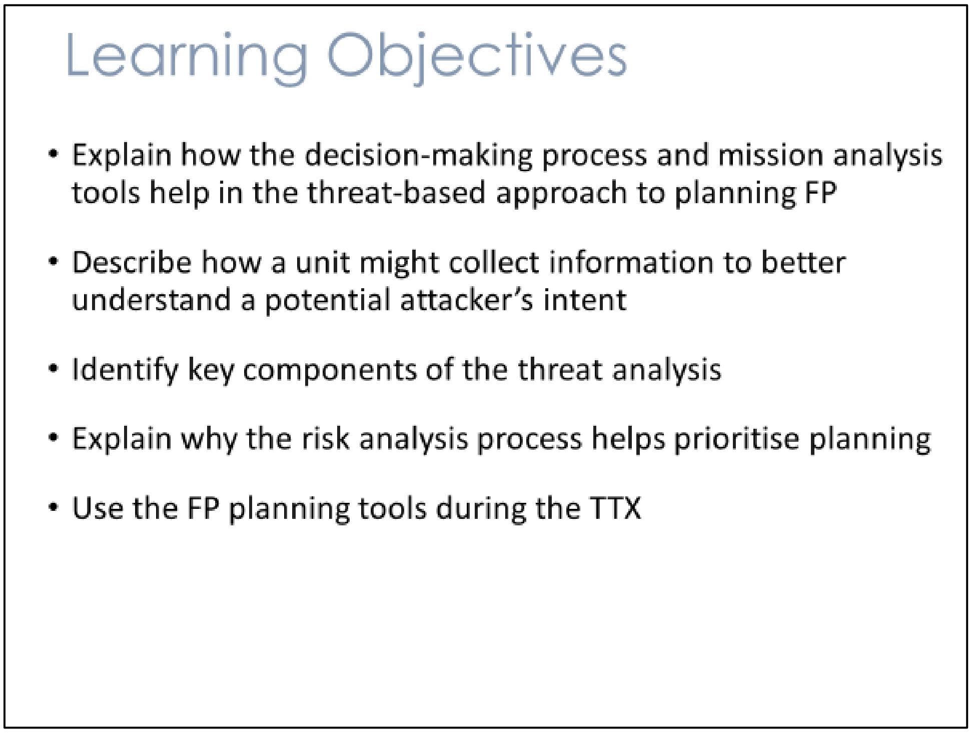
Content

- Using the Decision-Making Process for FP tactical planning considerations
- Threat based planning tools
- Threat analysis
- Risk analysis

Here is the content of the lesson:

- Using the Decision-Making Process for FP tactical planning considerations
- Threat-based planning tools
- Threat analysis
- Risk analysis

Slide 5



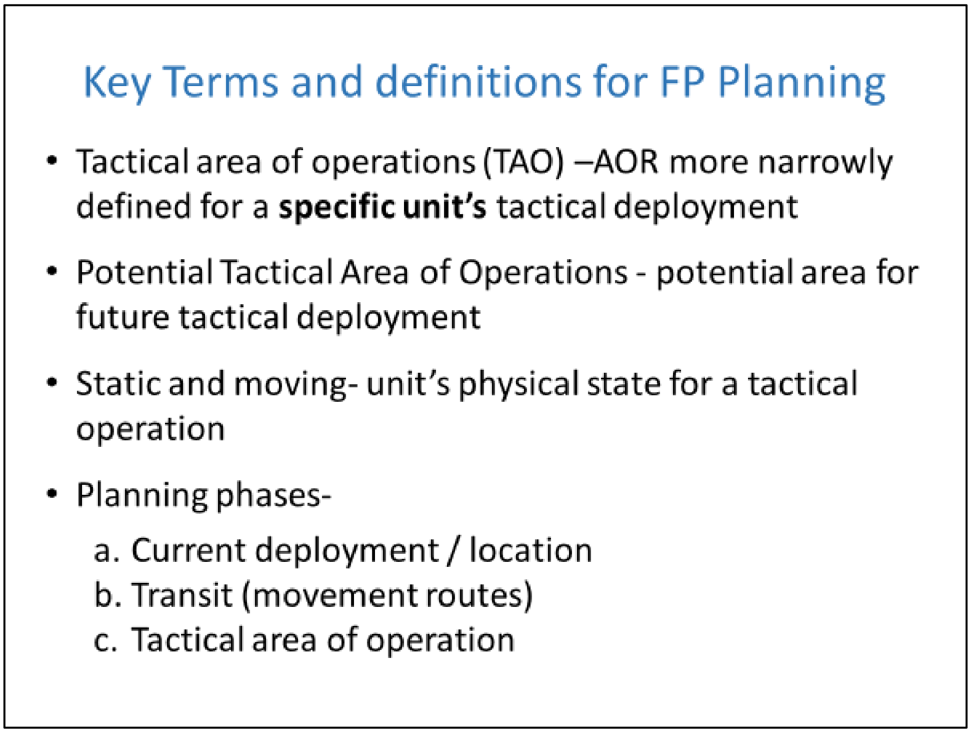
Learning Objectives

- Explain how the decision-making process and mission analysis tools help in the threat-based approach to planning FP
- Describe how a unit might collect information to better understand a potential attacker's intent
- Identify key components of the threat analysis
- Explain why the risk analysis process helps prioritise planning
- Use the FP planning tools during the TTX

Here are the learning objectives for this lesson. Take a few minutes to review.

- Explain how the decision-making process and mission analysis tools help in the threat-based approach to planning FP
- Describe how a unit might collect information to understand a potential attacker's intent better
- Identify key components of the threat analysis
- Explain why the risk analysis process helps prioritise planning
- Use the FP planning tools during the TTX

Slide 6



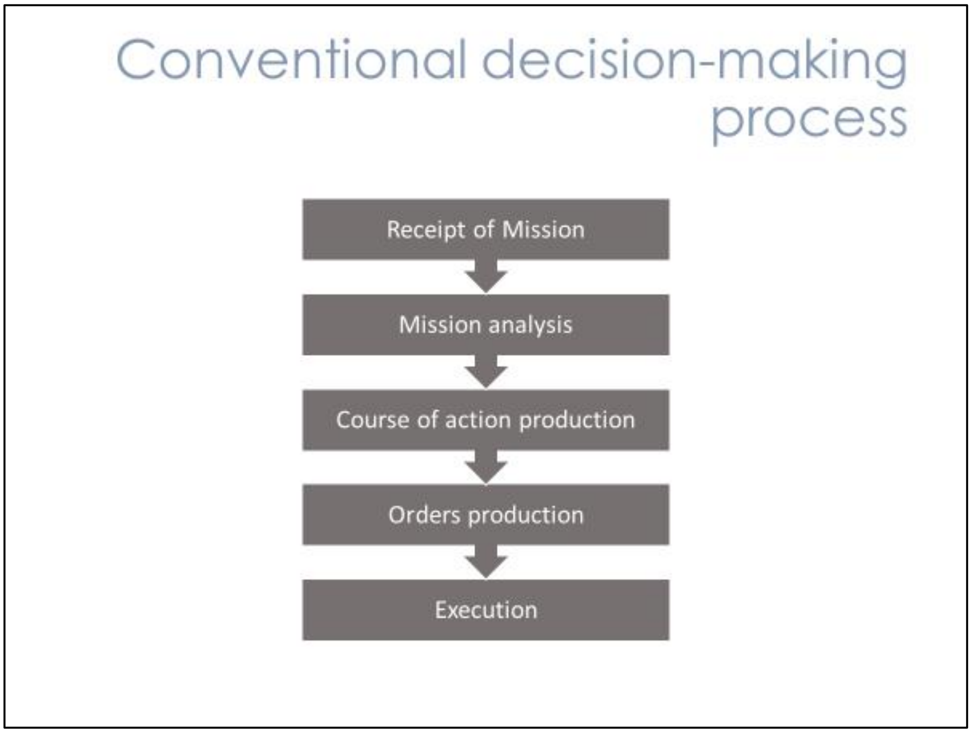
Key Terms and definitions for FP Planning

- Tactical area of operations (TAO) –AOR more narrowly defined for a **specific unit's** tactical deployment
- Potential Tactical Area of Operations - potential area for future tactical deployment
- Static and moving- unit's physical state for a tactical operation
- Planning phases-
  a. Current deployment / location
  b. Transit (movement routes)
  c. Tactical area of operation

Let us establish some key FP definitions that we will use in the FP planning framework.

- Many have used the Area of Responsibility (AOR); we will also use the term, Tactical area of operations (TAO) is an AOR more narrowly defined for a specific unit's tactical deployment; it will be used for both military and police units
- Potential Tactical Area of Operations - potential area for future tactical deployment
- Static and moving- unit's physical state for a tactical operation
- The three phases that should be used for FP planning: Current location/deployment, transit (movement routes); future TAO (or potential TAOs)

Slide 7



Conventional decision-making process

Receipt of Mission

Mission analysis

Course of action production

Orders production

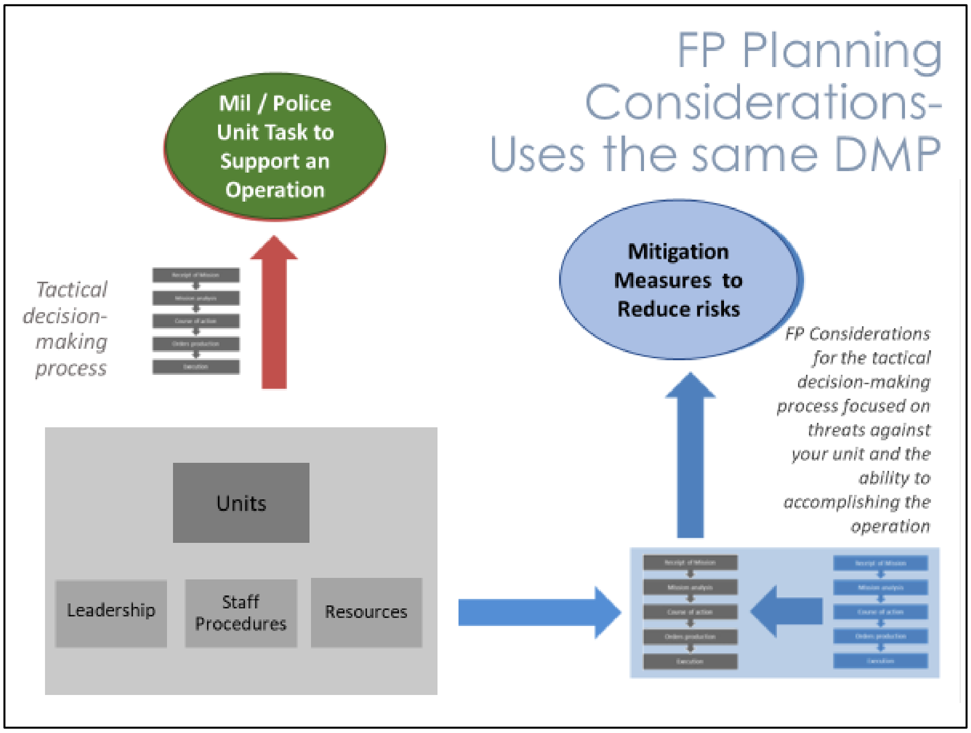
Execution

☞ ***Note to instructor:*** *In a conventional military operation, the planning phase plays a crucial role in determining the necessary resources such as troops and equipment to accomplish the mission. It's important to note that each Troop Contributing Country (TCC) has its own established military decision-making process as outlined in its national doctrine. This lesson aims to highlight the integration of Force Protection (FP) within a Peacekeeping Operations (PKO) environment, rather than training participants on a specific decision-making process. While the lesson utilises military planning tools, considerations, and guidance, it recognises that TCCs may have variations in their national doctrine.*

In module one, we presented this planning tool that encompasses five consecutive steps. While this process is visually depicted as linear, it is important to recognise that it is inherently cyclical in nature due to its continuous nature. Here are the five steps:

- Receipt of mission
- Mission analysis (including analysis of the Operational Environment)
- Course of Action Production
- Order production
- Execution

Slide 8



FP Planning Considerations- Uses the same DMP

FP Considerations for the tactical decision-making process focused on threats against your unit and the ability to accomplishing the operation

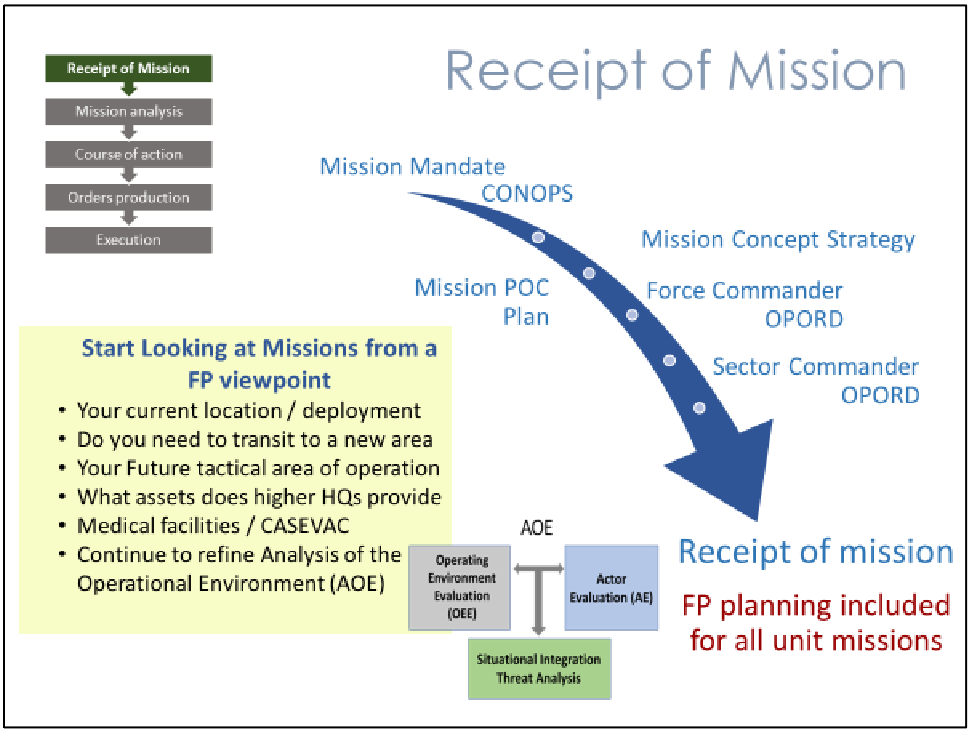
This slide showcases a comparison between UN peacekeeping and conventional operations. The previous discussion highlighted the importance of integrating Force Protection (FP) considerations into the planning process, given the distinct requirements and mindset required in UN peacekeeping compared to conventional operations. Although the Decision-Making Process (DMP) remains largely the same for both types of planning.

For effective functioning, military units require well-defined structures encompassing leadership, staff procedures, and resources. These structures may vary among different armies based on national doctrine, but they always serve as the fundamental building blocks for conventional armies. In the graphic, the red arrow represents the conventional DMP, military planning carried out in the face of an opponent or enemy, with the five steps of the tactical decision-making process clearly delineated.

On the other hand, the blue arrow illustrates the decision-making process for FP. Unlike conventional military operations, UN peacekeepers do not engage in typical attack/defence engagements against an enemy adversary.

Instead, their role involves defending third parties, particularly civilians, against the threat of physical violence from potential perpetrators / attackers. However, while carrying out their mandated tasks, military units in UN peacekeeping often encounter opposition or conflicting interests from certain groups. As a result, UN units are frequently targeted in these situations. FP planning has the same framework as a traditional DMP / planning process focused on threats.

Slide 9



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Receipt of Mission

Mission Mandate
CONOPS

Mission Concept Strategy

Mission POC
Plan

Force Commander
OPORD

Sector Commander
OPORD

Start Looking at Missions from a FP viewpoint

- Your current location / deployment
- Do you need to transit to a new area
- Your Future tactical area of operation
- What assets does higher HQs provide
- Medical facilities / CASEVAC
- Continue to refine Analysis of the Operational Environment (AOE)

AOE

Operating Environment Evaluation (OEE)

Actor Evaluation (AE)

Situational Integration Threat Analysis

Receipt of mission

FP planning included for all unit missions

This slide illustrates the progression from a mission's mandate to the operational plans for military units, highlighting the various planning documents involved in a peacekeeping mission.

The foundational elements of any mission encompass the Security Council Mandate, Mission Concept, Mission Plan, Concept of Operations (CONOPS), as well as the Mission POC Strategy, accompanying plans, and the relevant Operations Orders for Mission Headquarters, sectors, and units. In the conventional military decision-making process, the initial step is the receipt of the mission.

In UN Peacekeeping, the mission originates from the strategic documents discussed earlier, commencing with the Security Council mandate. Guided by the strategic and operational-level documents depicted in the slide (some of which have been previously addressed), the respective higher headquarters within a field mission will then issue orders to military units. The list provided in the bottom left of the slide presents examples of guidance/documents that should be considered when planning for Force Protection (FP) in all operations.

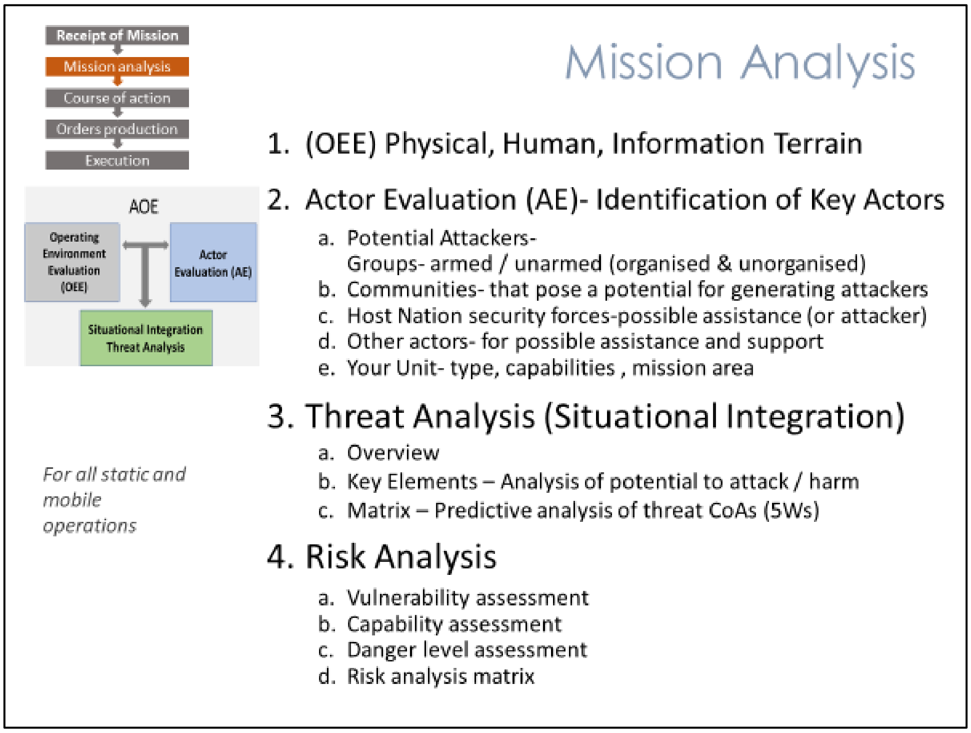
When planning for FP, it is crucial to view it as a comprehensive support structure for the entire mission. This approach aids in developing planning products, utilising peacekeeping-intelligence resources, and mitigating risks to UN forces. By employing planning tools, all components of the mission strategy (military, police, civilian, host state security forces) can be effectively integrated and coordinated.

Unit commanders are responsible to plan actions, up to and including the use of deadly force, aimed at preventing or responding to threats that can reduce or eliminate the unit's operational capabilities, and without prejudice to the responsibility of the host government to protect the UN Mission.

Start Looking at Missions from a FP viewpoint

- Your current location / deployment
- Do you need to transit to a new area
- Your Future tactical area of operation
- What assets do higher HQs provide
- Are medical facilities / CASEVAC available and how in the range of support
- Refine the Analysis of the Operational Environment (AOE) to identify potential groups that potentially can attack UN units

Slide 10



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

AOE
Operating Environment Evaluation (OEE)
Actor Evaluation (AE)
Situational Integration Threat Analysis

For all static and mobile operations

Mission Analysis

1. (OEE) Physical, Human, Information Terrain
2. Actor Evaluation (AE)- Identification of Key Actors
   a. Potential Attackers-
   Groups- armed / unarmed (organised & unorganised)
   b. Communities- that pose a potential for generating attackers
   c. Host Nation security forces-possible assistance (or attacker)
   d. Other actors- for possible assistance and support
   e. Your Unit- type, capabilities , mission area
3. Threat Analysis (Situational Integration)
   a. Overview
   b. Key Elements – Analysis of potential to attack / harm
   c. Matrix – Predictive analysis of threat CoAs (5Ws)
4. Risk Analysis
   a. Vulnerability assessment
   b. Capability assessment
   c. Danger level assessment
   d. Risk analysis matrix

This section delves into the mission analysis stage of the planning process, which holds significant importance as it defines the tactical problem to be addressed. As we have previously seen, the following steps are encompassed within Mission Analysis, and they will be explored further in the upcoming slides. It is worth reiterating that the analysis of the operating environment and threat assessments form a continuous process, generating updated products to assist the staff during mission analysis. This analysis framework aids in identifying potential attackers.

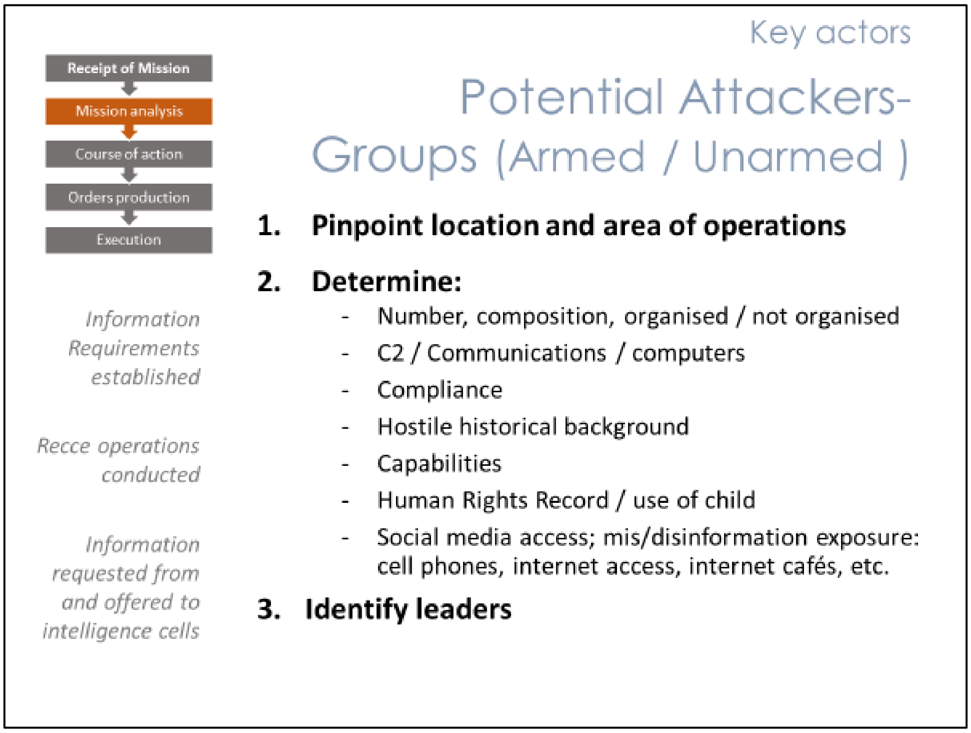
1. Operating Environment Evaluation (OEE): This involves assessing the physical, human, and informational terrain.

2. Actor Evaluation (AE): Key actors are identified, including potential attackers (armed and unarmed, organised, and unorganised), communities that may generate attackers, host nation security forces (as potential assistance or attackers), and other actors that could aid and support. Your own unit's type, capabilities, and mission area are also considered.

3. Threat Analysis (Situational Integration): Overview: Providing a comprehensive understanding of the threat landscape. Key Elements: Analysing the potential to attack or cause harm. Matrix: Conducting predictive analysis of threat Courses of Action (CoAs) using the 5Ws (Who, What, Where, When, Why).

4. Risk Analysis: Vulnerability Assessment: Evaluating vulnerabilities within the mission context. Capability Assessment: Assessing the capabilities required to counter threats. Danger Level Assessment: Determining the level of danger associated with identified risks. d. Risk Analysis Matrix: Utilising a matrix to analyse and prioritise risks based on their likelihood and impact.

Slide 11



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Information Requirements established

Recce operations conducted

Information requested from and offered to intelligence cells

Key actors

Potential Attackers- Groups (Armed / Unarmed)

1. **Pinpoint location and area of operations**
2. **Determine:**
   - Number, composition, organised / not organised
   - C2 / Communications / computers
   - Compliance
   - Hostile historical background
   - Capabilities
   - Human Rights Record / use of child
   - Social media access; mis/disinformation exposure: cell phones, internet access, internet cafés, etc.
3. **Identify leaders**

The subsequent step in Mission Analysis focuses on the identification of key actors that can be potential attackers who could pose a threat to our units or impede our operational freedom. This systematic analysis aims to provide a comprehensive understanding of the actors involved.

Mission components can offer valuable information, and early consultation with them enhances the military analysis process. It is crucial to gain a thorough understanding of potential attackers within the designated area of operations, as well as, insights from recent or ongoing operations. The following aspects need to be determined:

- Numbers and composition of potential perpetrators
- Command and control (C2) structure and communication capabilities
- Compliance with international law and regulations
- Hostile intent and historical background
- Capabilities and weaponry
- Human rights record, including the use of child soldiers

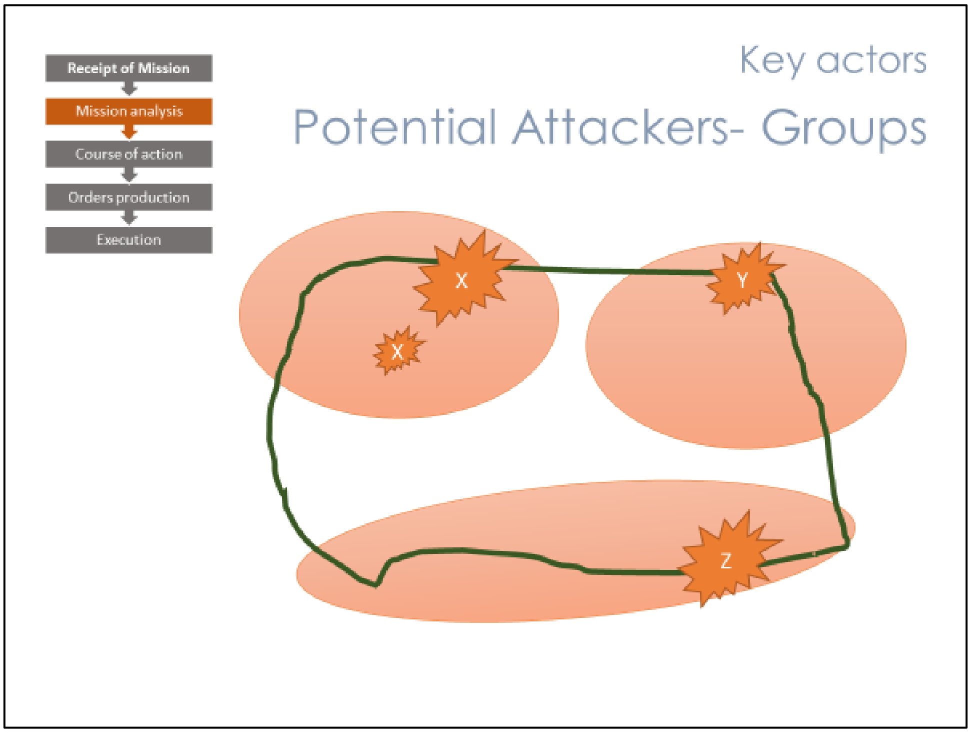
- Access to social media, exposure to misinformation/disinformation, availability of cell phones, internet access, hardware/software, internet cafés, etc.

The identification of key leaders within these groups is of vital importance. Peacekeeping commanders, for example, bear the responsibility of engaging with armed group leaders, reminding them of their obligations under international law, and emphasising potential consequences.

In addition to liaising with local communities, UN agencies/offices, and leaders of potential attackers, relevant information regarding the identification of groups can be obtained from various sources. This necessitates the establishment of Information Requirements (IRs). Patrols and reconnaissance operations are conducted in response to these IRs, and information is exchanged with other mission peacekeeping-intelligence and information management mechanisms.

Engage participants by asking which information or indicators they consider to be the most relevant when assessing potential attackers. The answer is that a comprehensive collection effort helps build the operational picture and key information holds significance, as each piece contributes to building the complete human terrain picture. This comprehensive understanding allows us to discern threat patterns and conduct predictive analysis effectively. Emphasise the importance of considering all available information as it forms the essential puzzle pieces required for a thorough assessment.

Slide 12



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

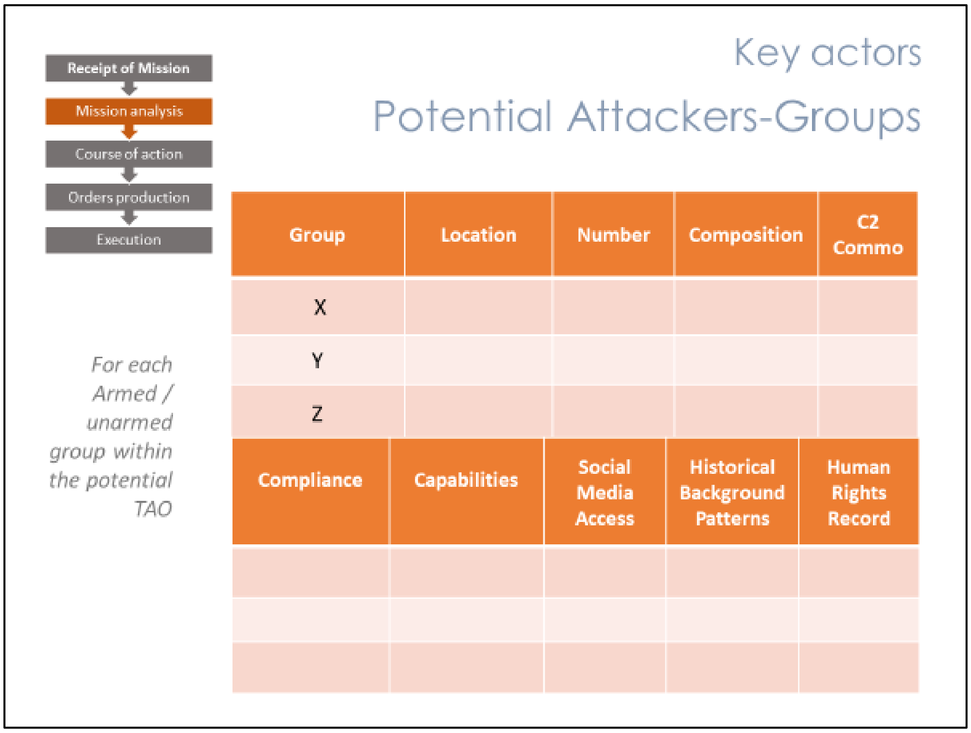
Key actors

Potential Attackers- Groups

Mapping the locations of potential attackers is a valuable approach that aids in outreach efforts and provides military planners with a clear understanding of areas that might attract their interest. The circles on the map represent the respective areas of influence of these potential perpetrators / attackers. It is important to note that these areas of influence may overlap with the designated area of responsibility of other peacekeeping units. In such instances, close coordination with the units responsible for adjacent areas of operations becomes essential in the planning processes.

Instructors note: Please note that in practice, planners would typically expand on the map by adding the specific locations of all key actors. However, for clarity and educational purposes, this module presents separate maps for each key actor identified during the Mission Analysis steps.

Slide 13



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Key actors

Potential Attackers-Groups

Group	Location	Number	Composition	C2 Commo
X				
Y				
Z				

Compliance	Capabilities	Social Media Access	Historical Background Patterns	Human Rights Record

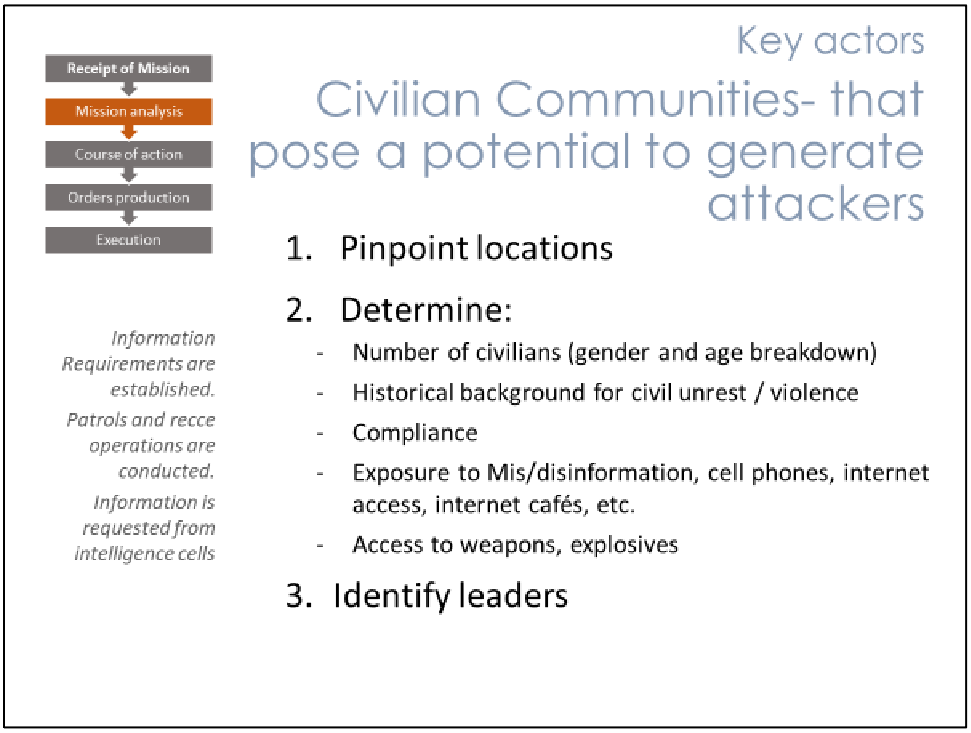
For each Armed / unarmed group within the potential TAO

To bolster the systematic analysis of potential attackers in both current and future operational areas, the use of a comprehensive table can be helpful. This slide serves as an example of how such an analysis can be conducted, with a focus on three groups and the inclusion of various factors and criteria such as location, number, composition, command and control, mandate compliance, capabilities, social media access and leverage, historical background patterns and history, and human rights record. It is imperative to conduct this analysis for all potential perpetrators / attackers your unit may encounter during operations or transit within the designated areas.

Moreover, it is crucial to recognise the value of gathering information from other mission and non-mission actors. Early consultation with these entities will significantly fortify military analysis and enhance the overall comprehension of potential threats and adversaries. Additionally, apart from using a table for analysis, the planning staff should be acquainted with diverse tools and resources accessible from peacekeeping-intelligence cells at all levels. These resources can provide invaluable insights, peacekeeping-intelligence reports, and specialised knowledge, enabling a more comprehensive and well-informed analysis of potential attackers.

By amalgamating these approaches, assimilating insights from multiple sources, and harnessing tools such as tables and peacekeeping-intelligence products, we can ensure a more robust and effective understanding of potential attackers. This heightened awareness will facilitate informed FP decision-making, strengthen operational preparedness, and ultimately contribute to the success of the mission.

Slide 14



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Information Requirements are established.

Patrols and recce operations are conducted.

Information is requested from intelligence cells

Key actors

Civilian Communities- that pose a potential to generate attackers

1. Pinpoint locations
2. Determine:
   - Number of civilians (gender and age breakdown)
   - Historical background for civil unrest / violence
   - Compliance
   - Exposure to Mis/disinformation, cell phones, internet access, internet cafés, etc.
   - Access to weapons, explosives
3. Identify leaders

The subsequent phase of Mission Analysis entails the identification of significant actors who could potentially serve as attackers within the local civilian communities present in your area of operations. While these communities typically exhibit peaceful and supportive behaviour toward the United Nations mandate, there exists a potential for violence, civil unrest, and the emergence of attackers. Armed and unarmed groups with specific agendas often motivate or agitate these communities, leading to civil unrest, riots, and a possible threat to our units or restriction of operational freedom. The objective of this systematic analysis is to acquire a comprehensive understanding of the actors involved.

Mission components possess valuable information, and early consultation with them enhances the military analysis process. Gaining a thorough understanding of potential attackers within the designated area of operations, as well as incorporating insights from recent or ongoing operations, is critical. The following aspects should be determined in order to facilitate the systematic analysis of key actors/groups in these communities:

- Pinpoint locations: Identify the specific areas within the community where potential attackers may emerge

- Determine the number of civilians: Break down the demographic information of the civilian population by gender and age to gain a comprehensive understanding

- Assess historical background: Investigate instances of civil unrest or violence in the community's past to identify patterns and potential triggers

- Evaluate compliance: Analyse the extent to which the community adheres to local laws and regulations

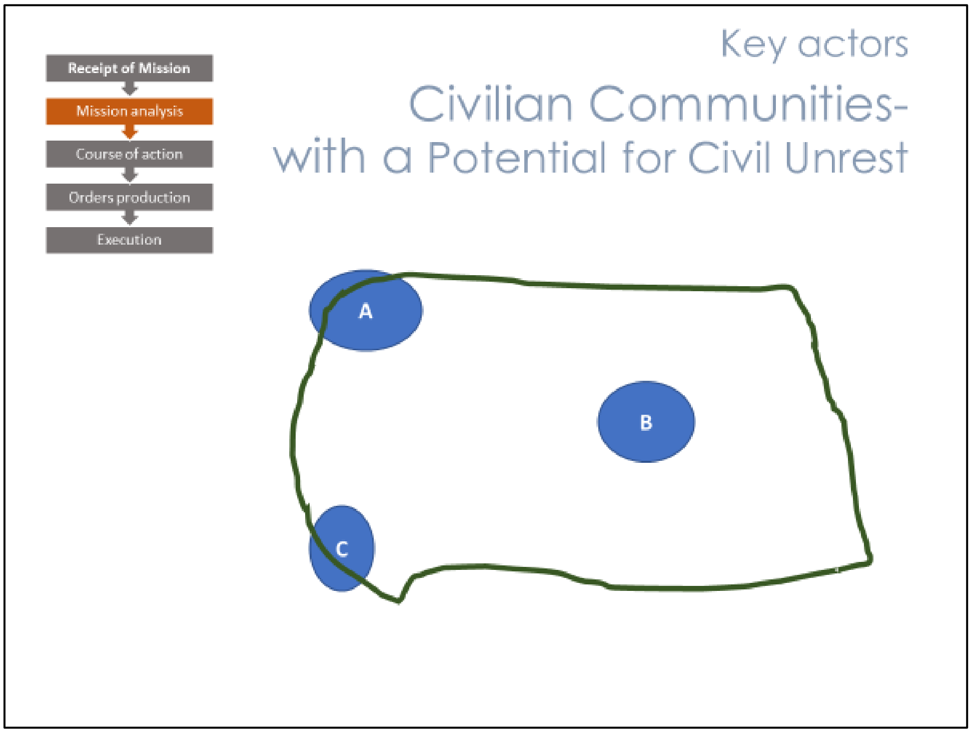
- Assess exposure to misinformation/disinformation: Examine the level of exposure community members have to false or misleading information, considering factors such as cell phone usage, internet access, internet cafés, and other relevant sources.

- Determine access to weapons and explosives: Investigate whether there is availability and accessibility of weapons or explosive materials within the community

- Identify leaders: Determine key figures or individuals who may have influence or leadership roles within the community, as they can significantly impact the behaviour and actions of the broader population.

By considering these criteria and factors, the systematic analysis of key actors and groups in these communities can be effectively facilitated. This comprehensive understanding will contribute to informed decision-making, risk assessment, and the development of strategies to address potential threats and challenges posed by these actors.

Slide 15



Key actors

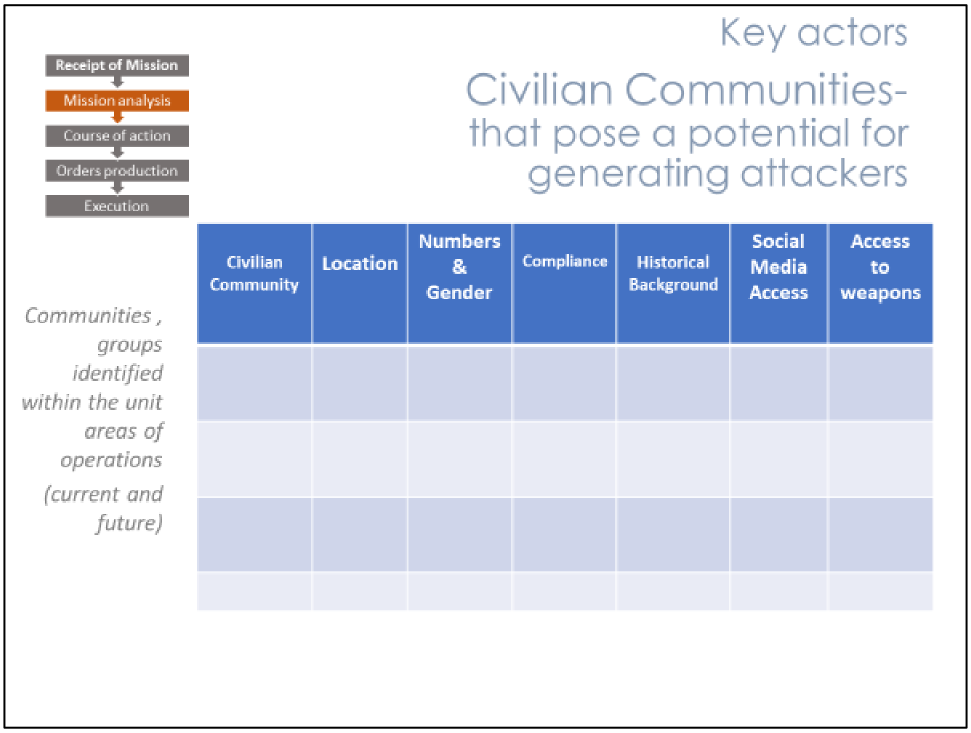
Civilian Communities-
with a Potential for Civil Unrest

Here is an illustrative tool that aids in visualising locations. Its purpose is to support the systematic analysis of populations in both your current operational areas and potential future areas of operations. By utilising map overlays alongside other overlays that depict crucial factors and locations, this tool enhances the synergistic effect and the ability to analyse the potential impact based on time and distance.

By integrating these map overlays with relevant data, the analysis process becomes more comprehensive and insightful. The visual representation allows for a clearer understanding of population distribution, concentration, and potential patterns of behaviour. It facilitates the identification of key areas, hotspots, or regions where specific factors may have a more significant influence.

The use of such visual tools enables a holistic approach to analysing the operational environment. It supports decision-making processes by providing a visual framework to consider various factors, their spatial relationships, and the potential implications for operations. This enhanced analysis empowers military personnel to make informed choices regarding resource allocation, force protection measures, and tactical planning.

Slide 16



Key actors

Civilian Communities- that pose a potential for generating attackers

Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Communities , groups identified within the unit areas of operations (current and future)

Civilian Community	Location	Numbers & Gender	Compliance	Historical Background	Social Media Access	Access to weapons

As we did earlier, to facilitate the systematic analysis of civilian communities that have the potential to generate attackers and impact our tactical operations in both current and future operational areas, the use of a comprehensive table proves beneficial. This slide provides an exemplification of how such an analysis can be conducted, focusing on communities, and incorporating various factors and criteria, such as:

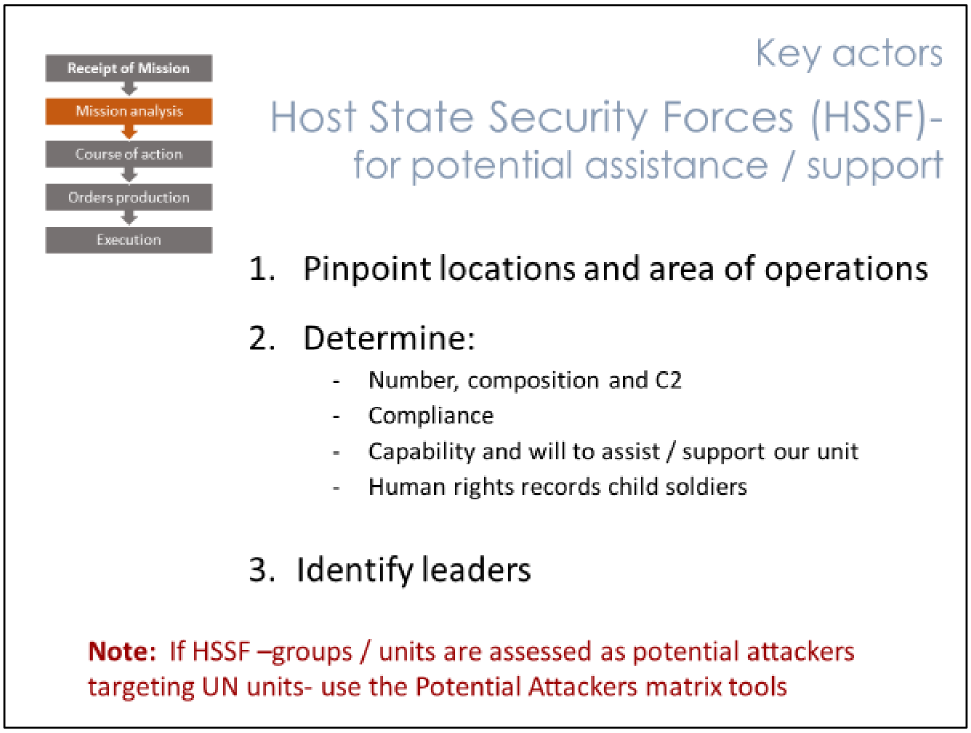
- Community identification: Clearly identify the specific communities under analysis
- Location: Determine the geographical locations of these communities
- Number and gender: Analyse the population size and breakdown by gender and Age composition
- Mandate compliance: Evaluate the extent to which the community adheres to the United Nations 'mandate and laws
- History/pattern of past violence: Study the community's historical background and patterns of violence
- Social media access and vulnerability to misinformation/disinformation: Explore the community's access to social media and assess their susceptibility to misinformation or disinformation campaigns Leverage; any influential factors

- Historical background patterns and history: Analyse the historical context and any recurring patterns
- Ease and access to weapons: Assess the community's accessibility to weapons and the ease with which they can obtain them

Additionally, recognising the value of gathering information from other mission and non-mission actors is crucial. Early consultation with these entities significantly strengthens military analysis and enhances overall comprehension of potential threats and adversaries. Moreover, the planning staff should familiarise themselves with diverse tools and resources available from peacekeeping-intelligence cells at all levels. These resources provide invaluable insights, peacekeeping-intelligence reports, and specialised knowledge, enabling a comprehensive and well-informed analysis of potential attackers.

By amalgamating these approaches, assimilating insights from multiple sources, and utilising tools such as tables and peacekeeping-intelligence products, we can achieve a more robust and effective understanding of potential adversaries. This heightened awareness will facilitate informed decision-making, strengthen operational preparedness, and ultimately contribute to the mission's success.

Slide 17



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Key actors

Host State Security Forces (HSSF)- for potential assistance / support

1. Pinpoint locations and area of operations
2. Determine:
   - Number, composition and C2
   - Compliance
   - Capability and will to assist / support our unit
   - Human rights records child soldiers
3. Identify leaders

Note: If HSSF –groups / units are assessed as potential attackers targeting UN units- use the Potential Attackers matrix tools

The subsequent phase of Mission Analysis involves the identification of host state security forces. These actors from the host government play a crucial role as they are responsible for ensuring access and protection for UN peacekeepers in carrying out their mandate. While this responsibility doesn't always materialise as desired, the host nation bears the primary responsibility.

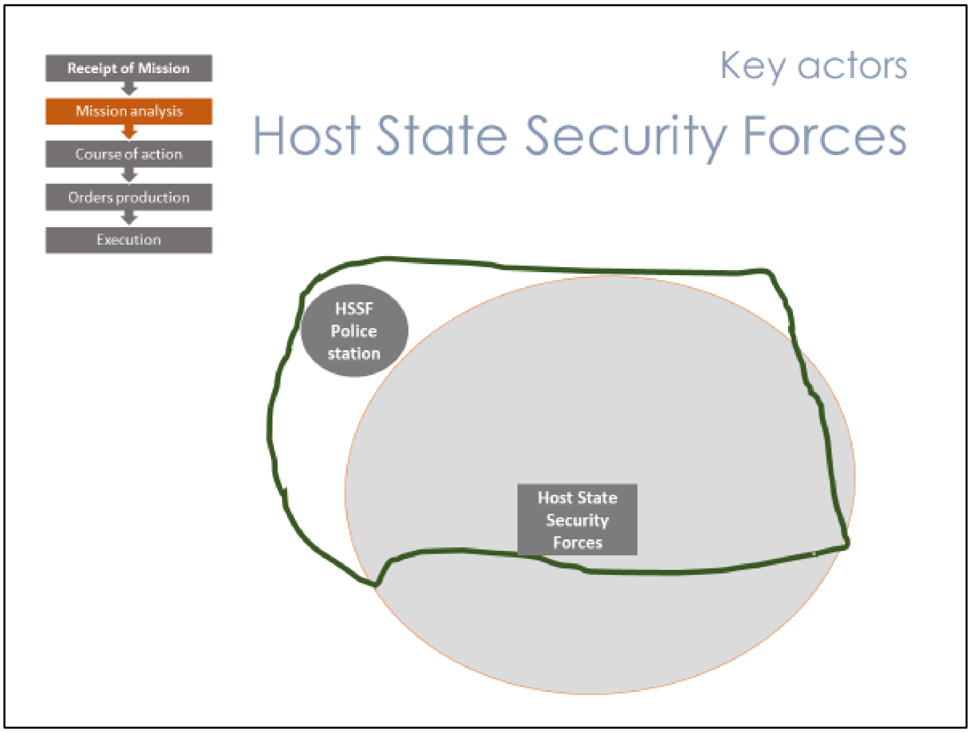
The impact of host state security forces on our unit's Framework for Protection (FP) hinges upon their capability and willingness to provide support and protection. Military planners, in collaboration with information provided by non-military mission components, need to assess these factors during the Mission Analysis stage. An essential aspect of this assessment is understanding the locations where these forces are positioned within the current and future areas of operations. The following elements need to be determined in relation to host state security forces:

- Number, composition: Type of unit, it make-up, size
- Command and control (C2): Evaluate the command structure and communications systems (well lead, organised or disorganised?)
- Compliance: The extent to which the host state security forces adhere to the UN-mandated responsibilities and guidelines

- Capability and willingness to assist: Have they supported in the past? Analyse the host state security forces' ability and willingness to provide support and assistance to UN peacekeepers
- Human rights records and use of child soldiers: Investigate the human rights records of the host state security forces and any involvement in the recruitment or use of child soldiers
- Identify the leaders: Identify key leaders within the host state security forces who hold positions of influence or decision-making authority

By considering these factors, military planners can gain a comprehensive understanding of the host state security forces' role and potential impact on the FP framework. This knowledge enables informed decision-making, resource allocation, and planning to ensure effective collaboration and security within the mission area.

Slide 18



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Key actors

Host State Security Forces

Similar to other previously identified key actors, the next crucial step is to ascertain the specific locations of the host state security forces in relation to our operations, both current and future, as well as the potential attackers. By mapping out the locations of these forces, military planners can streamline outreach efforts and gain a comprehensive understanding of areas that may potentially benefit from the protection or support provided by the host security forces. This knowledge allows for effective resource allocation and optimises the deployment of mission assets.

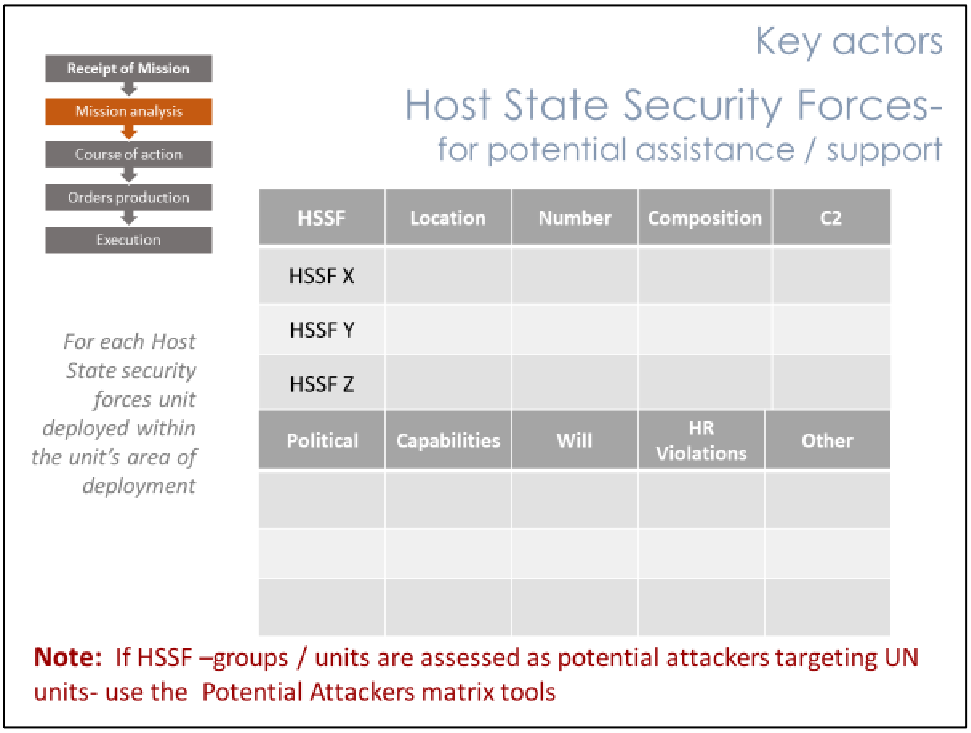
Mapping the locations of host state security forces offers several advantages. Firstly, it facilitates communication and collaboration between our forces and the host security forces, enabling a more seamless exchange of information, peacekeeping-intelligence, and operational coordination. By identifying areas where the host security forces are situated, military planners can establish lines of communication and engage in dialogue, fostering a stronger partnership in achieving common objectives.

Secondly, the mapping of host state security force locations provides insights into areas where potential protection or support from these forces can be leveraged. By understanding the proximity and coverage of host security forces, military planners can strategically allocate resources and prioritise operational activities. This enables mission assets to be freed up, allowing for their deployment to areas where their presence is most needed or where the potential threat from attackers is higher.

Furthermore, mapping these locations enhances situational awareness and operational preparedness. By visualising the geographic distribution of host state security forces, military planners gain a better understanding of the security landscape and potential gaps in coverage. This knowledge can inform operational planning, including the identification of areas that may require additional support measures.

In summary, mapping the locations of host state security forces relative to our operations and potential attackers offers numerous advantages. It streamlines outreach efforts, optimises resource allocation, fosters collaboration, and enhances situational awareness. By leveraging this information, military planners can make informed decisions, strengthen operational effectiveness, and ensure the safety and success of the mission.

Slide 19



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Key actors

Host State Security Forces- for potential assistance / support

For each Host State security forces unit deployed within the unit's area of deployment

HSSF	Location	Number	Composition	C2
HSSF X				
HSSF Y				
HSSF Z				

Political	Capabilities	Will	HR Violations	Other

Note: If HSSF –groups / units are assessed as potential attackers targeting UN units- use the Potential Attackers matrix tools

To enhance the systematic analysis of host state security forces, the use of a comprehensive table or matrix proves invaluable. This slide exemplifies how such an analysis can be conducted, here we are focusing on three distinct entities of host state security forces and incorporating some of the factors discussed in previous slides. It is crucial to conduct this analysis for all deployments of host state security forces within the areas of your unit's deployment, both current and future.

In addition to utilising a table or matrix, it is important to recognise that other mission and non-mission actors may possess valuable information. Early consultation with these entities strengthens the military analysis process and enhances the overall understanding of host state security forces. Here are the suggested factors and criteria to be used and analysed:

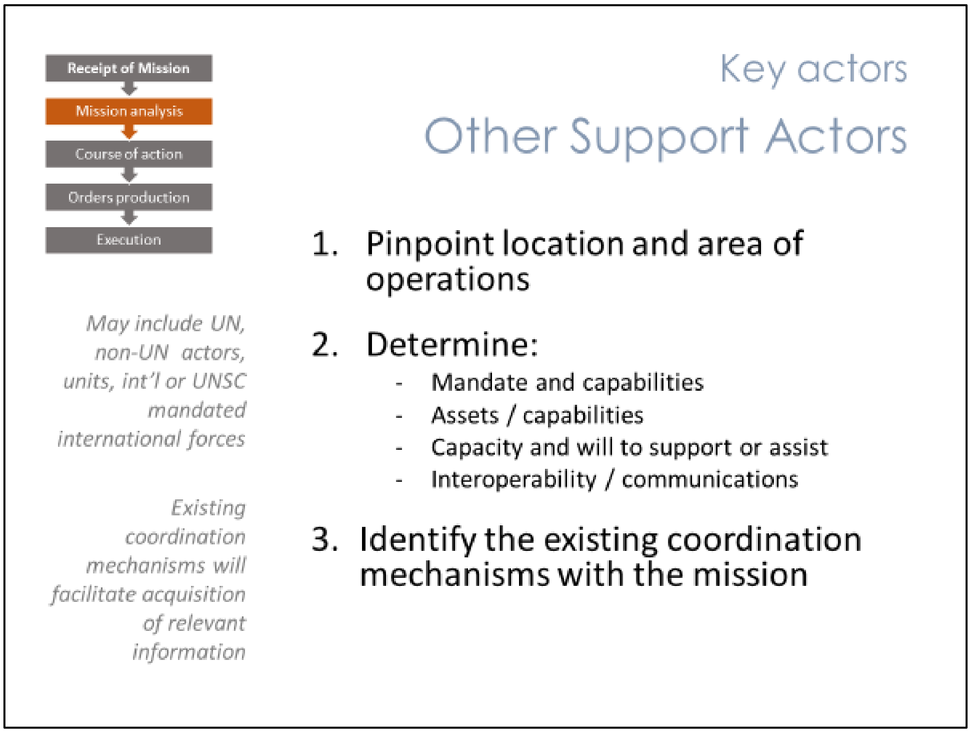
- Location: Determine the geographical locations where host state security forces are deployed
- Number and size: Assess the size and numerical strength of the host state security forces

- Composition: Evaluate the type of units, their makeup, and the equipment they possess
- Command and control (C2): Analyse the command structure and communication systems of the host state security forces. Assess whether they are well-led, organised, or disorganised
- Political affiliations: Consider any political affiliations that may impact the behaviour or effectiveness of the host state security forces
- Capabilities: Assess the special skills, abilities, and overall effectiveness of the host state security forces
- Willingness to assist: Analyse the historical track record of support provided by the host state security forces. Evaluate their ability and willingness to aid UN peacekeepers and UN operations.
- Human rights records and use of child soldiers: Investigate the human rights records of the host state security forces, particularly regarding any involvement in the recruitment or use of child soldiers or violence against civilians
- Other factors: Consider additional factors that the staff or UN unit commander deem important to the analysis based on the specific context of the mission

It is important to note that host state security forces can potentially become perpetrators or attackers. In such cases, it is essential to frame them as such in the mission analysis tools to accurately assess their impact on the operational environment.

By comprehensively analysing these factors and utilising appropriate mission analysis tools, a more robust understanding of host state security forces can be achieved. This knowledge supports informed decision-making, enhances FP tactical planning, and contributes to the overall success of the UN mission.

Slide 20



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

May include UN, non-UN actors, units, int'l or UNSC mandated international forces

Existing coordination mechanisms will facilitate acquisition of relevant information

Key actors

Other Support Actors

1. Pinpoint location and area of operations
2. Determine:
   - Mandate and capabilities
   - Assets / capabilities
   - Capacity and will to support or assist
   - Interoperability / communications
3. Identify the existing coordination mechanisms with the mission

In addition to Peacekeeping Operations, there are various other forces and security actors present in the mission area of operations. The next crucial step in Mission Analysis is to identify these actors who can contribute to and support our Framework for FP efforts. This list includes a range of entities such as Mission assets, other UN agencies (e.g., UNMAS), units and assets from Sector and Force HQs, international security forces, regional partners involved in security and safety, the UN Country Team, non-UN humanitarian partners, international and national NGOs, and other international forces authorised by the UN Security Council. Also, a key component is your Higher HQs' units and assets available that can provide support.

Similar to the process followed for other key actors, the initial step is to determine the locations and areas of influence of these additional actors. The following information needs to be determined:

- Exact mandate: Understand the specific mandate of each protection actor and assess whether they have the authority or legal bases to support and that they possess the necessary capabilities to effectively carry out support efforts within their mandate

- Capacity and willingness to support: Assess the capacity, availability, and willingness of these actors to provide support to peacekeeping operations. This includes their readiness to collaborate and contribute to the FP framework

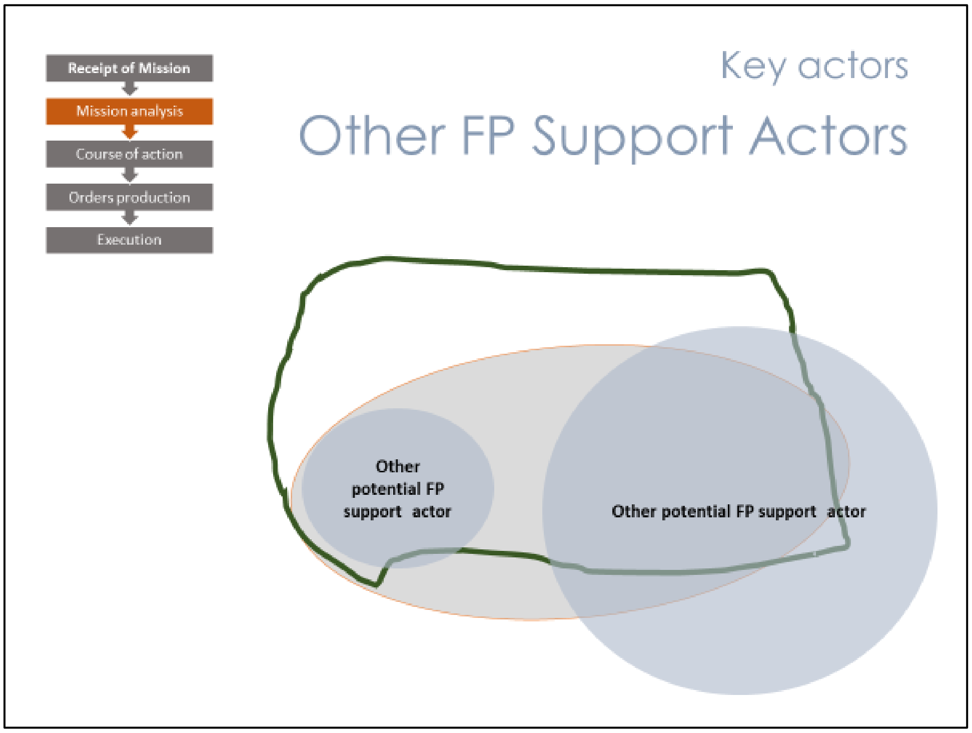
- Interoperability/communications: Evaluate the interoperability and communication capabilities between these actors and peacekeeping operations. Assess the extent to which they can effectively coordinate and exchange information

- Reliance on peacekeeping support: Determine whether these actors rely on peacekeeping support to carry out their mandate or if they operate independently

The necessary information for identifying these other protection actors can be gathered from various sources. Peacekeeping missions typically have established coordination mechanisms that facilitate outreach and information collection regarding the capabilities of these actors. To maximise the potential of complementary activities, planners need to coordinate and engage with the relevant protection actors in the areas where they may operate. Additionally, Force HQs and Sector HQs may have established support arrangements or Standard Operating Procedures (SOPs) that involve attaching or providing support units (e.g., Explosive Ordnance Disposal, Convoy Security Detachments, etc.).

By understanding the capabilities, mandates, and potential areas of collaboration with these additional support actors, military planners can effectively coordinate efforts, optimise resources, and enhance the overall effectiveness of the FP planning. This coordination ensures a holistic approach to security and protection within the mission area, ultimately contributing to the success of the peacekeeping mission.

Slide 21



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

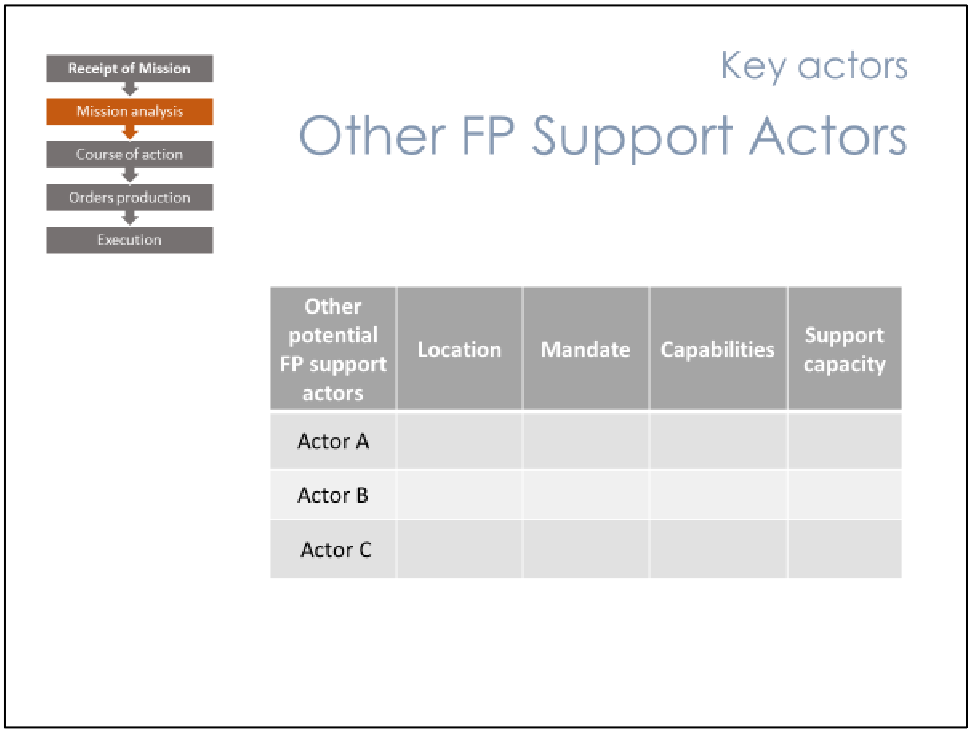
Key actors

Other FP Support Actors

Other potential FP support actor
Other potential FP support actor

Just like with the other key actors previously identified, the subsequent step involves determining the locations of other FP support actors. By mapping out these locations, military planners can streamline outreach efforts and gain a clear understanding of which areas might benefit from the protection provided by these additional security forces. This information will enable them to optimise the allocation of mission assets, ensuring that areas with limited or no coverage will need additional resources, while freeing up unit assets for other areas where support is provided. This approach to resource allocation enhances the overall effectiveness of force protection mitigation measures and contributes to the success of the mission.

Slide 22



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Key actors

Other FP Support Actors

Other potential FP support actors	Location	Mandate	Capabilities	Support capacity
Actor A				
Actor B				
Actor C				

To enhance the systematic analysis of other FP support actors, utilising a comprehensive table / matrix proves invaluable. This slide presents an exemplary analysis of three distinct protection actors, labelled as A, B, and C, incorporating the factors discussed in previous slides. Such an analysis should be conducted for all relevant support actors within your area of operations. The following factors should be considered and analysed:

Location: Determine the geographical locations of the protection actors in relation to your operational area. Assess the time and distance required for their support to reach different areas, considering the ease of accessibility and coordination.

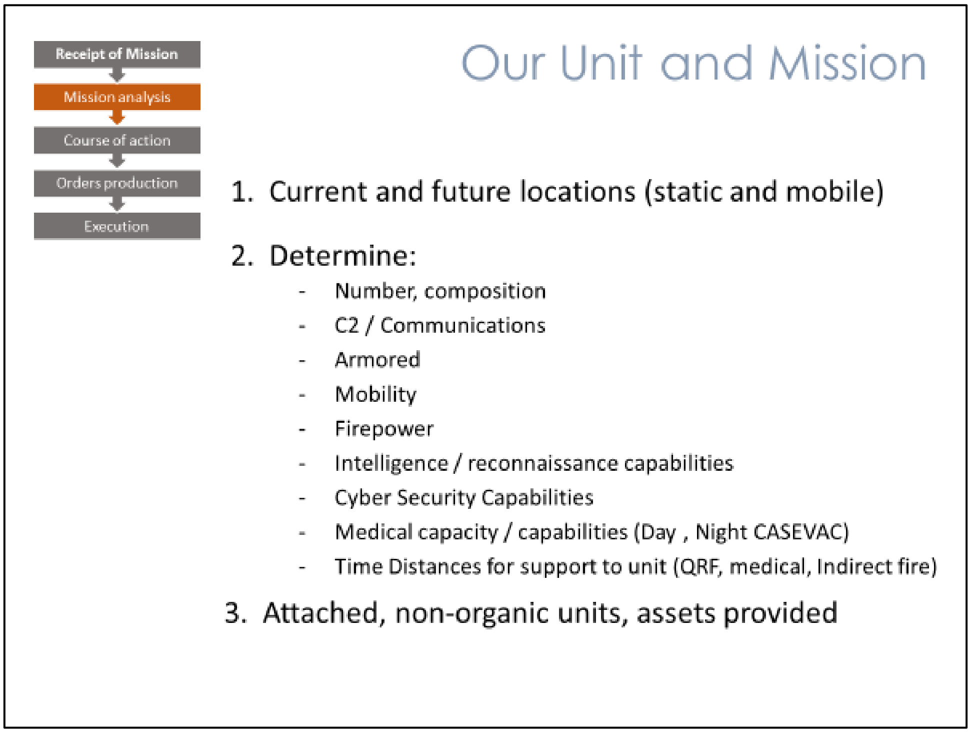
Mandate: Evaluate whether these actors possess the necessary mandate and authorisation to provide support within the context of the mission. Examine the legal bases that govern their mission and enable them to help.

Capabilities: Assess the organisational structure, equipment, and skills of the protection actors. Determine whether they possess the required capabilities to effectively carry out the tasks and responsibilities expected of them.

Support capacity: Analyse the capacity of these actors to allocate resources and personnel to fulfil their own mission while simultaneously providing support to your operations. Evaluate their ability to balance their commitments and commitments to supporting your mission.

By employing a table format to organise and evaluate these factors, military planners can gain a comprehensive understanding of the various support actors and their potential contributions. This analytical approach enables informed decision-making and facilitates effective coordination between different actors, ensuring optimal utilisation of resources and enhancing the overall effectiveness of the mission's FP efforts.

Slide 23



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Our Unit and Mission

1. Current and future locations (static and mobile)
2. Determine:
   - Number, composition
   - C2 / Communications
   - Armored
   - Mobility
   - Firepower
   - Intelligence / reconnaissance capabilities
   - Cyber Security Capabilities
   - Medical capacity / capabilities (Day , Night CASEVAC)
   - Time Distances for support to unit (QRF, medical, Indirect fire)
3. Attached, non-organic units, assets provided

During the Mission Analysis phase, it is vital to evaluate the assigned task and assess your unit's capability and preparedness to fulfil it. This assessment also helps identify and provide a baseline for analysing potential vulnerabilities that may be exploited by potential attackers. To ensure effective force protection planning (FP), consider the following factors:

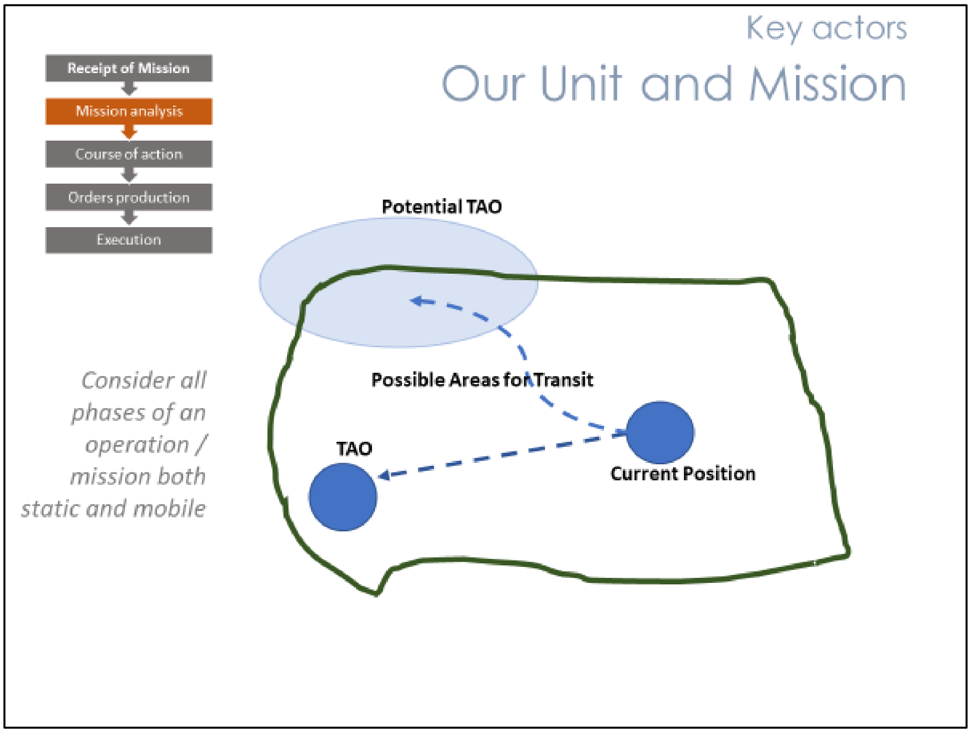
- Number and Composition: Determine the minimum required elements for a tactical deployment, including the appropriate size and composition of your unit
- Command and Control (C2) / Communications: Evaluate the effectiveness of your unit's C2 structure and its communication capabilities. Ensure that reliable and secure communication channels
- Armoured Capability: Assess the availability and suitability of armoured vehicles or equipment to enhance the protection of your unit against direct and indirect fires during deployments and operations
- Mobility: Evaluate the mobility of your unit, including the availability of vehicles and assets to facilitate rapid movement and response times
- Firepower: Consider the firepower capabilities of your unit, including the weapons and ammunition available to effectively respond to and neutralise threats

- Intelligence / Reconnaissance Capabilities: Assess the unit's peacekeeping-intelligence gathering and reconnaissance capabilities to gather essential information on potential threats and enhance situational awareness
- Cyber Security Capabilities: Evaluate the unit's cyber security / operational security measures to mitigate risks associated with cyber-attacks and ensure the security of the unit's communication and information systems.
- Medical Capacity / Capabilities: Determine the unit's medical resources, both during the day and at night, including the ability to provide casualty evacuation (CASEVAC)
- Time and Distance to Support: Consider the proximity and response time of supporting elements such as Quick Reaction Forces (QRF), medical support, and indirect fire support. Evaluate the effectiveness of these resources in providing timely assistance to your unit

Additionally, it is essential to assess the capabilities and resources provided by non-organic / attached units or assets. Consider how these additional resources can enhance your unit's overall force protection capabilities and contribute to mission success.

By thoroughly evaluating these factors, military planners can identify any gaps in force protection capabilities and make informed decisions regarding resource allocation, training, and operational strategies. This comprehensive assessment ensures that the unit is adequately prepared and equipped to fulfil its mission.

Slide 24



Key actors

Our Unit and Mission

Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Consider all phases of an operation / mission both static and mobile

Time / Distance is a crucial factor in tactical level planning as it directly impacts operational considerations. By mapping the locations within the area of operations, a clear visualisation of spatial relations can be obtained, aiding in effective force protection planning. When developing a force protection plan, it is important to consider the three phases of an operation:

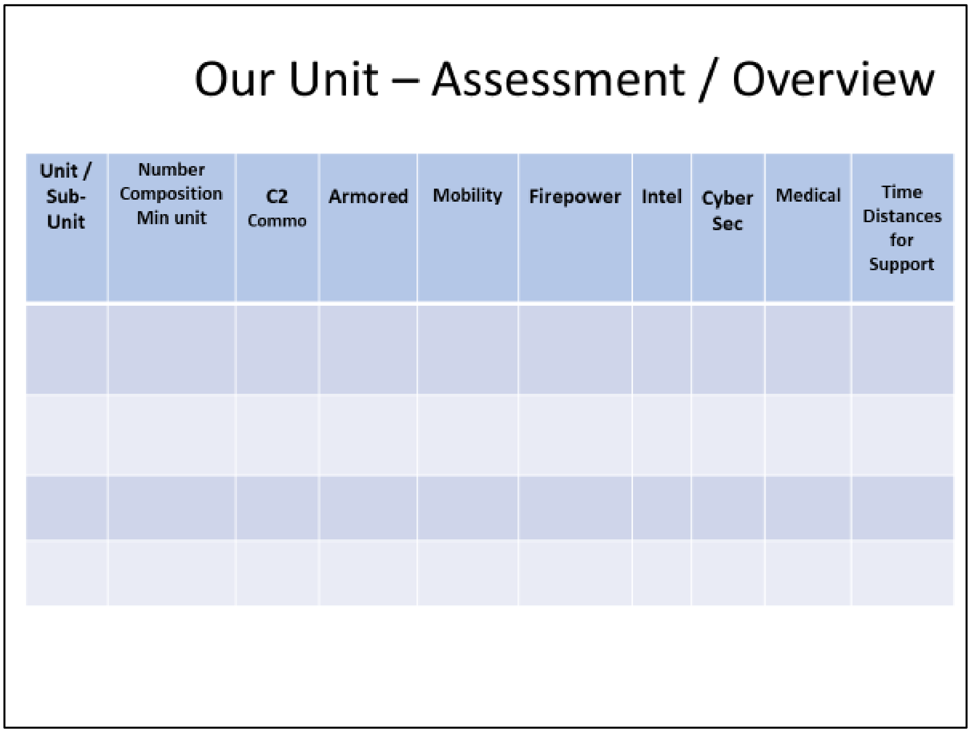
Phase 1: Current Location/Deployment
In this phase, the focus is on assessing the force protection mitigation requirements and vulnerabilities at the unit's current location or deployment site. Factors such as physical security measures, defence plans, communication systems, and access control need to be analysed to ensure the security of unit personnel and assets.

Phase 2: Transit
During the transit phase, careful consideration must be given to how the unit will travel from its current location to the designated area of operation. It is crucial to identify the routes, means of transportation, and potential risks associated with the movement.

Phase 3: Future Tactical Area of Operation (TAO)
In the future TAO or potential TAO, the force protection plan needs to account for the specific challenges and risks present in that area. Factors such as the local security environment, terrain characteristics, and the presence of potential threats should be assessed. Adequate force posture, security measures, and peacekeeping-intelligence-gathering efforts should be integrated into the plan to ensure the unit's mission success.

Expanding on these three phases provides a comprehensive understanding of the force protection requirements at different stages of the operation. By carefully considering the unique aspects and challenges of each phase, military planners can develop a robust force protection plan that addresses specific needs and effectively mitigates the risks to personnel, equipment, and mission objectives throughout the entire operation.

Slide 25



Our Unit – Assessment / Overview

Unit / Sub-Unit	Number Composition Min unit	C2 Commo	Armored	Mobility	Firepower	Intel	Cyber Sec	Medical	Time Distances for Support

To facilitate a comprehensive analysis of our unit, the utilisation of a table proves valuable. The following example presents an analysis of the unit's capabilities, encompassing all subunits, subordinate units, attached elements, and units assigned as direct support. The analysis should consider the following factors:

Number and Composition:
Assess the total number of personnel and the composition of the unit, including its minimal unit of deployment. Understanding the organisational structure and personnel resources is essential for effective planning.

Command and Control (C2) and Communications:
Evaluate the unit's command structure, leadership, and communication systems. A robust C2 framework is crucial for efficient coordination and decision-making processes within the unit.

Armoured Assets:
Identify the type of armoured assets available to the unit and assess their capabilities. Understanding the level of protection and mobility provided by armoured vehicles is vital for force protection planning.

Mobility:
Evaluate the unit's mobility capabilities, including transportation assets and equipment. Consider the ability to manoeuvre swiftly and effectively in different terrain, weather and operational environments.

Firepower:
Assess the unit's firepower capabilities, including small arms, heavy weapons, and supporting assets such as artillery or air support. Understanding the unit's offensive and defensive firepower is crucial for mission success and force protection.

Intelligence:
Consider the unit's peacekeeping-intelligence capabilities, including its ability to gather, process, and analyse relevant information. peacekeeping-intelligence support enhances situational awareness and enables decision-making.

Cyber and Operational Security:
Evaluate the unit's cyber and operational security measures to protect against potential threats in the digital and communications network domains. Assessing vulnerabilities and implementing appropriate mitigation measures is essential for mission success.

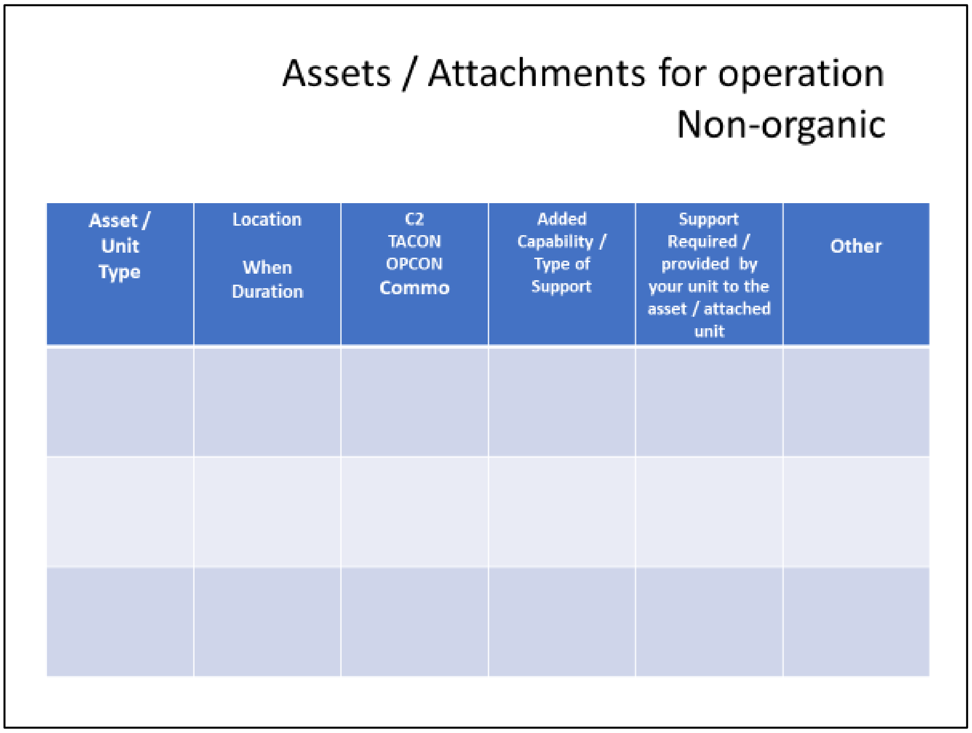
Medical Assets and Capability:
Assess the unit's medical assets, both internal and assigned or available from higher headquarters. Consider the unit's medical capabilities, including emergency medical treatment, casualty evacuation (CASEVAC), and medical support for both routine and operational emergency-related injuries.

Time Distance for Support:
Evaluate the time distance associated with the unit's ability to receive support from Quick Reaction Forces (QRFs), indirect fire support, air support, logistics resupply, or other support elements. Understanding the response time and availability of necessary support resources is critical for force protection and operational success.

By systematically analysing these factors and documenting them in a table / matrix, military planners can gain a comprehensive understanding of the unit's capabilities. This process also establishes a baseline / foundation for conducting a compare and contrast assessment, evaluating potential vulnerabilities against identified threats (which will be further discussed in the risk analysis phase).

This approach empowers informed decision-making, allowing military planners to make well-founded choices based on a comprehensive understanding of the unit's ability to execute a mission and provide the framework for FP planning. It also facilitates optimised resource allocation, ensuring that the necessary assets and support are allocated where they are most needed.

Slide 26



Assets / Attachments for operation
Non-organic

Asset / Unit Type	Location When Duration	C2 TACON OPCON Commo	Added Capability / Type of Support	Support Required / provided by your unit to the asset / attached unit	Other

To facilitate a systematic assessment, it is crucial to analyse the non-organic support units/assets assigned to or attached to our unit by higher headquarters. Developing a table can be a valuable tool in this process. The following example table demonstrates its usefulness.

There are various other UN units provided to us for operations either through standard operating procedures (SOPs) or specific assignments. Identifying these actors / units and their potential contributions to our force protection (FP) planning framework is a critical step in the Mission Analysis. These entities may include assets like Explosive Ordnance Disposal (EOD) teams, military police units, and convoy security teams.

Similar to the approach followed for other key actors, the initial step is to determine the type of unit and the specific support they will provide, as well as their locations. However, there are additional factors to consider:

Duration of support or attachment timeline: Assessing how long the support will be provided and understanding the duration of the support, as well as the process of how and where they will link-up or integrate with our unit.

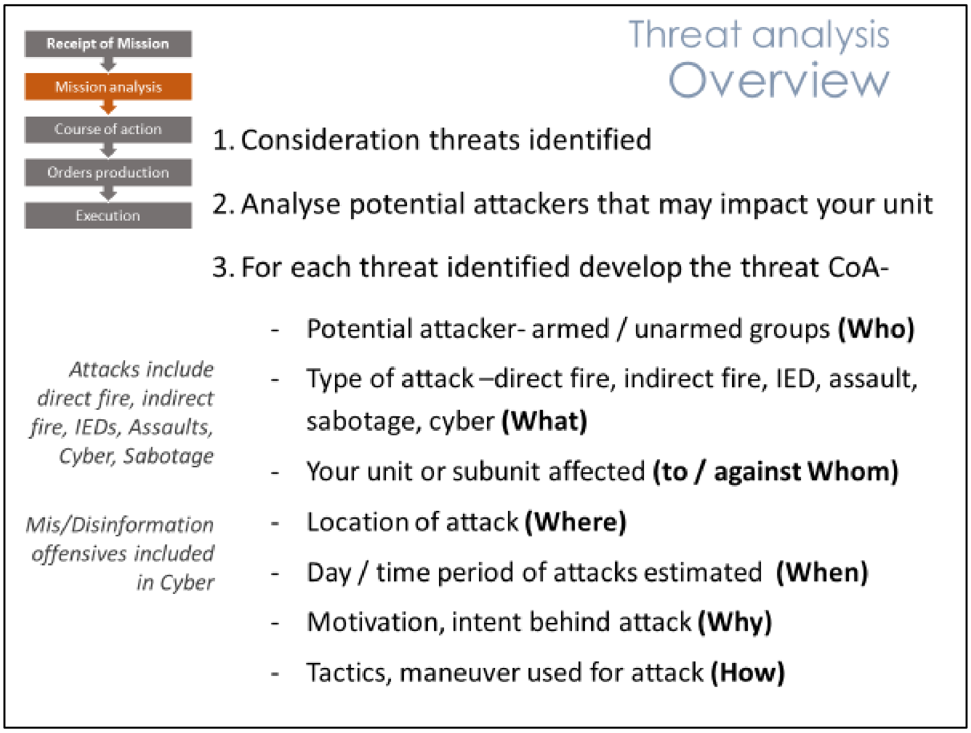
Command and control: Clarifying the command structure and relationship, including whether they will be attached, operationally controlled (OPCON), tactically controlled (TACON), or under a different command relationship / arrangement.

Additional support requirements: Identifying any specific support that our unit will need to provide to these non-organic units, such as security for an EOD team during an IED neutralisation / disposal operation.

Other relevant factors: Considering any other factors that the commander or staff deem important for assessing and analysing the supporting units.

By conducting a comprehensive analysis of these non-organic / attached support units, we can better understand their capabilities, determine their integration within our unit, and ensure effective coordination and collaboration. This analysis will contribute to a more robust force protection plan and enable successful mission execution.

Slide 27



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Threat analysis
Overview

1. Consideration threats identified
2. Analyse potential attackers that may impact your unit
3. For each threat identified develop the threat CoA-

- Potential attacker- armed / unarmed groups **(Who)**
- Type of attack –direct fire, indirect fire, IED, assault, sabotage, cyber **(What)**
- Your unit or subunit affected **(to / against Whom)**
- Location of attack **(Where)**
- Day / time period of attacks estimated **(When)**
- Motivation, intent behind attack **(Why)**
- Tactics, maneuver used for attack **(How)**

Attacks include direct fire, indirect fire, IEDs, Assaults, Cyber, Sabotage

Mis/Disinformation offensives included in Cyber

Identifying and analysing the various Key Actors and the associated components in your unit areas of deployment, transit, and future or potential Tactical Areas of Operations (TAOs), the next crucial step is to conduct an analysis of the specific threats that can impact your unit's operations. This analysis forms the basis for formulating a comprehensive force protection (FP) plan aimed at mitigating risks.

In this process, the unit planners are required to make a predictive analysis. Predictive analysis is the process of using the factors we have discussed, the data, historical patterns, and analytical techniques to forecast future events and outcomes. In the context of force protection planning, it involves analysing those factors such as key actors, affected units, locations, timing, motivations, and tactics to make informed predictions. Commanders and staff utilise this analysis to anticipate / identified threats. However, it is important to recognise that predictive analysis is based on available information and assumptions, and unexpected developments can still occur.

When identifying and examining the threats, it is essential to consider those that have already been identified at the Mission, Force and Sector HQs levels that are applicable to your area of operations. For each threat, the following factors should be determined:

- Situation and type of threat (What): Clearly define the nature and characteristics of the threat, identifying the specific type of attack that may be encountered

- Potential attackers (Who): Identify the groups responsible for posing the attack. This includes understanding their motivations, ideologies, affiliations, and any known patterns of behaviour

- Units or subordinate units potentially affected (Against whom): Determine which units or subordinate elements of your own force may be targeted or affected by the attack

- Area / location where your unit may be targeted (Where): Identify the geographical locations or specific areas where your unit may be targeted

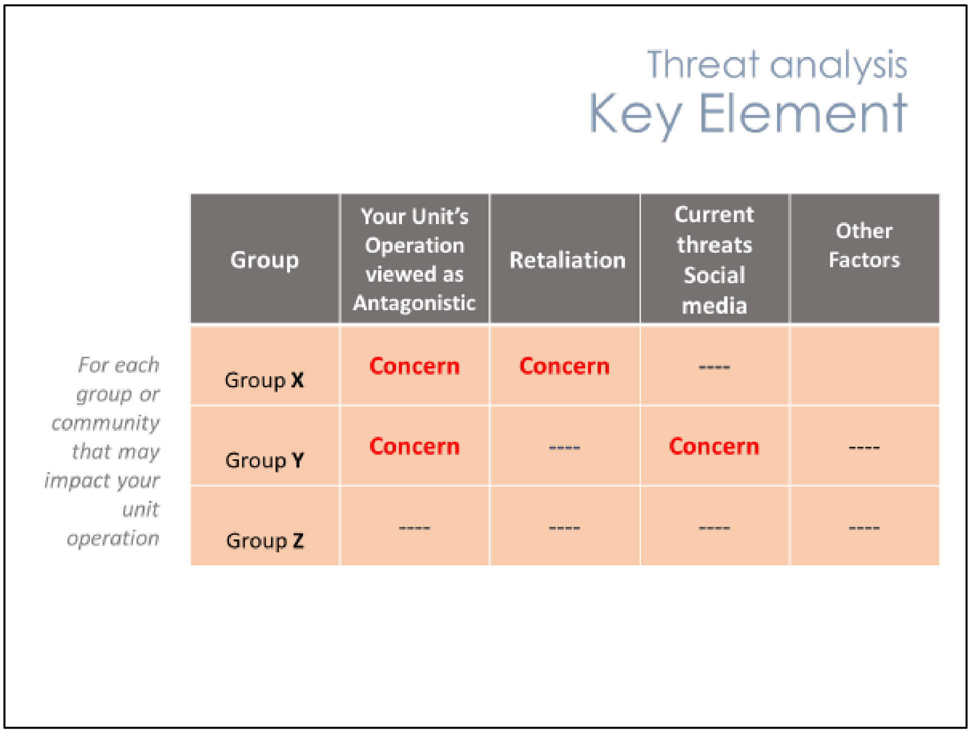
- Days and time of day attacks are most likely (When): Assess the patterns or preferences regarding the timing and frequency of attacks associated with the attackers / group. This includes considering specific days of the week or times of day when attacks are more likely to occur

- Motivation behind physical violence (Why): Understand the underlying motivations driving the potential attackers to engage in the violence. This may include factors such as political, ideological, religious, or economic motivations

- Possible movements and tactics of groups (How): Analyse the potential movements and tactics that the groups associated with the attack may employ. This includes their methodology and any known patterns or trends

By thoroughly examining these aspects for each identified threat, military planners can gain a comprehensive understanding of the potential risks and challenges they may face. This analysis serves as the foundation for developing a robust and effective force protection plan that addresses the specific threats and mitigates the risks.

Slide 28



Threat analysis

Key Element

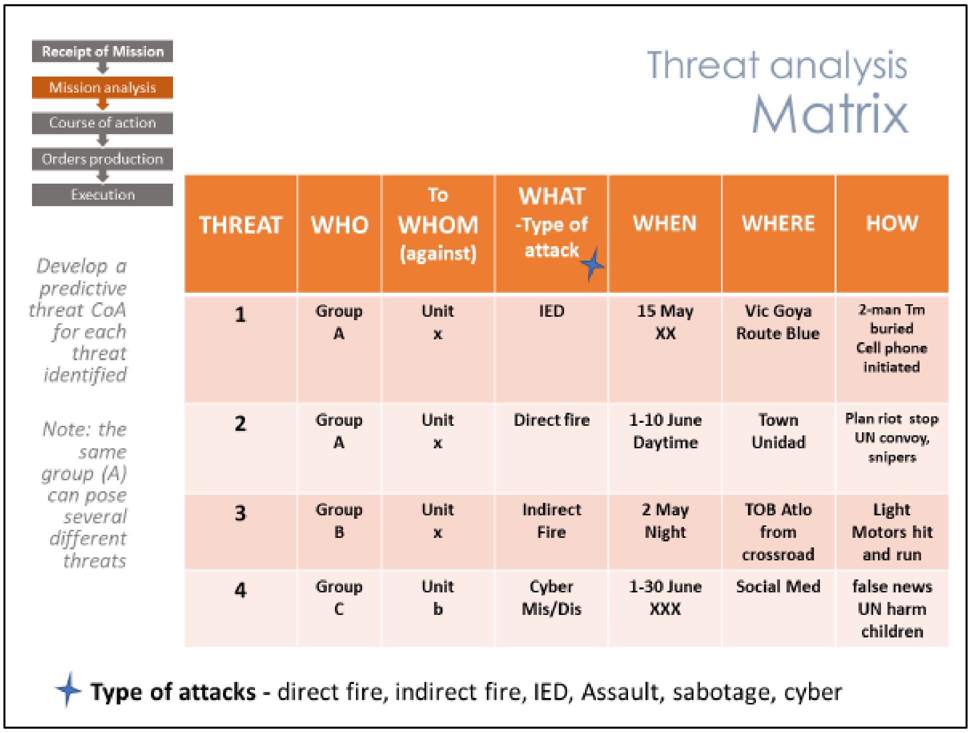
For each group or community that may impact your unit operation

Group	Your Unit's Operation viewed as Antagonistic	Retaliation	Current threats Social media	Other Factors
Group **X**	Concern	Concern	----	
Group **Y**	Concern	----	Concern	----
Group **Z**	----	----	----	----

Threat analysis in force protection planning extends beyond identifying potential attackers and assessing their capabilities. It is essential to evaluate the relationships between the United Nations and the various actors or groups present in the area of operations. This analysis involves understanding how the UN's operations might impact or be perceived by these actors / groups, considering the potential for retaliatory acts.

In this regard, analysing the information terrain, including social media, can provide valuable insights into attitudes towards the UN and its operations within the vicinity of these groups. Assessing the dynamics between groups is also crucial, as conflicts between groups can directly or indirectly pose threats to UN forces and the stability in the area of operations. By comprehensively considering these key elements / factors, force protection planners can better anticipate and analyse the threats' potential and impacts on our operations.

Slide 29



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Threat analysis Matrix

Develop a predictive threat CoA for each threat identified

Note: the same group (A) can pose several different threats

THREAT	WHO	To WHOM (against)	WHAT -Type of attack ✦	WHEN	WHERE	HOW
1	Group A	Unit x	IED	15 May XX	Vic Goya Route Blue	2-man Tm buried Cell phone initiated
2	Group A	Unit x	Direct fire	1-10 June Daytime	Town Unidad	Plan riot stop UN convoy, snipers
3	Group B	Unit x	Indirect Fire	2 May Night	TOB Atlo from crossroad	Light Motors hit and run
4	Group C	Unit b	Cyber Mis/Dis	1-30 June XXX	Social Med	false news UN harm children

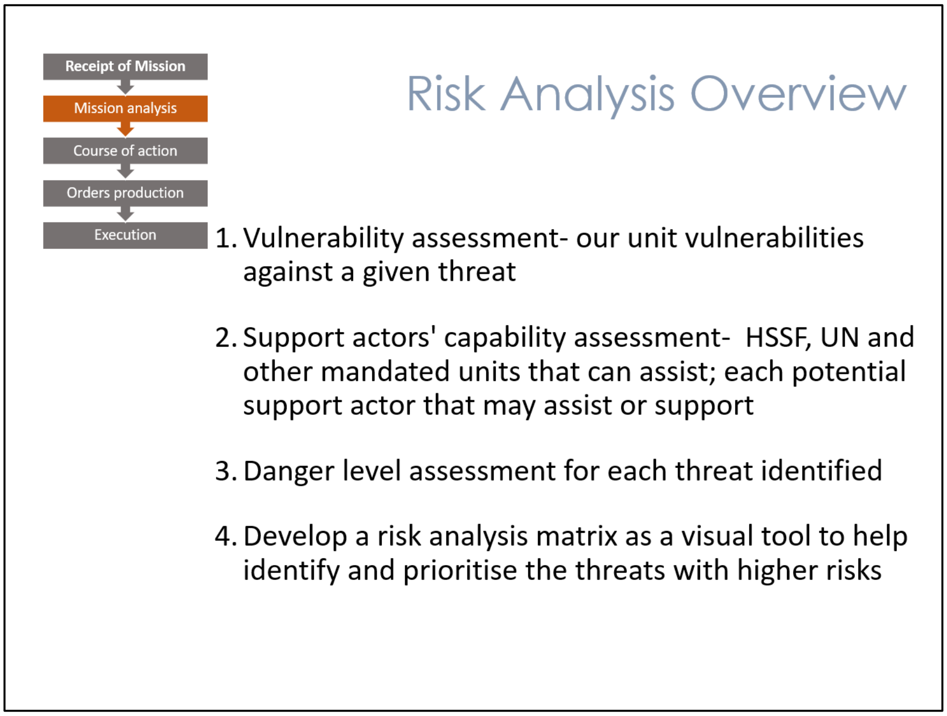
✦ **Type of attacks -** direct fire, indirect fire, IED, Assault, sabotage, cyber

The predictive analysis we discussed earlier plays a crucial role in this stage. By gathering information and conducting a systematic and comprehensive threat analysis, we can now tabulate each identified threat on a matrix. This matrix allows us to break down each threat into specific courses of action (COA) using the 5W framework. It serves as a useful tool for organising and analysing the identified threats. It is important to note that a single group may pose multiple distinctive threats (COA), which should be identified separately in the matrix. For example, Group “A” demonstrates two separate threats.

In the “What” or type of attack column of the matrix, we specify the group’s method or type of attack, which may include a combination of different approaches. We categorise and define six types of attacks discussed in Module One lessons: direct fire, indirect fire, assault, IED, sabotage, and cyber. It is crucial to recognise that a group may utilise a combination or complex attack by employing several of these methods sequentially or simultaneously.

Having developed and codified the threat COAs, the focus now shifts to risk analysis. With the potential threats identified, it becomes necessary to assess the risks associated with each threat and develop response options. This risk analysis aims to determine the likelihood and potential impact of each threat, enabling the formulation of effective response strategies.

Slide 30



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Risk Analysis Overview

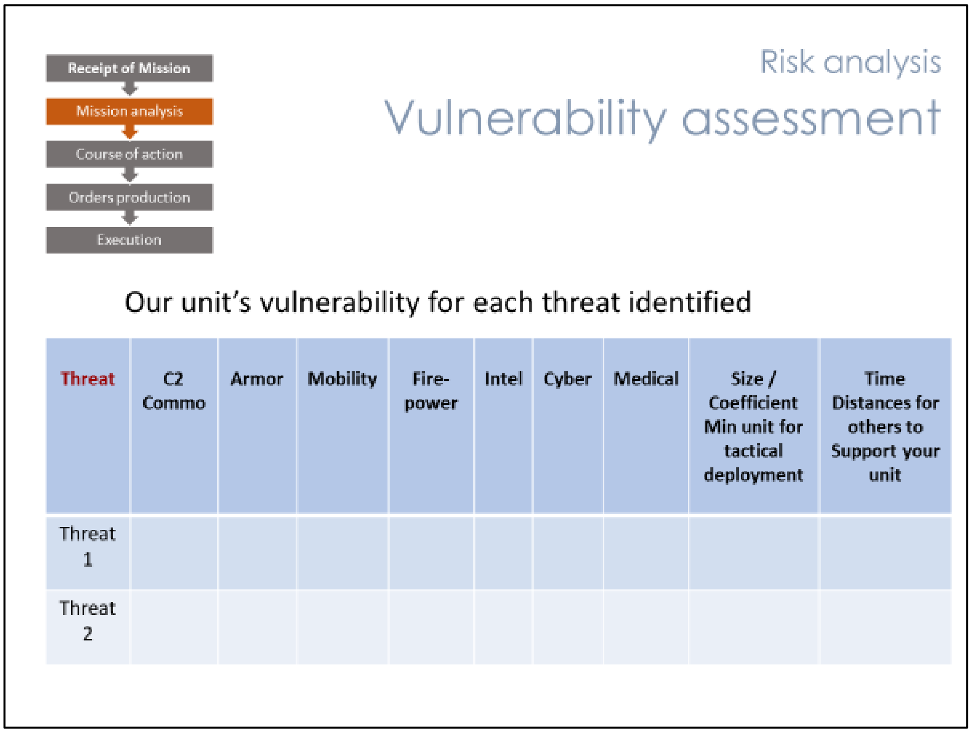
1. Vulnerability assessment- our unit vulnerabilities against a given threat
2. Support actors' capability assessment- HSSF, UN and other mandated units that can assist; each potential support actor that may assist or support
3. Danger level assessment for each threat identified
4. Develop a risk analysis matrix as a visual tool to help identify and prioritise the threats with higher risks

After conducting a thorough threat analysis, focusing on identified groups that pose a threat to our unit, the next crucial step is to assess these threats in terms of risk. This entails conducting a comprehensive assessment for each identified threat, carefully considering and likelihood to occur and on their potential impact on our operations.

Additionally, we evaluate our vulnerabilities and the level of danger associated with each threat, considering various factors. This assessment allows us to understand the potential severity of each threat. Furthermore, we identify potential support actors who can assist us in our operations, such as UN units / forces, local security forces, or specialised units. Their involvement can contribute to enhancing our capabilities.

To effectively manage, categorise and prioritise these threats, we develop a risk analysis matrix. This matrix provides a visual representation of the likelihood and impact of each threat on our unit. It serves as a valuable tool for decision-making, enabling us to allocate resources and implement appropriate measures to address the most significant risks we face.

Slide 31



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Risk analysis

Vulnerability assessment

Our unit's vulnerability for each threat identified

Threat	C2 Commo	Armor	Mobility	Fire-power	Intel	Cyber	Medical	Size / Coefficient Min unit for tactical deployment	Time Distances for others to Support your unit
Threat 1									
Threat 2									

To conduct a thorough vulnerability assessment, we compare and contrast our unit against the identified threats. This assessment is facilitated by a table of results, which serves as a tool to establish our vulnerabilities against the threat. It is important to note that different units may have varying degrees of vulnerability to specific threats based on their unique characteristics and capabilities. For example, an unarmoured wheeled transportation unit may be more vulnerable to certain threats compared to others.

It is crucial to recognise that vulnerability is a dynamic concept influenced by various factors, including changing circumstances and specific operational contexts. Our vulnerability assessment is based on a careful evaluation of our measured capabilities in relation to each identified threat. The factors considered in assessing vulnerability include:

Command and Control (C2): This factor assesses the effectiveness and efficiency of our unit's command and control structure. It evaluates the ability to coordinate and communicate orders, directives, and information within the unit and with higher headquarters. A robust and well-functioning C2 system ensures timely decision-making and effective response to threats.

Communications capabilities: This factor examines the reliability and security of our unit's communication systems. It includes assessing the availability of communication equipment, such as radios, satellites, and data networks, and evaluating their resilience against disruptions or electronic warfare threats. Effective and secure communication is essential for maintaining situational awareness and coordinating responses.

Armour protection: This factor focuses on the level of armour protection available to our unit. It considers the types of armoured vehicles or equipment at our disposal and evaluates their effectiveness in mitigating the risks posed by specific threats, such as direct fire or explosive attacks. Adequate armour protection enhances the survivability of our forces in hostile environments.

Mobility capabilities: This factor analyses our unit's ability to move swiftly and effectively within the operational area. It considers the types of vehicles, equipment, and transportation assets available and assesses their mobility characteristics, such as speed, off-road capabilities, and range. Mobility is critical for manoeuvring and avoiding potential threats.

Firepower capabilities: This factor evaluates our unit's offensive and defensive firepower capabilities. It assesses the types of weapons, ammunition, and supporting systems available and their effectiveness in engaging and neutralising threats. Robust firepower enhances our ability to deter or respond to hostile actions.

Intelligence gathering and situational awareness: This factor focuses on our unit's ability to collect, analyse, and disseminate peacekeeping-intelligence information. It considers the availability of surveillance assets, reconnaissance capabilities, and peacekeeping-intelligence support networks. Effective peacekeeping-intelligence gathering and situational awareness enable us to anticipate and proactively respond to threats.

Cybersecurity and operational security measures: This factor addresses the protection of our unit's information systems, networks, and sensitive data. It includes evaluating cybersecurity and operational security practices. Strong cybersecurity and operational security measures safeguard against cyber threats and unauthorised access to critical information and communication networks.

Medical capabilities: This factor assesses our unit's medical resources and capabilities to provide adequate healthcare and casualty management. It includes evaluating the availability of medical personnel, equipment, facilities, and evacuation procedures. Robust medical capabilities contribute to the preservation of personnel and the prompt treatment of injuries or medical emergencies.

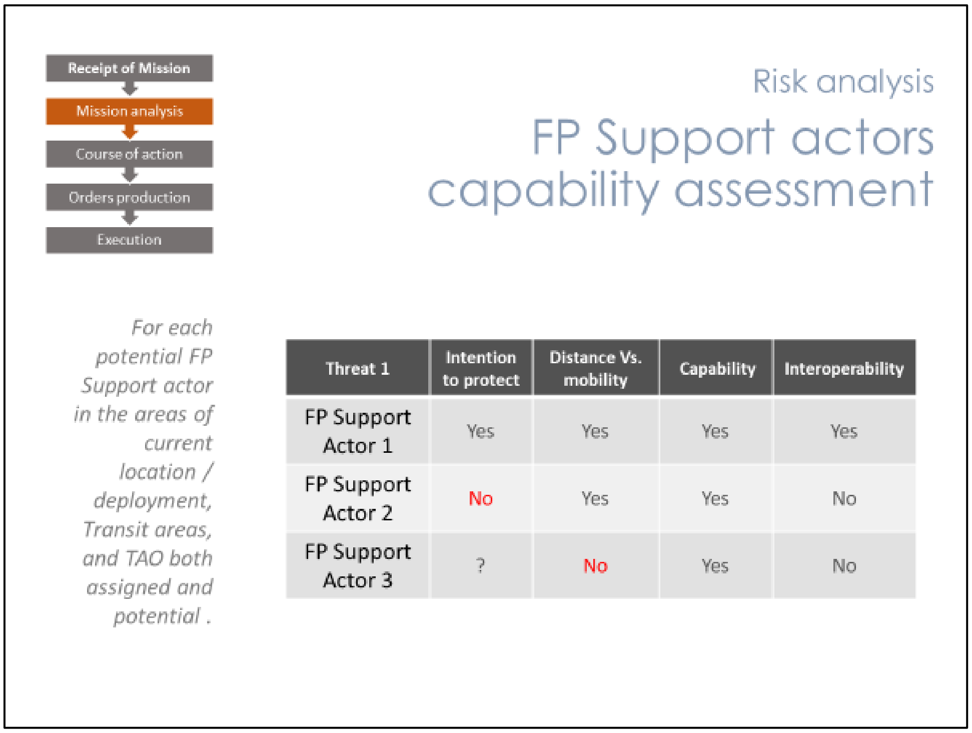
Coefficient of forces and minimum unit of deployment: This factor considers the composition and size of our unit. It evaluates the ratio between our units / forces against potential threats, as well as the minimum operational unit required for deployment. Understanding the coefficient of forces helps determine the unit's ability to withstand or counter threats effectively.

Time and distance for support: This factor examines the estimated time and distance required for support to reach our unit in case of emergencies or reinforcement needs. It considers the availability of quick reaction forces, medical evacuation assets, and logistical support. Minimising the response time and distance enhances our unit's resilience and effectiveness.

Unit isolation or density within the operational area: This factor assesses the proximity and interaction of our unit with other UN units or host nation security forces within the operational area. It considers whether our unit operates in isolation or as part of a larger force, as well as the potential implications for security and support. Unit isolation may increase vulnerability, while higher density can provide mutual support and protection.

By evaluating these factors in the vulnerability assessment, we gain insights into our unit's strengths, weaknesses, and areas that require additional attention. This information enables us to develop appropriate risk mitigation strategies and allocate resources effectively to enhance our overall FP.

Slide 32



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Risk analysis

FP Support actors capability assessment

For each potential FP Support actor in the areas of current location / deployment, Transit areas, and TAO both assigned and potential .

Threat 1	Intention to protect	Distance Vs. mobility	Capability	Interoperability
FP Support Actor 1	Yes	Yes	Yes	Yes
FP Support Actor 2	No	Yes	Yes	No
FP Support Actor 3	?	No	Yes	No

To gain a comprehensive understanding of the risk levels involved, peacekeepers must conduct an analysis of the capabilities of other protection actors. This analysis involves assessing various factors related to these actors' ability to provide support.

Firstly, their intention to protect is evaluated. This refers to their commitment and willingness to actively engage in protecting the mission and its personnel. Understanding their level of dedication helps determine the extent to which they can contribute to mitigating risks.

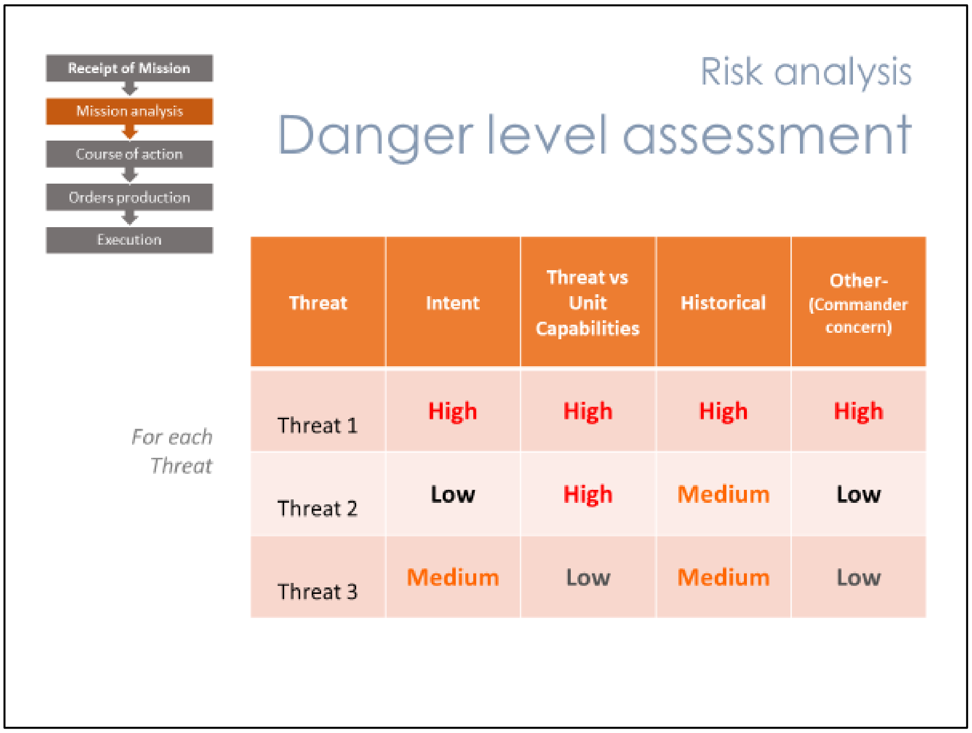
Next, the analysis considers the distance and mobility of these protection actors relative to the areas of interest. Their proximity to the operational areas and their ability to quickly respond and mobilise resources play a crucial role in their effectiveness as protection providers. Assessing their mobility capabilities allows missions to anticipate the level of support they can expect in different locations.

The overall capability of these protection actors is also assessed. This includes evaluating their training, equipment, and resources available for protection activities. An analysis of their capacity to counter potential threats provides insights into their effectiveness and the level of risk reduction they can offer.

Interoperability refers to the ability of a UN unit, a host nation security force, or another unit to work together effectively and seamlessly. It involves compatible communication systems, shared procedures, standardised protocols, and a mutual understanding of roles and responsibilities. By achieving interoperability, the units can enhance operational effectiveness, coordination, and cooperation in joint operations and peacekeeping missions. Additionally, it is important to determine whether these protection actors require assistance from the peacekeeping mission to be operational in the area. For example, they may rely on the mission for force protection or logistical support. Understanding their dependency on the mission enables better coordination and allocation of resources.

Once the capabilities of these potential support Units / actors are established, we can make informed decisions regarding the expected support they can receive in different areas. This assessment influences the level of risk associated with specific threats. For instance, if certain actors are expected to provide substantial support in certain locations, the risk level may be lower compared to areas where their presence is limited. This information plays a critical role in prioritising activities and resource allocation to effectively address a threat.

Slide 33



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Risk analysis

Danger level assessment

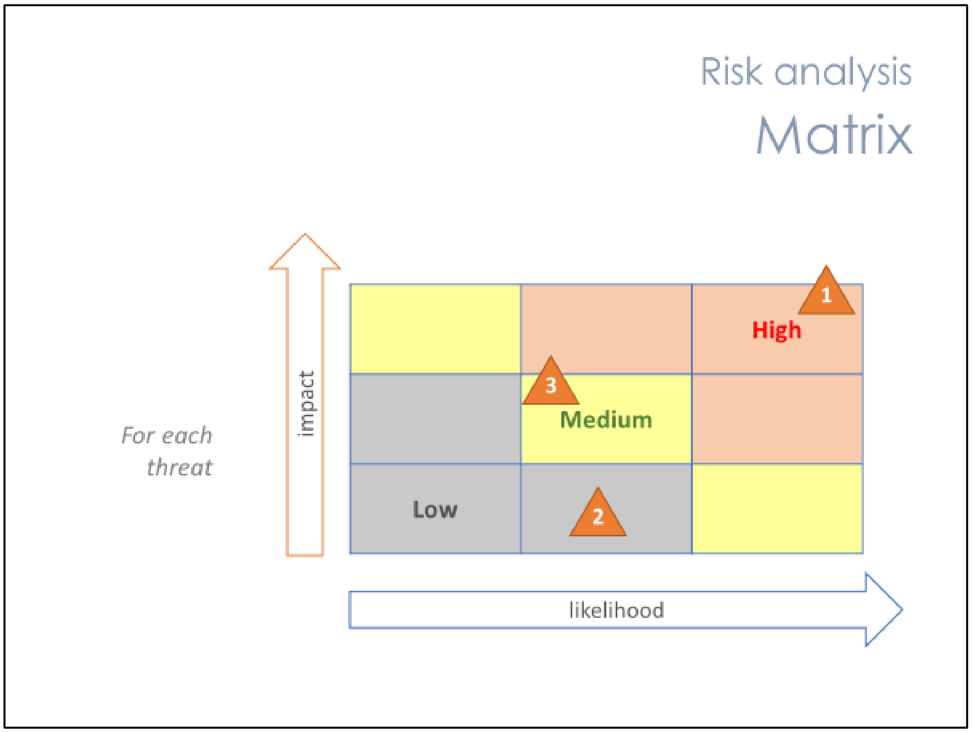
For each Threat

Threat	Intent	Threat vs Unit Capabilities	Historical	Other- (Commander concern)
Threat 1	High	High	High	High
Threat 2	Low	High	Medium	Low
Threat 3	Medium	Low	Medium	Low

Threat equals, capability times Intent and the threat to the units' current and future operations need to be identified. A potential adversary group with intent to cause harm but with minimal capability is a limited threat, whereas a group with significant capability but no intent poses almost no threat. The capability of a UN unit to counter or neutralise a threat also needs to be considered, because again, even if an adversary has every intent to oppose a peacekeeping force, if that peacekeeping force is able to prevent the militant group from operating effectively, they again pose a low risk to the operation.

Now, we assess each threat in terms of its potential danger to our unit and the operation. This assessment involves evaluating the threat's capabilities in relation to our capability gaps, as well as considering their intentions and historical background. Furthermore, we must consider other factors that the commander deems important, such as whether our operation contradicts the predominant goals and objectives of potential attackers. It is crucial to determine whether our operation has the potential to act as a catalyst for triggering violence. By considering these aspects, we can gain a comprehensive understanding of the level of danger associated with each threat and make informed decisions about the level of risk involved.

Slide 34



Risk analysis

Matrix

For each threat

To help visualise the threats, we use this matrix to help in the planning process, we take each threat and determine where in the matrix it should be portrayed.

The unit needs to prioritise threats in order to identify those where mitigating action is most needed. Risk is a product of the likelihood of an event occurring and the impact if that event does occur. The risk analysis determines (a) the likelihood a threat materialises, and (b) the impact the threat would have if it materialised. The combination of those two factors allows missions to determine the risk associated with each threat identified.

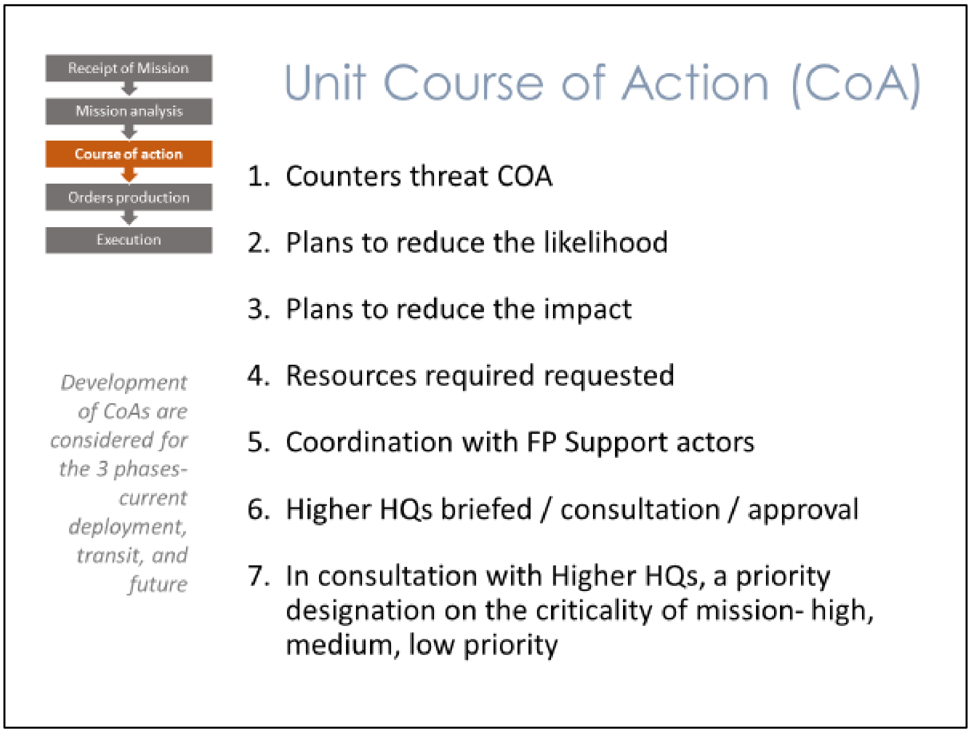
Risk Management is a process that takes reasonable operational mitigation measures to reduce the risk of a given operation. The probability and severity levels of a threat is estimated based on the probability of its occurrence and the severity of its consequences. In the sample graph here, the highest priority is assigned to the threat that is the most likely to occur, with the most impact. Threat #1 is the highest threat.

"Threat = Capability x Intent" serves as a basis for assessing the risks to the unit's current and future operation. It is important to identify all potential threats, considering that a group with minimal capability but strong intent poses a limited threat, while a group with significant capability but no intent poses almost no threat. Additionally, the UN unit's ability to counter or neutralise threats should be considered. Even if a group has the intent to oppose a peacekeeping force, if the force can effectively prevent the adversary from operating, the risk to the operation is low.

A risk analysis is conducted to evaluate the likelihood and impact of each threat, allowing units to determine the level of risk associated with each identified threat. To aid in the planning process and visualise the threats, a matrix is utilised. Based on the risk analysis performed, each threat is assessed, and risk is determined by assessing both the likelihood of an event occurring and the potential impact on the unit.

Prioritising threats is essential to identify where mitigating actions are most needed. Risk management involves implementing reasonable operational measures to mitigate risks in a given operation. The probability and severity levels of a threat are estimated by considering the likelihood of its occurrence and the severity of its consequences. In the provided graph, the highest priority is assigned to Threat #1, which represents the threat that is most likely to occur with the greatest impact on the unit's operation.

Slide 35



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Unit Course of Action (CoA)

1. Counters threat COA
2. Plans to reduce the likelihood
3. Plans to reduce the impact
4. Resources required requested
5. Coordination with FP Support actors
6. Higher HQs briefed / consultation / approval
7. In consultation with Higher HQs, a priority designation on the criticality of mission- high, medium, low priority

Development of CoAs are considered for the 3 phases- current deployment, transit, and future

In the next phase of the decision-making process, we delve into the development of Courses of Action (CoA). After conducting a thorough analysis of the mission, tasks, and associated risks, planners are tasked with formulating comprehensive and flexible CoAs. These plans must identify the key operational issues and their implications, drawing upon the operational factors derived from the Mission Analysis stage.

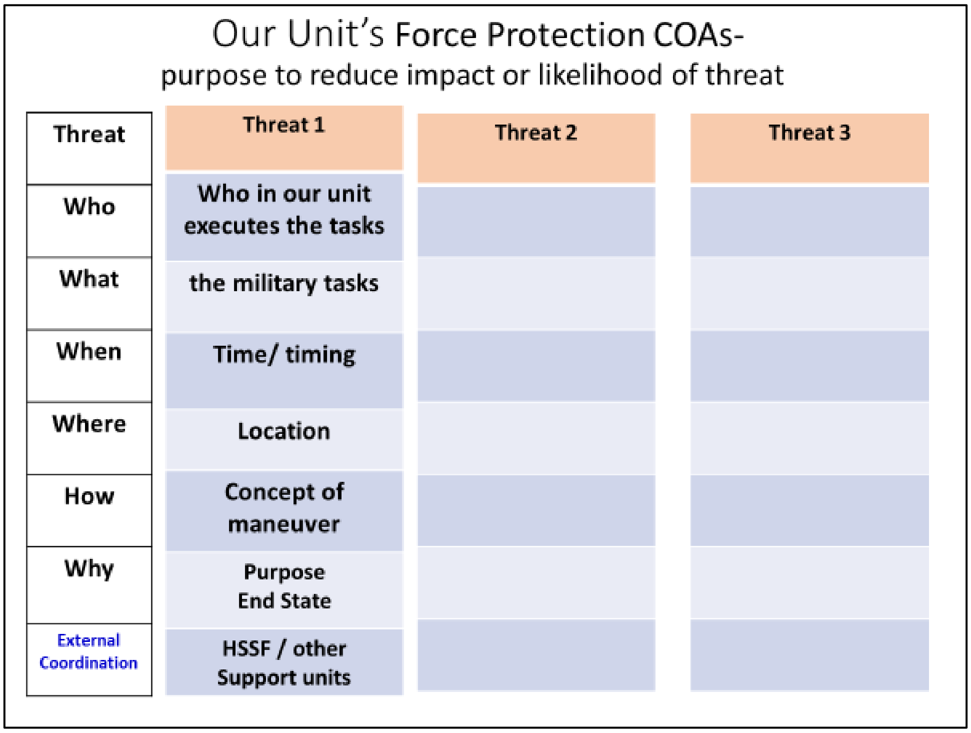
During this stage, it is crucial to scrutinise activities that could potentially escalate tensions with relevant actors, and the CoAs should undergo a rigorous vetting process in coordination with other mission components such as political, humanitarian, and rule of law entities. This collaborative approach aims to assess potential impacts on the UN mission objectives. The development of CoAs should encompass the following elements:

- Countering threat CoAs: CoAs designed to counter the identified threats
- Plans to reduce the likelihood: Strategies aimed at minimising the probability of threats materialising
- Plans to reduce the impact: Measures to mitigate the potential consequences if a threat were to occur
- Resources required/requested: Identification and assessment of the resources necessary to execute the CoAs effectively

- Coordination with FP support actors: Collaboration with other protection actors to ensure a unified and coordinated response
- Briefing/consultation/approval from higher headquarters: Sharing the developed CoAs with higher headquarters, seeking their input, consultation, and obtaining necessary approvals and support resources
- Priority designation: In consultation with higher headquarters, assigning a priority designation (high, medium, or low) based on the criticality of the mission

By incorporating these elements into the CoA development process, planners can create comprehensive and adaptable FP plans that address the identified threats and risks while aligning with the overall mission objectives and priorities.

Slide 36

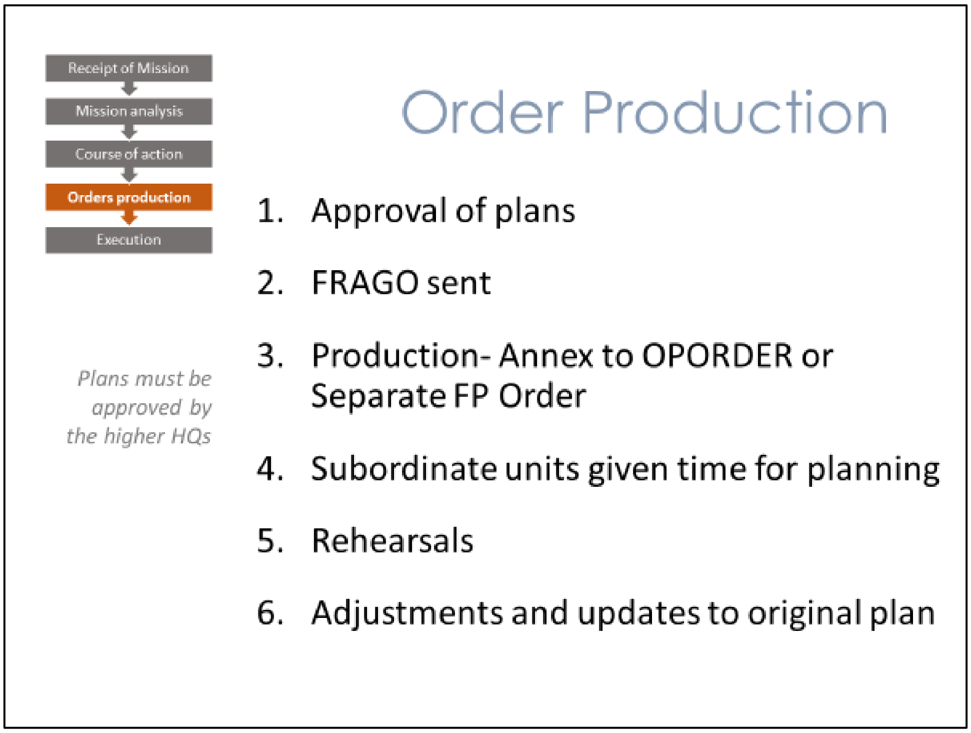


Our Unit's Force Protection COAs-
purpose to reduce impact or likelihood of threat

Threat	Threat 1	Threat 2	Threat 3
Who	Who in our unit executes the tasks		
What	the military tasks		
When	Time/ timing		
Where	Location		
How	Concept of maneuver		
Why	Purpose End State		
External Coordination	HSSF / other Support units		

Course of Action (CoA) development is a critical step in military decision-making. It involves formulating feasible FP options to accomplish mission objectives. Planners analyse the mission, tasks, and risks to develop comprehensive and flexible CoAs. CoAs help formulate the Mission and task statements by defining the purpose, objectives, and specific actions needed. Coordination with other mission components ensures comprehensive planning. CoA development is essential for effective mission execution. Utilising a table is an effective method to enhance the visualisation of Courses of Action (CoAs). It provides a structured format for organising and presenting the various CoAs under consideration.

Slide 37



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Plans must be approved by the higher HQs

Order Production

1. Approval of plans
2. FRAGO sent
3. Production- Annex to OPORDER or Separate FP Order
4. Subordinate units given time for planning
5. Rehearsals
6. Adjustments and updates to original plan

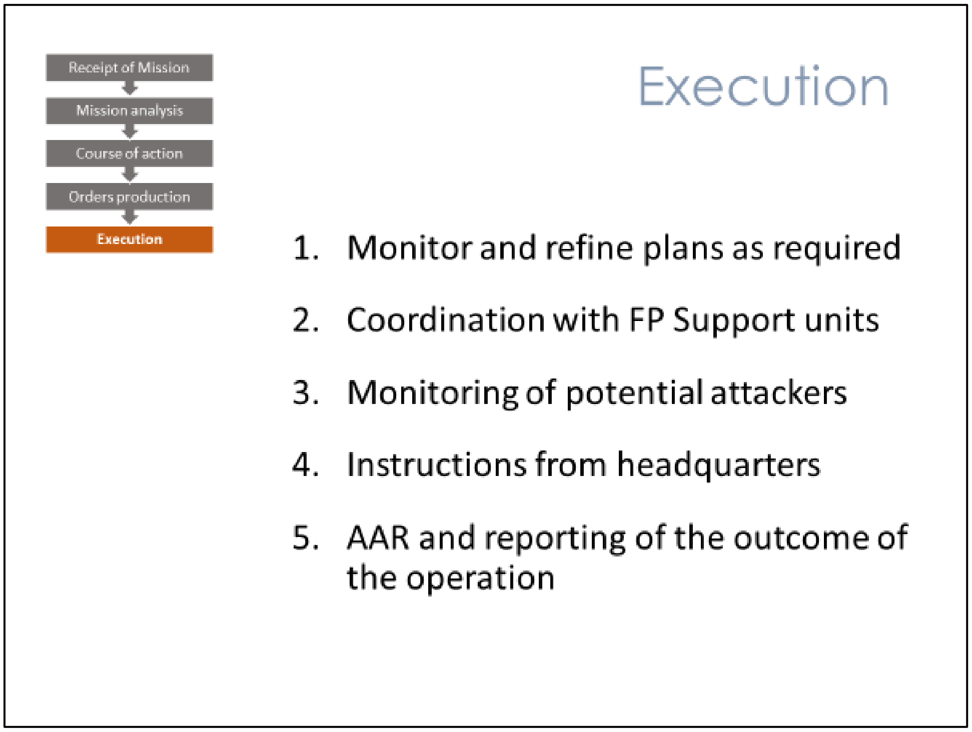
The next step in the decision-making process is to incorporate the approved Course of Action (CoA) into the Operations Order (OPORD). This involves several key steps:

- Approval of Plans: The CoA is reviewed and approved by higher command to ensure its feasibility and alignment with the mission objectives
- Fragmentary Order (FRAGO): A FRAGO is sent out to communicate any changes or updates to the original plan, ensuring that all units are aware of the modifications
- Production of Orders: The CoA is documented in the form of an annex to the OPORD or a separate Force Protection (FP) order, providing clear instructions to subordinate units
- Decision-Making Process (DMP): Subordinate units are given sufficient time to conduct their own decision-making process, analysing the orders and determining their specific actions and responsibilities
- Rehearsals: Units may conduct rehearsals to practice and refine their execution of the CoA, ensuring smooth coordination and understanding among all participants

- Plan and Order Adjustments: As new information becomes available or situational factors change, plans and orders may be adjusted and updated to adapt to the evolving circumstances.

Note that during discussions with higher headquarters, it is essential to assign a criticality level to each mission. This allows planners to prioritise their efforts and allocate resources accordingly. For instance, missions involving the neutralisation of immediate threats to civilians would be deemed high priority due to the potential impact on human lives. Conversely, tasks such as routine logistics resupply convoys may have a lower criticality level as they do not directly impact civilian protection or the immediate stability of the mission.

Slide 38



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Execution

1. Monitor and refine plans as required
2. Coordination with FP Support units
3. Monitoring of potential attackers
4. Instructions from headquarters
5. AAR and reporting of the outcome of the operation

The final stage in the decision-making process is the execution of the approved Course of Action (CoA) for the Force Protection (FP) plan. During this stage, several important tasks are undertaken to ensure the effective implementation of the plan:

Continuous Monitoring and Refinement: Throughout the execution phase, plans are continuously monitored and refined as necessary. This involves staying updated on the evolving situation, assessing the effectiveness of ongoing operations, and adjusting optimised outcomes.

Link-Up and Coordination: Coordination with FP Support units and assets is crucial during execution. This includes establishing communication links, coordinating joint operations, and leveraging the capabilities and resources of supporting units to enhance the overall effectiveness of the mission.

Monitoring Threat Groups and Potential Violent Communities: Constant monitoring of potential threat actors and violent communities is essential to stay aware of their activities, intentions, and capabilities. This enables proactive measures to be taken to mitigate risks and maintain situational awareness.

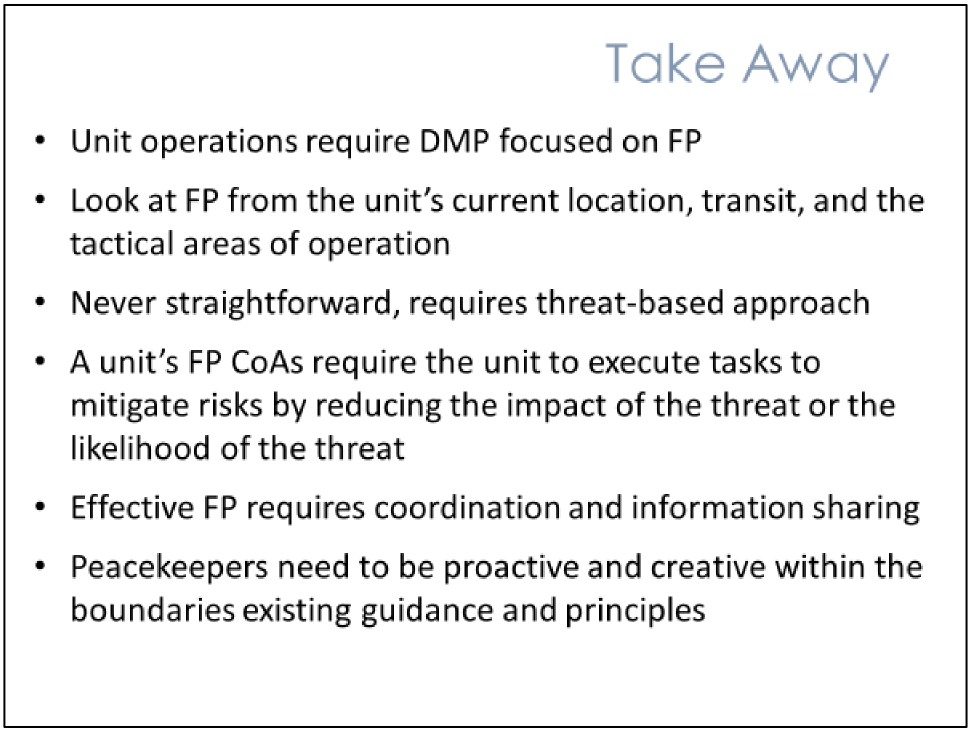
Instructions: Executing the approved CoA involves adhering to the instructions and guidance provided by the headquarters or the higher-level command. This ensures alignment with the overall mission objectives and enables effective coordination among different units and components.

Commander's Decision on Scene: The commander on the scene plays a critical role in making real-time decisions based on the situation at hand. Their judgment, experience, and reasonable belief guide the tactical actions taken during execution to adapt to changing circumstances and achieve mission success.

After-Action Review (AAR) and Reporting: Following the completion of the operation, an AAR is conducted to evaluate the outcomes, identify lessons learned, and document the results. Reporting the outcome of the operation is crucial for information sharing, accountability, and the continuous improvement of future operations.

By effectively executing the approved CoA and undertaking these tasks, the FP operation can mitigate risks and contribute to the overall success of the mission.

Slide 39



Take Away

- Unit operations require DMP focused on FP
- Look at FP from the unit’s current location, transit, and the tactical areas of operation
- Never straightforward, requires threat-based approach
- A unit’s FP CoAs require the unit to execute tasks to mitigate risks by reducing the impact of the threat or the likelihood of the threat
- Effective FP requires coordination and information sharing
- Peacekeepers need to be proactive and creative within the boundaries existing guidance and principles

Summary

Key takeaways from this lesson include:

- All unit operations require focused Force Protection (FP) planning
- Consider FP across the unit's current location, transit, and tactical areas of operation
- Mandate implementation requires a targeted approach and threat-based analysis.
- COAs should mitigate risks by neutralising, reducing impact, or likelihood of threats
- Effective FP requires coordination and information sharing within and outside the mission
- Peacekeepers must be proactive and creative within established guidance and principles

Lesson 3.2

Force Protection Tactical Planning Considerations (Police)

The Lesson

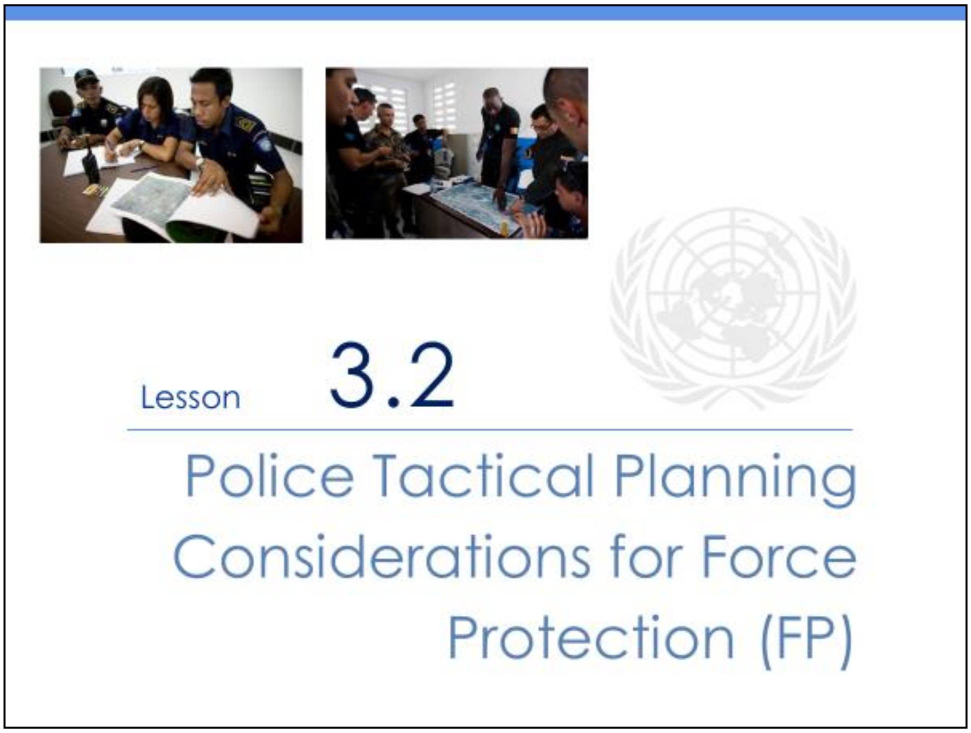
Starting the Lesson

To gain a comprehensive understanding of the concept of Force Protection (FP) and its implications for police units, it is crucial to inquire about participants' perspectives. Specifically, participants should be asked to define FP in a PKO environment and explore how police units can effectively plan for FP, considering its potential differences from conventional operations. In today's peacekeeping environment, there is an alarming rise in the targeting of UN units through acts of violence, as highlighted by numerous studies and reports from the Department of Peace Operations (DPO).

☞ ***Note to Instructor:*** *While discussing tactical planning considerations and guidelines, it is important to allow room for individual planners and commanders to incorporate their own processes. Each Police Contributing Country (PCC) operates under its own national doctrine and decision-making process. Thus, this lesson aims to present a decision-making framework as a guide and tool to assist how commanders and their staff to better integrate FP considerations into their decision-making process, rather than imposing a rigid structure. The focus of this training will be on addressing threats faced by tactical units in the field.*

References: Manual on Mission-based Police Planning in Peace Operations, pp. 15-16 and 20 and Guidelines for Police Operations in United Nations Peacekeeping Operations and Special Political Missions, par. 23

Slide 1



Lesson 3.2

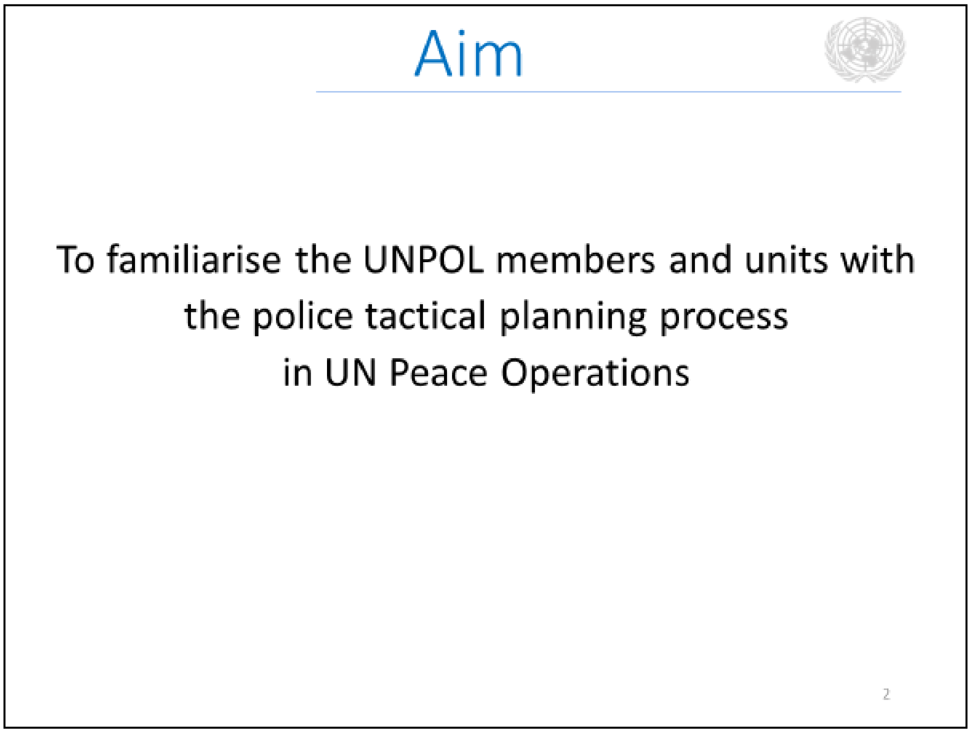
Police Tactical Planning Considerations for Force Protection (FP)

Police planning is a continuous process that requires optimal cooperation, coordination, and flexibility. It includes the systematic collection of information, assessment of the situation and issuance of directives and orders and consultation with other components involved in the operation in addition to directing and controlling the execution. It is important, to the extent possible, to follow general principles governing planning and execution in order to ensure a coherent and controlled tactical execution regardless of the nature of the situation.

To improve police planning, it is important to conduct an analysis of threats, risk and mitigating those risks. This can be done by identifying potential threats and vulnerabilities, assessing their likelihood and impact, and developing strategies to mitigate them. It is also important to involve all relevant stakeholders in the planning process, including other UN departments, offices, and mission components. This ensures that all perspectives are considered and that everyone is working towards a common goal.

☞ ***Note to Instructor**: The lesson does not aim to create or train participants on a particular decision-making process for UN Peacekeeping and does not discuss doctrines, which may vary between police contributing countries. Rather, the lesson offers planning guidance and considerations that commanders and their staffs should consider during the application of their own decision-making process, per their national doctrine.*

Slide 2



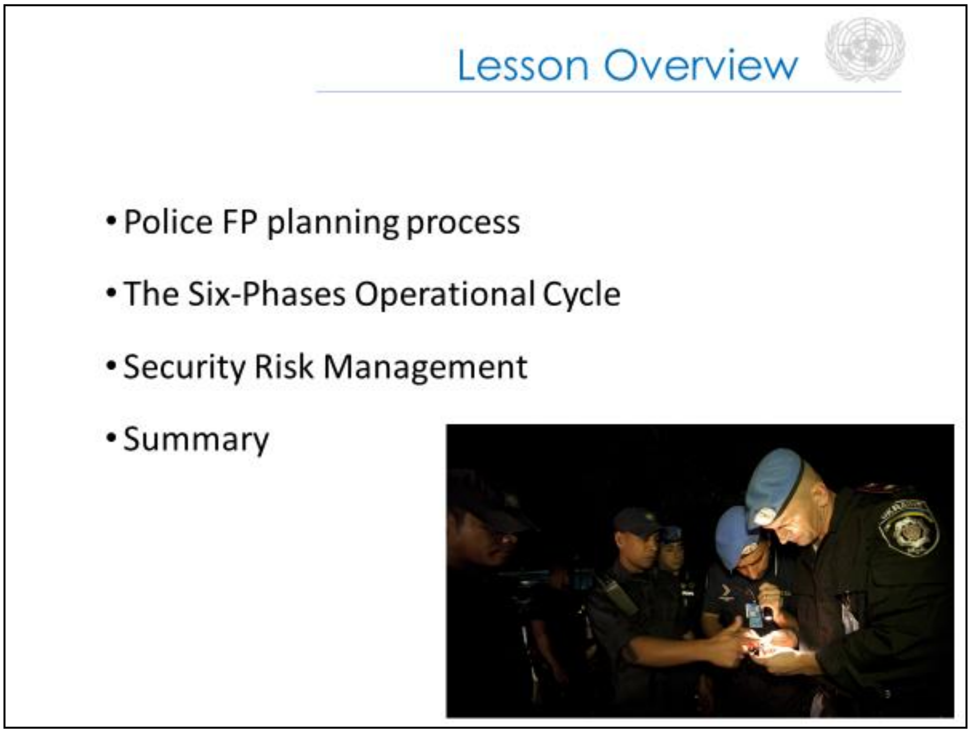
Aim

To familiarise the UNPOL members and units with the police tactical planning process in UN Peace Operations

2

The aim of this lesson is to provide a basic understanding of the force protection tactical planning process specifically tailored for police units involved in UN Peace Operations. This training aims to familiarise UNPOL members and units with the intricacies of the police tactical planning process within the context of UN Peace Operations. By the end of this lesson, participants will have a grasp of the key elements and considerations involved in ensuring effective force protection for police units in the challenging peacekeeping environment.

Slide 3



Lesson Overview

- Police FP planning process
- The Six-Phases Operational Cycle
- Security Risk Management
- Summary

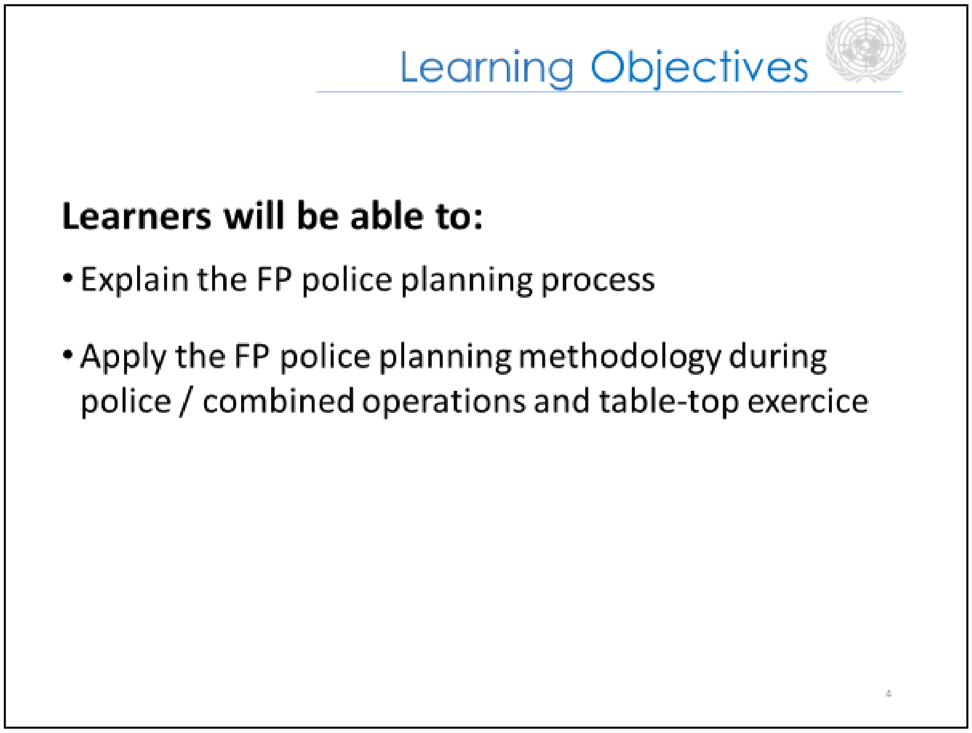
Here is the lesson Content:

Police Force Protection (FP) Planning Process: This section delves into the comprehensive planning process specifically designed for police units to ensure force protection. Participants will gain insights into the key components of the FP planning process, including threat assessment, vulnerability analysis, and risk mitigation strategies. Practical examples and case studies will be used to illustrate the application of these concepts in UN Peace Operations.

The Six-Phases Operational Cycle: In this section, participants will learn about the Six-Phases Operational Cycle, which provides a structured framework for effective planning and execution of police operations in UN Peace Operations.

Security Risk Management: Understanding and effectively managing risks is crucial for police units operating in UN Peace Operations. This segment will introduce participants to the principles and methodologies of risk management. Participants will learn how to assess and analyse threats and risks, develop appropriate risk management strategies, and implement proactive measures to mitigate potential threats to their operations.

Slide 4



Learning Objectives

Learners will be able to:

- Explain the FP police planning process
- Apply the FP police planning methodology during police / combined operations and table-top exercice

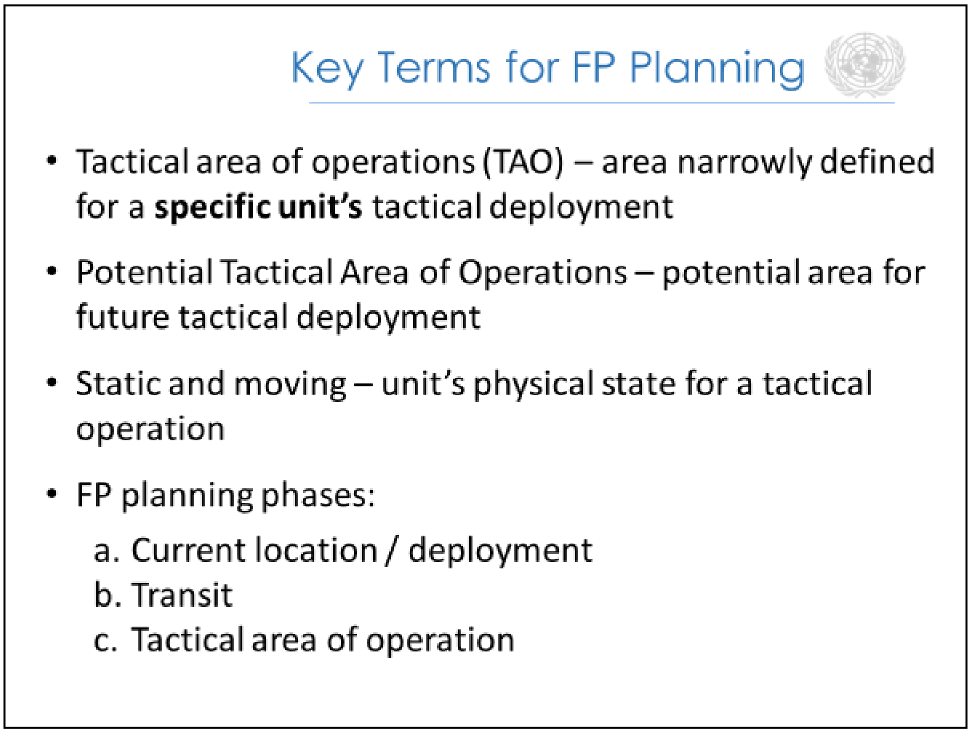
Here After completing this lesson, you will be able to:

Explain the Force Protection (FP) police planning process: Having gained a solid understanding of the FP police planning process, you will be able to articulate the key steps and components involved. You will be able to describe how threat assessment, vulnerability analysis, and risk mitigation strategies are incorporated into the planning process to ensure effective force protection for police units in UN Peace Operations.

Apply the police FP planning methodology during police/combined operations and tabletop exercises: With the knowledge acquired, you will be able to apply the FP police planning methodology in practical scenarios

Take a few minutes to review the key concepts covered in this lesson and reflect on how they can be applied to real-world scenarios.

Slide 5



Key Terms for FP Planning

- Tactical area of operations (TAO) – area narrowly defined for a **specific unit's** tactical deployment
- Potential Tactical Area of Operations – potential area for future tactical deployment
- Static and moving – unit's physical state for a tactical operation
- FP planning phases:
  a. Current location / deployment
  b. Transit
  c. Tactical area of operation

To ensure a shared understanding of key Force Protection (FP) concepts within the FP planning framework, let's establish some definitions that will be used throughout this lesson:

Tactical Area of Operations (TAO) - This term refers to a narrowly defined area designated for the tactical deployment of a specific unit. It encompasses the geographical boundaries within which the unit operates and carries out its assigned tasks.

Potential Tactical Area of Operations - The potential tactical area of operations refers to an area that may be identified and designated for future tactical deployment. It represents an area where the unit may be deployed based on operational requirements or anticipated contingencies.

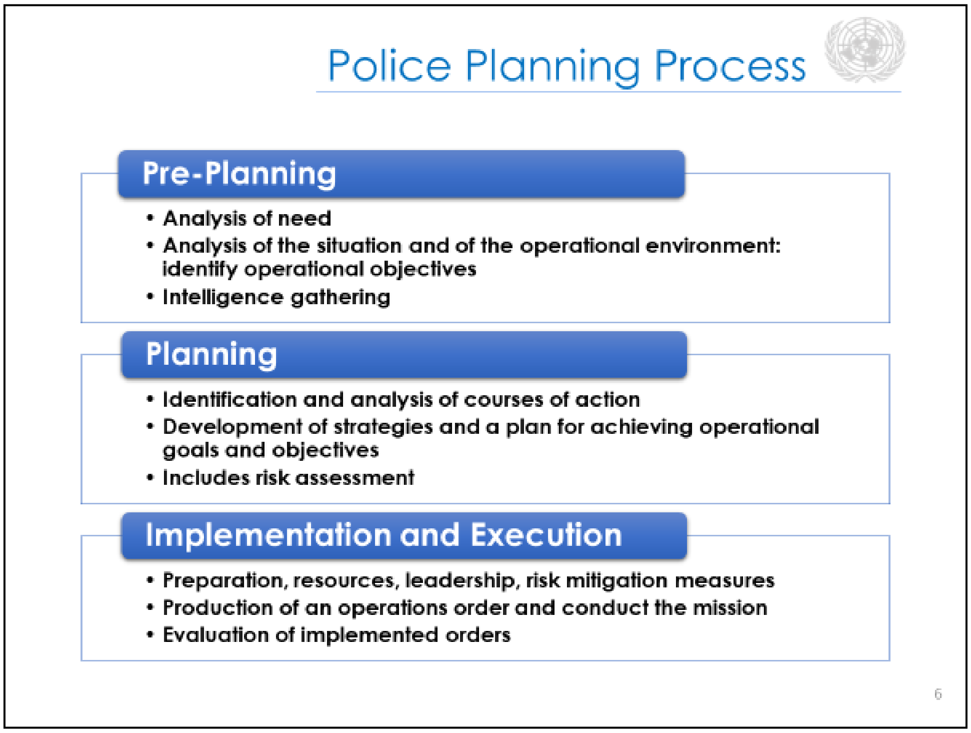
Static and Moving - In the context of FP planning, "static" and "moving" describe the physical states of a unit during a tactical operation. "Static" indicates a stationary position where the unit is deployed in a fixed location, whereas "moving" refers to a state where the unit is in transit or actively on the move between different areas within the operational theatre.

FP Planning Phases- During the FP planning process, the following phases will be addressed:

- Current Location/Deployment: This phase involves assessing and addressing the force protection considerations at the unit's current location or deployment site. It focuses on evaluating the existing security measures, vulnerabilities, and potential threats to ensure the safety and security of personnel and assets
- Transit: The transit phase involves planning for and managing force protection during the movement of units between different locations. This includes identifying potential risks and implementing measures to mitigate those risks during the transit process
- Tactical Area of Operation: This phase focuses on force protection measures within the designated tactical area of operations. It involves comprehensive planning and execution of strategies during tactical operations, considering the specific challenges and risks associated with the operational environment

By establishing these definitions and outlining the FP planning phases, we can ensure a common understanding as we proceed with the lesson, enabling effective communication and application of FP concepts in practice.

Slide 6



Police Planning Process

Pre-Planning

- Analysis of need
- Analysis of the situation and of the operational environment: identify operational objectives
- Intelligence gathering

Planning

- Identification and analysis of courses of action
- Development of strategies and a plan for achieving operational goals and objectives
- Includes risk assessment

Implementation and Execution

- Preparation, resources, leadership, risk mitigation measures
- Production of an operations order and conduct the mission
- Evaluation of implemented orders

6

The police planning process is a dynamic and iterative decision-making process that is commonly followed by most PCCs involved in UN Peace Operations. While there may be slight variations, three key areas are universally significant. In the upcoming slides, we will delve into a 6-step process that serves as a valuable tool for understanding Force Protection (FP) planning. As you progress through this lesson, we encourage you to explore ways to incorporate FP planning considerations into your own Decision-Making Process (DMP).

Preplanning Stage:
During the preplanning stage, several crucial steps need to be undertaken:

- Analysis of Need:

This step involves assessing the specific requirements and objectives of the operation. Understanding the purpose and scope of the mission is essential for effective FP planning.

- Analysis of the Situation and Operational Environment:

Thoroughly evaluating the current situation and the operational environment is crucial. This includes identifying key factors and challenges that may impact the mission's success and identifying operational objectives.

- Intelligence Gathering:

Gathering relevant peacekeeping-intelligence is vital for informed decision-making. This step involves collecting, analysing, and interpreting information to gain insights into potential threats, risks, and opportunities.

Planning Stage:
The planning stage focuses on developing a comprehensive strategy and plan for achieving operational goals and objectives. It consists of the following steps:

- Identification and Analysis of Courses of Action:

Evaluating various options and courses of action is essential to select the most suitable approach for the mission. This step involves assessing the advantages, disadvantages, and potential risks associated with each course of action.

- Development of Strategies and Operational Plan:

Based on the analysis of courses of action, strategies and an operational plan are formulated. This includes outlining specific actions, allocating resources, and establishing timelines for accomplishing objectives. Risk assessment is an integral part of this stage.

Implementing and Execution Stage:
The implementation and execution stage involves putting the plan into action. It consists of the following steps:

- Preparation, Resources, Leadership, and Risk Mitigation Measures:

Preparing personnel, acquiring necessary resources, ensuring strong leadership, and implementing risk mitigation measures are crucial elements for successful execution.

- Production of an Operations Order and Mission Conduct:

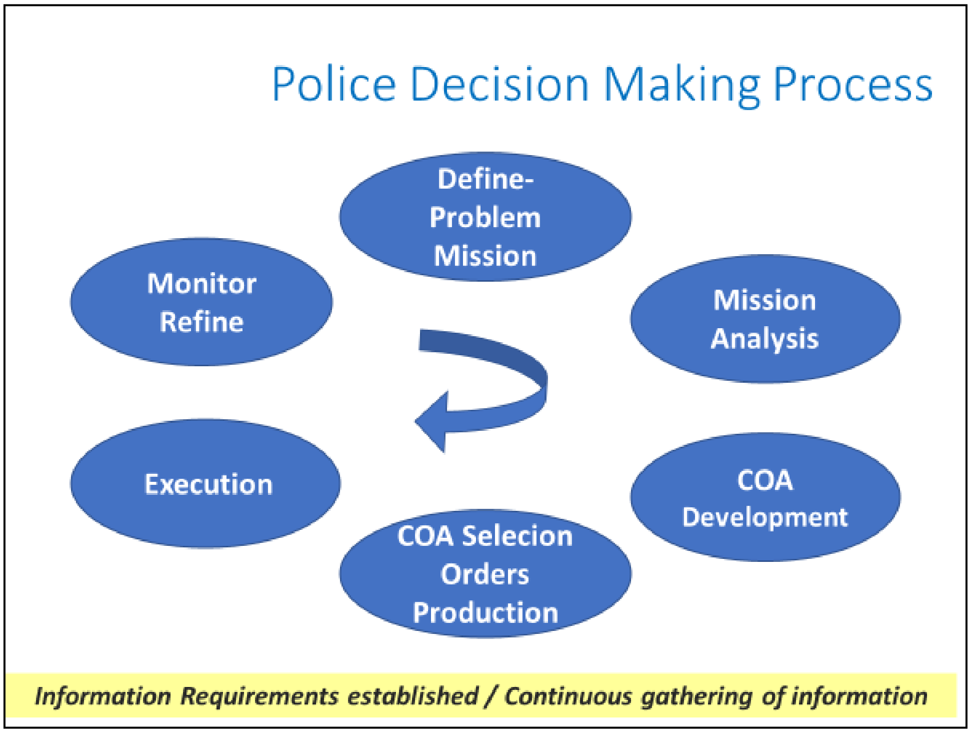
Producing a clear and concise operations order is essential for ensuring effective communication and coordination. This order serves as guidance for personnel during the mission's execution.

- Evaluation of Implemented Orders:

After the mission is carried out, a thorough evaluation is conducted to assess its effectiveness, identify lessons learned, and make improvements for future operations.

By following this structured approach, police units can enhance their FP planning capabilities and integrate them seamlessly into their overall operational decision-making process.

Slide 7



Police Decision Making Process

Define-
Problem
Mission

Mission
Analysis

COA
Development

COA Selection
Orders
Production

Execution

Monitor
Refine

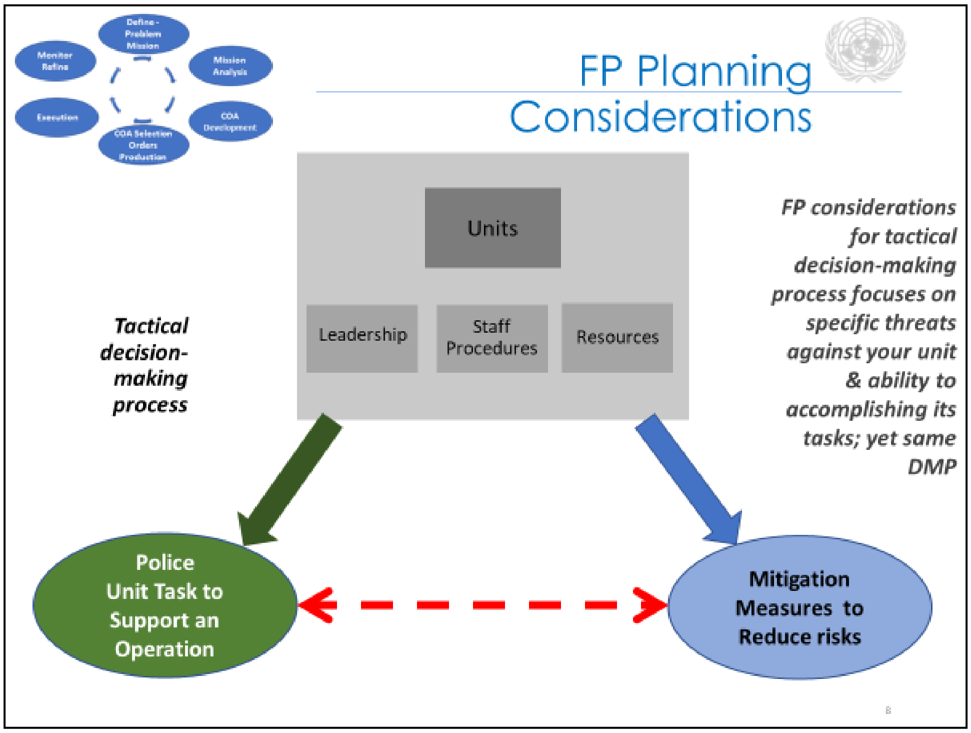
Information Requirements established / Continuous gathering of information

In this section, we will utilise the Decision-Making Process (DMP) to illustrate and guide tactical planning for Force Protection (FP). This DMP was previously covered in Module 1. To facilitate the planning of FP in Peacekeeping Operations, it is recommended that staff members use this DMP as a reference and adapt the tools presented in this lesson to their own planning processes. The focus of this lesson is on 'Mission Analysis' at the tactical level, which serves as the core element of an effective FP strategy.

It's important to note that tactical planning is not a static process but rather a dynamic and continuous cycle. It requires constant review and refinement as we update analytical products, make decisions, and issue orders to account for evolving threats, risks, environment, and objectives. It is crucial to emphasise that tactical planning is an inclusive staff process involving the entire team. Furthermore, Information Requirements (IRs) are continuously established, and both command staff and contingent members should continually gather information to refine plans, address planning assumptions, and verify facts.

By embracing this iterative approach and maintaining a continuous flow of information, unit members can enhance their FP planning efforts and adapt to changing circumstances in Peacekeeping Operations.

Slide 8



FP Planning Considerations

Tactical decision-making process

FP considerations for tactical decision-making process focuses on specific threats against your unit & ability to accomplishing its tasks; yet same DMP

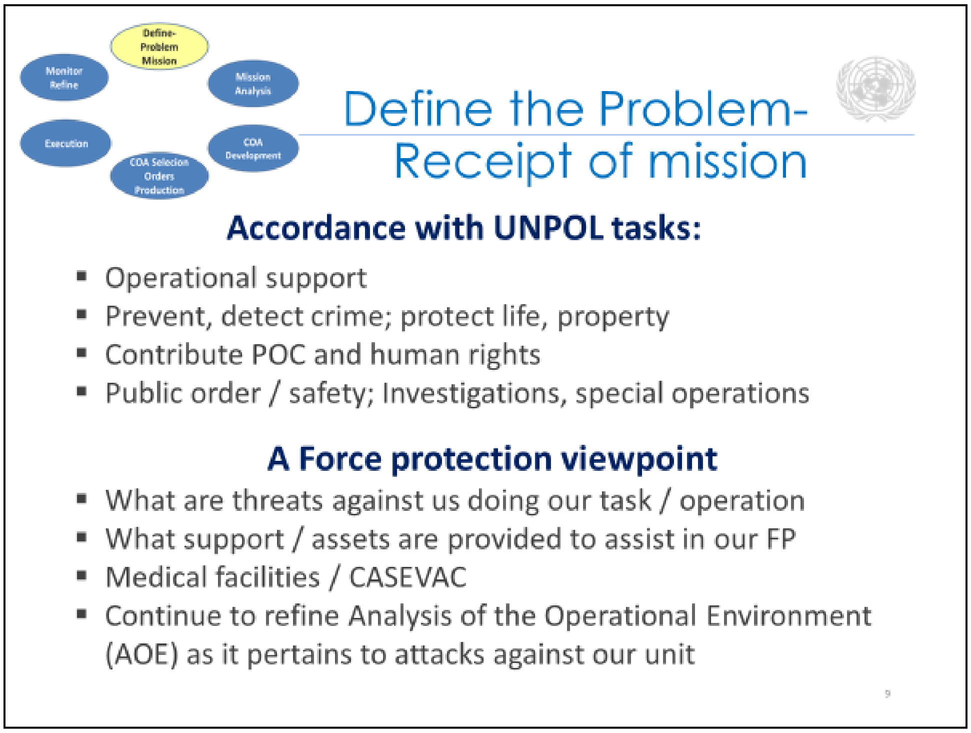
The preceding discussion on the distinctions between UN peacekeeping and conventional operations highlights the significance of incorporating Force Protection (FP) considerations into the planning process. Due to the unique requirements of UN peacekeeping, police units must adopt a PKO mindset, which should be reflected in their planning and operations.

To operate effectively, all units require well-defined structures encompassing leadership, staff procedures, and resources. While these structures may vary across different countries based on their national doctrines, they serve as the fundamental building blocks for conventional operations. In the accompanying graphic, the red (broken) arrow represents the conventional police tasks carried out in the field, aligning with the clear six-step tactical decision-making process.

On the other hand, the blue arrow depicts the decision-making process for FP tasks., UN peacekeepers typically do not engage in traditional engagements. Instead, their role involves supporting a mandate and protecting a third party from the threat of physical violence posed by potential perpetrators. To ensure that operations are tailored with a focus on FP, it is essential to adapt and align strategies in operational situations.

By acknowledging the distinctive nature of UN peacekeeping operations and integrating FP considerations into planning and decision-making processes, police units can effectively fulfil their mandates and ensure the safety and security of all involved parties.

Slide 9



Define-Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Define the Problem-
Receipt of mission

Accordance with UNPOL tasks:

- Operational support
- Prevent, detect crime; protect life, property
- Contribute POC and human rights
- Public order / safety; Investigations, special operations

A Force protection viewpoint

- What are threats against us doing our task / operation
- What support / assets are provided to assist in our FP
- Medical facilities / CASEVAC
- Continue to refine Analysis of the Operational Environment (AOE) as it pertains to attacks against our unit

9

The initial step in the decision-making process involves receiving the operational tasks and defining the problem at hand. These tasks are derived from the Security Council mandate and are guided by the strategic and operational level guidance provided by UNPOL head (Police Commissioner) .

Upon receiving a mission, it is crucial for the unit commander to promptly notify the staff about the upcoming planning process. This includes conducting an initial assessment of the mission, tasks, Force Protection (FP) considerations, and updating staff estimates to support planning. Additionally, necessary planning documents should be prepared during this stage.

In accordance with UNPOL and Formed Police Unit (FPU) tasks, the following key objectives are considered:

- Protect United Nations personnel and property
- Contribute to the Protection of Civilians (POC) and human rights
- Support operations that require a specialised response or capacity beyond the capabilities of Individual Police Officers (IPOs)
- Crime prevention and detection

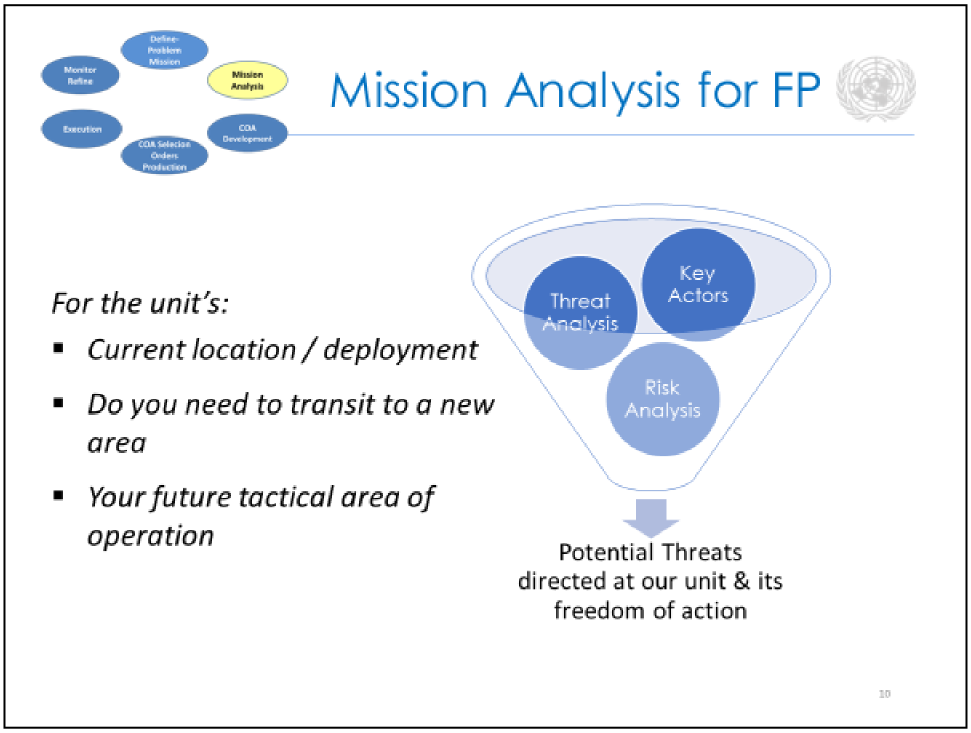
- Protection of life and property
- Maintenance of public order and safety
- Conducting investigations and special operations

From a Force Protection perspective, the following viewpoints should be considered during this stage:

- Identify threats that may hinder the execution of our tasks/operations
- Determine the support and assets available to assist in our Force Protection efforts
- Medical facilities and Casualty Evacuation (CASEVAC) capabilities
- Continuously refine the analysis of the Operational Environment (AOE) specifically related to potential attacks against our unit

By defining the problem, understanding the mission requirements, and considering the Force Protection perspective, the groundwork is laid for effective decision-making and planning in UNPOL/FPU operations.

Slide 10



Mission Analysis for FP

For the unit's:

- *Current location / deployment*
- *Do you need to transit to a new area*
- *Your future tactical area of operation*

Potential Threats directed at our unit & its freedom of action

Mission analysis plays a crucial role in the planning process for Force Protection (FP). It is a threat-based approach that assists in identifying potential perpetrators/actors. By understanding the threat landscape, a comprehensive threat and risk analysis can be conducted, enabling planners to prioritise threats and develop courses of action (COAs) aimed at mitigating risks effectively.

During the mission analysis phase, the following key steps are undertaken:

Threat Identification:

Thoroughly assessing the threat environment is essential. This involves identifying potential perpetrators / attackers such as armed groups, criminal organisations, or hostile violent actors that pose a risk to the mission's success and freedom of action.

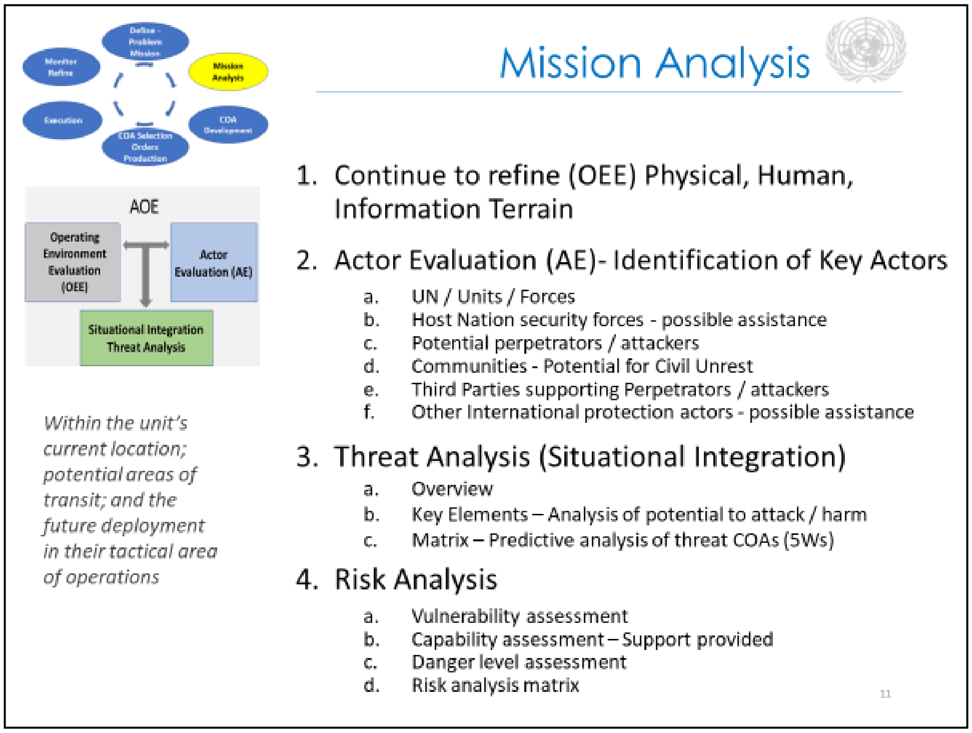
Risk Analysis:

Once the threats are identified, a comprehensive risk analysis is conducted. This process involves evaluating the likelihood and potential impact of each threat, taking into consideration the vulnerabilities, danger aspect and potential consequences to personnel, assets, and the mission objectives.

Prioritising Threats:
Based on the risk analysis, threats are prioritised according to their level of severity and potential impact. This prioritisation allows planners to focus on developing effective COAs to mitigate the identified threats.

By conducting a thorough mission analysis and incorporating a risk-based approach, planners can gain a deeper understanding of the threat landscape and make informed decisions to protect personnel and assets. This process enables the development of robust FP strategies that effectively address the identified threats and mitigate risks in UN Peace Operations.

Slide 11


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine
AOE
Operating Environment Evaluation (OEE)
Actor Evaluation (AE)
Situational Integration Threat Analysis

Mission Analysis

Within the unit's current location; potential areas of transit; and the future deployment in their tactical area of operations

1. Continue to refine (OEE) Physical, Human, Information Terrain
2. Actor Evaluation (AE)- Identification of Key Actors
   a. UN / Units / Forces
   b. Host Nation security forces - possible assistance
   c. Potential perpetrators / attackers
   d. Communities - Potential for Civil Unrest
   e. Third Parties supporting Perpetrators / attackers
   f. Other International protection actors - possible assistance
3. Threat Analysis (Situational Integration)
   a. Overview
   b. Key Elements – Analysis of potential to attack / harm
   c. Matrix – Predictive analysis of threat COAs (5Ws)
4. Risk Analysis
   a. Vulnerability assessment
   b. Capability assessment – Support provided
   c. Danger level assessment
   d. Risk analysis matrix

11

This section delves into the crucial aspect of mission analysis within the Force Protection (FP) planning process. As previously discussed, the steps involved in mission analysis will be examined in the upcoming slides. It is important to note that the DMP cycle diagram serves as a reminder that the analysis of the operating environment and threat assessments are continuous processes that generate updated products to aid the staff during mission analysis. During mission analysis, the following aspects are addressed and refined:

Analysis of the Operating Environment (OEE):
The physical, human, and information terrain is continuously refined and analysed to gain a comprehensive understanding of the operational environment. This includes evaluating factors such as geographic, social and actor dynamics, and information flow.

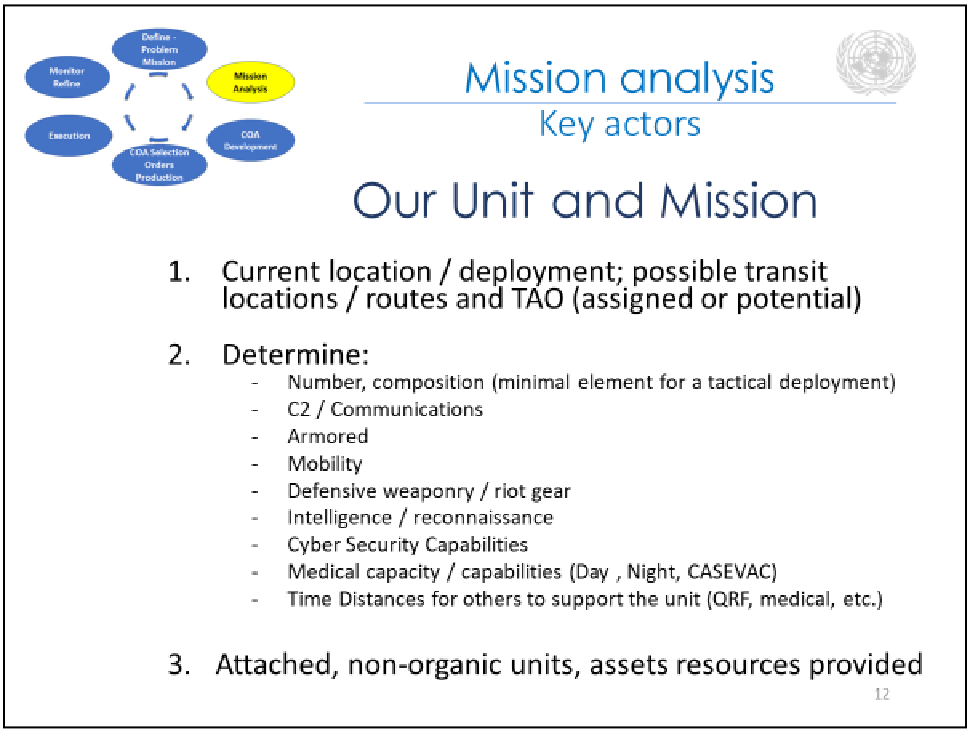
Actor Evaluation (AE):
Identifying key actors is crucial for mission analysis. This involves assessing the roles and significance of various actors, including your unit, UN units and forces, host nation security forces (potential assistance), potential perpetrators or attackers, communities (potential for civil unrest), and other international protection actors (potential assistance).

Threat Analysis (Situational Integration):
This stage entails providing an overview of the threat landscape, with a specific focus on potential attackers that can pose harm to your unit. Key elements of this analysis involve assessing the capabilities and intentions of potential threats and constructing a table / chart that features a predictive analysis of each threat's courses of action (COAs) against your unit’s / operation. The analysis incorporates the 5Ws (who, what, when, where, and why) to comprehensively understand the nature and potential impact of the threats faced by your unit.

Risk Analysis:
To effectively manage risks, a comprehensive risk analysis is conducted. This involves assessing vulnerabilities, evaluating support assets and capabilities provided, determining the danger level of each threat, and utilising a risk analysis matrix to help prioritise and address potential risks.

By conducting a thorough mission analysis encompassing these elements, the FP planning process can better identify and understand the operating environment, key actors, threats, and associated risks. This analysis lays the foundation for developing effective strategies and measures to mitigate risks and ensure the safety and security of personnel and assets.

Slide 12


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis

Key actors

Our Unit and Mission

1. Current location / deployment; possible transit locations / routes and TAO (assigned or potential)

2. Determine:
   - Number, composition (minimal element for a tactical deployment)
   - C2 / Communications
   - Armored
   - Mobility
   - Defensive weaponry / riot gear
   - Intelligence / reconnaissance
   - Cyber Security Capabilities
   - Medical capacity / capabilities (Day , Night, CASEVAC)
   - Time Distances for others to support the unit (QRF, medical, etc.)

3. Attached, non-organic units, assets resources provided

12

Mission analysis involves assessing key actors, including our own unit, and evaluating our mission, task, or operation. The following components are considered during this analysis:

Current Location/Deployment:
This includes examining our unit's current location or deployment site, understanding the geographical context, and assessing the security / defence measures in place.

Possible Transit Locations/Routes and Tactical Area of Operations (TAO):
Identifying potential transit locations, routes, and the assigned or potential Tactical Area of Operations (TAO) provides insights into the unit's mobility and operational reach.

Determining Factors:
Several factors need to be determined and evaluated, including:

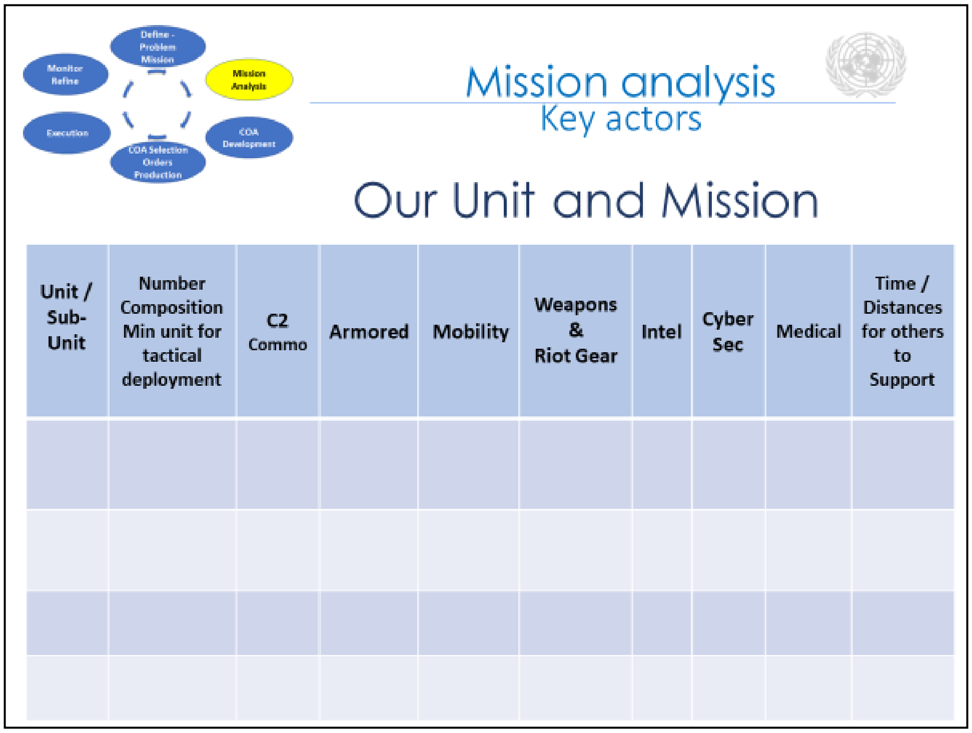
- Number and Composition: Assessing the minimum elements required for a tactical deployment
- Command, Control, and Communications: Evaluating the command structure and communication capabilities to ensure effective coordination

- Armoured and Mobility: Analysing the availability of armoured vehicles and assessing the unit's mobility capabilities
- Defensive Weaponry/Riot Gear: Examining the availability and adequacy of defensive weaponry and riot gear for personnel protection
- Intelligence/Reconnaissance Capabilities: Assessing the unit's ability to gather peacekeeping-intelligence and conduct reconnaissance to enhance situational awareness
- Cyber and Operational Security Capabilities: Evaluating the unit's capacity to address cyber threats and ensure operational security
- Medical Capacity/Capabilities: Considering the medical resources available for day and night operations, including Casualty Evacuation (CASEVAC) capabilities
- Time Distances for Support: Understanding the time it takes for other supporting units, Quick Reaction Forces (QRF), medical teams, etc., to reach and aid your unit. Also, identifying operations in an isolated area that may pose challenges for support

Attached and Non-Organic Units, Assets, and Resources:
Evaluating the availability of attached or non-organic units, assets, and resources that are provided for specialised support to your unit's operations that enhances operational capabilities and effectiveness

By thoroughly analysing these components during mission analysis, a comprehensive understanding of the unit's capabilities, limitations, and support systems is gained. This analysis serves as a foundation for effective decision-making and planning, ensuring the unit is adequately prepared to fulfil its mission tasks or operations.

Slide 13


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

Our Unit and Mission

Unit / Sub-Unit	Number Composition Min unit for tactical deployment	C2 Commo	Armored	Mobility	Weapons & Riot Gear	Intel	Cyber Sec	Medical	Time / Distances for others to Support

To enhance the systematic analysis of our unit, the table provided above serves as a valuable resource. This slide exemplifies the process of analysing a unit's ability to execute tasks or operations efficiently. It is crucial to conduct this analysis across all areas where your unit operates or transits through. The analysis should consider the following factors:

Number and Composition:
Assess the total number of personnel and the composition of the unit, including its minimal unit of deployment. Understanding the organisational structure and personnel resources is essential for effective planning.

Command and Control (C2) and Communications:
Evaluate the unit's command structure, leadership, and communication systems. A robust C2 framework is crucial for efficient coordination and decision-making processes within the unit.

Armoured Assets:
Identify the type of armoured assets available to the unit and assess their capabilities. Understanding the level of protection and mobility provided by the armoured vehicles is vital for force protection planning.

Mobility:
Evaluate the unit's mobility capabilities, including transportation assets and equipment. Consider the ability to manoeuvre swiftly and effectively in different terrain, weather and operational environments.

Firepower:
Assess the unit's firepower capabilities, including small arms, heavy weapons, and supporting assets such as artillery or air support. Understanding the unit's protective and defensive firepower is crucial for mission success and force protection.

Intelligence:
Consider the unit's peacekeeping-intelligence capabilities, including its ability to gather, process, and analyse relevant information. peacekeeping-intelligence support enhances situational awareness and enables decision-making.

Cyber and Operational Security:
Evaluate the unit's cyber and operational security measures to protect against potential threats in the digital and communications network domains. Assessing vulnerabilities and implementing appropriate mitigation measures is essential for mission success.

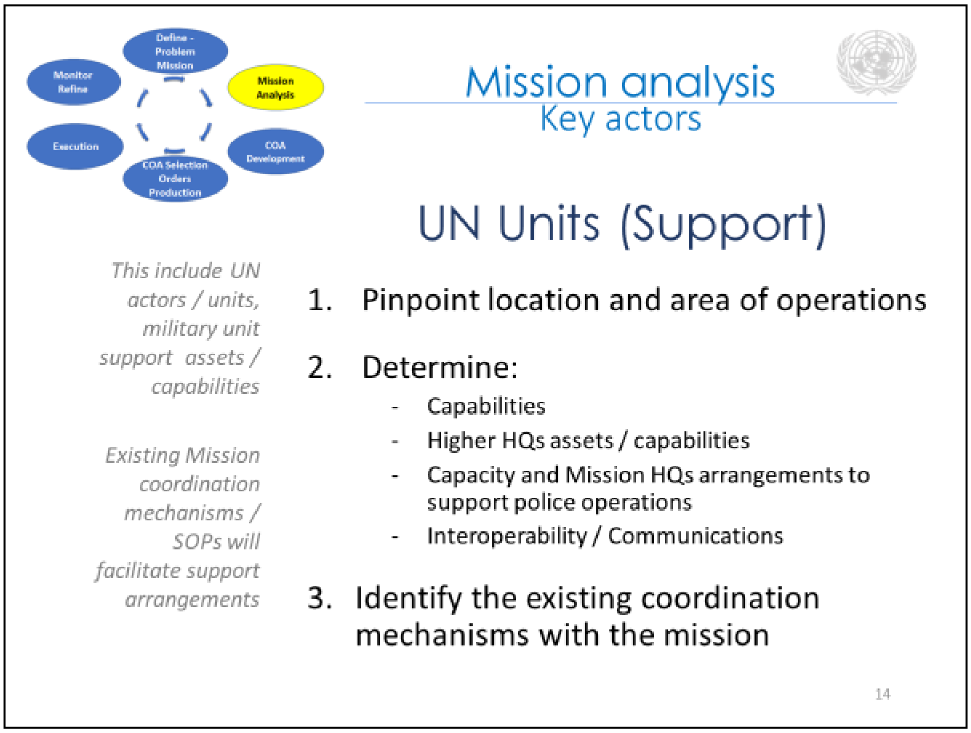
Medical Assets and Capability:
Assess the unit's medical assets, both internal and assigned or available from higher headquarters. Consider the unit's medical capabilities, including emergency medical treatment, casualty evacuation (CASEVAC), and medical support for both routine and operational emergency-related injuries.

Time Distance for Support:
Evaluate the time distance associated with the unit's ability to receive support from Quick Reaction Forces (QRFs), indirect fire support, air support, logistics resupply, or other support elements. Understanding the response time and availability of necessary support resources is critical for force protection and operational success.

By systematically analysing these factors and documenting them in a table / matrix, Police planners can gain a comprehensive understanding of the unit's capabilities. This process also establishes a baseline / foundation for conducting a compare and contrast assessment, evaluating potential vulnerabilities against identified threats (which will be further discussed in the risk analysis phase).

This approach empowers informed decision-making, allowing military planners to make well-founded choices based on a comprehensive understanding of the unit's ability to execute a mission and provide the framework for FP planning. It also facilitates optimised resource allocation, ensuring that the necessary assets and support are allocated where they are most needed.

Slide 14


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

UN Units (Support)

This include UN actors / units, military unit support assets / capabilities

Existing Mission coordination mechanisms / SOPs will facilitate support arrangements

1. Pinpoint location and area of operations
2. Determine:
   - Capabilities
   - Higher HQs assets / capabilities
   - Capacity and Mission HQs arrangements to support police operations
   - Interoperability / Communications
3. Identify the existing coordination mechanisms with the mission

14

Mission analysis involves assessing key actors, including other non-organic UN units, sections, and elements that are attached or assigned to support our operation or task. This includes UN Mission components and UN military units that provide support assets and capabilities. Of note, in many UN Missions, are standardised / routine support, coordination mechanisms and Standard Operating Procedures (SOPs) to facilitate these arrangements.

The following components should be assessed during mission analysis:
Pinpoint Location and Area of Operations: Accurately identifying the specific location and area of operations provides a foundation for effective planning and coordination.

Determine Capabilities:

- Assessing the capabilities of the involved units, both at the higher headquarters (HQ) and within the mission, is essential. This includes evaluating the assets and capabilities available to support police operations

- Higher HQs Assets/Capabilities: Analysing the assets and capabilities of higher headquarters allows for a clear understanding of the resources available for support, coordination, and decision-making

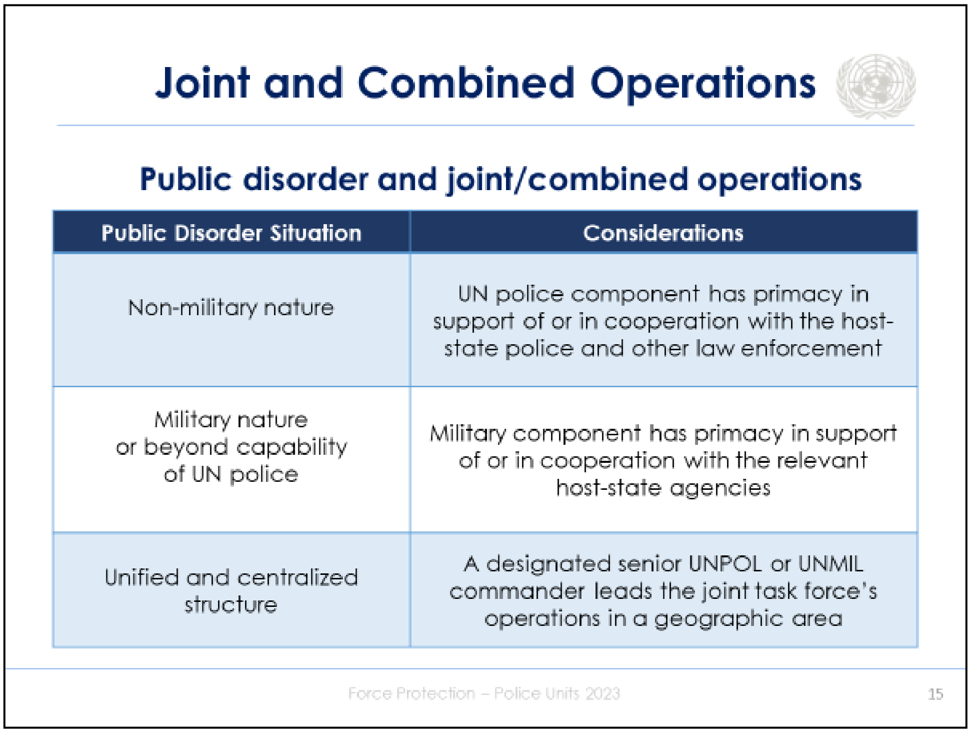
- Capacity and Mission HQs Arrangements to Support Police Operations: Examining the capacity and arrangements of the mission headquarters (HQs) to support police operations ensures that appropriate structures, processes, and resources are in place

- Interoperability/Communications: Evaluating the interoperability and communication systems between different units and actors within the mission facilitates effective coordination and information sharing

Identify Existing Coordination Mechanisms with the Mission:
Identifying and understanding the existing coordination mechanisms, such as coordination meetings, liaison officers, or joint planning groups, ensures effective collaboration and coordination among mission actors.

By thoroughly assessing these components during mission analysis, you can establish a comprehensive understanding of the additional capabilities that can complement your unit's existing capabilities, coordination mechanisms, and support arrangements. This analysis forms a baseline consideration for effective FP planning and execution of police operations within the mission environment. It enables you to identify areas where support assets can enhance your unit’s capabilities for an operation or mission.

Slide 15



Joint and Combined Operations

Public disorder and joint/combined operations

Public Disorder Situation	Considerations
Non-military nature	UN police component has primacy in support of or in cooperation with the host-state police and other law enforcement
Military nature or beyond capability of UN police	Military component has primacy in support of or in cooperation with the relevant host-state agencies
Unified and centralized structure	A designated senior UNPOL or UNMIL commander leads the joint task force's operations in a geographic area

Force Protection – Police Units 2023 15

This section of the presentation focuses on operations conducted in conjunction with the military component. It outlines the command-and-control dynamics during public disorder or incident response scenarios. In most cases, command and control authority resides with the UNPOL Incident Commander or senior UNPOL officer. However, there are specific conditions where command and control responsibilities may shift to the Military Tactical Commander (MTC) or a designated senior UNPOL/UNIML commander.

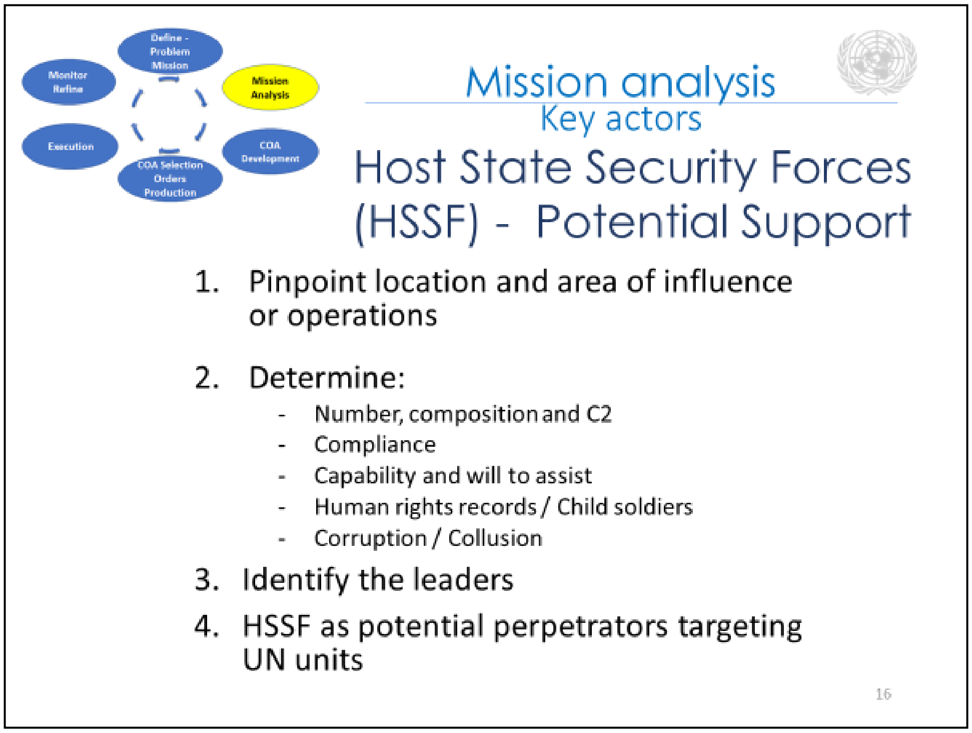
Incident Beyond UNPOL Capability or Military in Nature: If the incident exceeds the capability of UN police or involves a sustained and large-scale use of firearms or military weaponry, the MTC assumes command and control until the situation is once again within the capability of UN police.

Unified and Centralized Mission Organisational Structure: In cases where there is a unified and centralised mission organisational structure, with a designated senior UNPOL or UNIML commander leading joint task force operations in a specified geographic area, command and control arrangements may differ. Under these specific conditions, and with the approval of the Special Representative of the Secretary-General (SRSG)/Head of Mission, command and control authority may be transferred to the designated senior UNPOL/UNIML commander. It is important to note that this applies to units operating within the designated geographic area.

Understanding the specific conditions and command structures during joint operations between UNPOL and the military component is crucial for effective coordination and mission success. By adhering to established guidelines and policies, the appropriate command and control arrangements can be established to ensure the smooth and efficient operation of joint task forces in designated areas.

References:
To ensure compliance with established guidelines and policies, it is recommended to consult the "Guidelines for Combined Military and Police Coordination Mechanisms" (2019.16) and the "FPU Policy" (2016.10).

Slide 16



Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

Host State Security Forces (HSSF) - Potential Support

1. Pinpoint location and area of influence or operations
2. Determine:
   - Number, composition and C2
   - Compliance
   - Capability and will to assist
   - Human rights records / Child soldiers
   - Corruption / Collusion
3. Identify the leaders
4. HSSF as potential perpetrators targeting UN units

16

Mission analysis involves assessing the next key actors, the Host State Security Forces (HSSF), to determine their potential support for your unit's operation. The following assessment framework can be utilised:

Pinpoint Location and Area of Influence or Operations: Accurately identifying the specific location and the extent of the area of influence or operations provides a foundation for effective planning and coordination.

Determine:

- Number, Composition, and Command and Control (C2): Evaluate the size and composition of the HSSF units, their organisational structure, and the effectiveness of their command and control. Understanding their capabilities and structure is crucial for coordinating joint operations and leveraging their support

- Compliance: Assess the extent to which the HSSF complies with international standards, laws, and regulations, including human rights and humanitarian principles. This evaluation ensures alignment with the mission's objectives and values

- Capability and Will to Assist: Evaluate the HSSF's capacity and willingness to provide support to your unit's operation. This assessment includes considering their resources, training, and operational capabilities. Understanding their willingness to collaborate is important for building effective partnerships

- Human Rights Records/Child Soldiers: Examine the HSSF's human rights records, including instances of human rights abuses or involvement in the recruitment and use of child soldiers. This evaluation ensures that your unit aligns with human rights, UN principles, ethical standards and promotes respect from local population

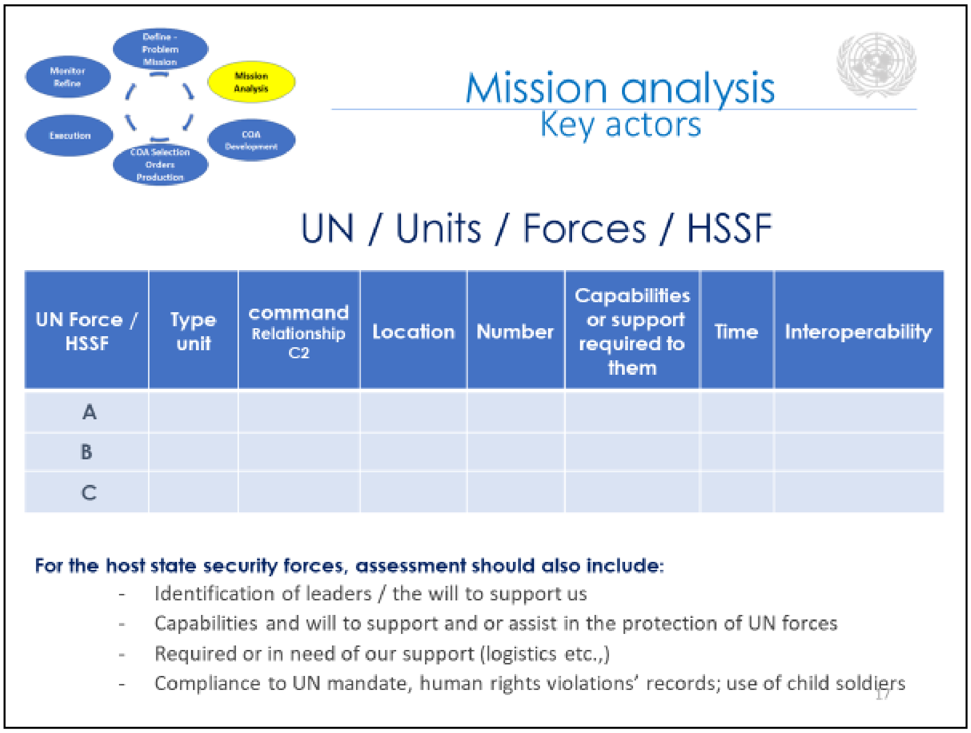
- Corruption/Collusion: Assess the level of corruption within the HSSF and potential collusion with criminal elements or other non-state actors. This evaluation helps identify potential risks and challenges that may affect the success of joint operations

Identify the Leaders:
Identifying the leaders within the HSSF, such as commanding officers or key decision-makers, allows for targeted engagement and effective coordination. Establishing communication and building relationships with the HSSF leaders facilitate better collaboration and understanding.

HSSF as predators / attackers:
In some missions, the Host State Security Forces (HSSF) can pose a threat to UN units. In such cases, the HSSF are potential perpetrators and attackers, and it is essential to use a specific potential predator assessment framework to evaluate these units.

By conducting a comprehensive assessment within this framework during mission analysis, you gain a deeper understanding of the capabilities, compliance, and potential support provided by the Host State Security Forces. This analysis helps inform decision-making, facilitates collaboration, and enhances coordination between your unit and the HSSF, ultimately contributing to the successful execution of your operation.

Slide 17


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

UN / Units / Forces / HSSF

UN Force / HSSF	Type unit	command Relationship C2	Location	Number	Capabilities or support required to them	Time	Interoperability
A							
B							
C							

For the host state security forces, assessment should also include:

- Identification of leaders / the will to support us
- Capabilities and will to support and or assist in the protection of UN forces
- Required or in need of our support (logistics etc.,)
- Compliance to UN mandate, human rights violations' records; use of child soldiers

To facilitate a systematic assessment, it is crucial to analyse non-organic support units/assets assigned to or attached to our unit by higher headquarters. Also, host state security forces (HSSF). Developing a table can be a valuable tool in this process. The above example table demonstrates its usefulness.

There are various other UN units provided to us for operations either through standard operating procedures (SOPs) or specific assignments. Also, HSSF operating or based in our vicinity can be potential support assets. Identifying these actors / units and their potential contributions to our force protection (FP) planning framework is a critical step in the Mission Analysis. These entities may include assets like Explosive Ordnance Disposal (EOD) teams, military security teams, HSSF / host state police, and convoy security teams.

Similar to the approach followed for other key actors, the initial step is to determine the type of unit and the specific support they will provide, as well as their locations. However, there are additional factors to consider:

Duration of support or attachment timeline: Assessing how long the support will be provided and understanding the duration of the support, as well as the process of how and where they will link-up or integrate with our unit.

Command and control: Clarifying the command and support structure and relationship.

Additional support requirements: Identifying any specific support that our unit will need to provide to these non-organic units.

Other relevant factors: Considering any other factors that the commander or staff deem important for assessing and analysing the supporting units.

When considering the utilisation of host state security forces to support our operations, an additional comprehensive assessment should encompass the following factors:

- Identification of Leaders and Willingness to Support: Identify and Evaluate the leaders within the host state security forces who demonstrate a strong willingness to support our mission. Assess their commitment to aligning with our objectives and values

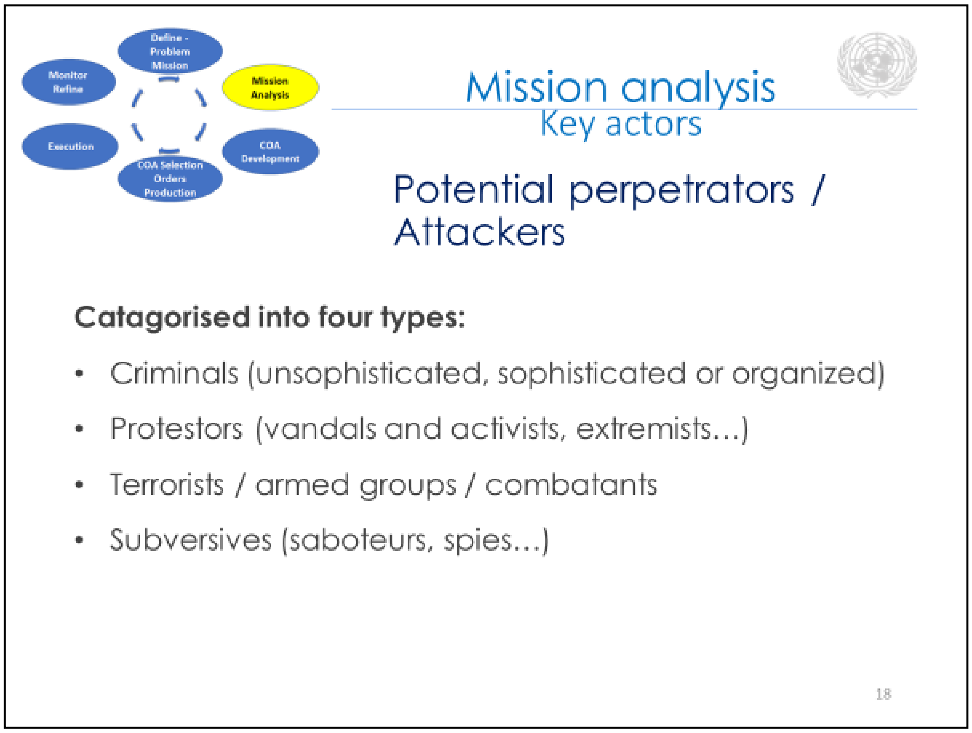
- Capabilities to Assist in supporting FP efforts: Analyse the capabilities of the host state security forces to determine their readiness and capacity to provide effective support

- Requirements for Support: Assess the host state security forces' specific requirements and areas where they may require our assistance, such as logistical support, fuel, or food. Determine the extent of our ability to meet those needs and support them effectively

- Compliance with UN Mandate and Human Rights: Scrutinise the host state security forces'/leaders track record regarding compliance with the UN mandate, including their adherence to international human rights standards. Evaluate any instances of human rights violations, such as the use of child soldiers, to ensure alignment with our UN principles

By conducting a comprehensive analysis of these non-organic / attached support units, we can better understand their capabilities, determine their integration within our unit, and ensure effective coordination and collaboration. This analysis will contribute to a more robust force protection plan and enable successful mission execution.

Slide 18


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

Potential perpetrators / Attackers

Catagorised into four types:

- Criminals (unsophisticated, sophisticated or organized)
- Protestors (vandals and activists, extremists…)
- Terrorists / armed groups / combatants
- Subversives (saboteurs, spies…)

18

Potential perpetrators or attackers can be categorized into four general types. All these actors have the potential to manifest threats against UN units if they possess the capabilities, intent and perceive the UN as interfering, countering their goals, objectives, or purpose:

Criminals:
Unsophisticated Criminals: They lack skills in weapon use and do not operate within a formal organisation. Their targets are typically driven by immediate needs, such as drugs, money, and easily pilferable items. They focus on low-risk targets.

Sophisticated Criminals: Working alone or in organised groups, they possess efficiency and expertise in using specific weapons and tools. They target high-value assets and frequently engage in large-scale activities.

Organised Criminals: These groups rely on specialised individuals to obtain equipment and achieve specific goals. They may target large quantities of money, equipment, arms, ammunition, and explosives.

Protestors / Demonstrators:
Vandals and Activists: Unsophisticated individuals who engage in superficial acts of destruction. They typically do not intend to harm people, but when confronted may pose a threat to UN units.

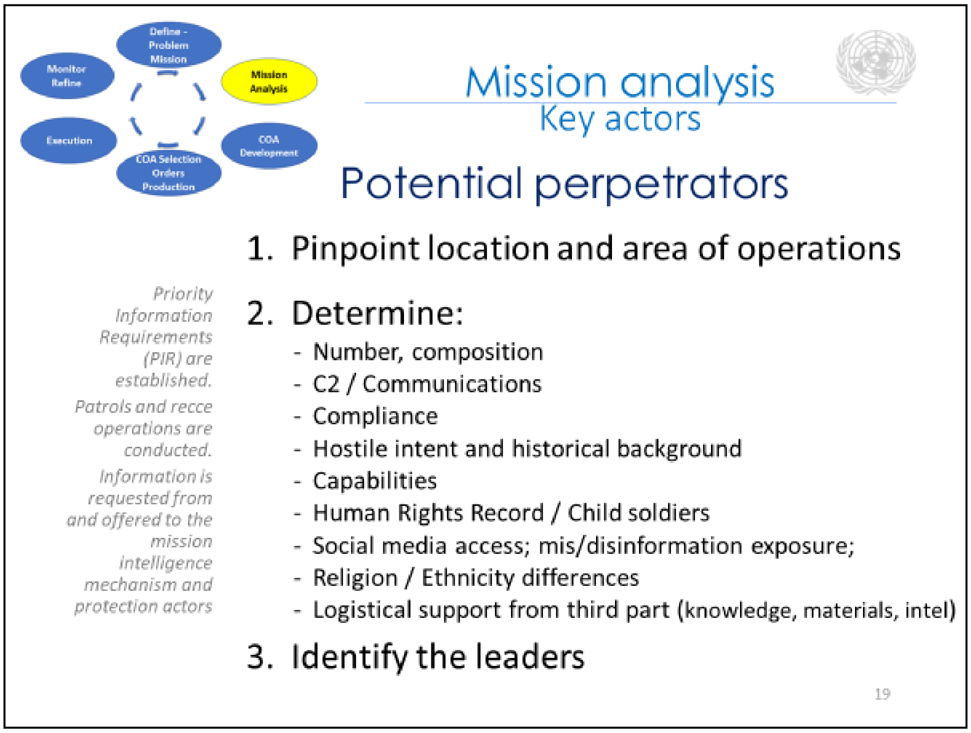
Extremists: Moderately sophisticated individuals engaging in more destructive actions. They are often overt in their actions and may involve violence against UN.

Terrorists/Armed Groups/Combatants: Motivated by ideology, political causes, or specific issues, they commonly operate in relatively small, well-organised groups. These individuals possess sophistication and efficient planning capabilities. Their actions include killing, destruction, theft, and seeking publicity. They are generally classified based on their affiliation with a named group.

Subversives:
Saboteurs are sophisticated and skilled individuals who employ meticulous planning and attacks. They often operate in small groups and have access to an extensive arsenal. Their targets are mission-critical personnel, equipment, or operations. Spies are highly skilled and sophisticated individuals, usually foreign agents, targeting military information while attempting to avoid detection. They may employ activists or other aggressors in their operations.

Understanding these general types of potential perpetrators or attackers provides insight into their capabilities, motivations, and methods of operation. This knowledge is crucial for developing effective FP strategies.

Slide 19



Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

Potential perpetrators

1. Pinpoint location and area of operations
2. Determine:
   - Number, composition
   - C2 / Communications
   - Compliance
   - Hostile intent and historical background
   - Capabilities
   - Human Rights Record / Child soldiers
   - Social media access; mis/disinformation exposure;
   - Religion / Ethnicity differences
   - Logistical support from third part (knowledge, materials, intel)
3. Identify the leaders

Priority Information Requirements (PIR) are established.

Patrols and recce operations are conducted.

Information is requested from and offered to the mission intelligence mechanism and protection actors

19

Assessing potential predators or attackers is a crucial step in identifying key actors who may target your unit. The following components should be considered during this assessment:

Pinpoint Location and Area of Operations:
Accurately determine the specific location of the groups and the operational area where your unit is deployed or expected to operate. This geographical context provides a foundation for assessing potential threats.

Number and Composition:
Evaluate the size and composition of the groups or potential attackers. Understand the number of individuals involved and their organisational structure to gauge their potential impact.

Command and Control (C2) / Communications:
Assess the command-and-control capabilities, as well as their communication systems. Understanding how they coordinate, and share information is crucial for anticipating their actions and strategies.

Compliance:
Evaluate the extent to which they adhere to international laws, UN mandate / presence, and agreements. Assess their willingness to respect human rights and humanitarian principles, which can impact the nature of their threats.

Hostile Intent and Historical Background:
Analyse their hostile intent based on past actions, historical background, or expressed intentions. Understanding their motivations, patterns of behaviour, and any previous hostile engagements.

Capabilities:
Assess their capabilities, including their training, weapons, equipment, and technical expertise. This evaluation provides insights into their ability to carry out hostile / violent actions effectively.

Human Rights Record / Child Soldiers:
Examine the potential predators' human rights record, focusing on any involvement in human rights abuses or the recruitment and use of child soldiers. This assessment helps identify ethical concerns.

Social Media Access; Mis/Disinformation Exposure:
Consider their access to social media platforms and their exposure to misinformation or disinformation campaigns. Understanding their online presence and tactics aids in anticipating their strategies.

Religion / Ethnicity / Ideology / Cultural Differences:
Evaluate potential conflicts or tensions related to religion or ethnicity that may influence the intentions or actions of potential predators. These factors contribute to the dynamics of the threat environment.

Logistical Support from Third Parties:
Assess whether they receive logistical support, such as knowledge, materials, or peacekeeping-intelligence, from third parties. Understanding external support networks helps identify potential sources of increased capabilities and ideology.

Identify the Leaders:
Identify key leaders within the groups or organisations. Understanding their roles, decision-making processes, and influence provides valuable insights into their strategies and tactics.

By considering these components during the assessment of potential predators or attackers, you gain a comprehensive understanding of the threat landscape. This information informs effective planning, risk mitigation strategies, and the development of appropriate force protection measures for your unit. Of note, remember in some UN Missions, the HSSF can be potential predators / attackers.

During the mission analysis process, it is essential to establish Priority Information Requirements (PIR) to guide peacekeeping-intelligence gathering efforts. Additionally, patrols and reconnaissance operations should be conducted to gather relevant information. Effective communication and information sharing between your unit and the mission peacekeeping-intelligence mechanism, as well as other protection actors, are vital aspects of the process.

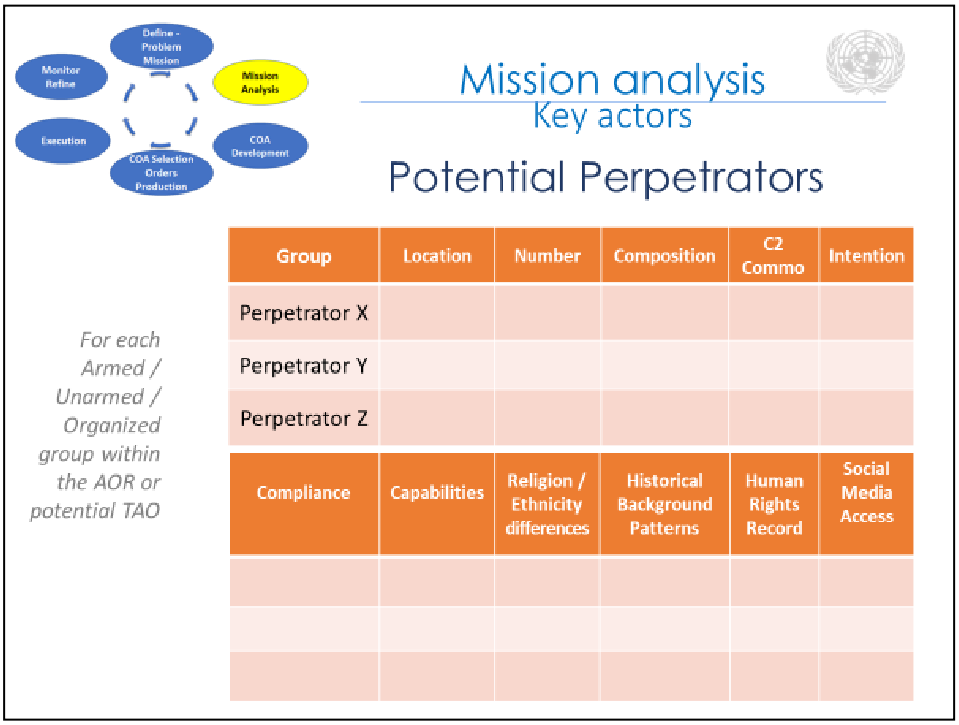
Priority Information Requirements (PIR) Establishment:
Identify the critical information needed to support the mission and prioritise the requirements accordingly. Establish specific PIRs that address key peacekeeping-intelligence gaps and provide guidance for information gathering.

Patrols and Reconnaissance Operations:
Implement regular patrols and reconnaissance operations within your area of operations to collect information first-hand. These activities allow for direct observation, monitoring of the environment, and the gathering of valuable peacekeeping-intelligence on potential threats.

Requesting and Offering Information:
Maintain close coordination with the mission peacekeeping-intelligence cells and other protection actors. Request relevant information from these entities to enhance situational awareness and support operational planning. Additionally, be proactive in offering any valuable information gathered by your unit to contribute to the shared peacekeeping-intelligence picture.

By establishing PIRs, conducting patrols and reconnaissance operations, and fostering effective information exchange with the mission peacekeeping-intelligence mechanism and other protection actors, your unit can gather the necessary peacekeeping-intelligence to inform decision-making and enhance overall situational awareness. This ensures a proactive and well-informed approach to force protection and mission success.

Slide 20



Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

Potential Perpetrators

For each Armed / Unarmed / Organized group within the AOR or potential TAO

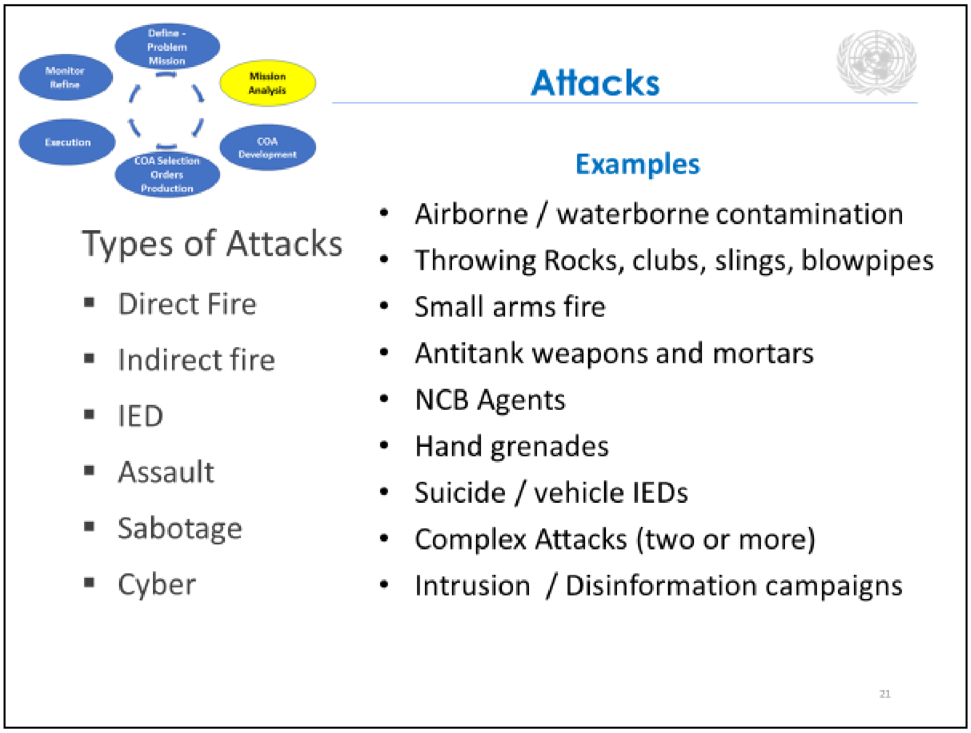
Group	Location	Number	Composition	C2 Commo	Intention
Perpetrator X					
Perpetrator Y					
Perpetrator Z					
Compliance	**Capabilities**	**Religion / Ethnicity differences**	**Historical Background Patterns**	**Human Rights Record**	**Social Media Access**

To bolster the systematic analysis of potential attackers in both current and future operational areas, the use of a comprehensive table can be helpful. This slide serves as an example of how such an analysis can be conducted, with a focus on three groups and the inclusion of various factors and criteria such as location, number, composition, command and control, mandate compliance, capabilities, social media access and leverage, historical background patterns and history, and human rights record. It is imperative to conduct this analysis for all potential perpetrators / attackers your unit may encounter during operations or transit within the designated areas.

Moreover, it is crucial to recognise the value of gathering information from other mission and non-mission actors. Early consultation with these entities will significantly fortify military analysis and enhance the overall comprehension of potential threats and adversaries. Additionally, apart from using a table for analysis, the planning staff should be acquainted with diverse tools and resources accessible from peacekeeping-intelligence cells at all levels. These resources can provide invaluable insights, peacekeeping-intelligence reports, and specialised knowledge, enabling a more comprehensive and well-informed analysis of potential attackers.

By amalgamating these approaches, assimilating insights from multiple sources, and harnessing tools such as tables and peacekeeping-intelligence products, we can ensure a more robust and effective understanding of potential attackers. This heightened awareness will facilitate informed FP decision-making, strengthen operational preparedness, and ultimately contribute to the success of the mission.

Slide 21



Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine
21

Attacks

Types of Attacks

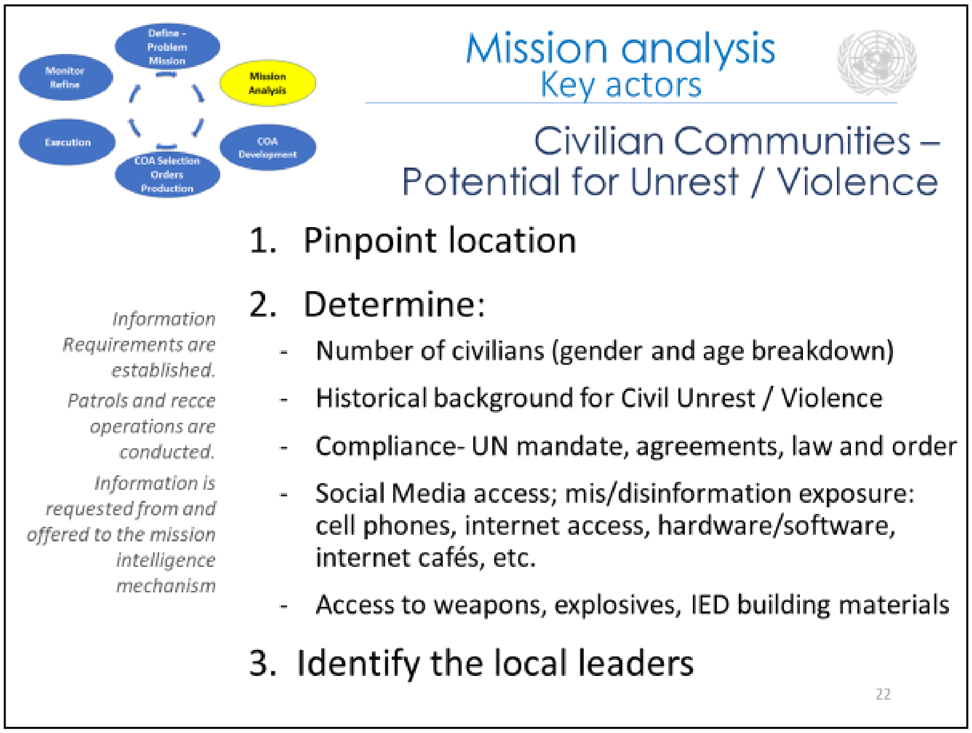
- Direct Fire
- Indirect fire
- IED
- Assault
- Sabotage
- Cyber

Examples

- Airborne / waterborne contamination
- Throwing Rocks, clubs, slings, blowpipes
- Small arms fire
- Antitank weapons and mortars
- NCB Agents
- Hand grenades
- Suicide / vehicle IEDs
- Complex Attacks (two or more)
- Intrusion / Disinformation campaigns

On this slide, we present different types of attacks that target UN peacekeepers, along with some examples. We encourage participants to actively engage by sharing any additional examples they have observed in UN Peacekeeping Operations (PKOs). By fostering an interactive discussion, we can collectively enhance our understanding of the diverse range of attacks encountered by UN peacekeepers in the field.

Slide 22



Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis
Key actors

Civilian Communities –
Potential for Unrest / Violence

1. Pinpoint location
2. Determine:
   - Number of civilians (gender and age breakdown)
   - Historical background for Civil Unrest / Violence
   - Compliance- UN mandate, agreements, law and order
   - Social Media access; mis/disinformation exposure: cell phones, internet access, hardware/software, internet cafés, etc.
   - Access to weapons, explosives, IED building materials
3. Identify the local leaders

Information Requirements are established.

Patrols and recce operations are conducted.

Information is requested from and offered to the mission intelligence mechanism

22

The next phase involves analysing Civilian Communities that may exhibit a propensity for demonstrations, violence, or civil unrest. These communities pose a potential threat to UN units and must be assessed.

Locations:
Our objectives include pinpointing their locations and meeting points.

Determine:

- Number and Composition: A comprehensive breakdown of the gender and age distribution within these communities is essential. This data will enable us to better understand the demographics and potentially identify groups

- Historical Background: It is crucial to examine the historical context of civil unrest and violence within these communities. Analysing past incidents will provide insights into the underlying causes and potential triggers, or attacks against the UN

- Compliance: to include with the UN Mandate, peace agreements, and law and order. Evaluating the community's adherence to UN mandates, agreements, and local law and order is imperative. This assessment will help identify the level of cooperation and potential challenges we may encounter

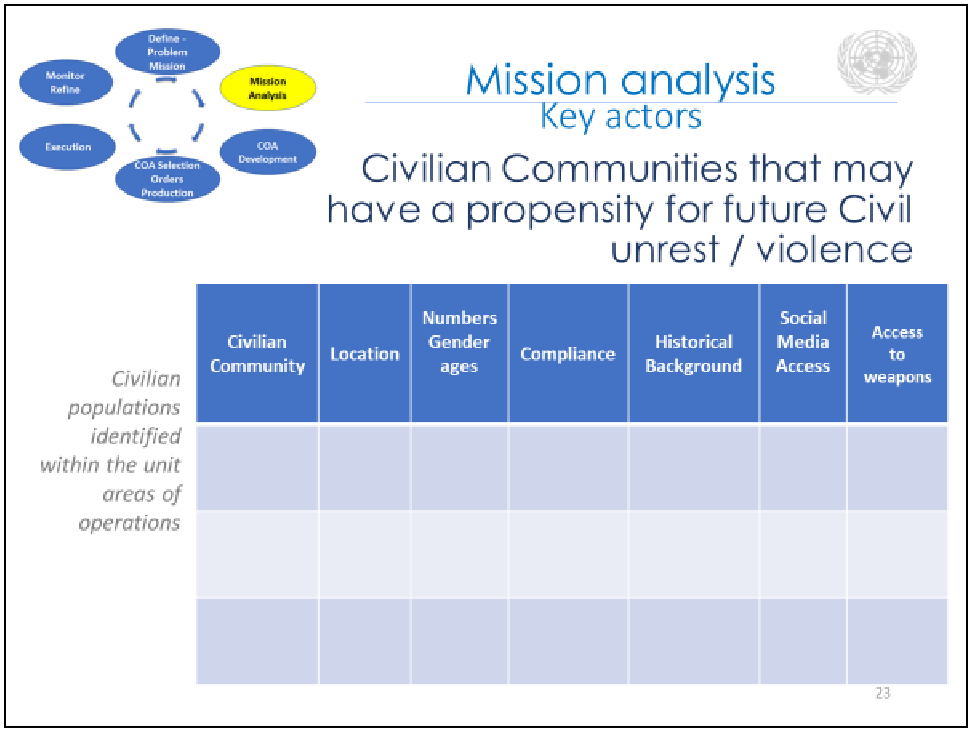
- Social Media Access and Mis/Disinformation Exposure: Understanding the extent of social media usage and the exposure to mis/disinformation within these communities is vital. Identifying access to platforms, such as cell phones, internet connectivity, hardware/software availability, and internet cafés, will assist in assessing communication channels and potential manipulation

- Access to Weapons, Explosives, and IED Building Materials: Determining the availability and accessibility of weapons, explosives, and materials used for constructing improvised explosive devices (IEDs) is crucial for gauging the potential threats

Identification of Local Leaders, Influencers, or Agitators: Identifying key individuals, actors who hold influential positions within these communities is paramount. Locating local leaders, influencers, or potential agitators will help understand power dynamics and enable engagement and conflict resolution strategies.

By conducting a comprehensive assessment of these factors, we can develop a more accurate threat analysis and tailor our approach to effectively conduct a risk analysis and mitigate potential risks.

Slide 23


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis

Key actors

Civilian Communities that may have a propensity for future Civil unrest / violence

Civilian populations identified within the unit areas of operations

Civilian Community	Location	Numbers Gender ages	Compliance	Historical Background	Social Media Access	Access to weapons

23

Mission analysis of key actors should also include an assessment of civilian populations and civilian municipalities in your area of deployment or future deployments. The goal is to gain a comprehensive understanding of the local context, identify potential risk factors for violence, and continue to monitor as conditions may change. The components of this assessment can include the following:

Location: Conduct a thorough analysis of the geographical areas where civilian populations reside. This includes identifying potential hotspots and marginalised communities. Understanding the specific locations can help target engagement.

Numbers, Genders, Ages: Collect accurate and up-to-date demographic data on the civilian communities. This should include the total population size, gender distribution, and age groups present. Knowing the age and gender composition can provide insights into the vulnerabilities and those who may pose as a group of interest.

Compliance to UN Mandate, Law, and Order: Assess the level of adherence to law and order, and their perception of the United Nations Mission. This involves investigating the extent to which local authorities uphold human rights, rule of law, and protect civilians.

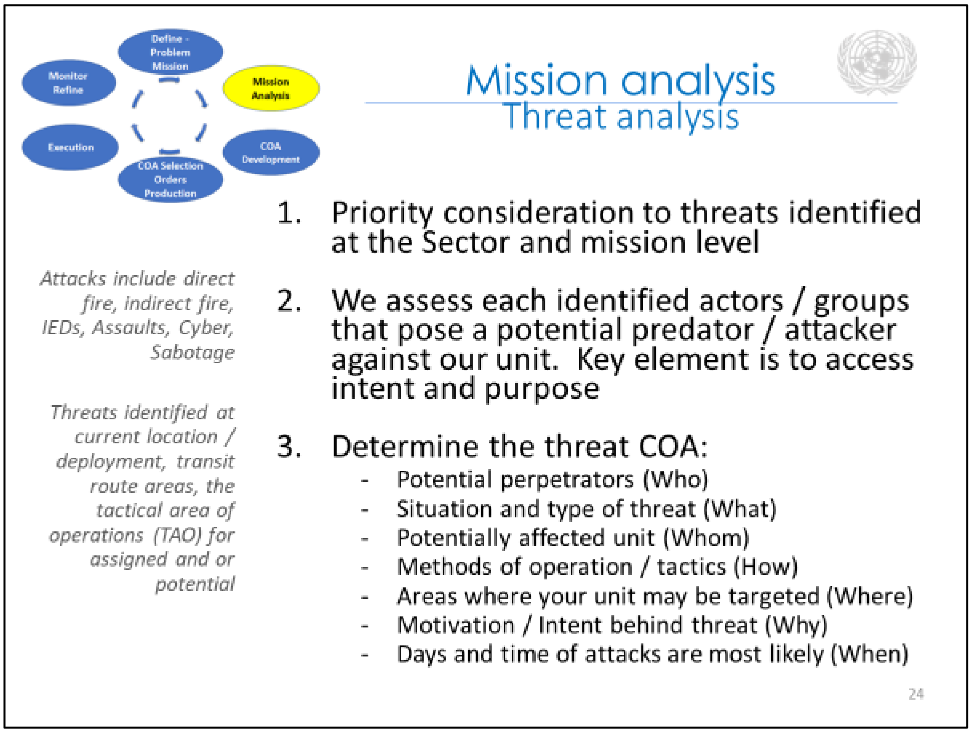
Historical Background for Civil Unrest or Use of Violence: Delve into the historical context of the region, analysing past incidents of civil unrest, violence, and conflicts. Identify underlying causes and triggers and learn from previous efforts to help mitigate unrest. Access the cultural and ethnic diversity in the region and how it may influence relationships between different communities. Identify potential sources of tension. Consider socioeconomic conditions in the area, as poverty and inequality can be contributing factors to civil unrest and violence

Access to Social Media and Misinformation: Understand the prevalence of social media usage within the community. Analyse the potential for the spread of misinformation or disinformation that could exacerbate tensions and contribute to violence. Consider strategies for countering false narratives and promoting accurate information.

Access to Weapons and Activist Group Influence: Investigate the availability of weapons within the community and neighbouring areas. Identify potential sources of weapons and assess the likelihood of them falling into the hands of groups.

To ensure a comprehensive assessment, collaborate with local experts, humanitarian organisations, and civil society representatives. Engage with the civilian population to gather their perspectives and involve them in decision-making processes. Regularly update the assessment to adapt to changing circumstances and new information. Remember that the primary aim of this assessment is to help promote peace and protect civilians you may deploy to.

Slide 24


Define -
Problem
Mission
Mission
Analysis
COA
Development
COA Selection
Orders
Production
Execution
Monitor
Refine

Mission analysis
Threat analysis

Attacks include direct fire, indirect fire, IEDs, Assaults, Cyber, Sabotage

Threats identified at current location / deployment, transit route areas, the tactical area of operations (TAO) for assigned and or potential

1. Priority consideration to threats identified at the Sector and mission level
2. We assess each identified actors / groups that pose a potential predator / attacker against our unit. Key element is to access intent and purpose
3. Determine the threat COA:
   - Potential perpetrators (Who)
   - Situation and type of threat (What)
   - Potentially affected unit (Whom)
   - Methods of operation / tactics (How)
   - Areas where your unit may be targeted (Where)
   - Motivation / Intent behind threat (Why)
   - Days and time of attacks are most likely (When)

24

In our ongoing Mission Analysis, the next pivotal step is to undertake an extensive and meticulous threat analysis. Having already completed a self-assessment of our unit and identified key actors/groups, it is imperative that we thoroughly evaluate the characteristics and intent. This threat analysis aims to provide a forward-looking assessment of the actors or groups that could target our unit. Let us delve into the essential components of this assessment:

Priority Consideration for Mission-Level Threat Analysis: It is crucial to identify the threats by analysing information from sources such as the Joint Mission Analysis Centre (JMAC). This will provide valuable insights and guidance for our assessment.

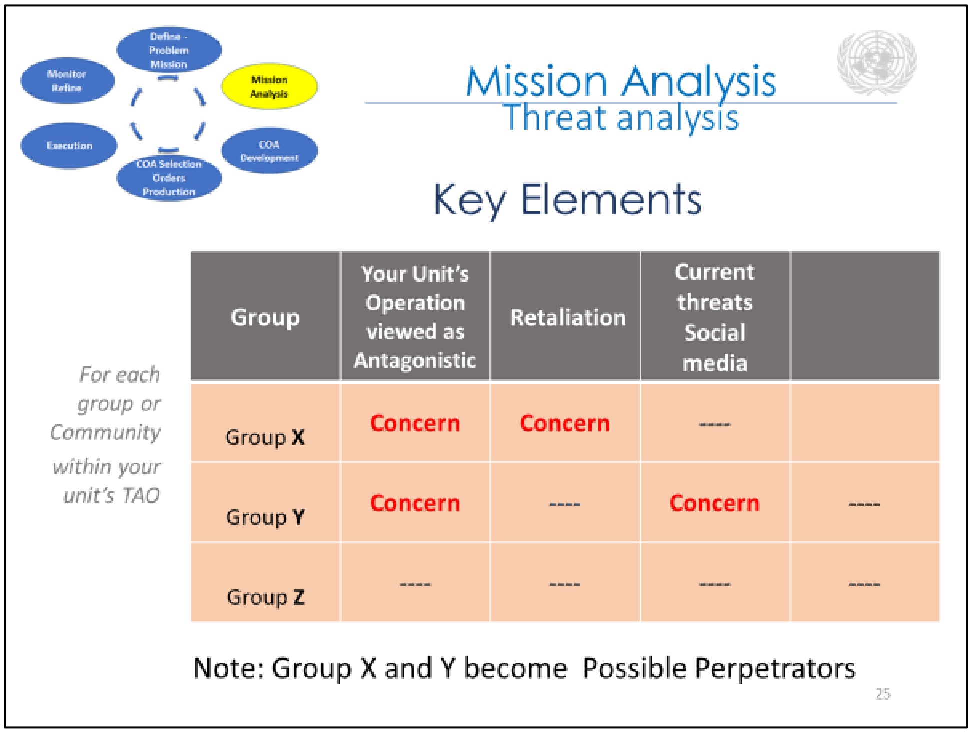
Key Elements / Concerns; Assessment: Each identified actor or group that potentially poses a predatory threat or can act as an attacker against our unit should be assessed. The key focus is to evaluate intent and purpose, understanding their motivations and whether they are a concern to our planned operation.

Determining Threat Course of Action (COA): at this stage, unit commanders and staff must conduct a predictive analysis. This is a methodology used to forecast future events or outcomes based on our threat analysis and historical data, patterns, information, and peacekeeping-intelligence. It involves the application of a course of action (COA) by the identified group/actors targeting our unit. It is threat-based, incorporating trends, patterns, and relationships to make informed predictions about future occurrences. The threat analysis should codify a threat COA that will include Who, What, To Whom, How, Where, Why, and When. See slide 26:

Examine threats in various phases, including those identified at our current location/deployment, along transit routes, and within the tactical area of operations (TAO) assigned or potentially assigned to us. This comprehensive perspective will ensure a thorough evaluation of potential risks and vulnerabilities throughout different operational stages.

By conducting a detailed threat analysis with these considerations, we can better understand what our unit may face, anticipate their actions, and implement appropriate measures to mitigate risks.

Slide 25



Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission Analysis

Threat analysis

Key Elements

For each group or Community within your unit's TAO

Group	Your Unit's Operation viewed as Antagonistic	Retaliation	Current threats Social media	
Group **X**	Concern	Concern	----	
Group **Y**	Concern	----	Concern	----
Group **Z**	----	----	----	----

Note: Group X and Y become Possible Perpetrators

25

For each group with the potential to attack your unit, we assess the following key elements:

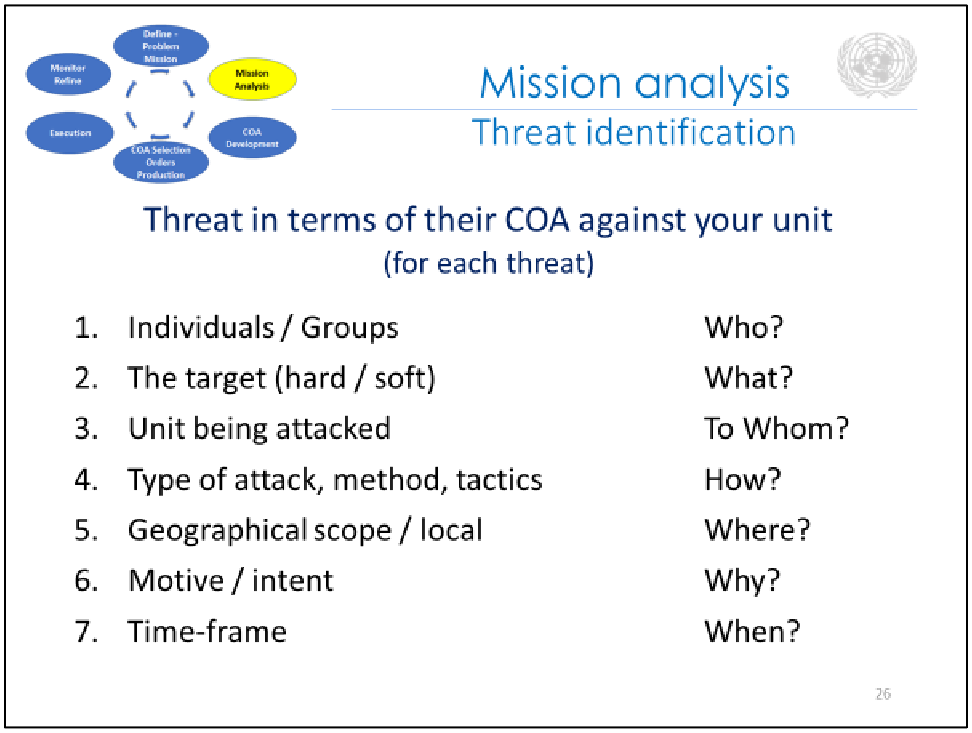
Motivation and Objectives: Thoroughly analyse the group's motivations and objectives. Understanding how your unit's operations are perceived as antagonistic or counter to the group's goals and objectives. Evaluate whether the group views your unit's past as antagonist actions and whether there is pressure within the group to take retaliatory or punishing actions against the UN or your unit.

Current Threats and Exploitation on Social Media: Monitoring and analysing the group's activities on social media platforms for indications of their involvement in attacks targeting the UN. Assessing how they exploit social media for recruitment, propaganda, or coordination related to attacks.

Criteria Deemed Important by Unit Commander or Higher Command: Also, consider any specific criteria or factors identified by the unit commander or higher command that are crucial to the analysis. Incorporating these additional elements into the threat assessment to provide a comprehensive understanding of the threat.

By diligently assessing these key elements, your unit can gain valuable insights into the threats posed by different groups, including IED threats. Understanding the motivations, support networks, and operational capabilities of potential groups is critical in effectively understanding and predicting the level of intent and fortitude to attack your unit.

Slide 26


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis

Threat identification

Threat in terms of their COA against your unit

(for each threat)

1.	Individuals / Groups	Who?
2.	The target (hard / soft)	What?
3.	Unit being attacked	To Whom?
4.	Type of attack, method, tactics	How?
5.	Geographical scope / local	Where?
6.	Motive / intent	Why?
7.	Time-frame	When?

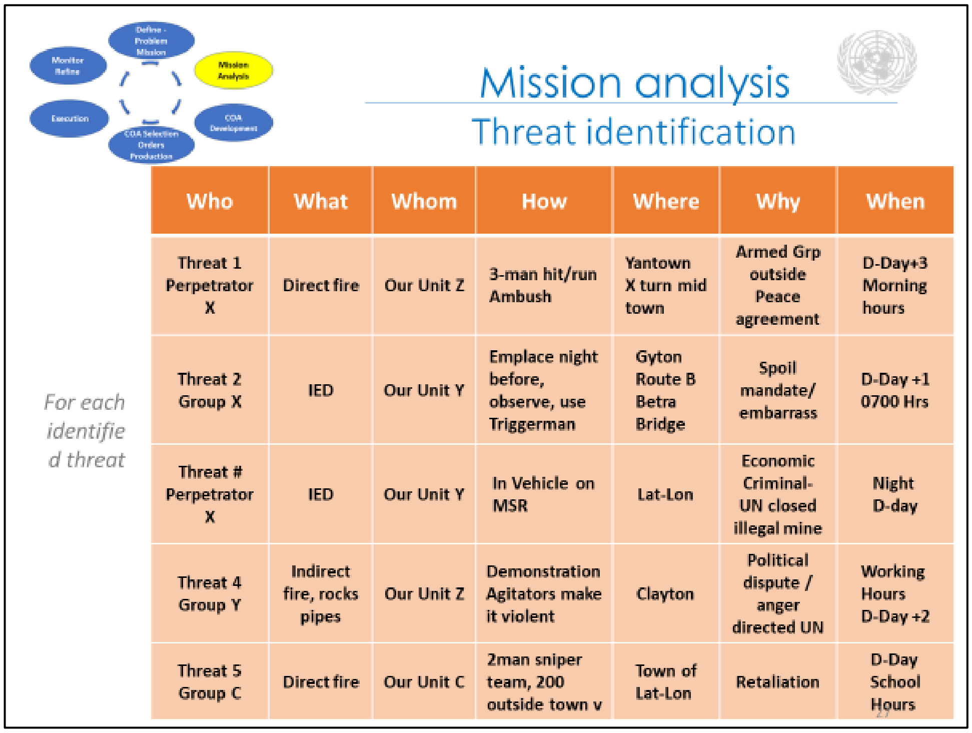
26

The Threat Identification include the following:

- Potential Perpetrators (WHO): Identify the specific individuals or groups who may carry out the attack
- Situation and Type of Threat (WHAT): Understand the circumstances and nature of the threat, including the methods they might employ
- Potentially Affected Unit (WHOM): Determine which unit or units are most likely to be targeted by the threat
- Methods of Operation/Tactics (HOW): Analyse the strategies, tactics, and techniques the threat actors may use in carrying out their attack
- Areas of Unit Targeting (WHERE): Pinpoint the specific geographical locations or areas where our unit is most vulnerable to an attack
- Motivation/Intent behind Threat (WHY): Uncover the underlying motivations or intentions that drive the identified threats

- Likely Days and Times of Attacks (WHEN): Assess the patterns or tendencies regarding when attacks are most likely to occur, taking into consideration factors such as timing, routines, or situational triggers

Slide 27


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Mission analysis

Threat identification

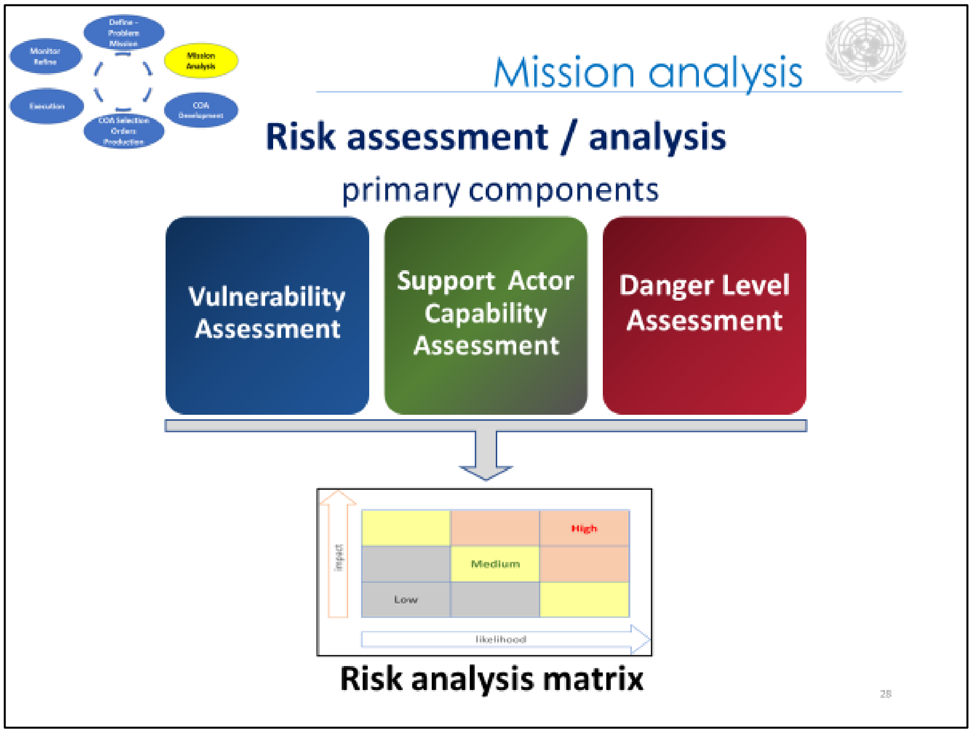
For each identified threat

Who	What	Whom	How	Where	Why	When
Threat 1 Perpetrator X	Direct fire	Our Unit Z	3-man hit/run Ambush	Yantown X turn mid town	Armed Grp outside Peace agreement	D-Day+3 Morning hours
Threat 2 Group X	IED	Our Unit Y	Emplace night before, observe, use Triggerman	Gyton Route B Betra Bridge	Spoil mandate/ embarrass	D-Day +1 0700 Hrs
Threat # Perpetrator X	IED	Our Unit Y	In Vehicle on MSR	Lat-Lon	Economic Criminal- UN closed illegal mine	Night D-day
Threat 4 Group Y	Indirect fire, rocks pipes	Our Unit Z	Demonstration Agitators make it violent	Clayton	Political dispute / anger directed UN	Working Hours D-Day +2
Threat 5 Group C	Direct fire	Our Unit C	2man sniper team, 200 outside town v	Town of Lat-Lon	Retaliation	D-Day School Hours

Presented here is an illustration of a Threat Analysis Course of Action (COA) Matrix, providing planners with the means to categorise multiple threats systematically. This aids in conducting a risk analysis that aligns with the threat-based approach to FP planning.

Each threat is categorised in the following aspects: Who is involved, the intended target (Whom), the type of the attack and in this case, it is an IED (What), the expected timing (When), the location (Where), and the modus operandi (How) of the potential attack on our unit. This predictive Threat Course of Action (COA) aids in establishing a baseline for the risk analysis, leading to the development of a risk mitigation strategy focused on addressing the higher-priority, high-risk threats.

Slide 28



Mission analysis

Risk assessment / analysis

primary components

Vulnerability Assessment

Support Actor Capability Assessment

Danger Level Assessment

Risk analysis matrix

Continuing with the mission analysis, the next crucial step is to conduct a comprehensive risk assessment. The risk assessment comprises the following components:

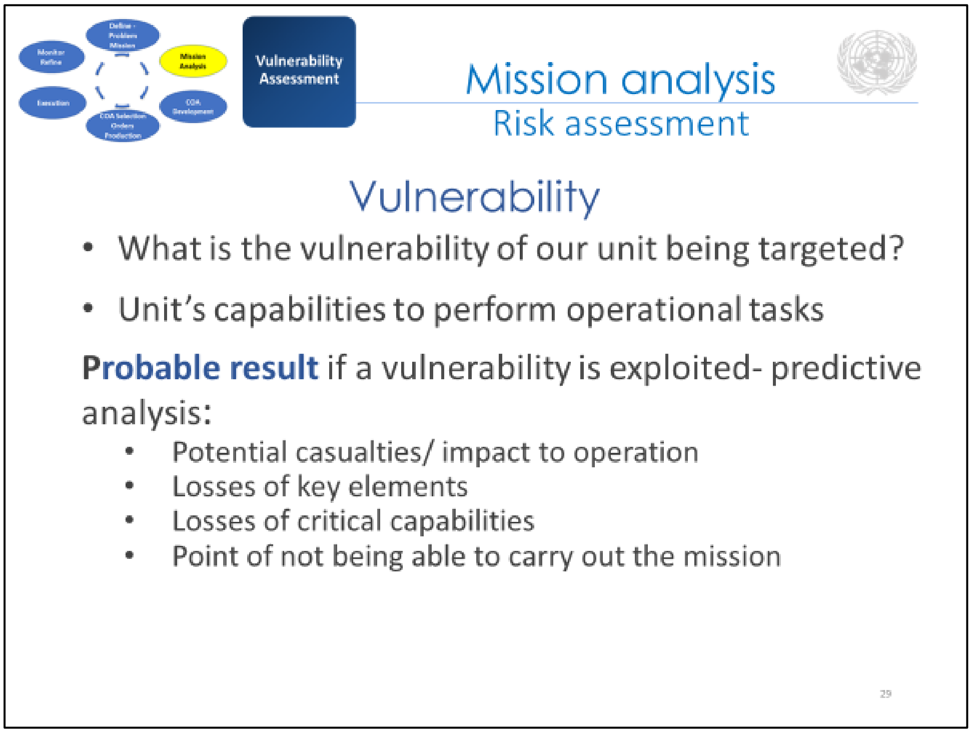
Vulnerability Assessment: This involves evaluating our unit's vulnerabilities by comparing and contrasting them with each potential threat's course of action (COA). By identifying and analysing our vulnerabilities, we can better understand how each threat may exploit them.

Support Actor Capability Assessment: It is essential to assess the support we can receive from other UN units/elements and the Host State Security Forces. This assessment helps identify additional capabilities and resources that can be leveraged to enhance our unit's operations. By utilising these available resources effectively, we can supplement our own capabilities and improve mission success.

Danger Level Assessment: This assessment focuses on evaluating the degree or level of danger associated with each threat. It considers both the potential impact on our unit and the operation, as well as the likelihood of the threat occurring. This analysis helps in prioritising each threat based on its potential severity and probability.

Combining and analysing these three components enables the development of a risk analysis matrix. The matrix provides a visual representation that allows for easy comparison and prioritisation of each threat relative to others. This matrix is a valuable tool for decision-making and resource allocation. In the upcoming slides, we will delve into more detailed explanations of each component and further explore their implications for our mission.

Slide 29


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine
Vulnerability Assessment

Mission analysis

Risk assessment

Vulnerability

- What is the vulnerability of our unit being targeted?
- Unit's capabilities to perform operational tasks

Probable result if a vulnerability is exploited- predictive analysis:

- Potential casualties/ impact to operation
- Losses of key elements
- Losses of critical capabilities
- Point of not being able to carry out the mission

29

As part of the risk assessment process, it is crucial to conduct a predictive analysis that assesses the probable outcomes if a vulnerability within our unit is exploited by a threat. This analysis helps us understand the potential consequences and allows for proactive planning to minimise risks. Here are some key aspects to consider when conducting this predictive analysis:

Potential Casualties/Impact on Operation: One of the primary concerns when a vulnerability is exploited is the potential for casualties among our personnel. This analysis assesses the likely number of casualties and the impact they may have on the overall operation. By considering factors such as the threat's capabilities, the nature of the vulnerability, and the operational context, we can estimate the potential casualties and their implications.

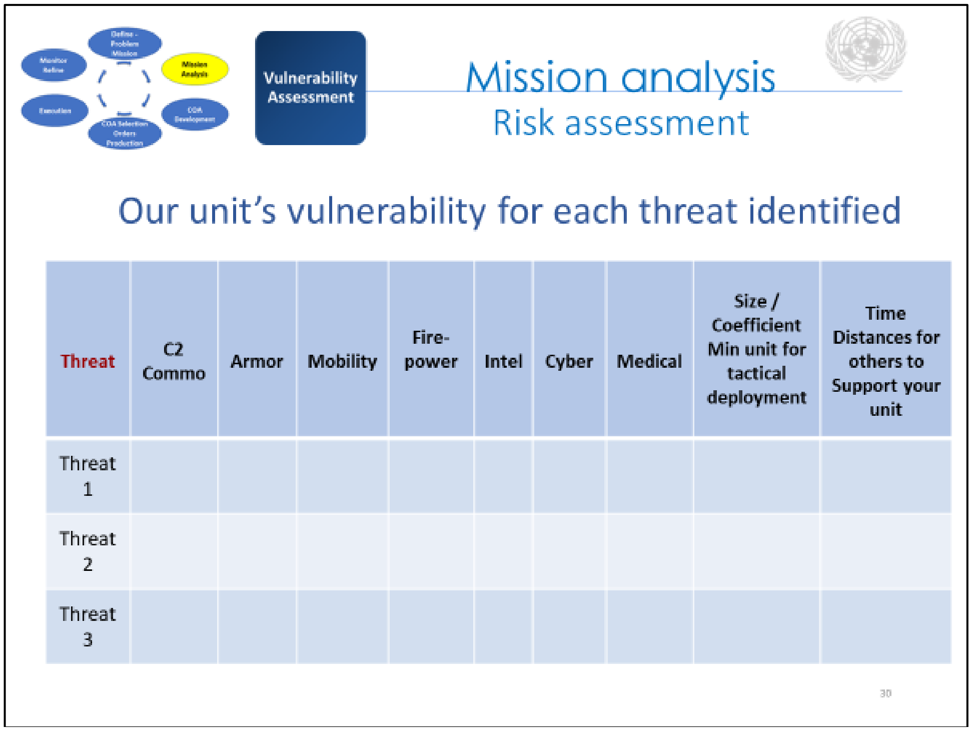
Losses of Key Elements: The exploitation of a vulnerability may result in the loss of key elements within our unit. These elements can include critical personnel, equipment, or infrastructure. By identifying and analysing the vulnerabilities associated with each threat, we can predict the possible losses and their impact on our operational effectiveness.

Losses of Critical Capabilities: Each vulnerability may correspond to a critical capability within our unit. This analysis examines the potential loss of these capabilities if a vulnerability is exploited. By understanding the dependencies between vulnerabilities and critical capabilities, we can determine the extent to which our operational effectiveness may be compromised.

Point of Not Being Able to Carry Out the Mission: The ultimate concern is reaching a critical threshold where the exploitation of vulnerabilities reaches a point where we can no longer carry out the mission effectively. This analysis involves determining the thresholds or tipping points where the cumulative impact of vulnerabilities and their exploitation becomes detrimental to the mission's success. By identifying these points in advance, we can develop contingency plans alternative courses of action, or allocate additional resources to prevent mission failure.

By conducting a predictive analysis that considers the potential casualties, losses of key elements, losses of critical capabilities, and the threshold of mission effectiveness, we gain insights into the potential consequences of vulnerability exploitation. This analysis allows us to make informed decisions, prioritise risk mitigation efforts, and develop strategies to ensure mission success even in the face of threats and vulnerabilities.

Slide 30


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Vulnerability Assessment

Mission analysis

Risk assessment

Our unit's vulnerability for each threat identified

Threat	C2 Commo	Armor	Mobility	Fire-power	Intel	Cyber	Medical	Size / Coefficient Min unit for tactical deployment	Time Distances for others to Support your unit
Threat 1									
Threat 2									
Threat 3									

30

In order to assess the relationship between each identified threat's course of action (COA) and our unit's capabilities and vulnerabilities, we can utilise a matrix or chart that considers various categories. These categories serve as valuable tools for the planner to evaluate the impact of each threat on our operation. Here are the categories that can assist in this analysis:

Command Control and Communications: This category examines our unit's ability to maintain effective command and control structures, as well as reliable communication channels, in the face of each threat. It evaluates how each COA may impact our ability to coordinate and communicate within our unit.

Armour: Assessing our unit's armour capabilities involves considering the protective measures available to mitigate certain types of attacks posed by enemy weaponry. This category analyses the adequacy of our unit's armoured vehicles and personal equipment in countering each specific threat.

Mobility: Evaluating mobility focuses on our unit's ability to manoeuvre and respond swiftly to changing circumstances. It examines how each threat's COA may impede our mobility and restrict our operational flexibility.

Firepower: This category explores our unit's offensive capabilities and the effectiveness of our weapons systems. It assesses how each COA may influence our ability to deliver firepower and neutralise threats effectively.

Intelligence Gathering and Situational Awareness: The capability to gather peacekeeping-intelligence and maintain situational awareness is crucial for mission success. This category examines our unit's ability to collect and analyse information and how each threat's COA may impact our peacekeeping-intelligence capacity.

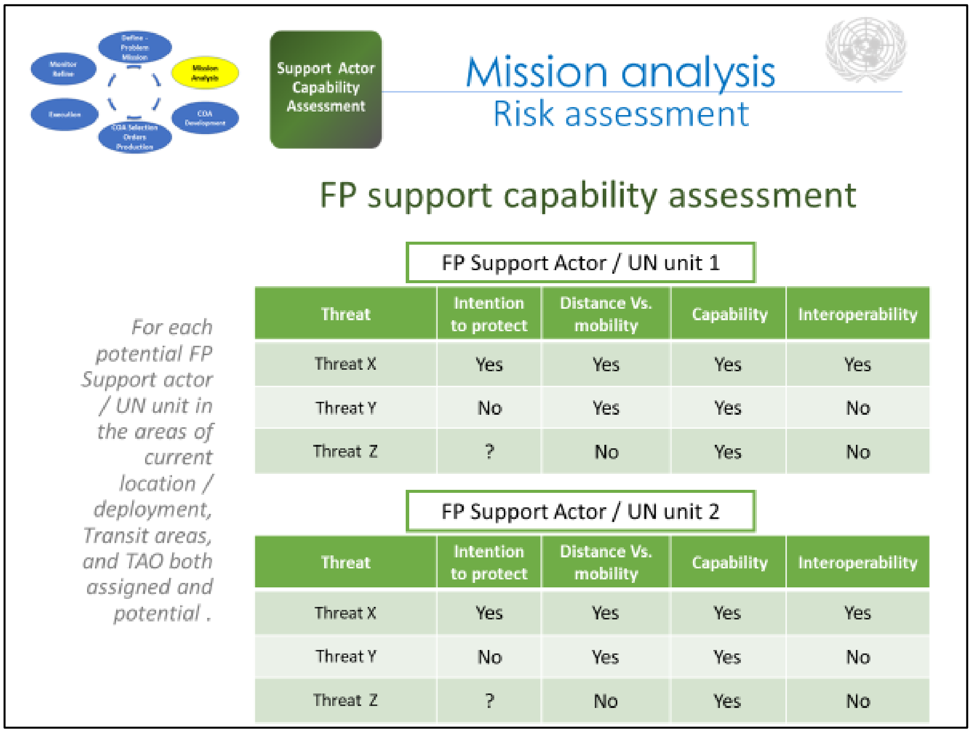
Medical Capacity and Capabilities: This category encompasses both the organic medical resources within our unit and the reach-back support available for casualty evacuation (CASEVAC). It evaluates our ability to provide medical care to our personnel in the face of each threat.

Coefficient of Forces Assessment: Assessing the coefficient of forces involves comparing our unit's tactical deployment and overall strength against that of the threat. This category examines the balance of power and assesses how our unit's capabilities align with each specific threat's COA.

Time-Distance Analysis: This analysis considers the time and distance required to provide additional support in times of crises or urgent need. It examines factors such as the availability of quick reaction forces (QRF) or CASEVAC assets and how they can assist our unit during critical situations.

By systematically evaluating each threat's COA within these categories, we can gain a comprehensive understanding of how our capabilities and vulnerabilities align with the potential risks. This analysis will enable us to prioritise threats and allocate resources effectively to mitigate their impact on our mission.

Slide 31


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Support Actor Capability Assessment

Mission analysis

Risk assessment

FP support capability assessment

For each potential FP Support actor / UN unit in the areas of current location / deployment, Transit areas, and TAO both assigned and potential .

FP Support Actor / UN unit 1

Threat	Intention to protect	Distance Vs. mobility	Capability	Interoperability
Threat X	Yes	Yes	Yes	Yes
Threat Y	No	Yes	Yes	No
Threat Z	?	No	Yes	No

FP Support Actor / UN unit 2

Threat	Intention to protect	Distance Vs. mobility	Capability	Interoperability
Threat X	Yes	Yes	Yes	Yes
Threat Y	No	Yes	Yes	No
Threat Z	?	No	Yes	No

To gain a comprehensive understanding of the risk levels involved, peacekeepers must conduct an analysis of the capabilities of other protection actors. This analysis involves assessing various factors related to these actors' ability to provide support.

Firstly, their intention to protect is evaluated. This refers to their commitment and willingness to actively engage in protecting the mission and its personnel. Understanding their level of dedication helps determine the extent to which they can contribute to mitigating risks.

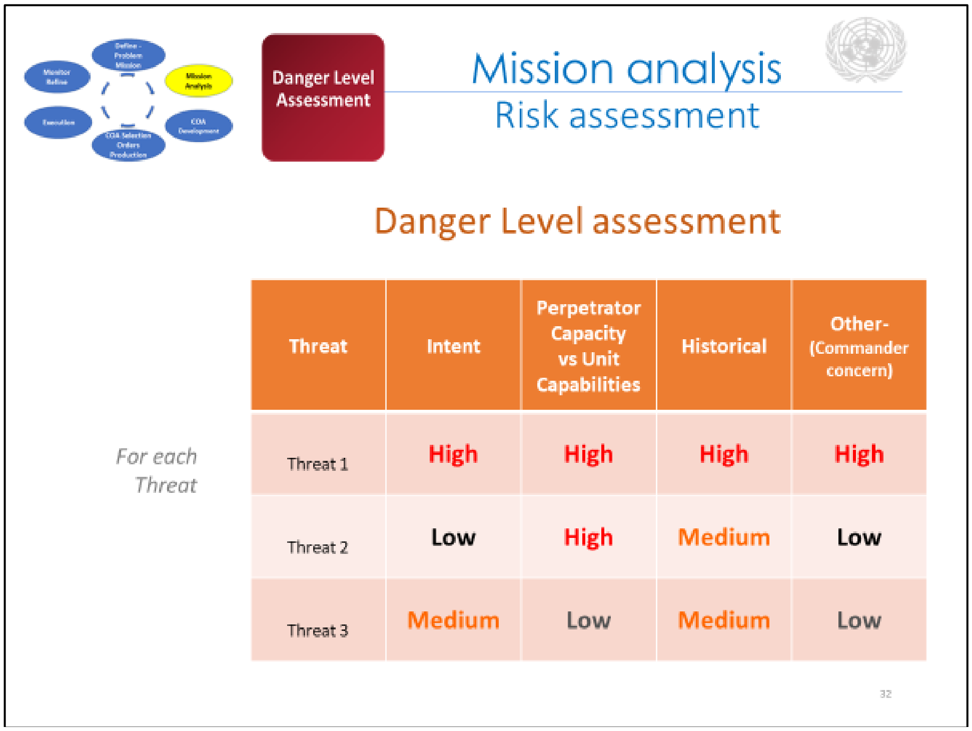
Next, the analysis considers the distance and mobility of these protection actors relative to the areas of interest. Their proximity to the operational areas and their ability to quickly respond and mobilise resources play a crucial role in their effectiveness as protection providers. Assessing their mobility capabilities allows missions to anticipate the level of support they can expect in different locations.

The overall capability of these protection actors is also assessed. This includes evaluating their training, equipment, and resources available for protection activities. An analysis of their capacity to counter potential threats provides insights into their effectiveness and the level of risk reduction they can offer.

Interoperability refers to the ability of a UN unit, a host nation security force, or another unit to work together effectively and seamlessly. It involves compatible communication systems, shared procedures, standardised protocols, and a mutual understanding of roles and responsibilities. By achieving interoperability, the units can enhance operational effectiveness, coordination, and cooperation in joint operations and peacekeeping missions. Additionally, it is important to determine whether these protection actors require assistance from the peacekeeping mission to be operational in the area. For example, they may rely on the mission for force protection or logistical support. Understanding their dependency on the mission enables better coordination and allocation of resources.

Once the capabilities of these potential support units/actors are established, we can make informed decisions regarding the expected support they can receive in different areas. This assessment influences the level of risk associated with specific threats. For instance, if certain actors are expected to provide substantial support in certain locations, the risk level may be lower compared to areas where their presence is limited. This information plays a critical role in prioritising activities and resource allocation to effectively address a threat.

Slide 32


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Danger Level Assessment

Mission analysis

Risk assessment

Danger Level assessment

For each Threat

Threat	Intent	Perpetrator Capacity vs Unit Capabilities	Historical	Other- (Commander concern)
Threat 1	High	High	High	High
Threat 2	Low	High	Medium	Low
Threat 3	Medium	Low	Medium	Low

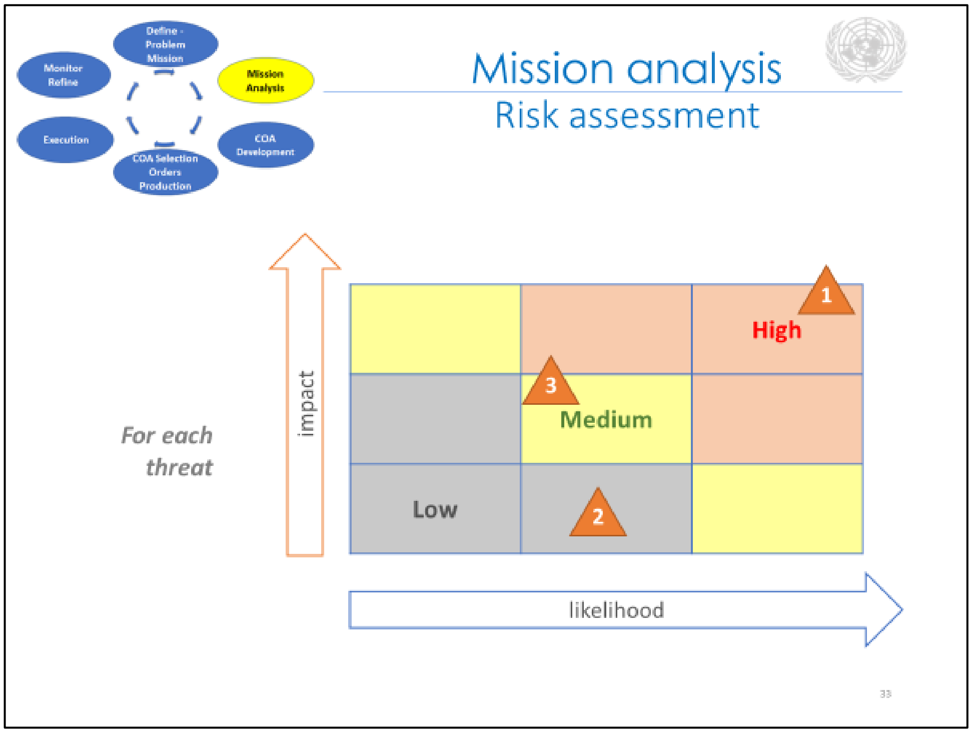
32

To visually portray the danger level assessment and help us prioritise threats effectively, the planner can use a chart that combines severity and probability factors. This assessment evaluates the degree or level of danger associated with each threat by considering both its potential impact on our unit and the likelihood of it occurring. By assessing the intent, the group's capacity/capability vs our unit capabilities, historical patterns, or background of violence against the UN or others, and any factor that the commander deems important.

Note that in this example, Threat 1 poses the greatest danger as it has both a high severity in relationship to our capabilities/vulnerabilities and a high level of intent and historical pattern to attack the UN. The group behind Threat 1 has the intent, along with the means and methods, to carry out the threat's course of action (COA). It is crucial to recognise that a threat's danger level is not solely determined by its capabilities but also by its intent. Even if a threat possesses significant capabilities, if it lacks the intent or reason to attack our unit, the probability is low, resulting in a lower danger/harm level.

By visually representing the danger level assessment in this chart, the planner can prioritise threats effectively, focusing on those with higher danger levels for more immediate attention and resource allocation. This helps ensure that appropriate measures are taken to mitigate the most significant risks to our unit and operation.

Slide 33



Mission analysis

Risk assessment

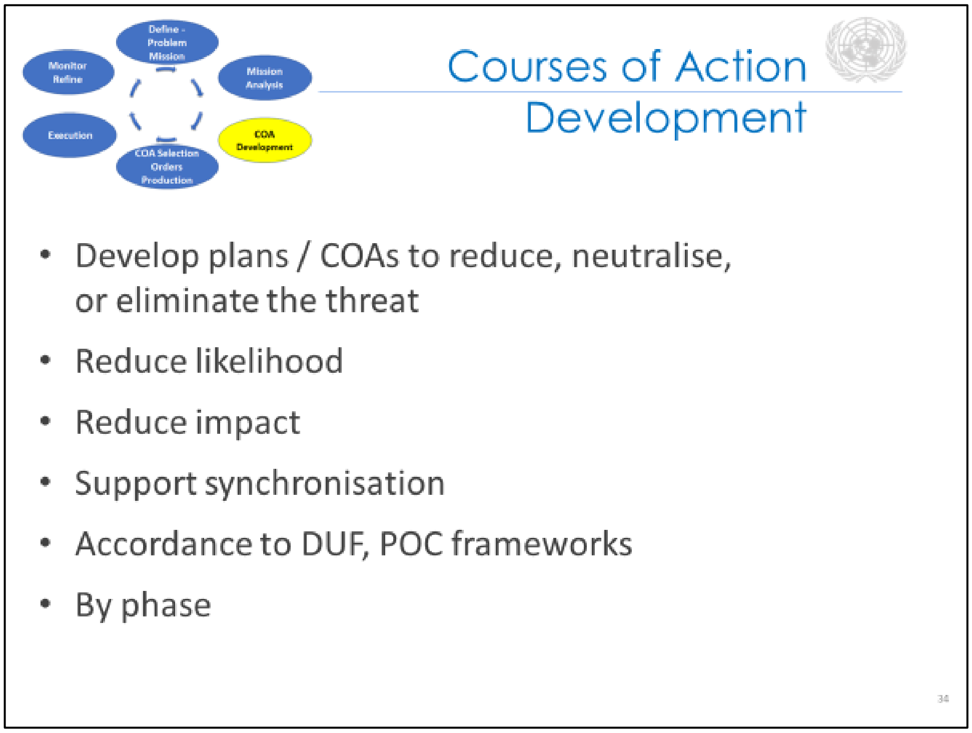
This graph will help planners visualise and prioritise multiple threats in terms of risk. Threat = Capability x intent, and all threats to our unit's current and future operations need to be identified. A potential perpetrator group with intent to cause harm but with minimal capability poses a limited threat, whereas a group with significant capability but no intent poses almost no threat. The capability of the peacekeeping unit to counter threats also needs to be considered because, again, even if a group has every intent to oppose a peacekeeping police unit if that peacekeeping police unit is able to prevent the group from operating effectively against them, they pose little threat to the operation.

The unit needs to prioritise FP threats in order to identify those situations where mitigating action is most needed. Risk is a product of the likelihood of an event occurring and the resulting impact if that event occurs. This process is facilitated by a risk analysis, which determines (a) the likelihood that a threat materialises and (b) the impact the threat would have if it materialised. The combination of those two factors allows missions to determine the risk associated with each threat identified (i.e. the threat COA).

Risk Management is a process that takes reasonable operational measures to reduce risk to personnel, equipment, and the operation. The probability and severity levels of threats are estimated based on the available knowledge of the probability of their occurrence and the severity of their consequences.

In the sample graph here, the highest priority is assigned to the threat that is the most likely to have the greatest impact (Threat 1). This threat was previously identified in the threat analysis table as a situation in which an armed group constituted a threat.

Slide 34


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Courses of Action Development

- Develop plans / COAs to reduce, neutralise, or eliminate the threat
- Reduce likelihood
- Reduce impact
- Support synchronisation
- Accordance to DUF, POC frameworks
- By phase

34

After completing the mission analysis in the Decision-Making Process (DMP), the focus now shifts to the development of courses of action (COA). This phase aims to mitigate the identified risks by formulating COAs that effectively reduce, neutralise, or eliminate the impact of the threats. Additionally, the objective is to decrease or eliminate the likelihood or potential of the threat's COA from occurring. However, it is essential to consider various factors and frameworks during the COA development process. Here is an expanded and improved explanation:

Mitigating Risk: The risk analysis conducted earlier provides valuable insights into the potential risks and vulnerabilities. The primary objective of COA development is to mitigate these risks by creating plans that effectively address and counteract/mitigate the identified threats. This involves designing COAs that reduce, neutralise, or eliminate the impact of the threats, as well as strategies to minimise the likelihood of their occurrence.

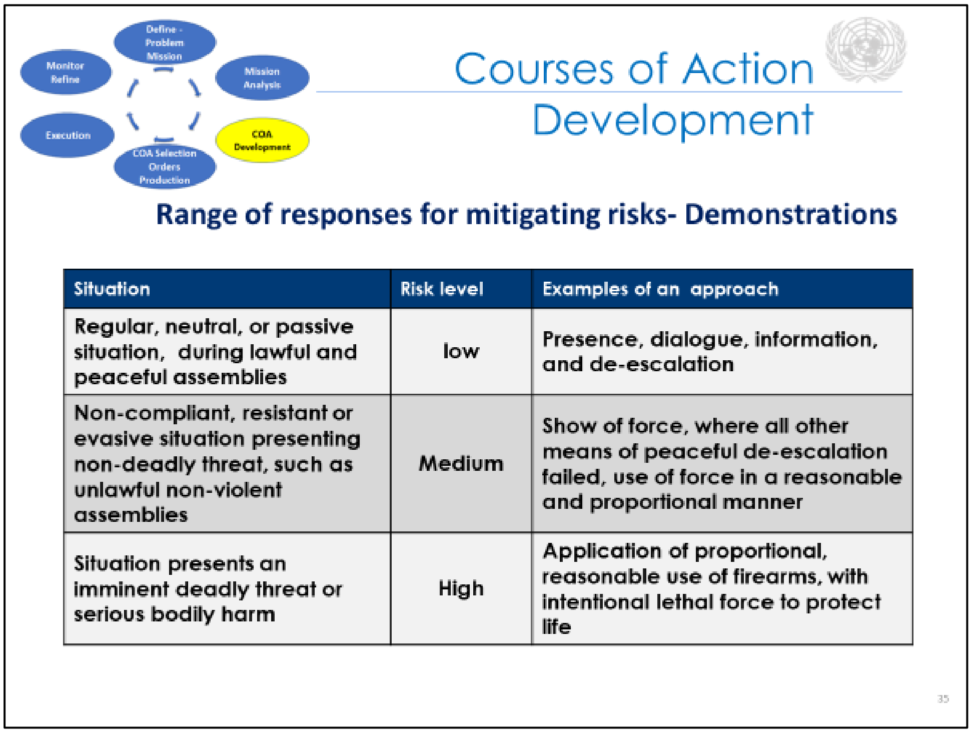
Compliance with Principles and Directives: While formulating COAs, it is imperative to consider and adhere to the principles and directives set forth by the United Nations (UN). These principles guide our actions and ensure that our operations align with the UN's mission and objectives. Additionally, compliance with the Directive on the Use of Force (DUF) is crucial to ensure the appropriate and lawful application of force when required. Furthermore, the protection of civilians and the prevention of collateral damage must be integral to the operational frameworks.

Resource Support, Synchronisation, and Coordination: During COA development, planners should consider the availability and coordination of resources and support from various mission components and support elements. This includes assessing the capabilities, capacities, and limitations of these resources to synchronise and coordinate effectively in the execution of the selected COA. This ensures that the required resources are available to support the successful implementation of the chosen plan.

Intelligence Acquisition Refinement: The development of COAs should be informed by accurate and up-to-date peacekeeping-intelligence. This involves refining the peacekeeping-intelligence acquisition process to gather relevant information and insights that further enhance the effectiveness of the COAs. By analysing and incorporating peacekeeping-intelligence findings, planners can make informed decisions and develop COAs that leverage actionable peacekeeping-intelligence.

Full Spectrum of Phases: Planners should consider the full spectrum of operational phases when developing COAs. This includes the current location, transit, and future area of deployment. By considering each phase, planners can ensure that the COAs are comprehensive.

Slide 35


Define - Problem Mission
Monitor Refine
Mission Analysis
Execution
COA Development
COA Selection Orders Production
35

Courses of Action Development

Range of responses for mitigating risks- Demonstrations

Situation	Risk level	Examples of an approach
Regular, neutral, or passive situation, during lawful and peaceful assemblies	low	Presence, dialogue, information, and de-escalation
Non-compliant, resistant or evasive situation presenting non-deadly threat, such as unlawful non-violent assemblies	Medium	Show of force, where all other means of peaceful de-escalation failed, use of force in a reasonable and proportional manner
Situation presents an imminent deadly threat or serious bodily harm	High	Application of proportional, reasonable use of firearms, with intentional lethal force to protect life

UN Police units should be ready and plan for risk mitigation. It is crucial in maintaining safety and security for all involved in various situations. Here are some examples of situations and a range of responses for mitigating risks at different levels:

Low Level - Lawful Peaceful Assembly:
Situation: Ensuring a peaceful assembly remains peaceful.
Response: Focus on dialogue and de-escalation techniques. Engage with protest organisers to understand their concerns, establish open lines of communication, and facilitate peaceful expression of grievances. Maintain a visible but non-threatening presence to deter potential disturbances. Use negotiators to address any potential conflicts or tensions and promote peaceful resolutions.

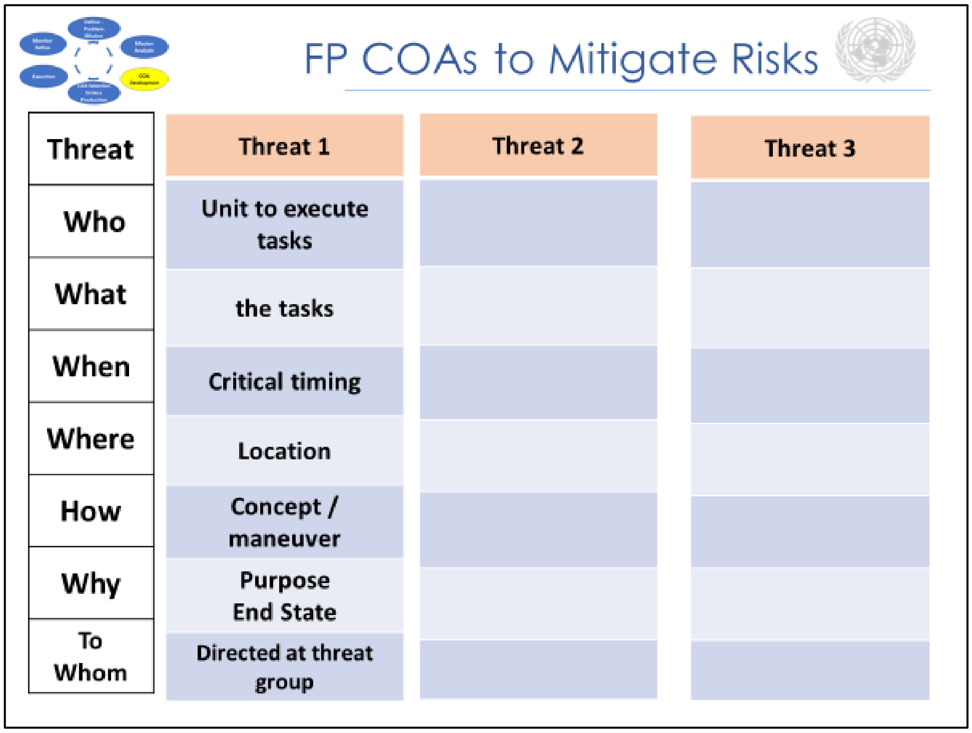
Medium Level - Unlawful Assembly with Non-Deadly Threats:
Situation: An unlawful assembly presents non-dead threats, such as property damage, public disruption, or threats of violence.
Response: Adopt a show of force and robust defensive posture. Deploy a visible, robust presence equipped with riot gear and non-lethal crowd control methodology.

Develop plans to disperse the crowd if necessary, using crowd management techniques and maintaining communication with protest leaders. If de-escalation attempts fail and there is an imminent threat, utilise reasonable force in a proportional manner to restore order and protect public safety.

High Level - Violent Demonstration with Potential for Bodily Harm or Deadly Consequences:
Situation: A demonstration turns violent, posing a risk of bodily harm or death to your unit or civilians.
Response: Use proportional and reasonable force to protect life and restore order. This may include the use of firearms in accordance with the DUF. Prioritise the safety of personnel and civilians by establishing secure perimeters and deploying specialised trained elements in handling high-risk situations. Maintain effective communication channels with local law enforcement, military, or other relevant agencies to coordinate response efforts. Utilise crowd control tactics, such as containment strategies, dispersal techniques, and targeted apprehensions, while adhering to human rights standards and UN Mission SOPs.

In all scenarios, it is crucial to conduct FP planning and maintain a strong emphasis on human rights and proportionality of the use of force to the extent possible. Regular training, adherence to established protocols, and effective coordination with other agencies and stakeholders contribute to successful risk mitigation in UN police operations.

Slide 36



FP COAs to Mitigate Risks

Threat	Threat 1	Threat 2	Threat 3
Who	Unit to execute tasks		
What	the tasks		
When	Critical timing		
Where	Location		
How	Concept / maneuver		
Why	Purpose End State		
To Whom	Directed at threat group		

In order to effectively mitigate risks and enhance force protection, unit commanders and staff must develop and codify Force Protection Courses of Action tailored to each identified threat. These FP COAs are designed to address risks and counter potential threats to the unit. The following chart helps visualise the COA components:

The UN unit, sub-unit, or support unit (WHO):
Clearly identify the specific element within the UN unit, sub-unit, or support unit that will be responsible for executing the task to combat the threat and mitigate risks. This could include specifying a particular company, platoon, or specialised team within the unit or a support unit.

The task to be executed (WHAT):
Define the mission or tasks that the identified unit element will execute to address the threat and mitigate risks. These tasks should be aligned with the overall FP objectives and may include activities such as enhanced perimeter security, conducting a patrol to overwatch an area where IEDs are normally emplaced, increased access control measures, and securing potential CASEVAC Landing Zones.

Methods of Operation/Tactics (HOW):
Outline the specific concepts, tactics, and techniques that the unit element will employ to execute the tasks. These methods should be based on best practices, standard operating procedures (SOPs), and lessons learned.

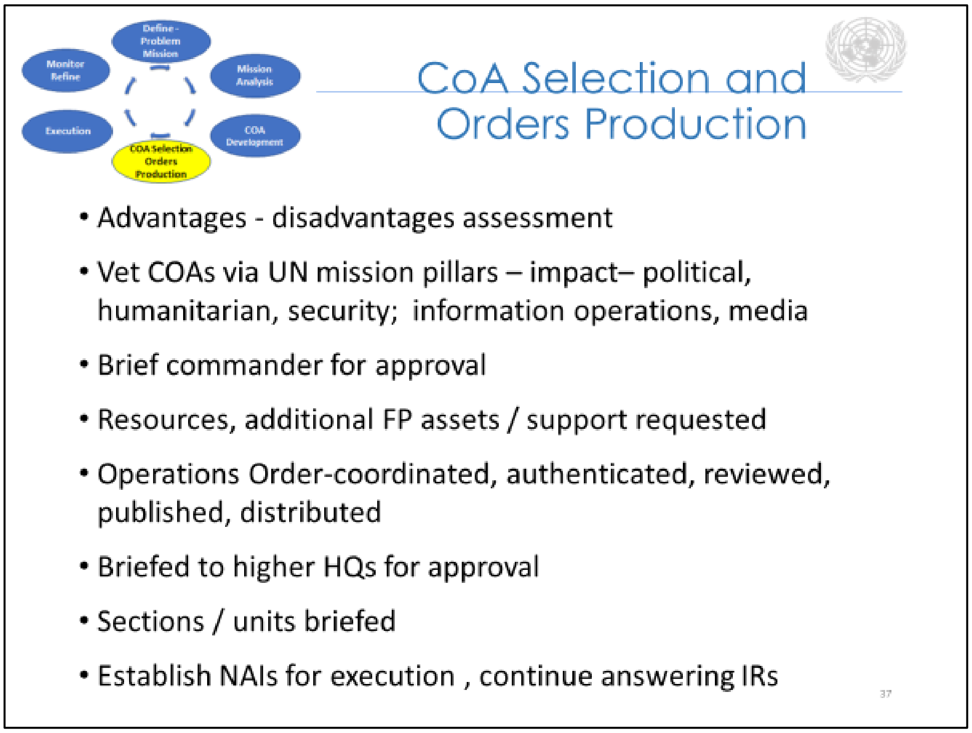
Areas/locations (WHERE):
Pinpoint the specific geographical locations or areas where the unit element will conduct the assigned tasks.

Reason (WHY):
Clearly articulate the purpose or reason behind the assigned tasks and how they contribute to the overall FP objectives. This could be expressed in terms of:
Commander's intentions, a desired end state and how the assigned tasks align with the broader FP strategy.

Date/time of execution (WHEN):
Specify when the tasks are to be executed, either by providing a specific date and time or by describing a sequence of events or conditions that must be met for the execution.

The identified group or threat element (To WHOM):
In certain situations, the executed tasks may be directed at a specific group or element that is part of the identified threat. Specify the target audience or recipient of the unit element's actions, such as hostile individuals, insurgent groups, or potential infiltrators.

Slide 37


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

CoA Selection and Orders Production

- Advantages - disadvantages assessment
- Vet COAs via UN mission pillars – impact– political, humanitarian, security; information operations, media
- Brief commander for approval
- Resources, additional FP assets / support requested
- Operations Order-coordinated, authenticated, reviewed, published, distributed
- Briefed to higher HQs for approval
- Sections / units briefed
- Establish NAIs for execution , continue answering IRs

37

After the development of the Force Protection Courses of Action, the subsequent steps involve vetting and analysing COAs using a criterion and getting the commander's approval.

Access advantages and disadvantages: Conduct a comprehensive assessment of each COA, weighing their respective advantages and disadvantages. This assessment should consider factors such as effectiveness, feasibility, and sustainability: Consider the long-term viability and sustainability of each COA, considering potential challenges and constraints.

Vetting COAs via UN mission pillars: Evaluate the potential impact of the COAs on the pillars of the UN Mission, political, humanitarian, and safety-security aspects. Consider how each COA aligns with the mission's goals and objectives, as well as the broader mandate of the UN. Additionally, assess the potential implications of the COAs on information operations and media perception, ensuring alignment with the mission's public affairs and communications strategies.

Commander COA briefing: The staff conducts a COA approval briefing that includes a summary of each COA, key elements, objectives, and expected outcomes.

Resource and additional FP assets/support request: Identify any additional resources or support required to execute the chosen COA(s). This could include requesting specific FP assets, such as additional personnel, specialised equipment, or enhanced peacekeeping-intelligence capabilities. Clearly articulate these resource requirements and justify their necessity to the commander.

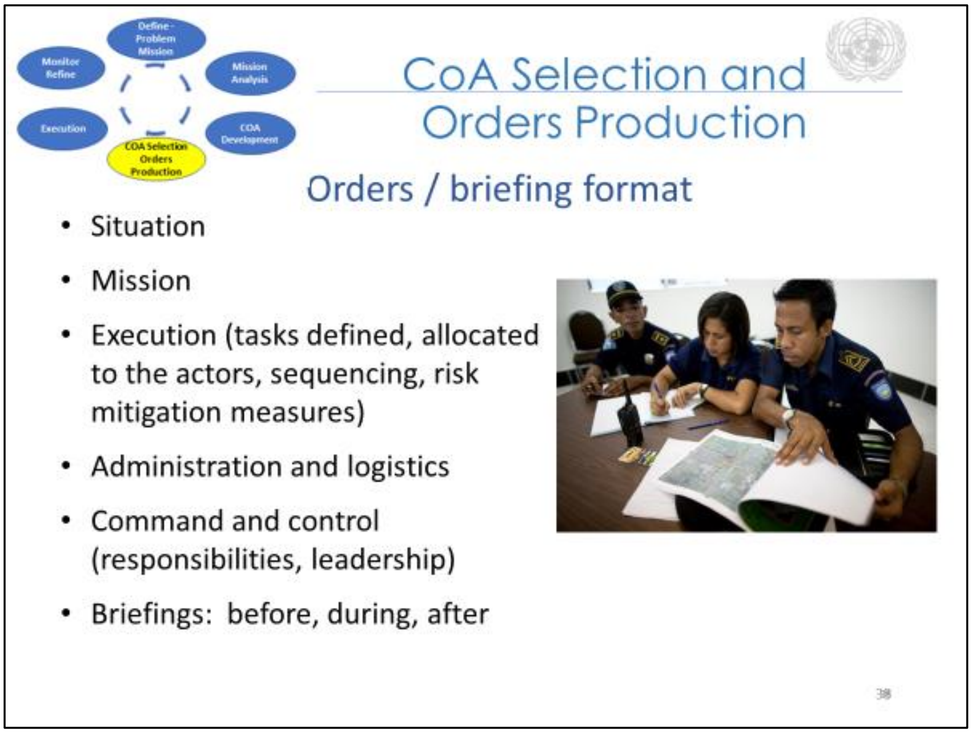
Operations Order Development: Following approval by the commander, the development of operations orders involves a series of steps, including coordination, review, and final authentication by the commander, as well as publication and distribution.

Briefing to higher HQs: The unit presents an order briefing to their higher headquarters, seeking guidance, approval, and any additional support. In case there are modifications to the original order, a fragmentation order (FRAGO) might be necessary to address any adjustments made by the higher HQs.

Sections/units briefed: Conduct briefings to all relevant sections and units involved in the execution. Ensure that each section or unit understands its roles, tasks, and responsibilities within the force protection plan.

Establish Named Areas of Interest (NAIs) for execution, continue answering Information Requirements (IRs): Define and establish Named Areas of Interest (NAIs) that serve as focal points for executing tasks. Additionally, continue addressing Information Requirements (IRs) to gather critical peacekeeping-intelligence and maintain situational awareness.

Slide 38



CoA Selection and Orders Production

Orders / briefing format

- Situation
- Mission
- Execution (tasks defined, allocated to the actors, sequencing, risk mitigation measures)
- Administration and logistics
- Command and control (responsibilities, leadership)
- Briefings: before, during, after

38

Each here is a recommended format for an Operations Order and Briefing:

Situation:
This section provides a comprehensive overview of the current overall situation, including the existing threats and risks. Identify the key environmental factors that may impact the mission and the overall operational environment.

Mission:
Clearly articulate the mission statement, defining the objectives, desired end-state, and any specific tasks that need to be accomplished. The mission statement should be concise, measurable, and aligned with the higher headquarters' intent.

Execution:
Break down the execution phase into sub-sections, sub-units covering the following aspects:

Specify the tasks that need to be performed to achieve the mission. Each task should be clearly defined and allocated to the relevant actors or units responsible for its execution.

Sequencing the tasks by outlining the chronological order in which the tasks should be carried out, considering any dependencies or prerequisites. Provide a logical flow of actions to ensure smooth coordination and maximise efficiency.

Identify and address potential risks and hazards associated with the execution of the tasks. Propose specific measures and procedures to minimise these risks, ensuring the safety of personnel and the successful completion of the mission.

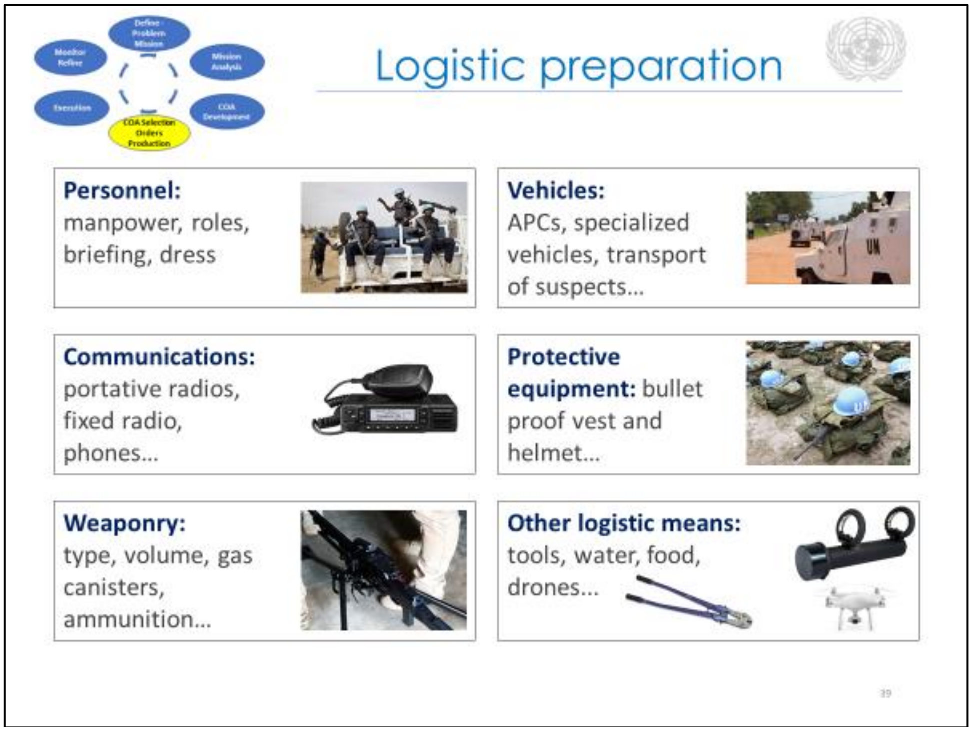
Administration and Logistics:
Include relevant information regarding administrative and logistical support required for the operation. This may involve details about supply chains, transportation, communication systems, medical support, and other necessary resources.

Command and Control:
Clearly define the responsibilities and roles of key personnel involved in the operation. Establish a command structure that ensures effective communication, coordination, and decision-making throughout the mission. Highlight the chain of command and any delegation of authority.

Briefings:
Outline the pre-mission briefings necessary to ensure all personnel are informed about the mission objectives, tasks, and any critical information relevant to their roles. Specify the requirements for in-mission briefings, such as regular updates, situational awareness reports, and any changes or developments that need to be communicated to the team. Describe the post-mission briefings to analyse the outcomes, assess the mission’s success, capture lessons learned, and identify areas for improvement in future operations.

By following this recommended format, the operations order and briefing will provide a comprehensive and structured plan that facilitates effective execution, minimises risks, and ensures the mission’s success.

Slide 39


Define Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Logistic preparation

Personnel: manpower, roles, briefing, dress

Vehicles: APCs, specialized vehicles, transport of suspects…

Communications: portative radios, fixed radio, phones…

Protective equipment: bullet proof vest and helmet…

Weaponry: type, volume, gas canisters, ammunition…

Other logistic means: tools, water, food, drones…

39

During the order production phase of the Decision-Making Process (DMP), meticulous logistics and support preparations play a crucial role. This section highlights key areas of focus for effective preparations.

Personnel Preparation:
Ensure that personnel are adequately prepared for the upcoming operation. This includes assessing their readiness, verifying their training and qualifications, and addressing any additional training needs. Verify the availability of required personnel and their assigned roles within the operation.

Communications Preparation:
Establish robust and reliable communication systems to facilitate effective coordination and information flow during the operation. Ensure that communication equipment is operational, properly configured, and compatible with other units and higher headquarters. Test communication protocols and conduct exercises to validate communication procedures.

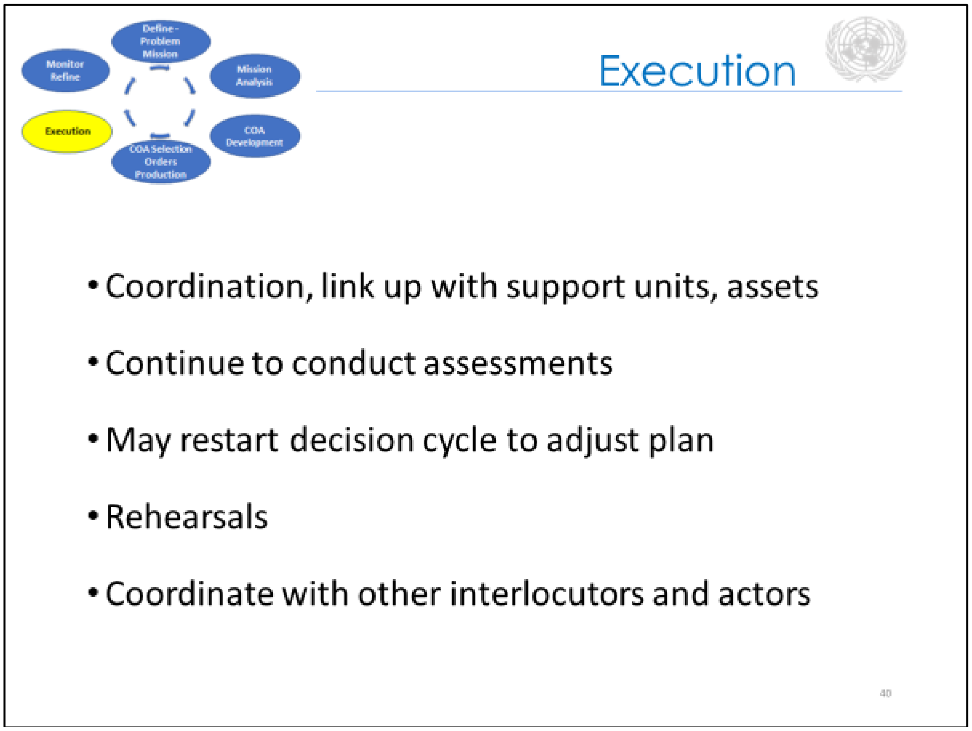
Weapons Preparation:
Thoroughly inspect, maintain, and prepare weapons systems to guarantee their operational readiness. Conduct functional checks, verify ammunition stocks, and ensure proper storage and transportation procedures. Coordinate with the appropriate units for any specialised weapons or equipment requirements.

Vehicles Preparation:
Assess and prepare all vehicles required for the operation. Conduct routine maintenance, fuel, and fluid checks, and ensure proper functioning of essential vehicle systems. Coordinate transportation requirements, verify vehicle availability, and assign drivers or operators as necessary.

Protection and Specialised Equipment Preparation:
Evaluate and prepare specialised equipment necessary for the protection and safety of personnel during the operation. This includes personal protective gear, medical supplies, and any specialised equipment specific to the mission's requirements. Ensure that all protective equipment is inspected, maintained, and readily available for deployment.

By prioritising logistics and support preparations in these key areas, the overall operational readiness is enhanced. This comprehensive approach ensures that personnel are adequately trained, communication channels are established, weapons and vehicles are in optimal condition, and necessary protection and specialised equipment are readily accessible. These preparations contribute to the successful execution of the mission and FP tasks while maintaining the effectiveness of the police unit.

Slide 40


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Execution

- Coordination, link up with support units, assets
- Continue to conduct assessments
- May restart decision cycle to adjust plan
- Rehearsals
- Coordinate with other interlocutors and actors

40

Tasks During the Execution Phase:

Coordination and Link-Up with Support Units and Assets:
Maintain ongoing coordination and establish necessary link-ups with support units and assets to ensure seamless integration and collaboration. This includes coordinating with adjacent units, support elements, and any external organisations or agencies involved in the operation. Regular communication and synchronisation with these entities are crucial for mission success.

Continuous Assessments:
Throughout the execution phase, conduct regular assessments to evaluate the progress of the operation. Monitor the evolving situation, gather information, and assess the effectiveness of actions taken. This allows for real-time adjustments, identification of emerging challenges, and informed decision-making.

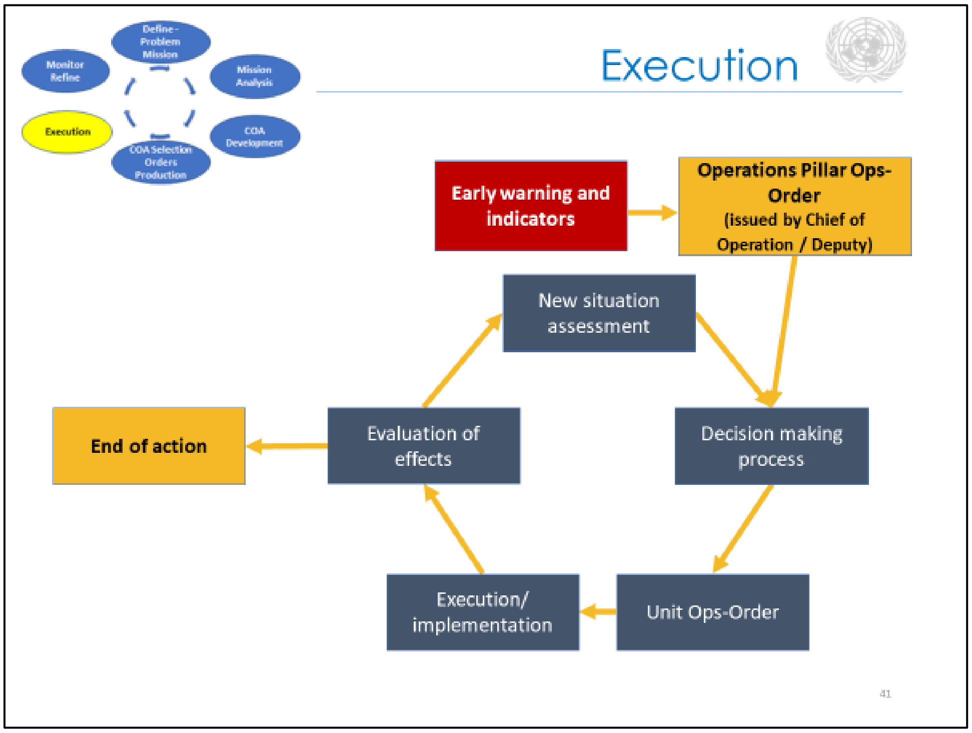
Decision Cycle Adjustment:
Be prepared to restart the decision cycle if required. As the situation evolves, it may be necessary to reassess the plan and adjust. Revisit the decision-making process, reassess the mission objectives, and update the plan accordingly to maintain alignment with the changing circumstances.

Rehearsals:
Conduct rehearsals to ensure that all personnel are familiar with their roles, responsibilities, and the overall operational plan. Rehearsals provide an opportunity to validate coordination procedures, refine tactics, techniques, and procedures (TTPs), and identify potential areas for improvement. This enables the team to enhance cohesion, synchronisation, and overall operational effectiveness.

Coordination with Other Interlocutors and Actors:
Maintain coordination and communication with relevant interlocutors and actors involved in the operation. This may include liaising with local authorities, partner forces, civilian organisations, or other stakeholders. Effective coordination fosters cooperation, shared situational awareness, and the ability to leverage collective resources and capabilities.

By actively engaging in these tasks during the execution phase, you can optimise operational efficiency, adapt to changing conditions, and enhance overall coordination and effectiveness. These actions contribute to the successful achievement of mission objectives while promoting flexibility, responsiveness, and collaboration among all involved.

Slide 41



Execution

Define - Problem Mission

Mission Analysis

COA Development

COA Selection Orders Production

Execution

Monitor Refine

Early warning and indicators

Operations Pillar Ops-Order (issued by Chief of Operation / Deputy)

New situation assessment

Decision making process

Unit Ops-Order

Execution/ implementation

Evaluation of effects

End of action

41

During the execution stage, a continuous analysis process and assessment cycle are vital for effective operations. Leaders and staff engage in ongoing monitoring and make necessary adjustments to the existing plan. A diagram visually represents this cycle of analysis. Key to this (indicated in the red box) is the maintenance of a common operational picture and situational awareness that provides early warning and specific indicators which are crucial for informed decision-making.

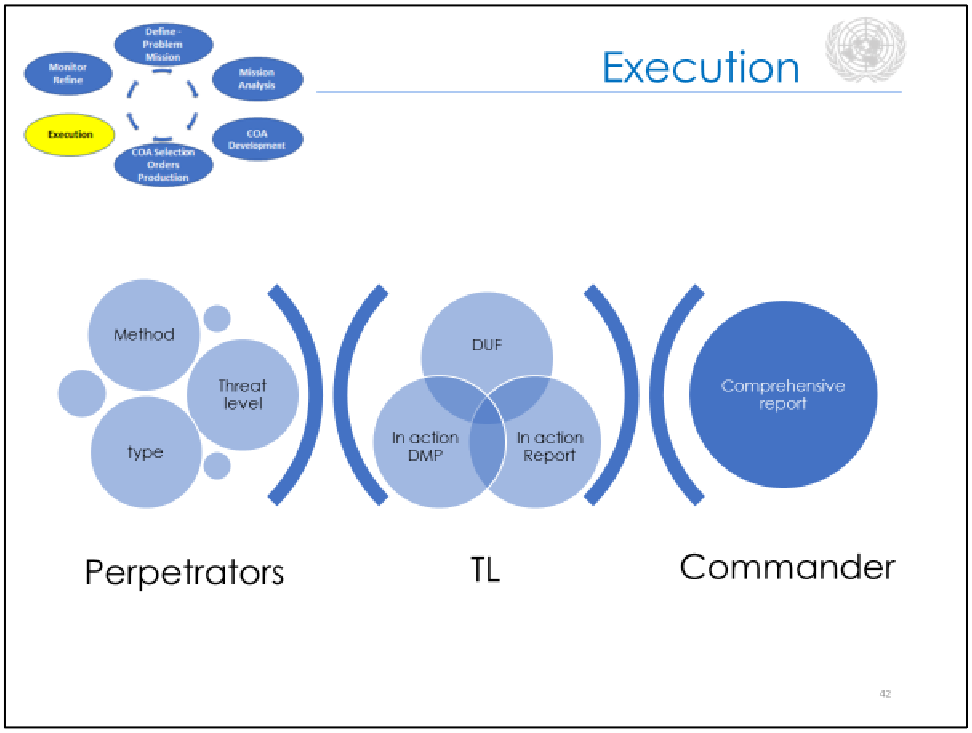
Within the execution stage, an iterative analysis process and assessment cycle are conducted. Leaders and staff actively monitor the progress of the operation, evaluate its effectiveness, and gather relevant data and information. This continuous analysis allows for the timely identification of potential issues, challenges, or changing circumstances that may require adjustments to the plan.

Leadership and staff utilise the feedback gathered during the analysis process to assess the current situation accurately. They compare it against the desired outcomes and objectives set forth in the initial plan. Changes and adjustments from the original plan may be required.

The diagram illustrating this analysis cycle visually represents the ongoing nature of this process. It showcases the iterative nature of monitoring, evaluation, and adjustment, emphasising the dynamic and adaptive nature of operations.

In summary, within the execution stage, continuous analysis and assessment are conducted to ensure operational effectiveness. Maintaining a common operational picture and situational awareness is essential for informed decision-making. By incorporating feedback, monitoring progress, and adjusting the plan accordingly, leaders and staff can optimise outcomes and adapt to changing circumstances during the execution of the operation.

Slide 42



Execution

This slide demonstrates the dynamic nature of operations, where both the unit and the perpetrators continuously adjust their Courses of Action during execution. While the Force Protection plan serves as an initial starting point, it is common for units to transition to actions on contact or predefined drills to mitigate risks effectively. However, comprehensive and robust FP planning plays a crucial role in enabling the unit to execute reaction drills more effectively.

In the execution phase, it is essential to recognise that the operational environment is fluid, and unexpected developments can arise. Both the unit and the attackers constantly adapt and modify their COAs based on the evolving situation. This necessitates a flexible and agile approach to response and countermeasures.

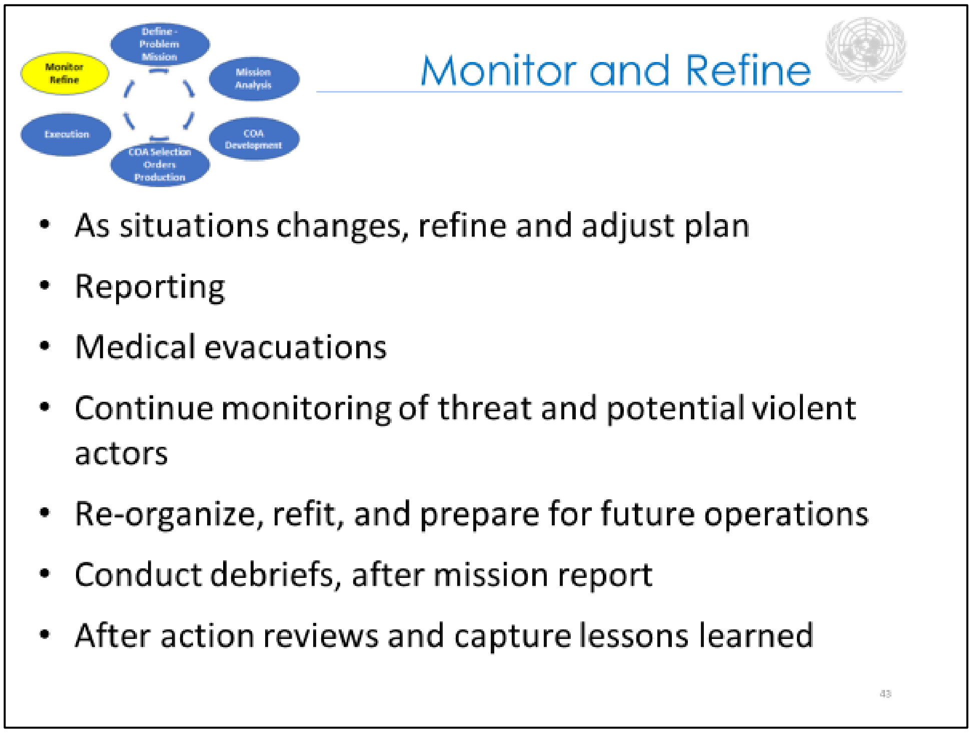
While units may initially rely on the FP plan, they often transition to actions on contact or drills that have been practised and rehearsed. These predefined drills enable the unit to respond swiftly and effectively to threats, reducing the potential risks and vulnerabilities. The use of reaction drills allows for rapid decision-making and execution in high-stress situations where time is of the essence.

However, it is important to emphasise that solid planning forms the foundation for successful execution. A well-developed FP plan, based on thorough risk assessments, peacekeeping-intelligence analysis, and understanding of the operational environment, enhances the unit's preparedness. By identifying potential threats, vulnerabilities, and critical assets in advance, the unit can proactively develop strategies and countermeasures to address them.

Moreover, comprehensive planning facilitates the establishment of protocols, communication channels, and coordination mechanisms necessary for the efficient execution of reaction drills. It ensures that the unit is equipped with the necessary resources, equipment, and training to respond effectively.

In summary, this slide highlights the iterative nature of COA adjustments by both the unit and the perpetrators during execution. While relying on actions on contact or drills is a common approach to mitigate risks, solid planning remains a critical factor in enabling units to be better prepared for execution. By incorporating continuous evaluation, dynamic response mechanisms, and comprehensive preparation, units can enhance their operational effectiveness and mitigate potential threats more efficiently.

Slide 43


Define - Problem Mission
Mission Analysis
COA Development
COA Selection Orders Production
Execution
Monitor Refine

Monitor and Refine

- As situations changes, refine and adjust plan
- Reporting
- Medical evacuations
- Continue monitoring of threat and potential violent actors
- Re-organize, refit, and prepare for future operations
- Conduct debriefs, after mission report
- After action reviews and capture lessons learned

43

During the monitor and refine phase of the DMP, the following key tasks should be accomplished:

Refining and Adjusting the Plan:
As situations change on the ground, it is essential to continually assess and adapt the plan accordingly. Refine and adjust to any emerging challenges and maintain situational awareness.

Reporting:
Maintain a robust reporting system to provide timely and accurate updates. Report significant events, changes in the operational environment, and any pertinent information that may impact future operations or require higher-level attention.

Medical Evacuations:
Ensure the timely and efficient evacuation of casualties and wounded personnel requiring medical attention. Prioritise the well-being of all personnel, promptly coordinate medical evacuation procedures, and provide necessary support and resources to medical teams.

Continuously Monitoring Threats and Potential Violent Actors:
Maintain vigilant surveillance and monitoring of threats and potential violent actors within the operational area. This includes gathering and analysing peacekeeping-intelligence, tracking the activities of hostile elements, and maintaining situational awareness to mitigate risks and ensure FP.

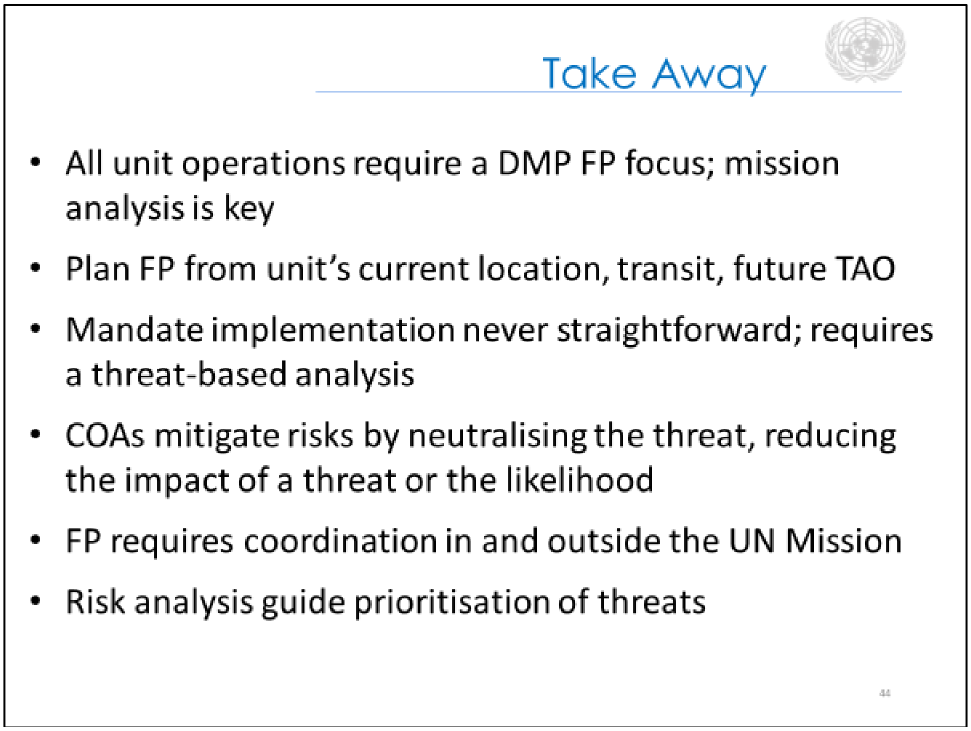
Re-organising, Refitting, and Preparing for Future Operations:
After the completion of a mission, allocate time and resources for re-organisation, refitting, and preparing for future operations. This includes conducting maintenance on equipment, replenishing supplies, and repositioning forces as necessary to maintain readiness and operational effectiveness.

Conducting Debriefs and After Mission Reports:
Conduct debriefing sessions with personnel involved in the operation to gather insights and lessons learned. Compile the information gathered into comprehensive After Mission Reports, documenting the successes, challenges, and recommendations for improvement.

After Action Reviews and Capturing Lessons Learned:
Facilitate Action Reviews (AARs) to collectively analyse the mission’s outcomes, identify strengths and areas for improvement, and capture lessons learned. This valuable feedback informs future planning, enhances performance, and fosters a culture of continuous improvement.

By accomplishing these key tasks during the monitor and refine phase of the DMP, we promote flexibility, adaptability, and informed decision-making. This comprehensive approach ensures the ongoing refinement of plans, effective reporting, proper medical support, continuous threat monitoring, readiness for future operations, and the capture of valuable lessons for organisational growth and operational excellence.

Slide 44



Take Away

- All unit operations require a DMP FP focus; mission analysis is key
- Plan FP from unit's current location, transit, future TAO
- Mandate implementation never straightforward; requires a threat-based analysis
- COAs mitigate risks by neutralising the threat, reducing the impact of a threat or the likelihood
- FP requires coordination in and outside the UN Mission
- Risk analysis guide prioritisation of threats

44

Summary

Integrating FP considerations into the Decision-Making Process (DMP) for all operations ensures that the security of personnel, assets and freedom of action remain a priority.

Recognise that mission analysis plays a vital role in effective FP planning. Thoroughly assess the operational environment, including the current location, transit routes, and future Tactical Area of Operations (TAO). This analysis enables the identification of potential risks specific to each phase of the operation.

Acknowledge that the implementation of the mandate is not always straightforward, requiring a comprehensive threat-based analysis. Understand the potential threats and assess their impact and likelihood. This analysis enables the development of countermeasures (COAs) that can mitigate risks, reducing their impact or likelihood.

Effective coordination ensures the exchange of relevant information, the alignment of efforts, and the optimisation of resources to enhance FP planning and execution.

Utilise risk analysis as a guide to prioritise threats. Evaluate the likelihood and potential impact of each identified threat, enabling the allocation of resources and efforts based on their relative significance. This prioritisation ensures that FP measures are focused on addressing the most critical threats to mission success.

Lesson 3.3

Tactical Planning Considerations for IED Risk Mitigation

Starting the Lesson

For an interactive start to this Lesson, ask the participants if they have had experience in a UN Peace Operation with the specific challenges planning operations in a IED threat environment.

☞***Note to instructor –*** *recommend that the lesson be presented by a trainer who has some personal experience with explosive hazards, EOD expertise, or has worked with UNMAS*

☞ ***Recommend-*** *that instructors review the UN IED Threat Mitigation Handbook and Lessons concerning IEDs and EOD in the UNIBAT STM.*

Slide 1

Lesson 3.3
Tactical Planning Considerations for IED Risk Mitigation
(Supplemental to Lessons 3.1 & 3.2)

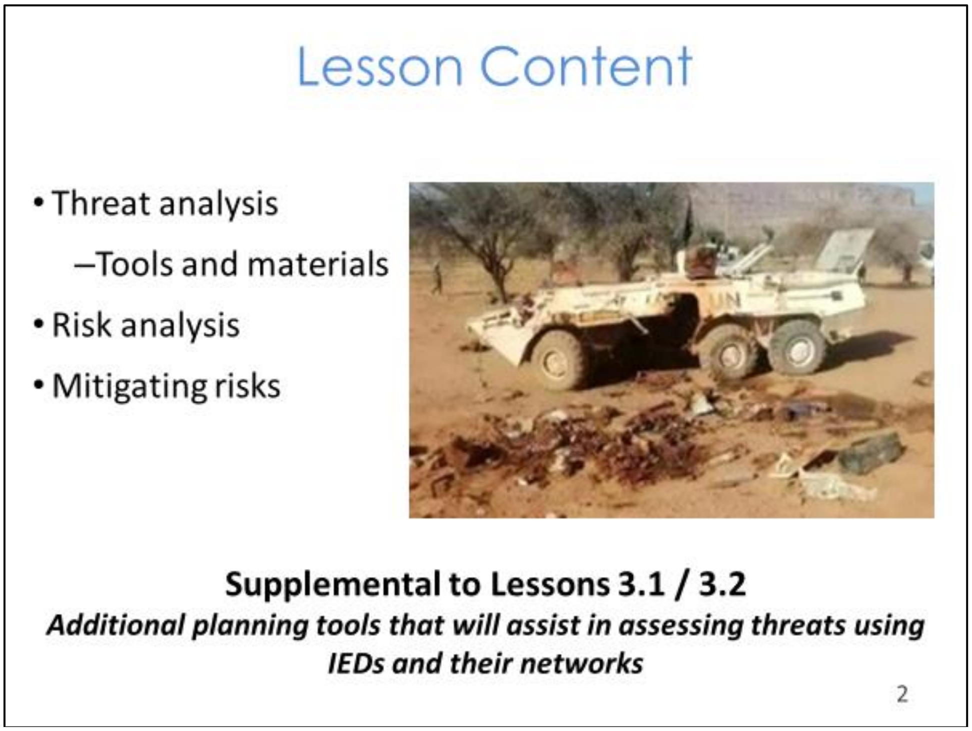
1

The frequency of IED attacks targeting peacekeepers has reached an alarming level, resulting in an increasing number of fatalities and injuries. In this lesson on Planning Considerations (Supplemental) for Improvised Explosive Devices (IED), we aim to enhance your understanding and provide additional planning tools to address the persistent threat of IED attacks and their associated networks. This lesson serves as a supplement to lessons 3.1 and 3.2, offering additional materials and tools to support a comprehensive analysis of the IED networks.

By employing these additional resources, we can adopt a more holistic approach to planning, with a strong focus on preventive and remedial measures to mitigate the risk of explosions. Our goal is to identify and disrupt various segments within the IED network, aiming to neutralise and ultimately eliminate the dangers posed to our peacekeeping forces.

Together, by implementing comprehensive threat-based planning, we can effectively anticipate and address potential IED threats.

Slide 2



Lesson Content

- Threat analysis
  - Tools and materials
- Risk analysis
- Mitigating risks

Supplemental to Lessons 3.1 / 3.2

Additional planning tools that will assist in assessing threats using IEDs and their networks

2

Here is the Lesson Outline:

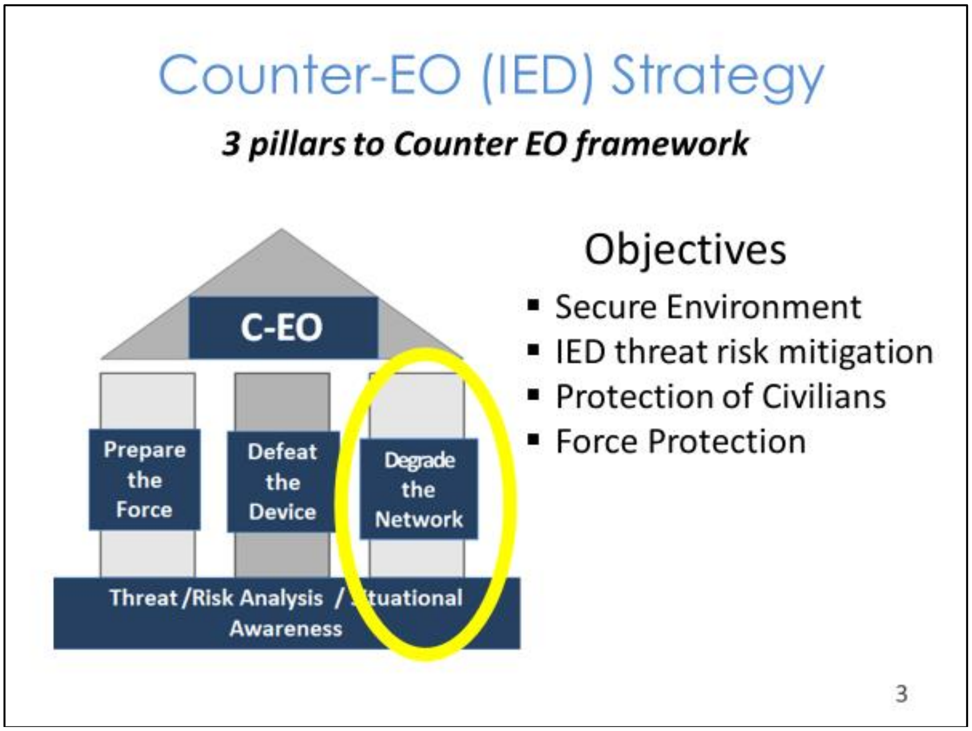
Threat Analysis: In this section, we will thoroughly examine the various threats associated with IED attacks, considering their nature, origin, and potential impact on peacekeepers. By conducting a comprehensive threat analysis, we can gain a deeper understanding of the risks involved.

Risk Analysis: Building upon the threat analysis, we will proceed to assess the risks posed by IED attacks. This step involves evaluating the probability and potential impact of such attacks, allowing us to prioritise our mitigation efforts effectively.

Mitigating Risks/Neutralising: This section focuses on proactive measures aimed at mitigating the identified risks and neutralising the IED threat. We will explore preventive strategies and countermeasures to reduce the likelihood of attacks and minimise their impact on peacekeepers.

☞***Note:*** *This lesson serves as a supplement to lessons 3.1 and 3.2 and does not replace them. While the same FP planning process is utilised to identify threats related to IED attacks, this lesson introduces additional planning tools. Rather than repeating the entire process, we focus on enhancing planners' abilities to mitigate IED risks and degrade the IED networks.*

Slide 3



Counter-EO (IED) Strategy

3 pillars to Counter EO framework

C-EO

Prepare the Force

Defeat the Device

Degrade the Network

Threat /Risk Analysis / Situational Awareness

Objectives

- Secure Environment
- IED threat risk mitigation
- Protection of Civilians
- Force Protection

3

As discussed in Module 1, the Counter-EO (IED) Strategy relies on three pillars:

Prepare the Force/Units: We emphasise the importance of thorough preparation, equipping our units with the necessary knowledge, skills, and resources to combat the IED threat effectively. This includes comprehensive training, peacekeeping-intelligence gathering, and the implementation of appropriate protocols and procedures.

Defeat the Device: We focus on developing techniques and tactics to neutralise and defeat IED devices themselves. This involves utilising specialised equipment, employing advanced detection methods, and conducting safe disposal operations.

The third pillar is to degrade the network. In this lesson, our primary focus will be on the degradation of the IED network. Our strategy places significant emphasis on collecting and developing mitigating strategies on the IED network itself. By degrading the network, we disrupt the supply chains, communication channels, and logistical support vital to the functioning of IED operations. This proactive approach may help prevent detonations and impede the overall effectiveness of an IED network.

Rather than solely addressing post-IED actions, we aim to shift our perspective towards a more proactive approach to mitigating IED risks. Our objective is to take necessary measures to degrade, impede, or neutralise the network before any detonation occurs.

The overall goals and objectives of the – EO (IED) strategy are as follows:

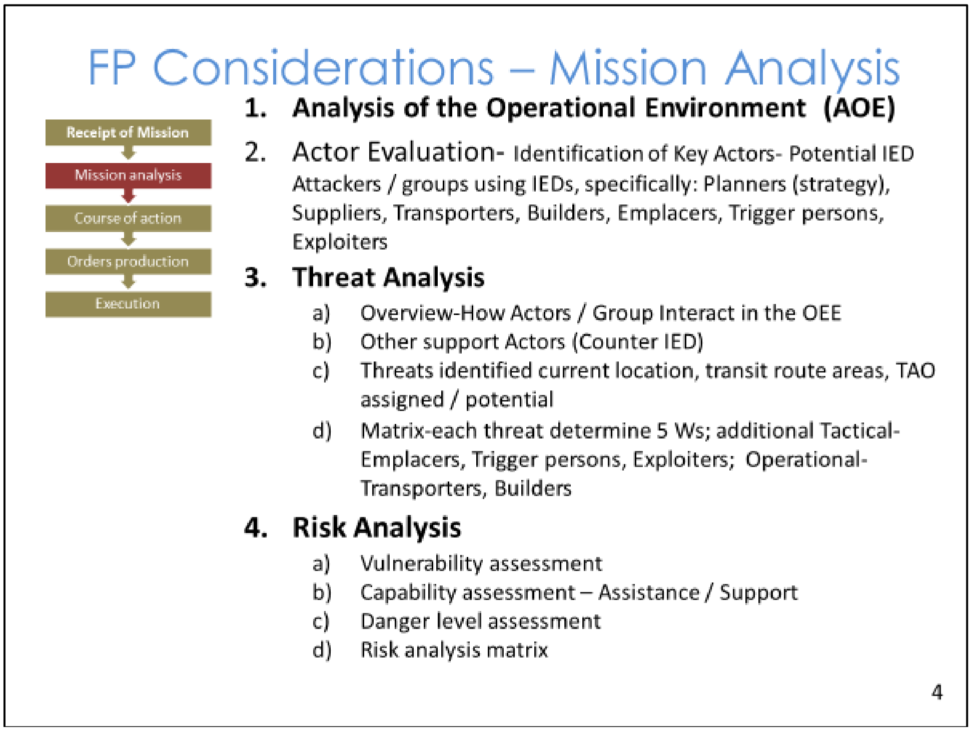
Create a Secure Environment: We aim to create a safe and secure environment for all UN personnel. By degrading the IED network, we can significantly reduce the risk level and enhance overall security in order to accomplish the UN mandate.

IED Threat Risk Mitigation: Through proactive FP planning and pre-emptive actions, we seek to mitigate the risks associated with IED attacks. This involves implementing comprehensive strategies to minimise the likelihood of incidents and their impact.

Protection of Civilians: We recognise the importance of protecting civilian populations in conflict areas. By degrading the IED network, we can effectively reduce the risk posed to innocent civilians, ensuring their safety and well-being.

Force Protection: By degrading the IED network, we actively work towards preserving freedom of action and minimising casualties.

Slide 4



FP Considerations – Mission Analysis

Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

1. **Analysis of the Operational Environment (AOE)**
2. Actor Evaluation- Identification of Key Actors- Potential IED Attackers / groups using IEDs, specifically: Planners (strategy), Suppliers, Transporters, Builders, Emplacers, Trigger persons, Exploiters
3. **Threat Analysis**
   a) Overview-How Actors / Group Interact in the OEE
   b) Other support Actors (Counter IED)
   c) Threats identified current location, transit route areas, TAO assigned / potential
   d) Matrix-each threat determine 5 Ws; additional Tactical- Emplacers, Trigger persons, Exploiters; Operational- Transporters, Builders
4. **Risk Analysis**
   a) Vulnerability assessment
   b) Capability assessment – Assistance / Support
   c) Danger level assessment
   d) Risk analysis matrix

4

In the Mission Analysis stage, we will continue to follow the process we discussed in lessons 3.1 and 3.2. However, our specific focus now shifts to IED attacks and their associated IED networks. We will not repeat the entire process in these two lessons. Instead, we will highlight the tools and suggested FP planning methodology focused on IED threats.

Item #1, Analysis of the Operational Environment (AOE): We will thoroughly examine the operational environment to gain a comprehensive understanding of the factors that influence IED attacks. This includes studying the geographical, information terrain, social, and political aspects that shape the context in which these attacks occur.

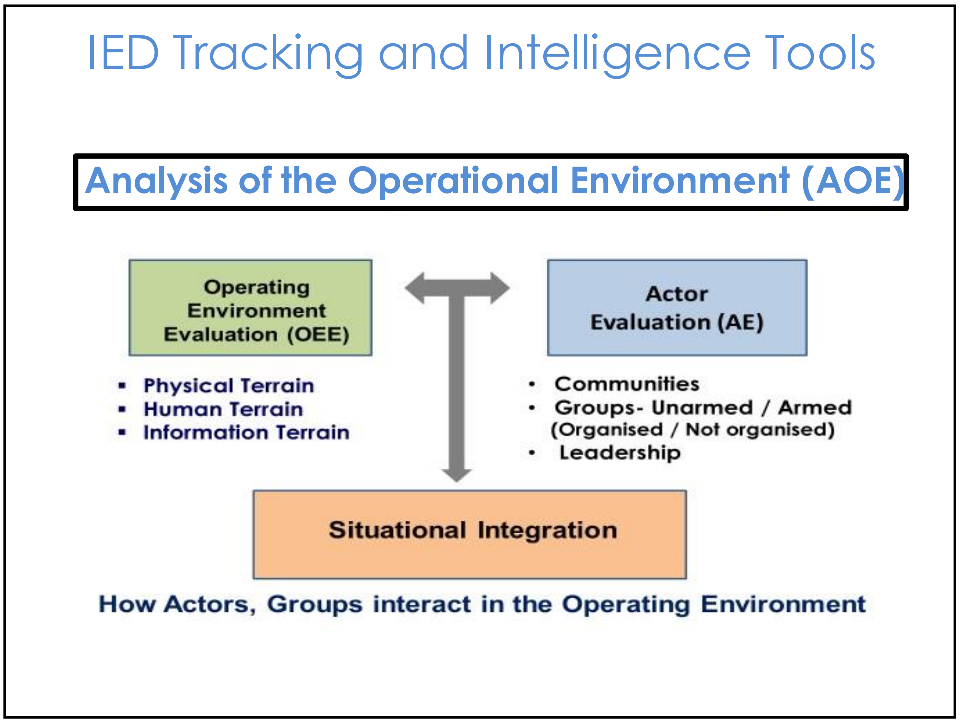
Actor Evaluation: During this step, we identify key actors within the operational environment who are involved in potential IED attacks. These may include planners responsible for strategy, suppliers, transporters, builders, emplacers, trigger persons, and exploiters. By understanding the roles and interactions of these IED-specific actors, we can better assess the IED network.

Threat Analysis: We conduct an in-depth examination of the identified threats associated with IED attacks. This includes analysing the current locations of threats, transit route areas, and potential target areas. We use a matrix approach to analyse the five Ws for each threat and expand the assessment tasks and groups that emplace, transport/trigger, and exploit, and any other operational considerations for building.

Risk Analysis: This step involves assessing the risks posed by IED attacks through a comprehensive analysis. We evaluate vulnerability by identifying potential weaknesses in our capabilities and defences, conduct a capability assessment to determine the assistance or support available and assess the danger level associated with each identified threat. This information is then used to construct a risk analysis matrix for the effective development of COA to mitigate risks associated with that IED threat. This will also include (mid/long term) COAs to degrade components of the network.

By carefully analysing the operational environment, evaluating key actors and their interactions, conducting threat analysis, and performing a thorough risk analysis, we can enhance our understanding of the IED threat landscape. This knowledge equips us to make informed decisions and develop robust strategies to counter IED attacks or disrupt the network, ultimately ensuring our units can accomplish their missions.

Slide 5



IED Tracking and Intelligence Tools

Analysis of the Operational Environment (AOE)

Operating Environment Evaluation (OEE)

- Physical Terrain
- Human Terrain
- Information Terrain

Actor Evaluation (AE)

- Communities
- Groups- Unarmed / Armed (Organised / Not organised)
- Leadership

Situational Integration

How Actors, Groups interact in the Operating Environment

As discussed in Lessons 1.3 and 3.1, the analysis of the operational environment (operating environment evaluation is the same with a focus on Actor evaluation of the IED network, and the situational integration provides commanders and staff with a threat-based approach to planning and situational awareness that assists the decision makers. In a UNPKO, peacekeeping-intelligence serves as a critical pillar for mission success and risk mitigation. One key element of peacekeeping-intelligence is the Analysis of the Operational Environment (AOE), which involves a comprehensive assessment of various factors within a specific operational area. The importance of AOE and its subcategories, including Operating Environment Evaluation (OEE) and Actor Evaluation, to provide a holistic understanding of the operational environment is key to a successful mission analysis.

Operating Environment Evaluation (OEE):

The OEE is a crucial subcategory of AOE that encompasses a multidimensional assessment of the operational environment. It involves three key subcategories: Physical Terrain Assessment, Human Terrain Assessment, and Information Terrain Assessment.

Physical Terrain Assessment: This subcategory focuses on analysing the geographical features, natural obstacles, and infrastructure within the operational area. By understanding the physical terrain, such as mountains, rivers, urban areas, and road networks, peacekeeping-intelligence analysts can identify potential advantages, disadvantages, and logistical challenges for operations. It is important to assess key terrain that supports potential IED emplacements, routes, and populated areas that support the network.

Human Terrain Assessment: Human Terrain Assessment involves studying the social, cultural, and political aspects of the operational environment. This includes evaluating the local population, their beliefs, customs, and socio-political dynamics. By assessing the human terrain, peacekeeping-intelligence analysts can gain insights into the local population's support, potential conflicts, and factors that may influence or support IED networks.

Information Terrain Assessment: In the digital age, the Information Terrain Assessment has become increasingly vital. It focuses on understanding the information environment, including communication networks, media channels, and online platforms. peacekeeping-intelligence analysts assess the flow of information, propaganda, and disinformation campaigns that can impact the operational environment and influence public sentiment pertaining to IED attacks and exploitation.

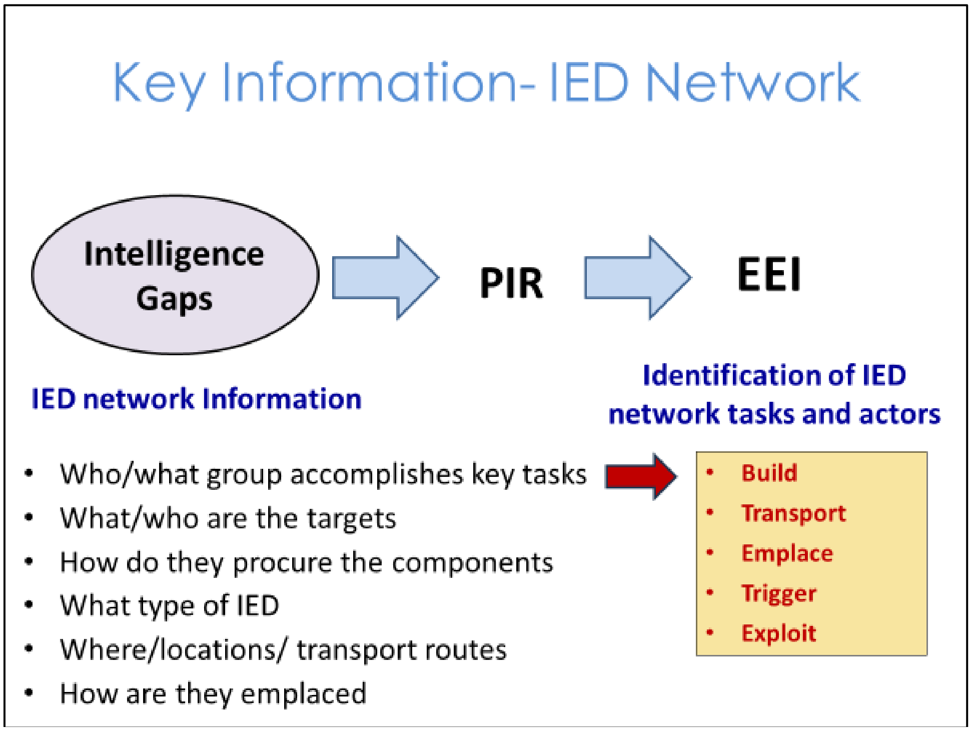
Actor Evaluation:

Another crucial aspect of AOE is Actor Evaluation, which involves assessing the various actors operating within the operational environment. This includes UN and host nation units and forces, potential attackers, non-state actors, and other influential entities. Analysts examine their capabilities, intentions, relationships, and potential threats they pose to the mission's objectives. By evaluating IED-associated actors and groups that use IEDs, peacekeeping-intelligence supports decision-makers in understanding the complex web/network of alliances, conflicts, and potential collaborations.

The Analysis of the Operational Environment (AOE) is an essential component of peacekeeping-intelligence in UNPKOs. By conducting a comprehensive assessment of the operational environment, including the subcategories of Operating Environment Evaluation (OEE) and Actor Evaluation, peacekeeping-intelligence analysts provide decision-makers with a holistic understanding of the challenges, opportunities, and IED threats. This knowledge enables informed decision-making, effective FP IED strategy development, and mitigating measures to ensure the success of UN unit operations.

The purpose of FP planning is to mitigate the risks that IED threats pose to our units. The goal is to be preventive to mitigate IED risks. However, historical data and accessing past IED attacks can be helpful in predicting future attacks. The following planning tools are examples / suggested considerations for FP planning associated with IED attacks.

Slide 6



Key Information- IED Network

Intelligence Gaps → PIR → EEI

IED network Information

Identification of IED network tasks and actors

- Who/what group accomplishes key tasks
- What/who are the targets
- How do they procure the components
- What type of IED
- Where/locations/ transport routes
- How are they emplaced

→

- Build
- Transport
- Emplace
- Trigger
- Exploit

This section focuses on reinforcing the importance of peacekeeping-intelligence and the identification of knowledge gaps in the operational environment concerning IED networks. Leadership plays a crucial role in this process during the direction phase of the peacekeeping-intelligence cycle.

Coordination and Prioritisation: Effective coordination involves aligning information acquisition with established priorities. Priority Intelligence Requirements (PIRs) should primarily stem from the commander's direction but can also be derived from other sources. Well-defined and focused PIRs serve as the foundation for acquisition and collection planning, guiding the tasking of assets. PIRs play a significant role in the development of the Information Acquisition Plan (IAP).

Essential Elements of Information (EEIs): Breaking down Priority Peacekeeping Intelligence Requirements (PIRs) into specific, targeted questions is where the Essential Elements of Information (EEIs) come into play. These EEIs provide detailed information necessary for developing the Information Acquisition Plan (IAP).

Answering the EEIs should equip planners with information to deliver FP plans. EEIs closely relate to PIRs, establishing a seamless connection that facilitates effective information gathering and analysis. For example,

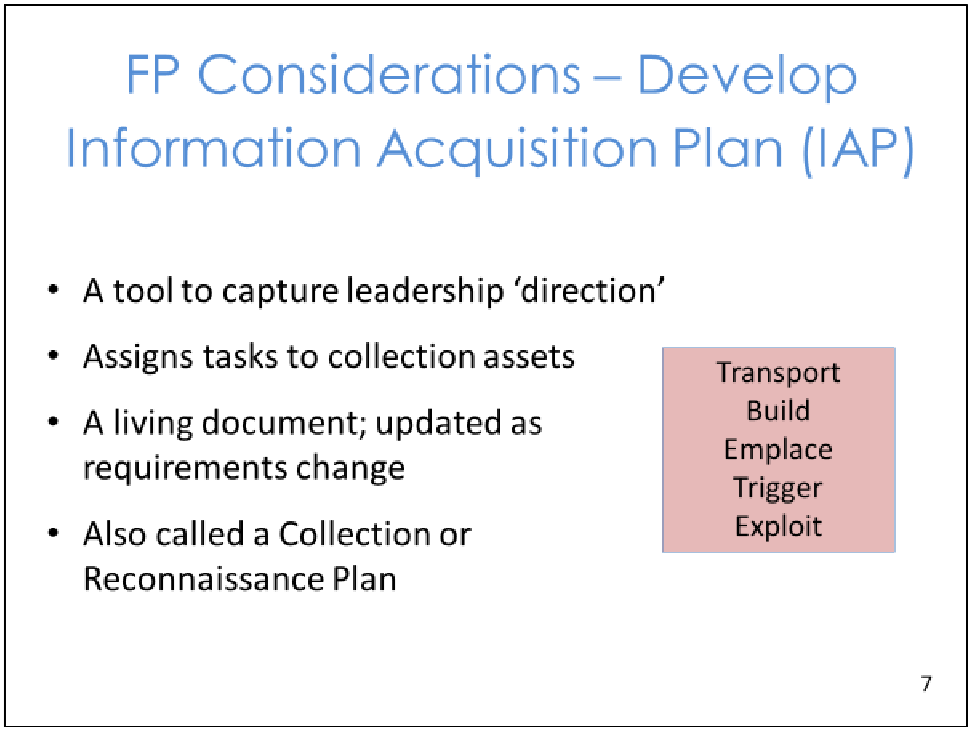
In a scenario involving security threats, an EEI could be identifying the overwatch/trigger person positions on potential routes used by UN units or looking for trucks with hidden compartments in select areas.

When analysing IED networks, the following information is vital:

- Identification of the individuals or groups responsible for key tasks within the IED network
- Identification of targets or potential targets of the IED attacks
- Understanding how they acquire the components necessary for constructing the IEDs
- Determining the type of IEDs being used in an area
- Identifying locations, transport routes, and potential areas of emplacement
- Examining the methods employed for triggering the IEDs
- Assessing how the network exploits the outcomes of the attacks

The goal is to identify the tasks involved in the IED network and the actors/groups responsible for each task, including building, transporting, emplacing, triggering, and exploiting the IEDs. By gathering this information, we can develop a comprehensive understanding of the IED network and devise effective strategies to counter its operations.

Slide 7



FP Considerations – Develop Information Acquisition Plan (IAP)

- A tool to capture leadership 'direction'
- Assigns tasks to collection assets
- A living document; updated as requirements change
- Also called a Collection or Reconnaissance Plan

Transport
Build
Emplace
Trigger
Exploit

7

Once these knowledge gaps are identified, it becomes crucial to develop a plan to address them and complete the peacekeeping-intelligence puzzle. This is accomplished through the development of an Information Acquisition Plan (IAP).

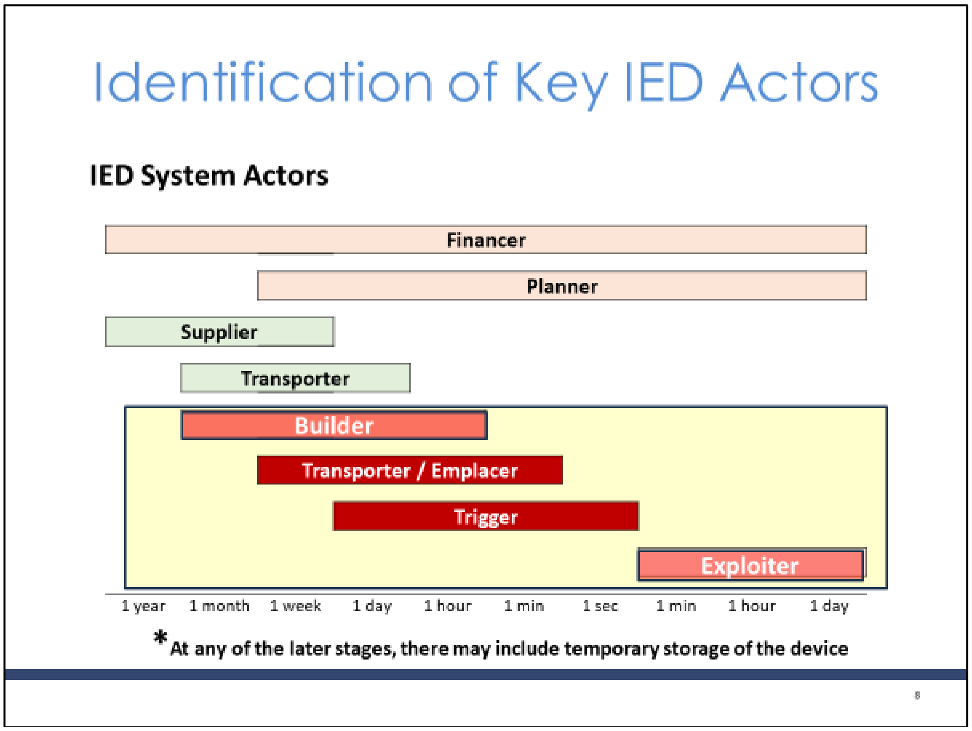
The IAP serves to capture the leadership's direction. The IAP is a tool to capture the leadership's guidance and direction regarding peacekeeping-intelligence requirements. The IAP assigns specific tasks to collection assets or resources. It outlines which assets are responsible for gathering the required information to fill in the identified gaps. This task assignment facilitates effective information acquisition and ensures that the right resources are utilised to address the peacekeeping-intelligence needs.

The IAP is a dynamic and living document that is continuously updated as requirements change. It adapts to the evolving operational environment and adjusts to new peacekeeping-intelligence priorities and gaps that emerge over time. Regular updates to the IAP enable efficient and targeted collection efforts.

The IAP may also be referred to as a Collection Plan or Reconnaissance Plan, as it outlines the specific actions and tasks required for effective information collection. It serves as a comprehensive framework for collecting the necessary peacekeeping-intelligence to understand and counter the IED network.

The primary purpose of the IAP in relation to IED networks is to assist planners in identifying the different tasks involved in the life cycle of an IED and the actors responsible for each task.

Slide 8



Identification of Key IED Actors

IED System Actors

*At any of the later stages, there may include temporary storage of the device

8

This slide is designed to facilitate the identification of key actors and their activities within the IED network, aiding in Force Protection (FP) planning for the prevention and mitigation of IED threats. The graphic representation depicts the IED system in terms of a timeline before and during an IED attack, providing insight into the different actors and tasks involved. To enhance our understanding of the crucial actors and their activities within the IED network, enabling us to develop effective FP plans to counter IED threats. Additionally, it emphasises the importance of influencing or disrupting individual components of the IED network through direct or indirect countermeasures.

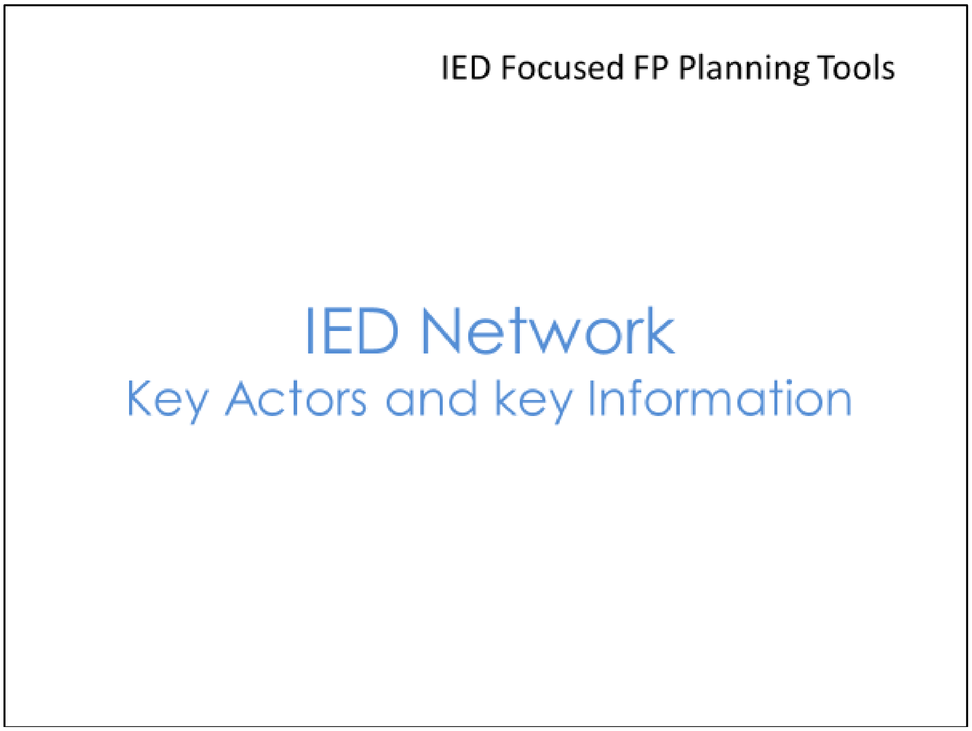
Activities Within the Yellow Box:
These activities can potentially be detected by developing a robust tactical peacekeeping-intelligence acquisition plan. Emphasis should be placed on gathering peacekeeping-intelligence in the right place and at the right time. Measures should be implemented to enhance peacekeeping-intelligence capabilities. The two activities depicted in the dark red boxes, if detected, provide tactical commanders with a valuable timeframe to implement mitigating Courses of Action (COAs) in a preventive or pre-emptive manner. Notably, potential building activities can be identified. In that case, tactical commanders may be able to hand over the disruption or neutralisation efforts to specialised units such as the Host State Security Forces (HSSF) or special operations units, which are better suited to reduce or neutralise this phase of the network.

Activities Outside the Yellow Box:
These activities pose significant challenges at the tactical level in terms of influence or detection. While directly influencing these activities may be difficult, we can persistently collect possible second-order indicators or subtasks associated with these critical activities. Opportunities for indirect influence (usually beyond the tactical framework) may exist through UN missions and interlocutor support operations. Examples include information operations, civil cooperation, and engagement with relevant stakeholders, law enforcement agencies and host state security/police forces to disrupt or impede these activities.

Noteworthy: Within the yellow box, there exists a potential opportunity to uncover a temporarily stored IED before its detonation. This grants UN units the chance to detect and prevent its placement.

Understanding the key actors and their activities within the IED network during the execution timeframe is crucial for effective FP planning. A robust peacekeeping-intelligence acquisition plan, specifically focused on IED threats, is essential to identify and address these activities effectively.

Slide 9



IED Focused FP Planning Tools

IED Network

Key Actors and key Information

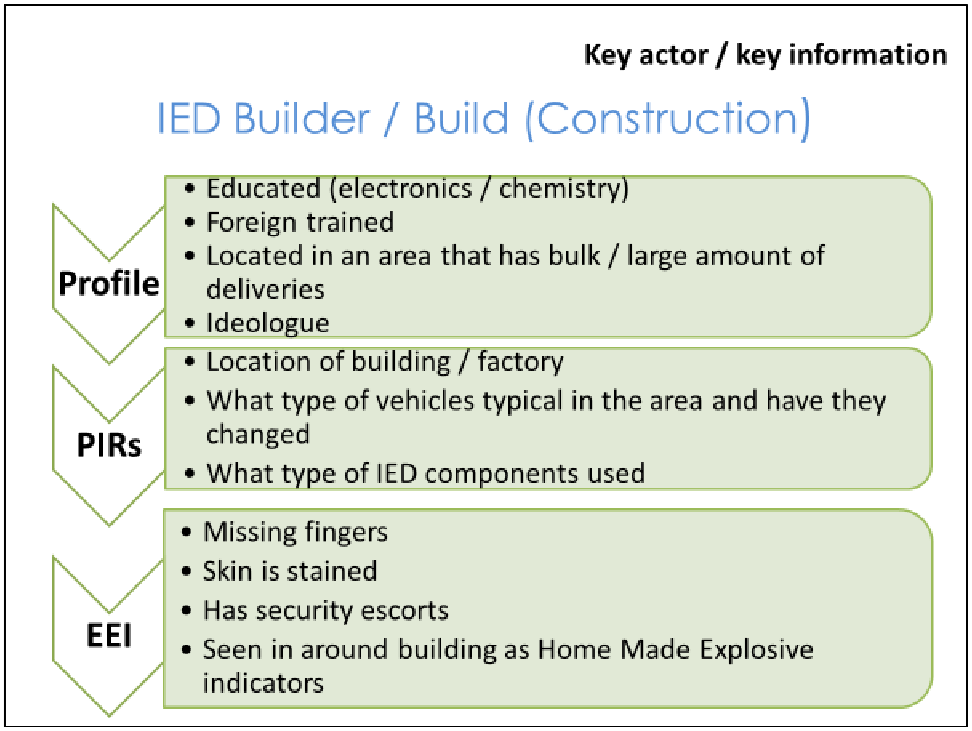
In order to enhance our comprehension and evaluation of IED networks from a tactical unit's standpoint and to effectively identify and potentially neutralise key actors or their operations, we have meticulously devised a set of peacekeeping-intelligence and planning tools. This endeavour has culminated in the creation of Profile-Priority Intelligence Requirements (PIR)- Essential Elements of Information (EEI) charts.

These basic charts serve as examples, starting points and aids for planners and intelligence cells during Step 2 (Actor Evaluation) of the suggested FP mission analysis planning process, which involves the identification of key actors within the IED network, and Step 3 (Threat Analysis), which focuses on obtaining critical information pertaining to the network's structure and capabilities.

The charts are structured to assist and help focus collection efforts to identify the IED network's activities, methods, and affiliations. By consolidating a wide array of information, including human peacekeeping-intelligence, UAV, signals peacekeeping-intelligence, and open-source peacekeeping-intelligence, these charts provide a starting point to help us understand the threat posed by the IED network.

Within each chart, we look at the profile of suspected individuals or entities involved in IED activities, outline suggested PIRs, and highlight the critical aspects that demand attention and recommended EEI, which are specific pieces of peacekeeping-intelligence crucial for unravelling the network's workings. Planners can use these tools to form a comprehensive picture of an IED network's modus operandi.

Slide 10



Key actor / key information

IED Builder / Build (Construction)

Profile

- Educated (electronics / chemistry)
- Foreign trained
- Located in an area that has bulk / large amount of deliveries
- Ideologue

PIRs

- Location of building / factory
- What type of vehicles typical in the area and have they changed
- What type of IED components used

EEI

- Missing fingers
- Skin is stained
- Has security escorts
- Seen in around building as Home Made Explosive indicators

The actors-IED Builder. The action or operation - build / construction of the IED or components of the IED.

Profile: The IED Builder is characterised by the following traits:

- Educated in electronics and chemistry, demonstrating technical expertise in crafting sophisticated explosive devices
- Trained abroad, suggesting potential affiliations or exposure to foreign militant networks
- Operates in an area with significant volumes of deliveries, potentially indicating access to essential components or materials
- Driven by strong ideological beliefs, likely influencing their targeting and overall motivations.

Priority Intelligence Requirements (PIRs):

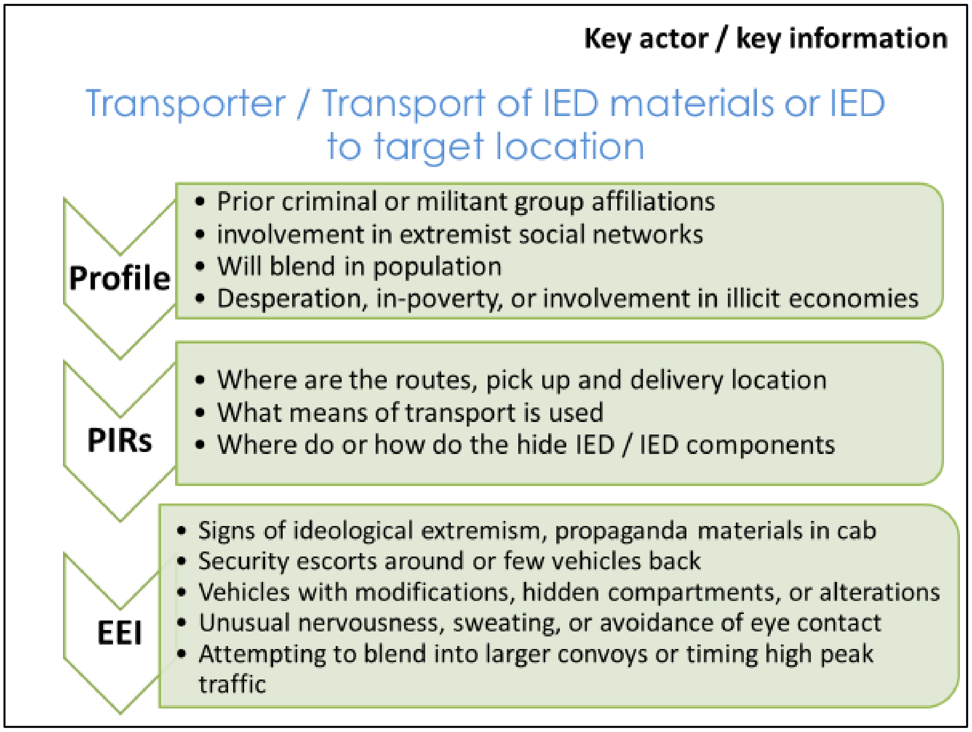
- The precise location of the building or factory where the IEDs are manufactured to facilitate targeting operations against their production capabilities
- Identification of any changes in the types of vehicles commonly observed in the area, as it may indicate inconsistencies from normal traffic in the IED builder's location/town or high volume of traffic
- Detailed information on the components and materials employed in the IED construction, enabling effective countermeasures and detection strategies

Essential Elements of Information (EEIs):

- The presence of missing fingers, which could be a distinctive physical trait indicating a history of handling explosive materials
- Any signs of skin staining, potentially caused by exposure to chemical substances during the IED assembly process
- The usage of security escorts or the presence of individuals acting as lookouts, implying a high-value target or someone seeking protection due to their involvement in illicit activities
- Frequent materials or construction apparatus sightings and chemical smells in and around a specific building indicate homemade explosive chemicals. They are potentially serving as indicators of locations where homemade explosive devices are being assembled or stored.

By thoroughly analysing the profile and employing the outlined PIRs and EEIs, we can enhance our ability to track, identify, and disrupt the construction of these dangerous devices. Understanding the IED Builder's patterns, affiliations, and vulnerabilities is paramount in mitigating the risks they pose to our operations and safeguarding civilian populations from potential harm.

Slide 11



Key actor / key information

Transporter / Transport of IED materials or IED to target location

Profile

- Prior criminal or militant group affiliations
- involvement in extremist social networks
- Will blend in population
- Desperation, in-poverty, or involvement in illicit economies

PIRs

- Where are the routes, pick up and delivery location
- What means of transport is used
- Where do or how do the hide IED / IED components

EEI

- Signs of ideological extremism, propaganda materials in cab
- Security escorts around or few vehicles back
- Vehicles with modifications, hidden compartments, or alterations
- Unusual nervousness, sweating, or avoidance of eye contact
- Attempting to blend into larger convoys or timing high peak traffic

The Transporter and their Role in IED Activities.

Profile: The Transporter plays a critical role in the IED network, primarily responsible for the transportation of IED materials to the Builder or the fully assembled IED to its intended target location. Their profile includes the following characteristics:

- Prior Criminal or Militant Group Affiliations: Transporters often have a history of involvement with criminal networks or past associations with militant groups, providing them with knowledge and experience in covert logistics
- Involvement in Extremist Social Networks: Many Transporters maintain ties to extremist social circles, making them susceptible to recruitment or radicalisation
- Ability to Blend in with the Population: Transporters are adept at camouflaging their activities and appearance, seamlessly blending into everyday life to avoid suspicion
- Desperation, In-Poverty, or Involvement in Illicit Economies: Some Transporters are driven by financial desperation, poverty, or their involvement in illicit economies, making them vulnerable to exploitation by IED networks

Priority Intelligence Requirements (PIRs):

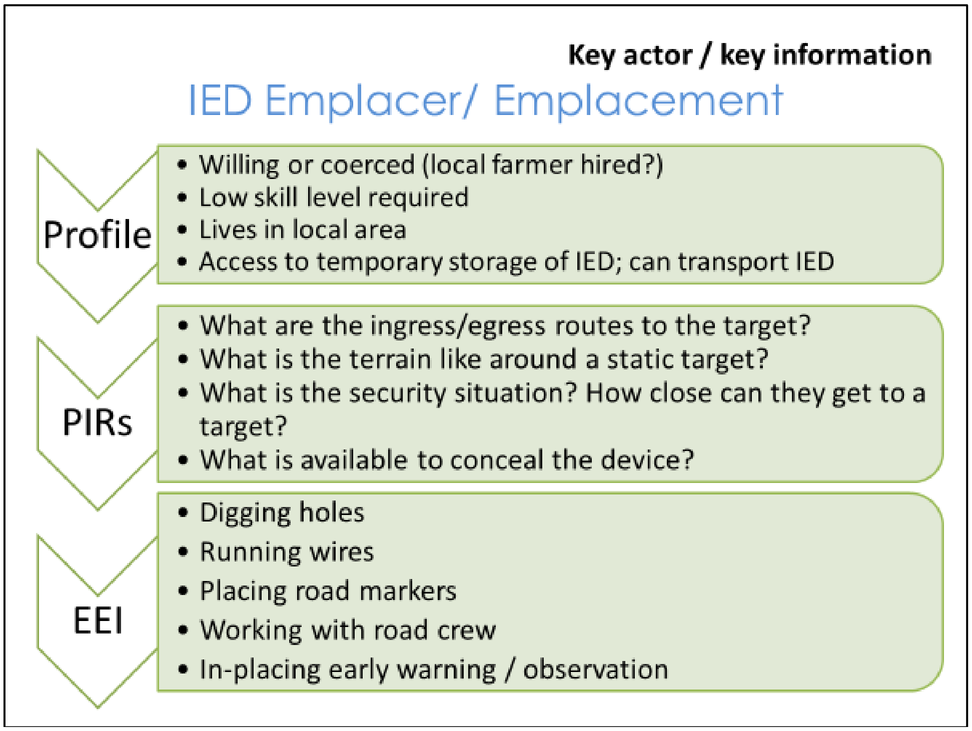
- Routes, Pick-Up and Delivery Locations: Identifying the specific routes used by Transporters for transporting IED materials and the locations where pick-ups and deliveries occur is crucial to intercepting their operations
- Means of Transport Used: Gaining peacekeeping-intelligence on the types of vehicles or modes of transport utilised by Transporters allows for targeted interception efforts
- Locations for Hiding IED/IED Components: Understanding where and how Transporters hide IEDs or their components during transportation is vital in disrupting their activities

Essential Elements of Information (EEIs):

- Signs of Ideological Extremism: Detecting propaganda materials or indicators of ideological extremism within the vehicle or on the person of the Transporter can provide insights into their motivations and affiliations
- Security Escorts or Surveillance: Observing the presence of security escorts around the Transporter or several vehicles back can indicate high-value or suspicious cargo being transported
- Vehicles with Modifications or Hidden Compartments: Identifying vehicles with alterations or hidden compartments can suggest their use for clandestine transportation
- Unusual Behaviour: Recognising signs of nervousness, excessive sweating, or avoidance of eye contact during transportation operations may signal illicit activities
- Blending into Larger Convoys or Timing High-Peak Traffic: Noticing attempts by Transporters to blend into larger convoys or time their movements during high-traffic periods can aid in interception efforts

To effectively counter the IED threats, we must focus on understanding the profile, actions, and tactics of Transporters.

Slide 12



Key actor / key information

IED Emplacer/ Emplacement

Profile

- Willing or coerced (local farmer hired?)
- Low skill level required
- Lives in local area
- Access to temporary storage of IED; can transport IED

PIRs

- What are the ingress/egress routes to the target?
- What is the terrain like around a static target?
- What is the security situation? How close can they get to a target?
- What is available to conceal the device?

EEI

- Digging holes
- Running wires
- Placing road markers
- Working with road crew
- In-placing early warning / observation

The Emplacement of Improvised Explosive Devices (IEDs): Actors, actions, general operation: Understanding the profile of the individuals involved, their modus operandi and key indicators of their activities are crucial in devising effective countermeasures. This chart aims to provide an overview of IED emplacers, their tactics, Priority Intelligence Requirements (PIRs), and Essential Elements of Information (EEIs).

Profile of Emplacers:

- Willing or Coerced Actors: IED emplacers can be individuals willingly collaborating with armed groups, driven by ideological beliefs, financial incentives, or personal grievances. Alternatively, some may be coerced, threatened, or blackmailed into carrying out these actions
- Low Skill / Educational Level Required: Emplacers typically do not need advanced expertise. However, someone with a basic knowledge of IED construction, placement, and activation may also be recruited, making it easier for less skilled actors to get involved
- Local Residency: The majority of emplacers are likely to live in the vicinity of the target location. This local residency facilitates their understanding of the terrain and helps them blend in with the community

- Access to Temporary Storage: Emplacers may have access to temporary storage facilities, allowing them to keep IED components discreetly until the ideal time for placement
- Disguised as Construction Teams: Emplacers may camouflage themselves as construction workers or road crews to avoid suspicion and move freely within the target area

Priority Intelligence Requirements (PIRs):

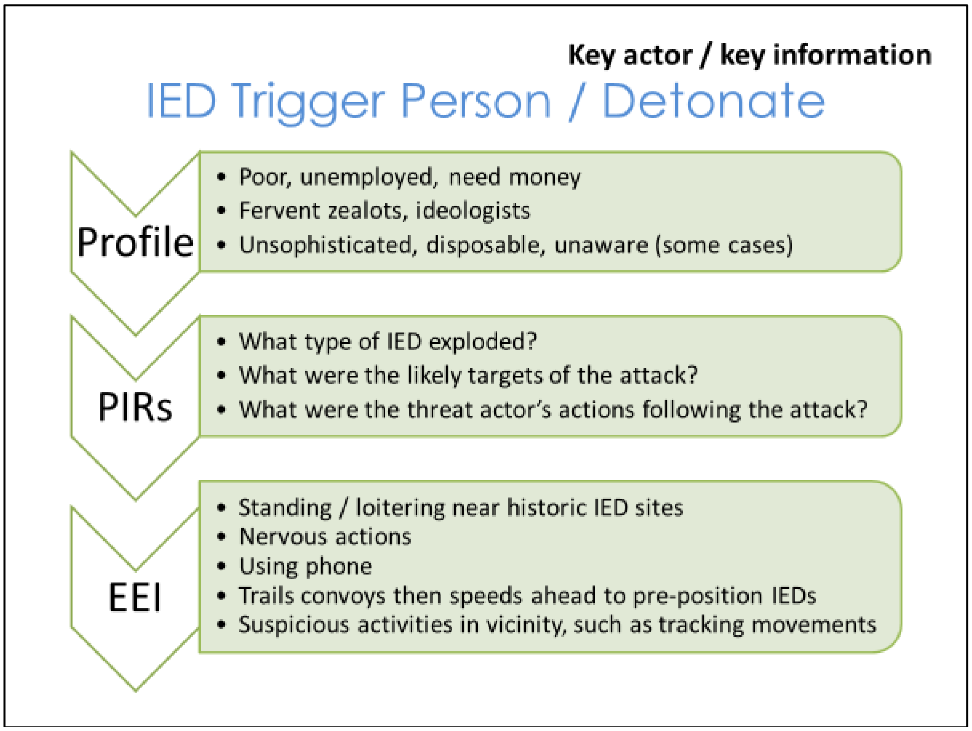
- Ingress/Egress Routes: Identify the potential routes that emplacers might use to approach the target area, including hidden paths or unconventional transportation methods
- Terrain Analysis: Understand the topography surrounding the target location to determine possible vantage points for emplacers and areas where IEDs could be effectively concealed
- Security Situation: Assess the security measures in place and gauge how close emplacers can get to the target without raising suspicion
- Concealment Opportunities: Identify natural or man-made elements that could be used to conceal IEDs effectively, such as vegetation, debris, or existing infrastructure.
- Residents and Local Inhabitants: Gather peacekeeping-intelligence on the local community to identify potential sympathisers or individuals susceptible to coercion, as they might inadvertently support or provide cover for emplacers

Essential Elements of Information (EEIs):

- Partially Dug Holes: Look for signs of recently dug holes or disturbed soil, which might indicate the preparation of IED emplacement sites
- Team Activity: Observe suspicious individuals or groups exhibiting coordinated actions, such as measuring distances, positioning markers, or laying wires, which could be indicative of an imminent IED attack
- Road Markers: Monitor the placement of unauthorised road markers or other seemingly innocuous objects that could be used as reference points for IED placement
- Interaction with Road Crew: Watch for suspicious individuals interacting with legitimate road construction crews, especially when there is no apparent reason for their presence
- Early Warning / Overwatch: Detect potential overwatch or observation teams stationed nearby to monitor the emplacement process and warn the emplacers of approaching security forces

Understanding the profile of IED emplacers and analysing their tactics, along with identifying key indicators through PIRs and EEIs, is crucial in later developing effective countermeasures to prevent and mitigate the risks posed by these improvised explosive devices.

Slide 13



Key actor / key information

IED Trigger Person / Detonate

Profile
- Poor, unemployed, need money
- Fervent zealots, ideologists
- Unsophisticated, disposable, unaware (some cases)

PIRs
- What type of IED exploded?
- What were the likely targets of the attack?
- What were the threat actor's actions following the attack?

EEI
- Standing / loitering near historic IED sites
- Nervous actions
- Using phone
- Trails convoys then speeds ahead to pre-position IEDs
- Suspicious activities in vicinity, such as tracking movements

Understanding the IED Trigger Person and Detonation Tactics. The role of the IED trigger person is pivotal in executing an explosive attack. This analysis focuses on the profile of trigger persons, their motivations, and the indicators that can help identify them. Additionally, we will examine the priority intelligence requirements (PIRs) and essential elements of information (EEIs) that can aid in predicting and helping in future countering IED attacks.

Profile of the Trigger Person:

- Motivations: The trigger person is often driven by financial desperation, unemployment, or the promise of financial rewards. Some may also be fervent zealots or ideologists, motivated by extremist ideologies, making them willing to sacrifice their lives for their cause
- Diversity: While traditionally referred to as "triggermen," we acknowledge the growing trend of using women and young girls as trigger persons. This diversification is often an attempt to exploit societal norms and potentially bypass security measures, as women and young girls may be subjected to less scrutiny
- Unsophistication and Disposable Nature: Trigger persons are typically selected for their expendability, with some being unaware of the full extent of the plot. They

may receive minimal training and are seen as disposable assets by those orchestrating the attacks

Priority Intelligence Requirements (PIRs):

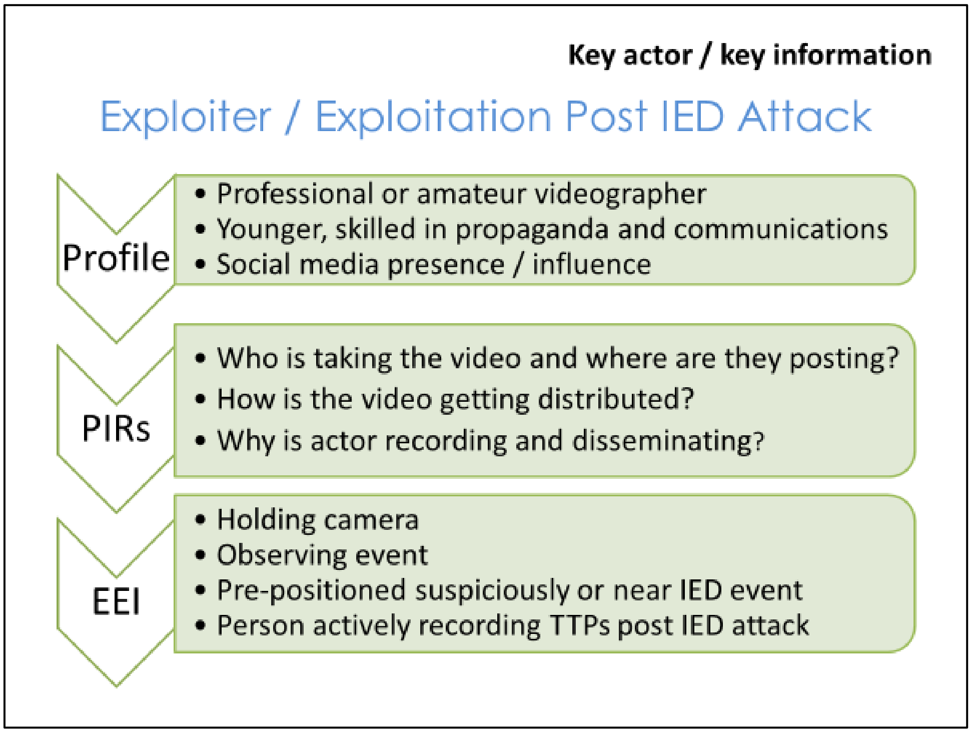
- IED Type: Identify the specific type of IED used in the attack. Understanding the construction and sophistication of the device can provide valuable insights into the threat actor's capabilities and affiliations
- Likely Targets: Analyse the targets of the attack to determine the threat actor's intentions and potential objectives. Identifying patterns in target selection can aid in predicting future attacks
- Post-Attack Actions: Gather peacekeeping-intelligence on the threat actor's actions following the attack. This can include escape routes, attempts to blend into the crowd, or coordination with other team members

Essential Elements of Information (EEIs):

- Loitering near the historically high volume of IED attack sites: Observe individuals lingering near locations of previous IED attacks or where historical IED incidents have occurred. This behaviour could indicate potential reconnaissance or preparation for future attacks
- Nervous Actions: Look for signs of nervousness or agitation in individuals, particularly in crowded places or areas of high foot traffic, as they might be carrying an IED or preparing to initiate an attack
- Use of Phone: Monitor individuals who seem overly reliant on their phones, especially if they appear to be receiving or sending messages. The use of a phone could be the initiator of the detonation or communication might be essential in coordinating the detonation
- Trail and Speed Ahead: Watch for suspicious vehicles or individuals that trail convoys, only to speed ahead, potentially to pre-position IEDs or carry out a vehicular-borne IED attack
- Tracking Movements: Observe anyone exhibiting unusual interest in tracking the movements of security personnel, government officials, UN convoys, UN forces or other potential targets. This could suggest a pre-operational surveillance phase

Understanding the profile of the IED trigger person and the key indicators of their activities is vital in pre-empting and countering explosive attacks. By focusing on PIRs and EEIs related to IED detonations, law enforcement, UN units and security agencies can enhance their peacekeeping-intelligence gathering and surveillance efforts to possibly apprehend and or prevent catastrophic consequences. Additionally, acknowledging the evolving trend of using women and young girls in such roles is critical to staying ahead of the threat landscape and effectively countering future IED attacks.

Slide 14



Key actor / key information

Exploiter / Exploitation Post IED Attack

Profile
- Professional or amateur videographer
- Younger, skilled in propaganda and communications
- Social media presence / influence

PIRs
- Who is taking the video and where are they posting?
- How is the video getting distributed?
- Why is actor recording and disseminating?

EEI
- Holding camera
- Observing event
- Pre-positioned suspiciously or near IED event
- Person actively recording TTPs post IED attack

Exploiting Post-IED Attack: Profiling Exploiter Actors and their Activities: In the aftermath of an IED attack, exploiter actors play a crucial role in disseminating propaganda and influencing public perception. This chart will help examine the profile of exploiter actors and their tactics, focusing on their use of media and communication platforms to propagate their agendas. Additionally, we explore priority peacekeeping-intelligence requirements (PIRs) and essential elements of information (EEIs) to better understand their actions and counter their manipulative efforts.

Profile of Exploiter Actors:

- Professional or Amateur Videographer: Exploiter actors may range from professional videographers with advanced technical skills to amateurs with basic recording capabilities. Their aim is to capture compelling footage that aligns with their narrative
- Youthful and Skilled in Propaganda: Exploiter actors are often young individuals with a keen understanding of propaganda techniques and how to manipulate emotions through visual storytelling

- Social Media Presence/Influence: Exploiter actors are well-versed in utilising social media platforms to reach a broader audience quickly. They may have a significant following or access to networks that can amplify their content

Priority Intelligence Requirements (PIRs):

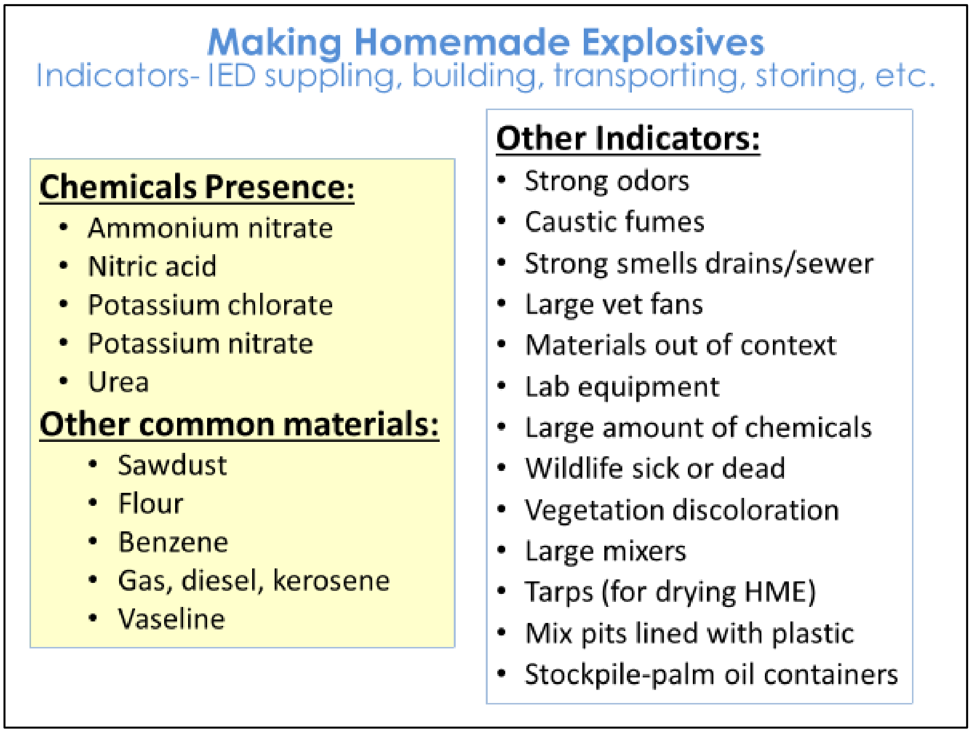
- Video Source and Posting Location: Identify who is capturing the video footage and where they are posting it. Understanding the source helps trace the origin of the content and its potential affiliations (UN units will require additional support from UN Mission level assets and agencies to assist. UN tactical units should develop information requirements to include in their higher HQ IAP
- Distribution Channels: How are the videos being posted, distributed, and shared? This includes tracking the platforms, websites, or channels through which the content is disseminated
- Motivations for Recording and Disseminating: Unravel the underlying motivations behind the actor's actions. Determine whether the primary goal is propaganda, recruitment, intimidation, or advancing a specific ideological agenda

Essential Elements of Information (EEIs):

- Holding a Camera: Look for individuals holding cameras or recording devices in the vicinity of the post-IED attack site. This is a critical indicator of potential exploiter actors
- Observing the Event: Identify individuals who seem more interested in recording the event rather than rendering assistance or displaying empathy towards the victims. Their dispassionate behaviour may raise suspicion
- Suspicious Pre-Positioning: Observe anyone suspiciously positioned near potential IED attack sites to anticipate the attack and capture the footage
- Recording UN unit Tactics, Techniques and Procedures: Pay attention to exploiter actors post-event to capture footage of our unit's responses, emergency services, and other post-IED attack activities. This can reveal their intentions and focus

The role of exploiter actors in propagating post-IED attack narratives is a concerning aspect of modern conflicts. Understanding their profile and tactics is crucial in countering their efforts to manipulate public perception and spread propaganda. By focusing on PIRs related to the dissemination of exploitative content and EEIs to identify potential exploiter actors, we can better develop strategies to counter their activities and better predict future IED threats in an operational area.

Slide 15



Making Homemade Explosives

Indicators- IED suppling, building, transporting, storing, etc.

Chemicals Presence:

- Ammonium nitrate
- Nitric acid
- Potassium chlorate
- Potassium nitrate
- Urea

Other common materials:

- Sawdust
- Flour
- Benzene
- Gas, diesel, kerosene
- Vaseline

Other Indicators:

- Strong odors
- Caustic fumes
- Strong smells drains/sewer
- Large vet fans
- Materials out of context
- Lab equipment
- Large amount of chemicals
- Wildlife sick or dead
- Vegetation discoloration
- Large mixers
- Tarps (for drying HME)
- Mix pits lined with plastic
- Stockpile-palm oil containers

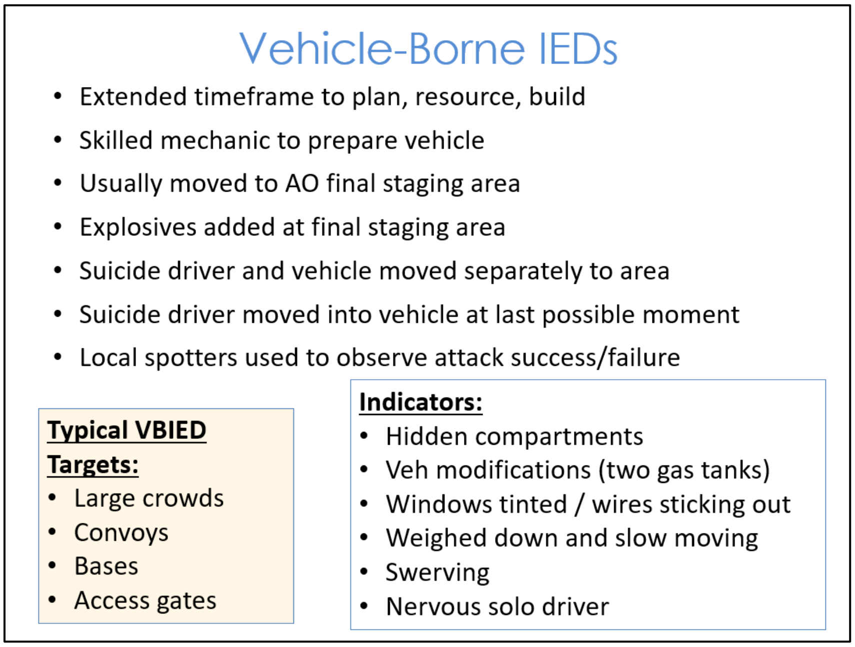
Identifying Homemade Explosives: In our Profile-PIR-EEI analysis, we highlighted the significance of homemade explosives used in IEDs. This slide provides a more comprehensive overview of the chemicals and materials involved in their construction, along with key indicators that can be refined into Essential Elements of Information (EEIs). By identifying these EEIs, peacekeepers can assist in the identification of IED suppliers, builders, transporters, and storage areas, thereby uncovering portions of the IED network. It is vital to equip our peacekeepers with proper training and education on IEDs and homemade explosives to ensure their well-being during reconnaissance, cordon/search, and checkpoint operations. Additionally, having access to Explosive Ordnance Disposal (EOD) experts becomes crucial in handling and safely disposing of explosives when necessary.

Chemicals and Materials: Elaborate on the various chemicals and materials typically used in homemade explosive production. Include examples such as easily accessible precursors, common household items, and industrial chemicals, as seen here.

Indicators for Identifying Threats: Discuss specific indicators that can be utilised to identify IED suppliers, builders, transporters, and storage areas. Emphasise the importance of keen observation, situational awareness, and peacekeeping-intelligence sharing. Encourage peacekeepers to stay vigilant and report any suspicious activities promptly.

Conclusion: In conclusion, this slide can be refined as EEIs to assist in identifying IED suppliers, builders, transporters, and storage areas. Understanding homemade explosives and their associated indicators is crucial for identifying components the network / framework and to facilitate peacekeepers' safety during discovery. By recognising these indicators and developing EEIs focused on homemade explosives, we can start to piece together the network, disrupt their operations, and mitigate risks associated with future IED attacks. Continuous vigilance, and cooperation with local authorities are important elements in degrading the network.

Slide 16



Vehicle-Borne IEDs

- Extended timeframe to plan, resource, build
- Skilled mechanic to prepare vehicle
- Usually moved to AO final staging area
- Explosives added at final staging area
- Suicide driver and vehicle moved separately to area
- Suicide driver moved into vehicle at last possible moment
- Local spotters used to observe attack success/failure

Typical VBIED Targets:

- Large crowds
- Convoys
- Bases
- Access gates

Indicators:

- Hidden compartments
- Veh modifications (two gas tanks)
- Windows tinted / wires sticking out
- Weighed down and slow moving
- Swerving
- Nervous solo driver

Vehicle-Borne Improvised Explosive Devices (VBIEDs) present a highly intricate challenge when it comes to identifying the threat and developing effective risk mitigation measures to counter potential attacks. The groups that utilise VBIEDs have distinctive techniques and tactics for targeting UN units or any other designated objectives. Understanding the characteristics and indicators of VBIED attacks is crucial in gathering information and enhancing security and mitigating measures.

Extended Timeframe: One of the prominent features of VBIED attacks is the extended period required for planning, resource gathering, and building the device. These attackers invest considerable time in carefully planning their operation to maximise the impact and reduce the chances of detection.

Skilled Mechanic: VBIEDs demand technical expertise to prepare the vehicle for carrying explosives. These groups have skilled mechanics or bomb-makers who modify the vehicle to accommodate the explosive payload effectively.

Final Staging Area: Typically, the VBIED is transported to a final staging area, which is relatively close to the intended target. This allows the attackers to minimise the time spent traveling with the armed vehicle, reducing the risk of premature detection.

Explosive Addition: The actual addition of explosives to the vehicle usually occurs at the final staging area to avoid accidental detonation during transportation. This step ensures that the attackers can approach the target area without risk to themselves.

Separation of Driver and Vehicle: To maximise the chances of success and to conceal the intent, VBIED attackers often separate the suicide driver from the loaded vehicle during transportation. This tactic adds an extra layer of complexity to detecting their intentions. Also, the trigger often is failsafe dual system in case the suicide driver fails to detonate the IED.

Last-Minute Loading: The suicide driver is typically moved into the vehicle at the last possible moment before the attack is executed. This measure reduces the chances of detection during transit and improves the element of surprise.

Local Spotters: The attackers may employ local spotters/exploiters who observe the attack from vantage points to assess its success or failure. These spotters may also provide real-time feedback to the attackers, enhancing their coordination and adaptability.

Typical VBIED Targets include:

- Large Crowds: VBIEDs are often used to target events or locations with large gatherings of people, as this increases the potential casualty count and media attention
- Convoys: VBIEDs pose a significant threat to military, police or civilian convoys due to their potential to cause widespread damage and disruption
- UN Bases: Military, police, or other high-value facilities are attractive targets for VBIED attacks due to their operational importance
- Access Gates: Entry points to secured areas are vulnerable to VBIED attacks, as they can breach perimeter defences and cause chaos within the facility

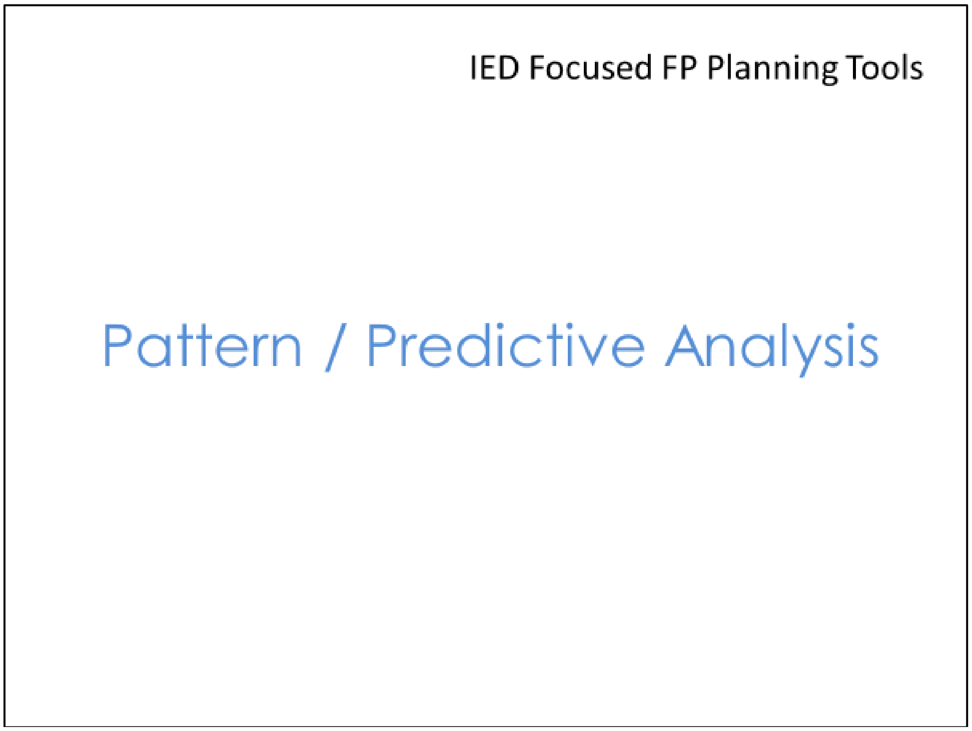
Indicators of a possible VBIED attack include:

- Hidden Compartments: Suspicious compartments within the vehicle may indicate the presence of explosives
- Vehicle Modifications: Unusual vehicle modifications, such as the addition of extra gas tanks or wires sticking out, might suggest attempts to carry a hidden payload
- Tinted Windows / Tarps, Boxed loads: Windows heavily tinted or obscured or unseen loads can be an effort to conceal the presence of suspicious objects inside the vehicle
- Weighed Down and Slow Moving: A vehicle visibly weighed down by a heavy load and moving unusually slowly might be a sign of a potential VBIED
- Swerving: A vehicle driving erratically or swerving might indicate the driver's nervousness or lack of familiarity with the laden vehicle

- Nervous Solo Driver: A single driver displaying signs of nervousness or anxiety, particularly if the vehicle is being inspected at a CP, could be an indication of a potential VBIED attack

Understanding these characteristics and indicators is essential for early detection and the implementation of effective risk mitigation measures against VBIED attacks. It allows security forces to be proactive in their approach and minimise the potential harm caused by such devastating attacks.

Slide 17



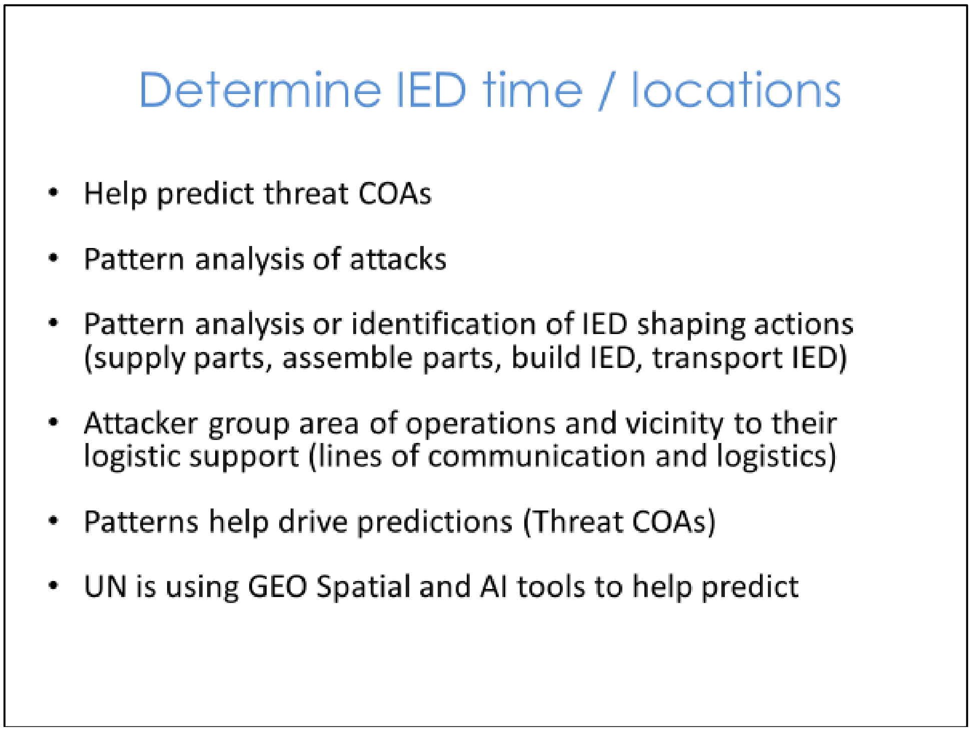
IED Focused FP Planning Tools

Pattern / Predictive Analysis

Pattern and predictive Analysis is a crucial practice for countering IED threats, playing a pivotal role in decision-making processes. The following slides showcase tools that units can utilise to help track and predict IED attacks.

Pattern and predictive Analysis is essential for countering IED threats. It involves examining past attacks, understanding historical trends, and using deductive and inductive methods to anticipate future scenarios. Key aspects include pattern analysis, identifying the IED network shaping actions like the supply of IED components, assembling IEDs, and transportation. Logistic support to the armed group and network areas are considered, including supply routes and safe havens. Comprehensive data gathering, intelligent processing, and geospatial analysis aid in understanding the environment. Predictive modelling and scenario “what if drills” help develop risk-mitigating strategies. The United Nations is also exploring the use of Artificial Intelligence and geospatial software to enhance data analysis and predictive products for UN units.

Slide 18



Determine IED time / locations

- Help predict threat COAs
- Pattern analysis of attacks
- Pattern analysis or identification of IED shaping actions (supply parts, assemble parts, build IED, transport IED)
- Attacker group area of operations and vicinity to their logistic support (lines of communication and logistics)
- Patterns help drive predictions (Threat COAs)
- UN is using GEO Spatial and AI tools to help predict

Past Patterns to Identify IED Attack Times and Locations: One of the key components in predicting threat courses of action (COAs) is conducting pattern analysis of past attacks. By analysing historical data, we can identify recurring patterns in IED attacks, which can then help us anticipate potential attack times and locations.

Pattern Analysis of IED Shaping Actions: Another critical aspect of pattern analysis involves identifying the shaping actions undertaken by attackers during the IED creation and deployment process. This includes analysing how attackers supply themselves, assemble components, build the IED itself, and transport it to its intended location. By recognising these patterns, we gain insights into their area of operations, potential locations, tactics, techniques, and procedures (TTPs) used by the attackers, which aids in predicting their future actions.

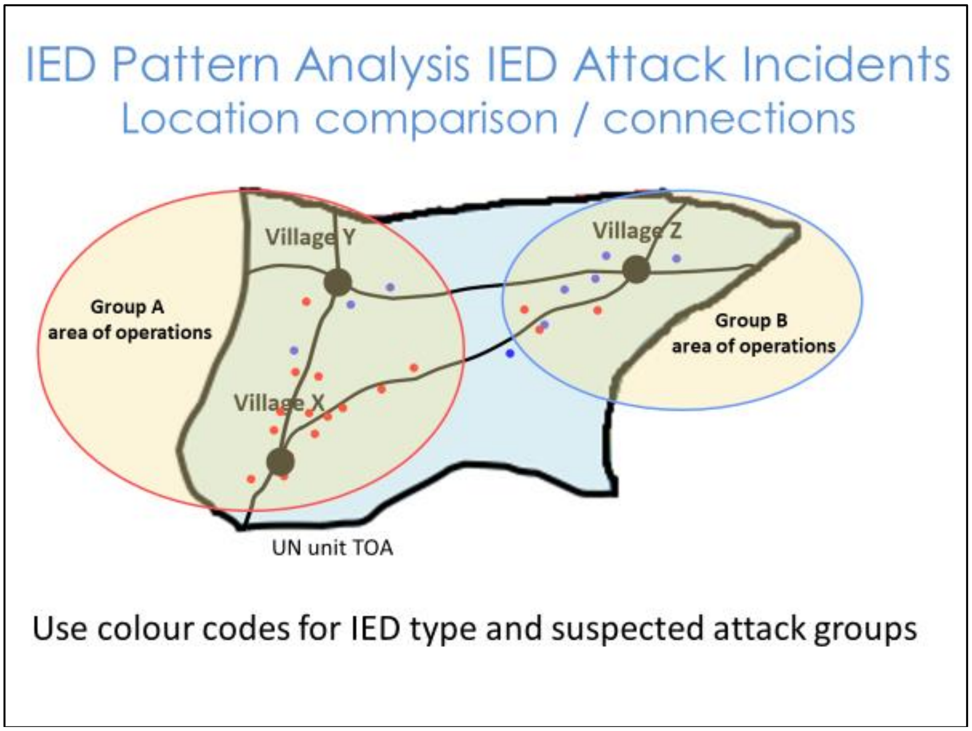
Assessing Attacker Group Area of Operations and Logistic Support: Additionally, pattern analysis assists in examining the attacker group's area of operations and its proximity to logistic support. By considering their lines of communication and logistics, such as supply routes and safe havens, we gain a better understanding of their operational reach, access to resources, and potential vulnerabilities.

Driving Predictions Through Patterns: Patterns are instrumental in driving predictions, particularly regarding potential threat COAs. By recognising patterns in IED attacks and attacker behaviours, we can make informed projections about their future actions, enabling us to better prepare and respond proactively to potential threats.

Utilising GEO Spatial and AI Tools for Predictions: The United Nations is actively leveraging advanced tools, such as geospatial (GEO) and artificial intelligence (AI) technologies, to enhance the prediction capabilities. By harnessing the power of GEO special software and AI algorithms, we can process and analyse vast amounts of data efficiently, leading to more accurate and timely predictions of potential IED threats.

In summary, pattern analysis is a fundamental aspect of predicting IED attacks. By understanding past patterns and identifying shaping actions, attacker areas of operations, and logistic support, we can drive accurate predictions of threat COAs. Leveraging GEO special and AI tools further enhances our capabilities in anticipating potential threats, ensuring a proactive and effective approach to countering IED attacks before they happen.

Slide 19



IED Pattern Analysis IED Attack Incidents
Location comparison / connections

Use colour codes for IED type and suspected attack groups

Introducing an IED Pattern Tool for Visualising IED Attack Incidents: The Enhanced IED Pattern Tool is designed to display and help analyse IED Attack Incidents. This upgraded tool incorporates various features, providing a more in-depth and informative representation of IED-related events, suspected group areas of operations, and locations. It aims to enhance the understanding and decision-making processes.

Event Types: In addition to basic event types like "detonations," "failed," and "disposal," the Enhanced IED Pattern Tool allows users to establish categories based on severity, impact, and method of deployment and trigged. This expanded classification enables users to distinguish between severity, major impact, attempted/failed attacks, and IED-related incidents that were prevented or neutralised.

Timestamps: The tool can include detailed timestamps for each incident, enabling users to analyse patterns over time, identify trends, and detect any seasonal or periodic variations in IED activities. A timeline view with a filtering option allows users to focus on specific date ranges or specific days of the week.

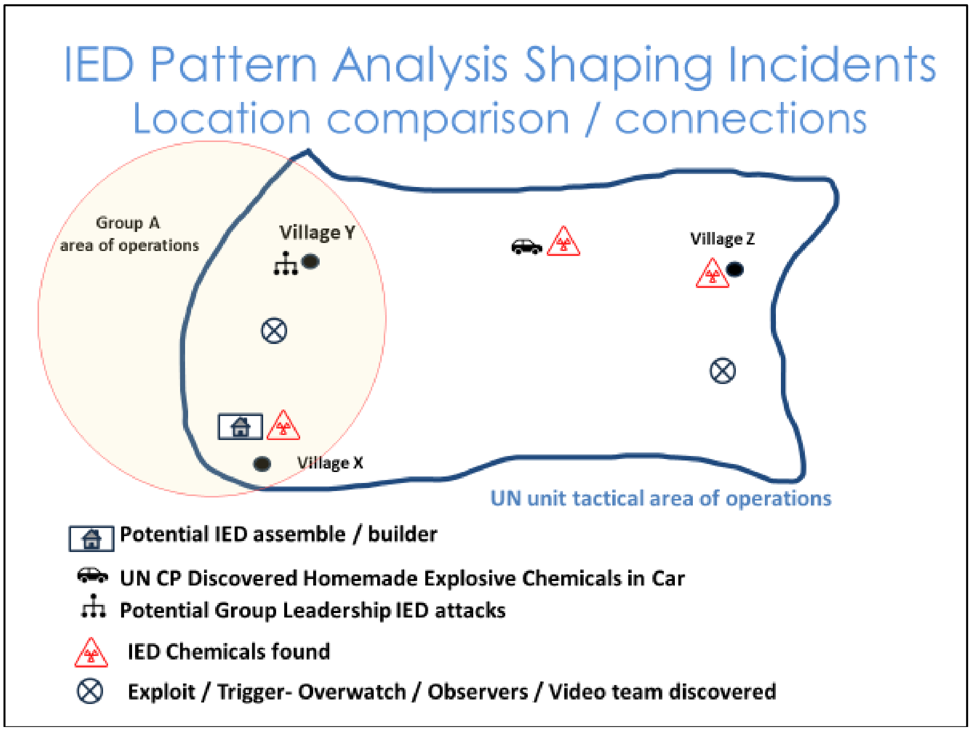
Geolocational Data: To facilitate comprehensive situational awareness, the IED Pattern Tool incorporates precise geographical data for each incident. This includes coordinates, maps, and other relevant information that can be easily integrated with external mapping software for better visualisation and spatial analysis.

Attacking Group Identification: This tool is adept at assimilating intelligence reports and data, facilitating the inclusion of a distinctive code or marker to identify the aggressor entities. It enables users to attribute IED (Improvised Explosive Device) incidents to specified recognised organisations or networks, thereby enhancing the granularity of incident analysis.

Colour Coding Scheme: A unique colour coding scheme is employed for each identified aggressor entity. By associating distinct colour codes with specific IED types, aggressor groups, or temporal periods, this feature significantly aids in discerning trends, be it similarities or disparities, in IED-related incidents.

In conclusion, the IED Pattern Analysis Tool presents a sophisticated and broadened approach towards visualising IED attack incidents. With the integration of various features such as event categorisation, timestamping, geospatial data, aggressor entity identification, and colour-coded visualisation, it significantly empowers users to delve deeper into the analysis of IED-related threats, thereby fostering a more nuanced understanding of the prevailing security landscape.

Slide 20



IED Pattern Analysis Shaping Incidents

Location comparison / connections

⌂ Potential IED assemble / builder

🚗 UN CP Discovered Homemade Explosive Chemicals in Car

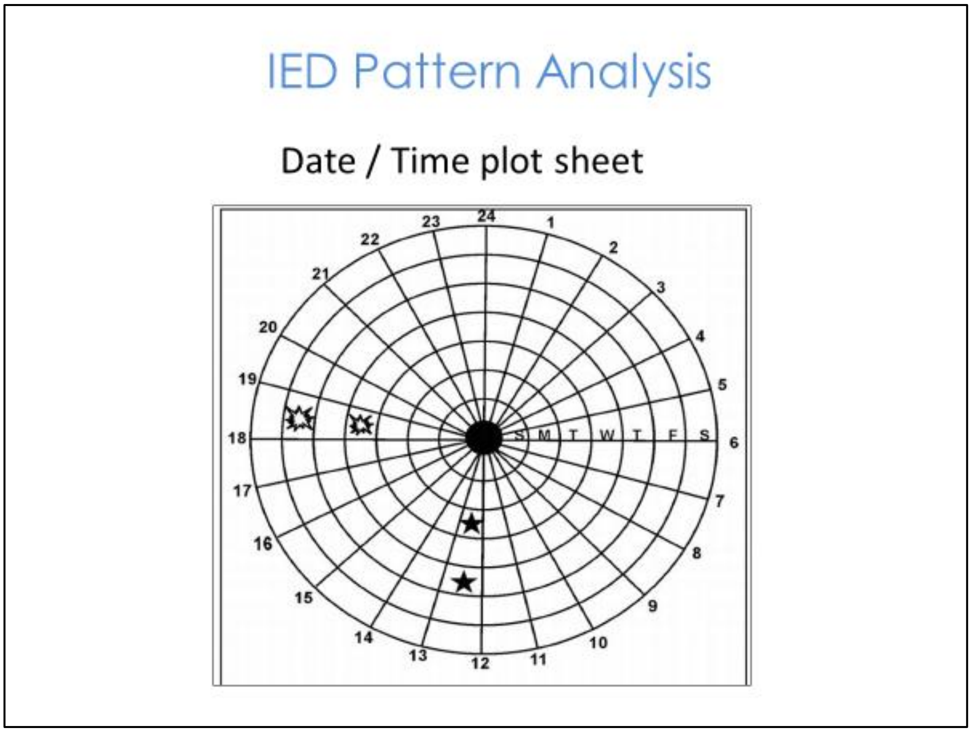
品 Potential Group Leadership IED attacks

⚠ IED Chemicals found

⊗ Exploit / Trigger- Overwatch / Observers / Video team discovered

This slide is an example of an IED Pattern Analysis Tool focusing on IED network shaping Incidents. This application helps to access and identify the IED network shaping activities, actors, and record indicators. Through integration with the previous product, it provides a deeper understanding of IED-related supply chains, lines of communication, events, suspected group areas of operations, and support locations. This product can help improve decision-making and situational awareness.

Slide 21

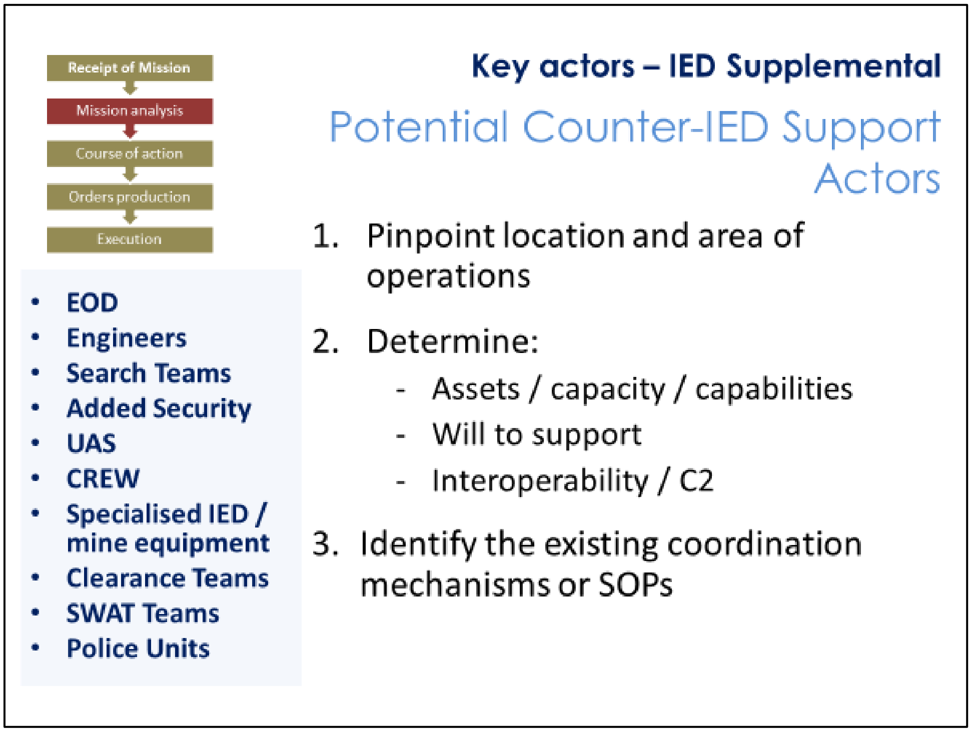


IED Pattern Analysis

Date / Time plot sheet

To enhance predictive analysis, a simple date/time plot sheet proves invaluable, enabling the establishment of patterns in dates/times and predicting IED attack seasonal and time-driven trends. It's worth noting that these products are increasingly captured and processed by geospatial software and advanced artificial intelligence capabilities, which greatly assist in the analysis process.

Slide 22



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Key actors – IED Supplemental

Potential Counter-IED Support Actors

- **EOD**
- **Engineers**
- **Search Teams**
- **Added Security**
- **UAS**
- **CREW**
- **Specialised IED / mine equipment**
- **Clearance Teams**
- **SWAT Teams**
- **Police Units**

1. Pinpoint location and area of operations
2. Determine:
   - Assets / capacity / capabilities
   - Will to support
   - Interoperability / C2
3. Identify the existing coordination mechanisms or SOPs

In lessons 3.1 and 3.2 of the mission analysis phase, we conducted a comprehensive assessment to identify potential support actors, units, and HSSF capable of aiding us in executing a Force Protection strategy. In this lesson, we want to focus on the assets best suited for an IED threat environment. This assessment covered various critical aspects:

Locations: We evaluated the locations/proximity of potential support units and their available assets,

Assets, Support Capacity, and Capabilities: Considering their support capacity and capabilities. This allowed us to understand their potential contributions to our force protection efforts.

Will or Mandate to Support: Assessing the willingness or mandate of these support actors to assist us was crucial to determine the level of commitment and cooperation we could expect in the mission.

Interoperability Issues and Command/Control Ability: To ensure effective collaboration, we examined potential interoperability challenges and the support actors' command/control ability in a joint operational environment.

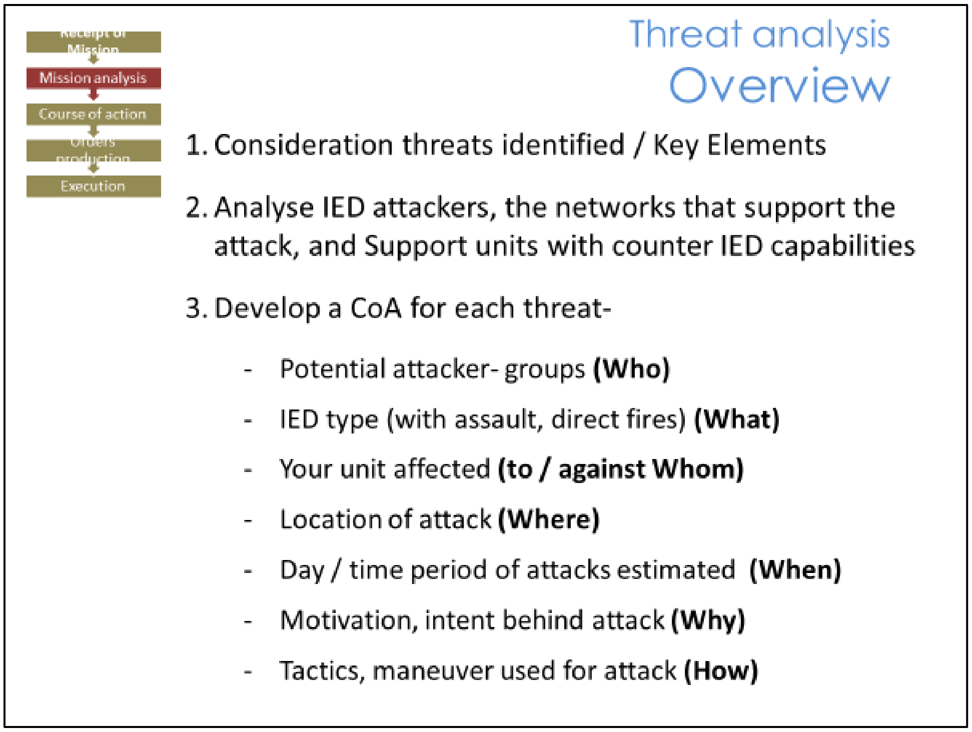
Existing Coordination Mechanisms or SOPs: We investigated any existing coordination mechanisms or Standard Operating Procedures (SOPs) already in place to facilitate smooth integration and collaboration with the support units.

Here is a sample list of possible support elements needed in an IED threat environment:

- Explosive Ordnance Disposal (EOD) Units and Teams: EOD units and teams play a critical role in identifying, rendering safe, and disposing of IEDs, mitigating the threat they pose
- Engineers' Assets for Clearing and Search Teams: Engineer assets are instrumental in clearing IEDs and conducting search operations. And, in some cases, disposal.
- Search Teams: Specialised search teams are essential in detecting hidden IEDs and neutralising potential threats
- Added Security Elements for Convoy Movements: Enhanced security measures during convoy movements are crucial to safeguard against IED ambushes / attacks
- Unmanned Aerial Systems (UAS) for Early Warning and Reconnaissance: UAS provides valuable early warning, reconnaissance, and situational awareness capabilities to detect and monitor potential threats
- CREW and Counter RCIED: Counter Radio-controlled IED Electronic Warfare (CREW) and Counter Remote Controlled Improvised Explosive Device (RCIED) equipment are essential in countering remote-controlled IED threats
- Specialised IED/Mine Clearing Equipment: These specialised vehicles, tools and equipment aid in protection, identification, and clearance operations
- Clearance Teams: Dedicated clearance teams are crucial in neutralising and removing IED threats effectively
- SWAT Teams for Targeting and Degrading Networks: SWAT teams play a vital role in targeting and dismantling (degrading) IED networks; an example is a known IED storage facility or factory that builds IEDs
- Police Units for Cordon and Search Activities or police canine units: Police units contribute to cordon and search activities, effectively degrading IED networks

By focusing on these assets and support units, we can better prepare and enhance our force protection strategy, effectively countering the IED threat environment.

Slide 23



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Threat analysis

Overview

1. Consideration threats identified / Key Elements
2. Analyse IED attackers, the networks that support the attack, and Support units with counter IED capabilities
3. Develop a CoA for each threat-

   - Potential attacker- groups **(Who)**
   - IED type (with assault, direct fires) **(What)**
   - Your unit affected **(to / against Whom)**
   - Location of attack **(Where)**
   - Day / time period of attacks estimated **(When)**
   - Motivation, intent behind attack **(Why)**
   - Tactics, maneuver used for attack **(How)**

Threat Analysis Overview - IED (Improvised Explosive Device) Threat. This Slide is a reminder of the Threat Analysis Overview with a modified focus on IED threats and associated networks. And emphasising support units with counter IED capabilities for FP mitigation efforts.

Consideration threats identified / Key Elements:

- Improvised Explosive Devices (IEDs) employed by groups
- Potential network groups or personnel
- Networks that support the attackers, including logistics, funding, and recruitment channels
- Our own units' capabilities, as we developed in lessons 3.1 and 3.2
- Potential locations of our unit, support units and groups
- Estimated day/time periods when attacks are likely to occur
- Motivations and intentions behind the attacks
- Past tactics and manoeuvres used by attackers during the IED assaults

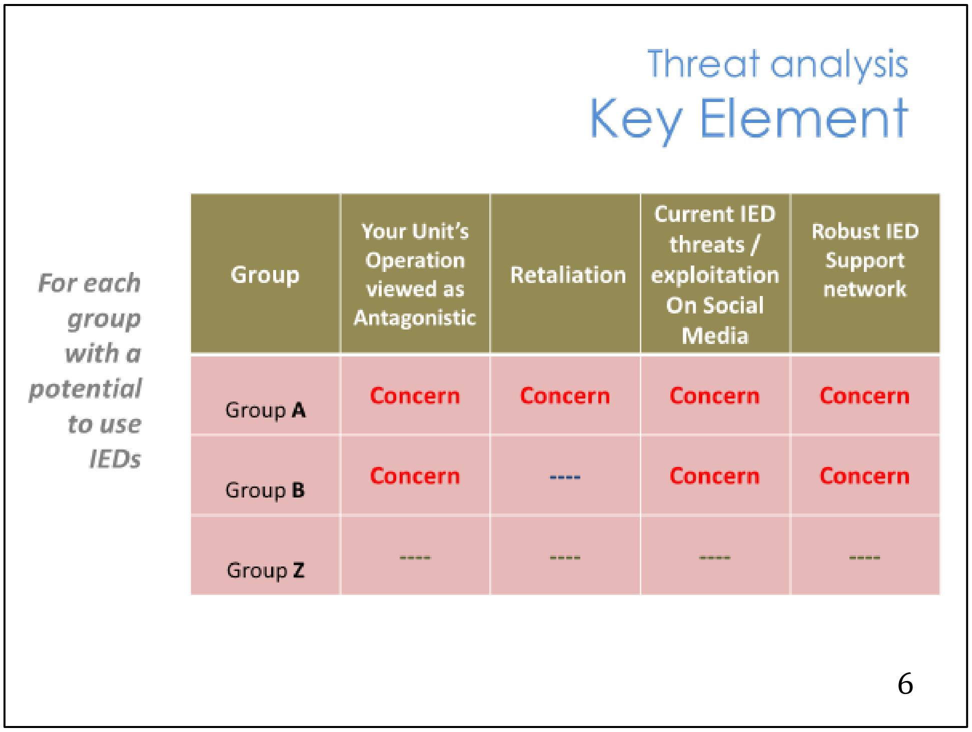
We conduct an analysis that focuses on groups with the potential to use Improvised Explosive Devices (IEDs). Key elements include understanding their motivations, objectives, and operational freedom. It also examines whether our unit's actions are perceived as antagonistic or retaliatory and whether the group exploits current IED threats on social media. Additionally, the presence of a robust IED support network is considered, along with criteria important to higher command. The goal is to gain insights into the group's intent, resolve, and targeting strategies to help in developing a predictive threat COA.

Develop a Course of Action (CoA) for each threat:

- Potential attacker- groups (Who)
- IED type and if any inclusion of a complex attack with an assault or direct fires (What)
- Your unit/element affected (to/against Whom)
- Location of attack (Where)
- Day/time period of attacks estimated (When)
- Motivation, intent behind attack (Why)
- Tactics, manoeuvres used for attack (How)

By carefully considering these threats, analysing potential attackers and support networks, and developing specific courses of action, your unit can be better prepared to counter IED attacks and mitigate their impact. It is crucial to maintain continuous vigilance and adapt your strategies based on evolving threats and peacekeeping-intelligence inputs.

Slide 24



Threat analysis

Key Element

For each group with a potential to use IEDs

Group	Your Unit's Operation viewed as Antagonistic	Retaliation	Current IED threats / exploitation On Social Media	Robust IED Support network
Group **A**	Concern	Concern	Concern	Concern
Group **B**	Concern	----	Concern	Concern
Group **Z**	----	----	----	----

6

For each group with the potential to use Improvised Explosive Devices (IEDs), we assess the following key elements:

Motivation and Objectives: Thoroughly analyse the group's motivations and objectives for employing IEDs. Understanding how your unit's operations are perceived as antagonistic or counter to the group's goals and objectives. Evaluate whether the group views your unit's past actions and whether there is pressure within the group to take retaliatory or punishing actions against the UN or your unit, influencing their IED usage.

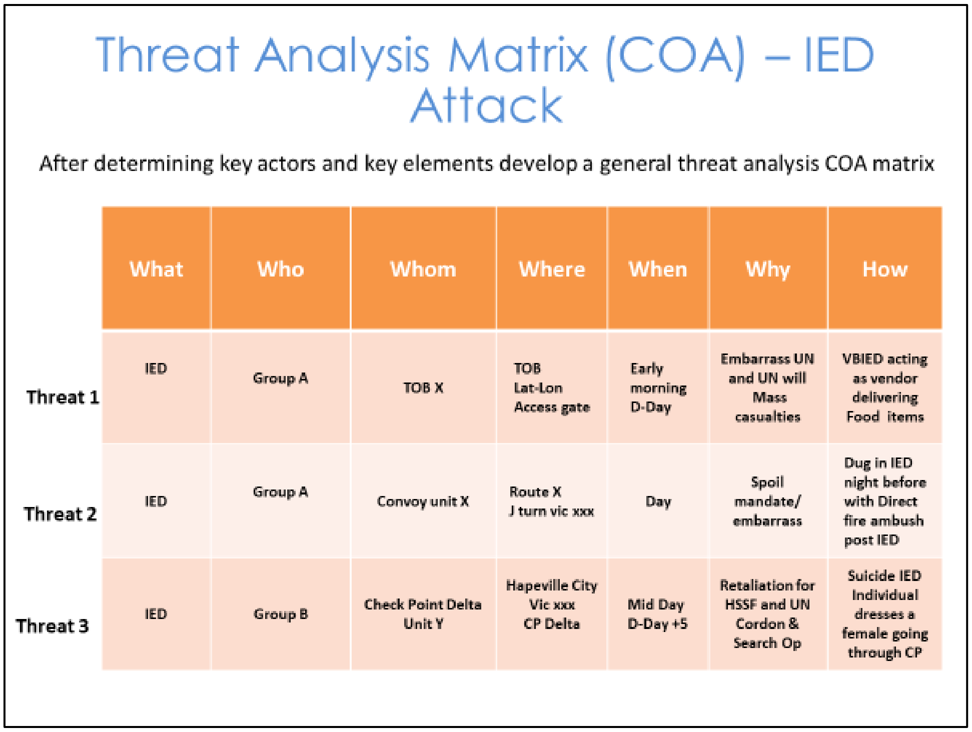
Current IED Threats and Exploitation on Social Media: Monitoring and analysing the group's activities on social media platforms for indications of their involvement in IED usage and assessing how they exploit social media for recruitment, propaganda, or coordination related to IED attacks.

Robust IED Support Network: Investigating the existence of a robust internal or external network that supports and supplies the group with IED materials and expertise. Identifying key nodes and entities involved in this support network.

Criteria Deemed Important by Unit Commander or Higher Command: Also, consider any specific criteria or factors identified by the unit commander or higher command that are crucial to the analysis. Incorporating these additional elements into the threat assessment to provide a comprehensive understanding of the IED threat.

By diligently assessing these key elements, your unit can gain valuable insights into the IED threat posed by different groups. Understanding the motivations, support networks, and operational capabilities of potential adversaries is critical in effectively understanding and predicting the level of intent and fortitude to attack your unit.

Slide 25



Threat Analysis Matrix (COA) – IED Attack

After determining key actors and key elements develop a general threat analysis COA matrix

	What	Who	Whom	Where	When	Why	How
Threat 1	IED	Group A	TOB X	TOB Lat-Lon Access gate	Early morning D-Day	Embarrass UN and UN will Mass casualties	VBIED acting as vendor delivering Food items
Threat 2	IED	Group A	Convoy unit X	Route X J turn vic xxx	Day	Spoil mandate/ embarrass	Dug in IED night before with Direct fire ambush post IED
Threat 3	IED	Group B	Check Point Delta Unit Y	Hapeville City Vic xxx CP Delta	Mid Day D-Day +5	Retaliation for HSSF and UN Cordon & Search Op	Suicide IED Individual dresses a female going through CP

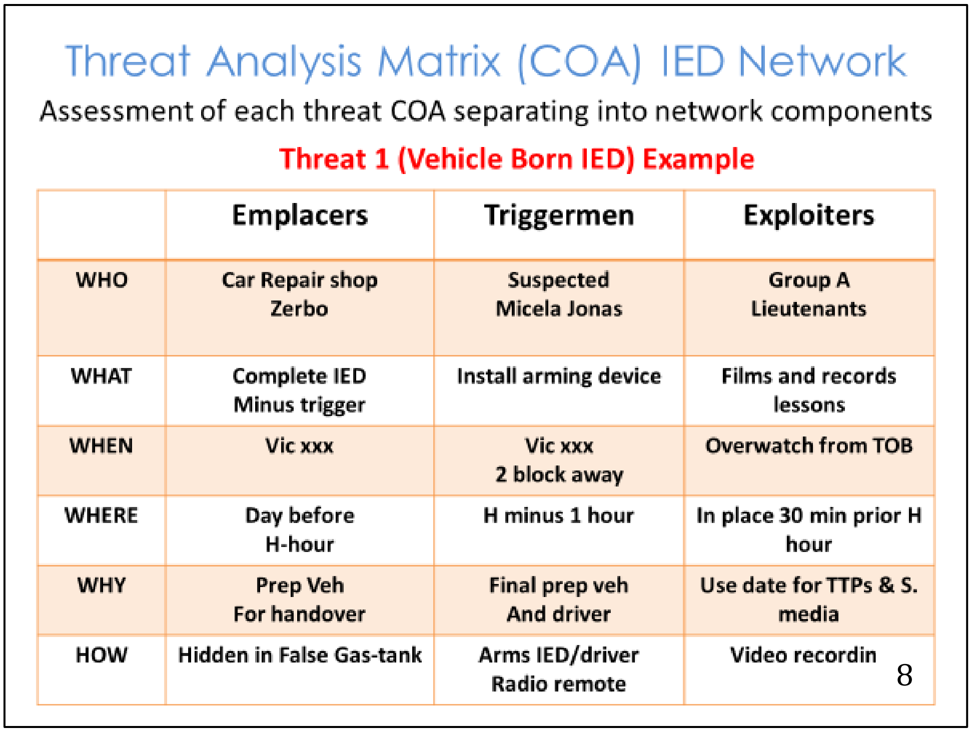
Presented here is an illustration of an IED-centric Threat Analysis Course of Action (COA) Matrix, providing planners with the means to categorise multiple threats systematically. This aids in conducting a risk analysis that aligns with the threat-based approach to FP planning.

Each threat is categorised in the following aspects: Who is involved, the intended target (Whom), the type of the attack and in this case, it is an IED (What), the expected timing (When), the location (Where), and the modus operandi (How) of the potential attack on our unit. This predictive Threat Course of Action (COA) aids in establishing a baseline for the risk analysis, leading to the development of a risk mitigation strategy focused on addressing the higher-priority, high-risk threats.

In order to effectively counter IEDs, it is crucial to take a proactive approach. This involves breaking down the Course of Action (COA) into more specific elements to gain a better understanding of how IED networks contribute to the overall threat. By separating and analysing the components of the Threat COA in terms of network actors and activities, we can enhance our assessment of the threat before proceeding to the Risk analysis phase.

The following slides will assist in creating supplementary threat COAs that centre on the actors or activities of the network groups.

Slide 26



Threat Analysis Matrix (COA) IED Network

Assessment of each threat COA separating into network components

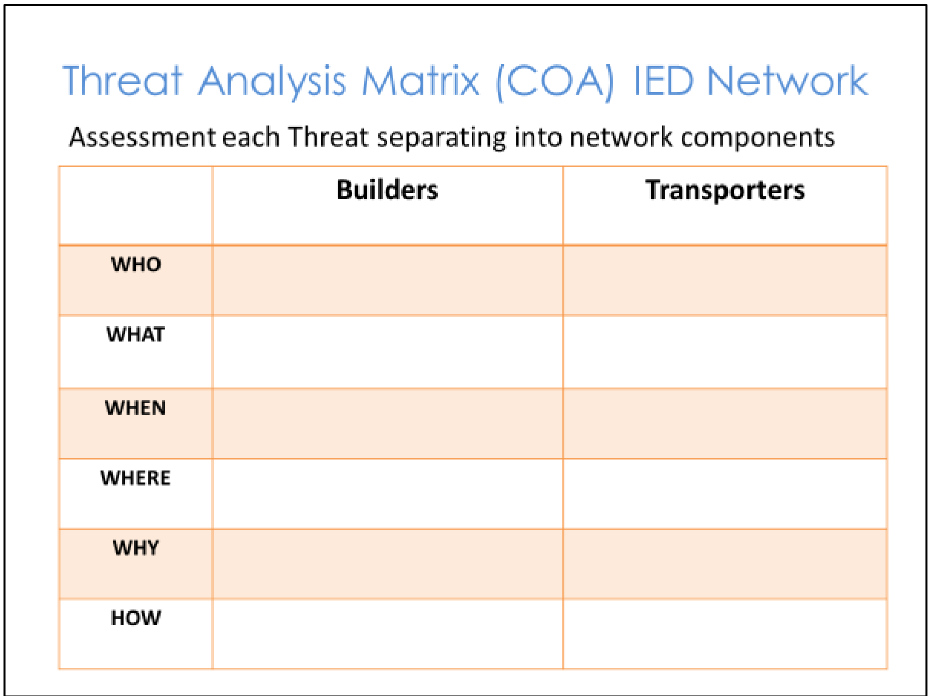
Threat 1 (Vehicle Born IED) Example

	Emplacers	Triggermen	Exploiters
WHO	Car Repair shop Zerbo	Suspected Micela Jonas	Group A Lieutenants
WHAT	Complete IED Minus trigger	Install arming device	Films and records lessons
WHEN	Vic xxx	Vic xxx 2 block away	Overwatch from TOB
WHERE	Day before H-hour	H minus 1 hour	In place 30 min prior H hour
WHY	Prep Veh For handover	Final prep veh And driver	Use date for TTPs & S. media
HOW	Hidden in False Gas-tank	Arms IED/driver Radio remote	Video recordin

8

Threat Analysis COA Matrix for IED Networks: This matrix outlines the various threat actors and their corresponding activity COAs that support a particular threat identified within the same group operating as a network. We assess each threat COA by breaking it down into its network components. To illustrate this process, we provide an example for Threat 1 (Vehicle-Borne IED) as shown on the previous Slide.

Slide 27



Threat Analysis Matrix (COA) IED Network

Assessment each Threat separating into network components

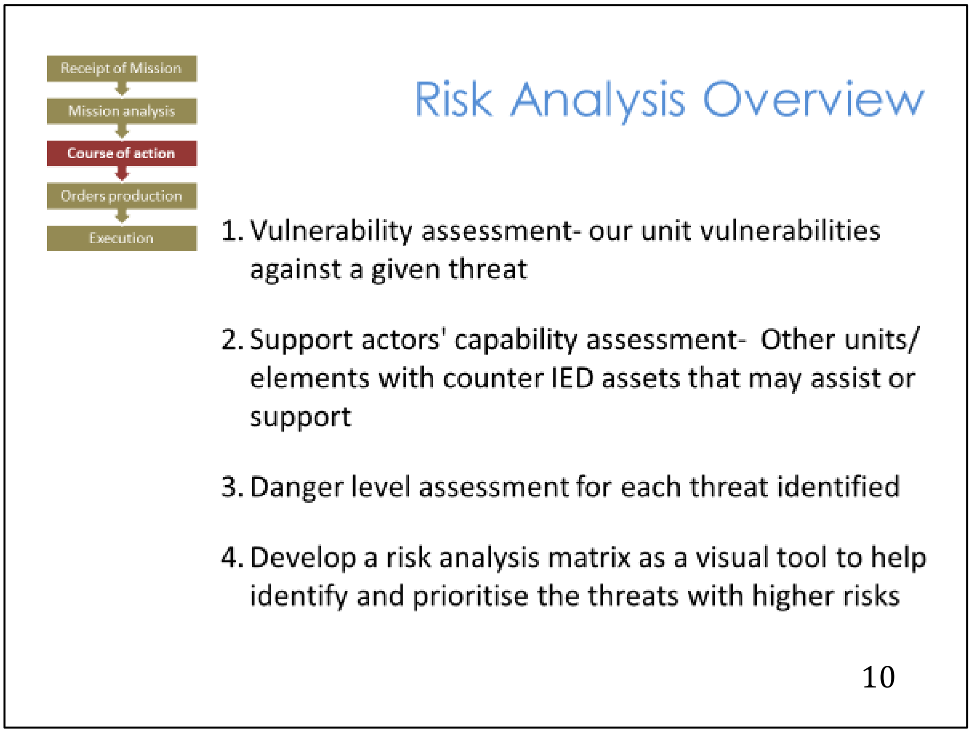
	Builders	Transporters
WHO		
WHAT		
WHEN		
WHERE		
WHY		
HOW		

As discussed earlier, it appears that builders and transporters within the network might be more distant from the tactical environmental / framework. However, as we continue to gather peacekeeping-intelligence from various sources, including Mission components and community engagement, we may gain the peacekeeping-intelligence capability to disrupt or influence the network's efforts in constructing and transporting IEDs. Developing a chart/matrix like the one provided here could offer some insights and data into the network's critical components. This information becomes instrumental during the risk analysis phase, aiding in the formulation of an effective mitigating strategy.

For example, a tactical unit could implement a series of checkpoints along a known IED transporter's route, conducting inspections of cargo and vehicle loads to disrupt their operations.

Expanding on this further, by understanding the network's key players and their roles, we can identify points of intervention. Builders and transporters might not be directly engaged in executing attacks, but they play crucial roles in facilitating the threat. Disrupting their activities could significantly impede the overall effectiveness of the network. Overall, by adopting this approach and employing a collection plan we can help disrupt IED networks

Slide 28



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Risk Analysis Overview

1. Vulnerability assessment- our unit vulnerabilities against a given threat
2. Support actors' capability assessment- Other units/ elements with counter IED assets that may assist or support
3. Danger level assessment for each threat identified
4. Develop a risk analysis matrix as a visual tool to help identify and prioritise the threats with higher risks

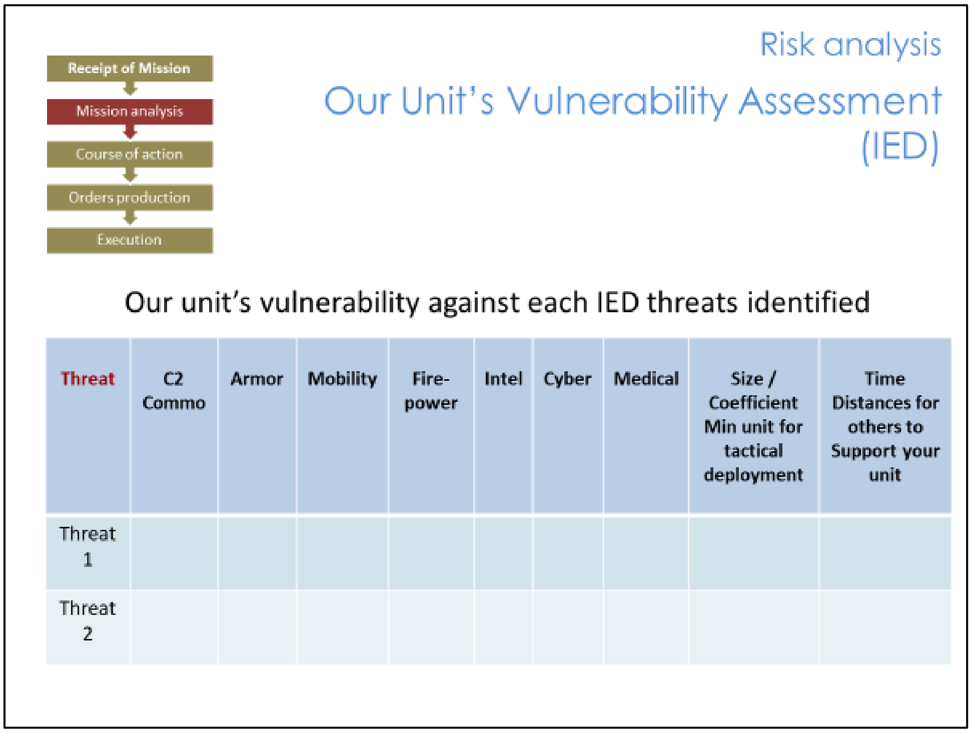
10

The Risk Analysis Overview comprises the following components:

- Vulnerability Assessment: Assessing our unit's vulnerabilities concerning a specific threat to understand potential weaknesses
- Support Actors' Capability Assessment: Evaluating the capabilities of other units or elements equipped with counter-IED assets, which can assist or support our unit
- Danger Level Assessment: Determining the danger level associated with each identified threat to gauge its severity
- Risk Analysis Matrix: Developing a risk analysis matrix as a visual tool to effectively identify and prioritise threats with higher risks

By conducting a comprehensive risk analysis, we can better understand the potential threats and allocate resources strategically to mitigate risks and enhance overall force protection.

.Slide 29



Receipt of Mission

Mission analysis

Course of action

Orders production

Execution

Risk analysis

Our Unit's Vulnerability Assessment (IED)

Our unit's vulnerability against each IED threats identified

Threat	C2 Commo	Armor	Mobility	Fire-power	Intel	Cyber	Medical	Size / Coefficient Min unit for tactical deployment	Time Distances for others to Support your unit
Threat 1									
Threat 2									

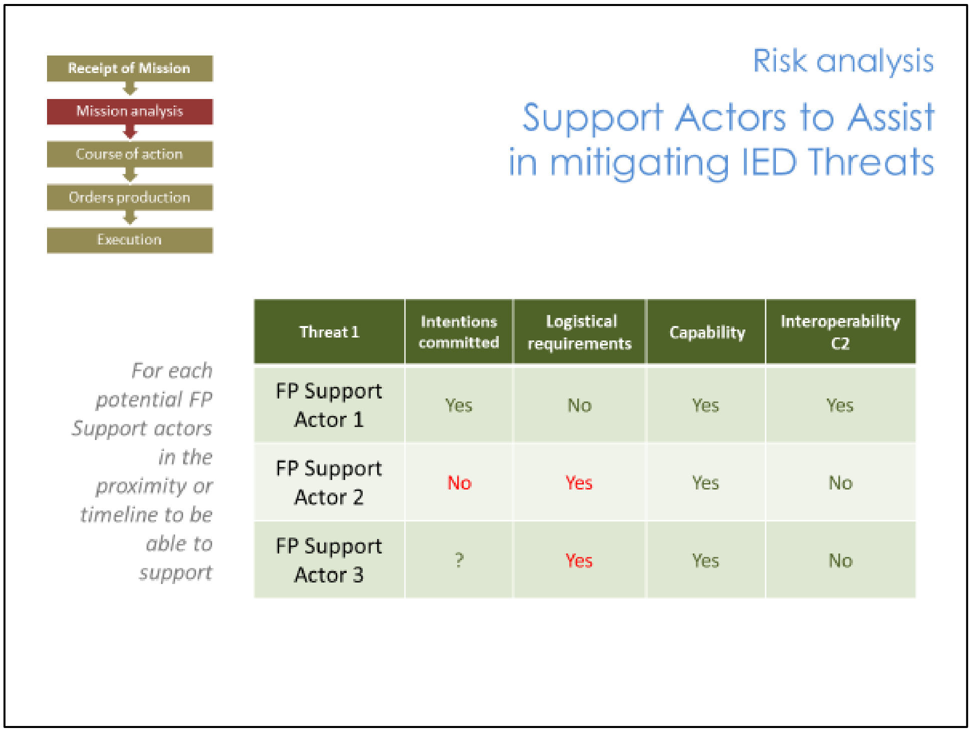
Presented here is a matrix tool designed to assess our unit's vulnerability against each identified IED threat. The components of the matrix are as follows:

- Threat: Lists the specific IED threats under consideration
- C2 (Command and Control): Evaluates the unit's ability to maintain effective command and control during an IED attack
- Commo (Communication): Assesses the unit's communication systems' resilience and effectiveness when facing an IED threat
- Armour: Determines the level of protection provided by the unit's armoured vehicles against IED attacks
- Mobility: Gauges the unit's ability to manoeuvre swiftly and respond to IED threats
- Firepower: Assesses the unit's offensive capabilities in countering IED threats

- Intelligence: Evaluates the unit's peacekeeping-intelligence gathering and analysis capabilities to detect and pre-empt IED attacks
- Cyber: Considers the unit's cyber defence measures and their impact on countering cyber-enabled IED threats
    - Medical: Examines the unit's medical support and preparedness to respond to casualties resulting from IED attacks
    - Size / Coefficient: Assigns coefficients to indicate the relative impact of each component on the overall vulnerability assessment
    - Min Unit for Tactical Deployment: Specifies the minimum unit size required for tactical deployment when facing each IED threat
    - Time Distances for Others to Support Your Unit: Estimates the time required for neighbouring units or support elements to aid your unit during an IED threat

By utilising this matrix tool, we can gain valuable insights into our unit's vulnerabilities against different IED threats. This will enable us to prioritise and allocate resources effectively to enhance our force protection and readiness in countering IED attacks.

Slide 30



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Risk analysis

Support Actors to Assist in mitigating IED Threats

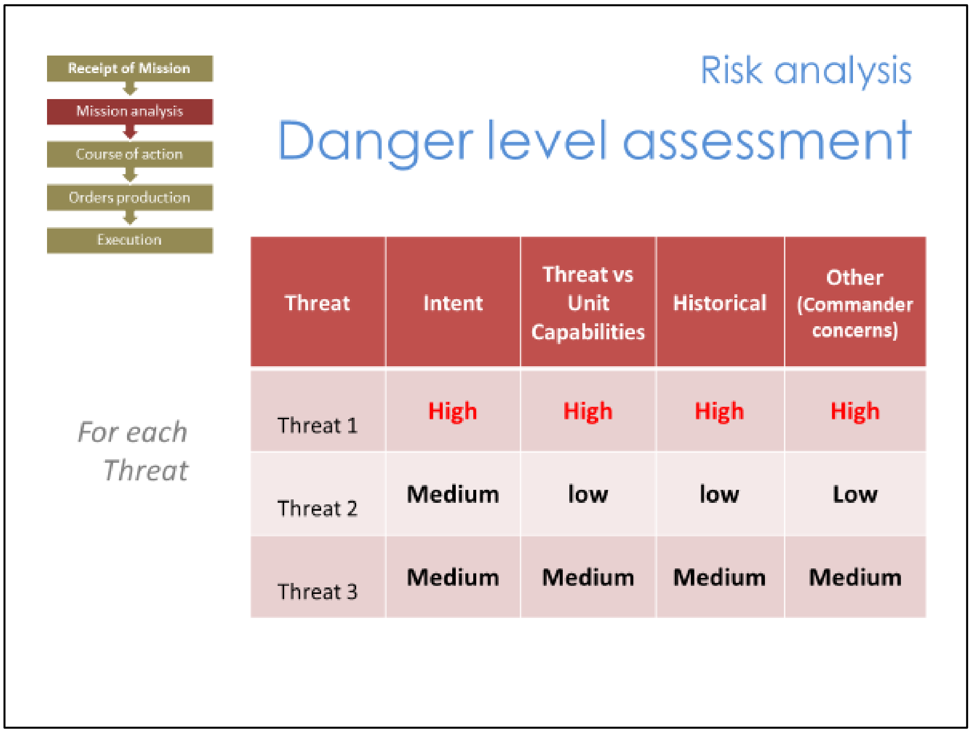
For each potential FP Support actors in the proximity or timeline to be able to support

Threat 1	Intentions committed	Logistical requirements	Capability	Interoperability C2
FP Support Actor 1	Yes	No	Yes	Yes
FP Support Actor 2	No	Yes	Yes	No
FP Support Actor 3	?	Yes	Yes	No

Risk Analysis - Supporting Actors in Mitigating IED Threats: In the risk analysis process, we focus on supporting actors who can assist in mitigating IED threats. Our evaluation includes the following aspects:

- Intentions and Commitment: We assess whether the supporting actors are genuinely willing and committed to linking up or providing the required support to our unit during the operation
- Logistical Support: We determine if the assets, elements, or units in question require logistical support from either the United Nations or us and, if so, whether we can accommodate those needs effectively
- Capabilities: We examine whether the supporting actors possess the necessary Counter IED capabilities/assets to effectively mitigate the risks associated with IED threats
- Interoperability: We consider the level of interoperability between our unit and the supporting actors, ensuring seamless coordination and cooperation in dealing with IED-related challenges. Also, that the command-and-control relationship is set and agreed to by all parties

Slide 31



Receipt of Mission
Mission analysis
Course of action
Orders production
Execution

Risk analysis

Danger level assessment

For each Threat

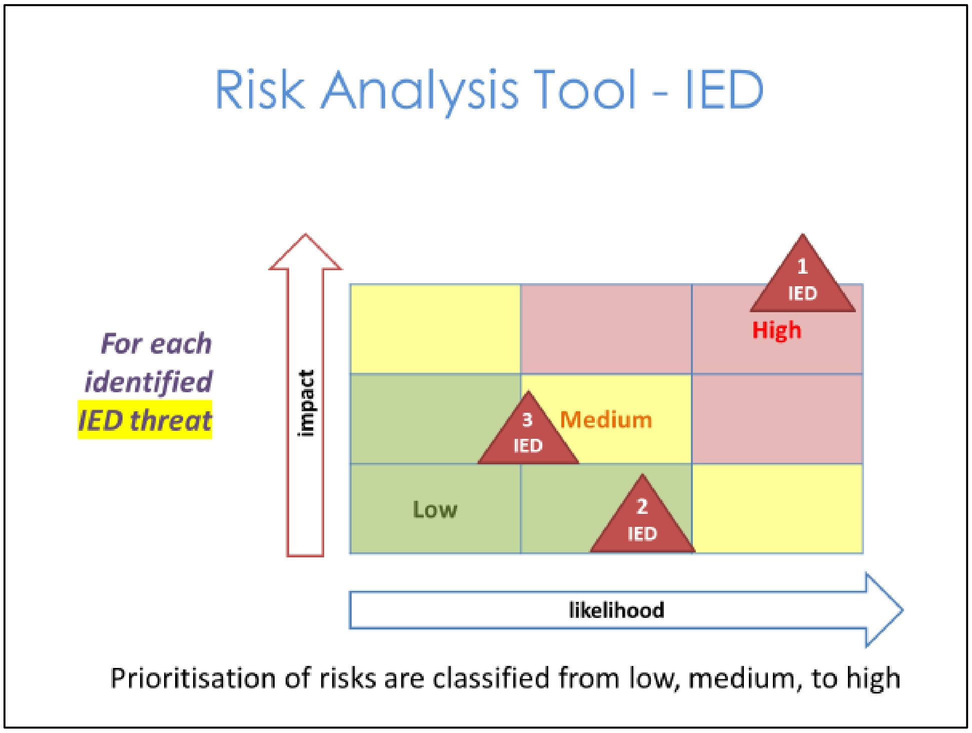
Threat	Intent	Threat vs Unit Capabilities	Historical	Other (Commander concerns)
Threat 1	High	High	High	High
Threat 2	Medium	low	low	Low
Threat 3	Medium	Medium	Medium	Medium

Risk Analysis - Assessment of Danger Levels: In the risk analysis process, we conduct a thorough assessment of the danger level for each identified threat. This assessment includes evaluating the following components:

- Intent: Understanding the intentions behind the potential threats
- Threat vs. Unit Capabilities: Evaluating the match between the identified threats and the capabilities of our unit to effectively respond
- Historical Data: Analysing past incidents and patterns to gain insights into potential likelihood of the threat to happen
- Other Concerns: Considering additional factors, including concerns raised by the commander or any other pertinent information

By carefully examining these components, we aim to establish a comprehensive understanding of the risks and potential dangers faced by our unit.

Slide 32



Risk Analysis Tool - IED

For each identified IED threat

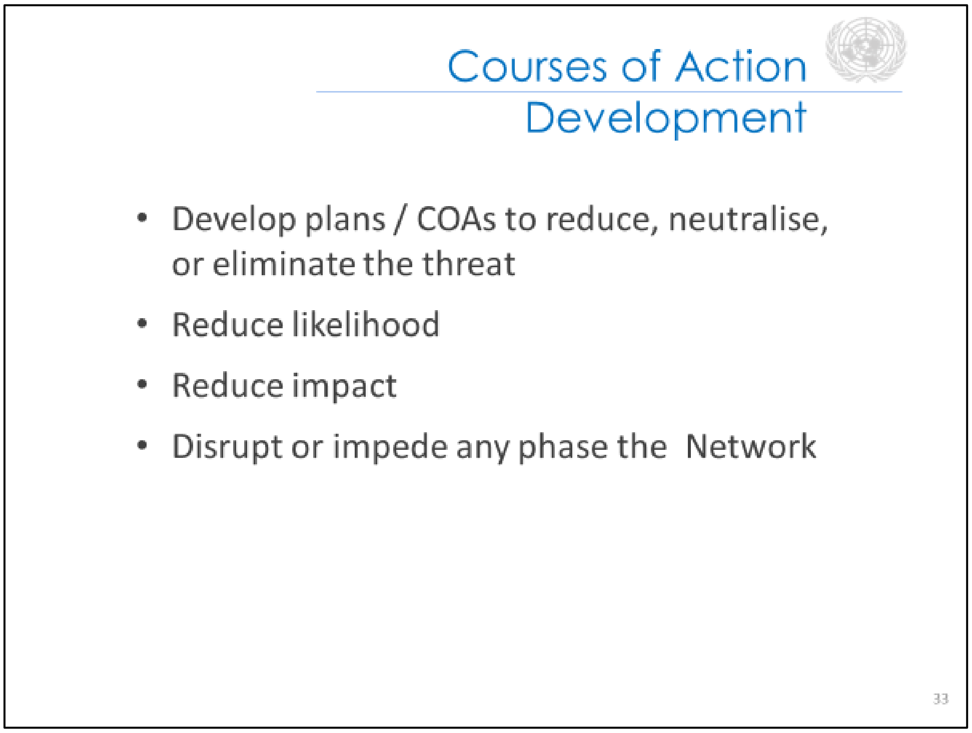
Prioritisation of risks are classified from low, medium, to high

This graph/chart will help planners visualise and prioritise multiple IED threats in terms of risk. Threat = Capability x intent, and all threats to our unit's current and future operations need to be identified. A potential group that uses IEDs with intent to cause harm but with minimal capability is a limited threat, whereas a group with significant capability but no intent poses almost no threat. The capability of the peacekeeping unit to counter IED threats also needs to be considered because, again, even if a group has every intent to oppose a peacekeeping unit, if that unit can prevent the group from operating effectively against them or disrupt the network, they pose little threat to the operation.

Risk mitigation is a process that takes reasonable operational measures to reduce risk to personnel, equipment, and the operation.

The highest priority is assigned to the threat that is the most likely to have the greatest impact. That is Threat #1. It is here where we should focus efforts to mitigate and degrading the network that supports this group.

Slide 33



Courses of Action Development

- Develop plans / COAs to reduce, neutralise, or eliminate the threat
- Reduce likelihood
- Reduce impact
- Disrupt or impede any phase the Network

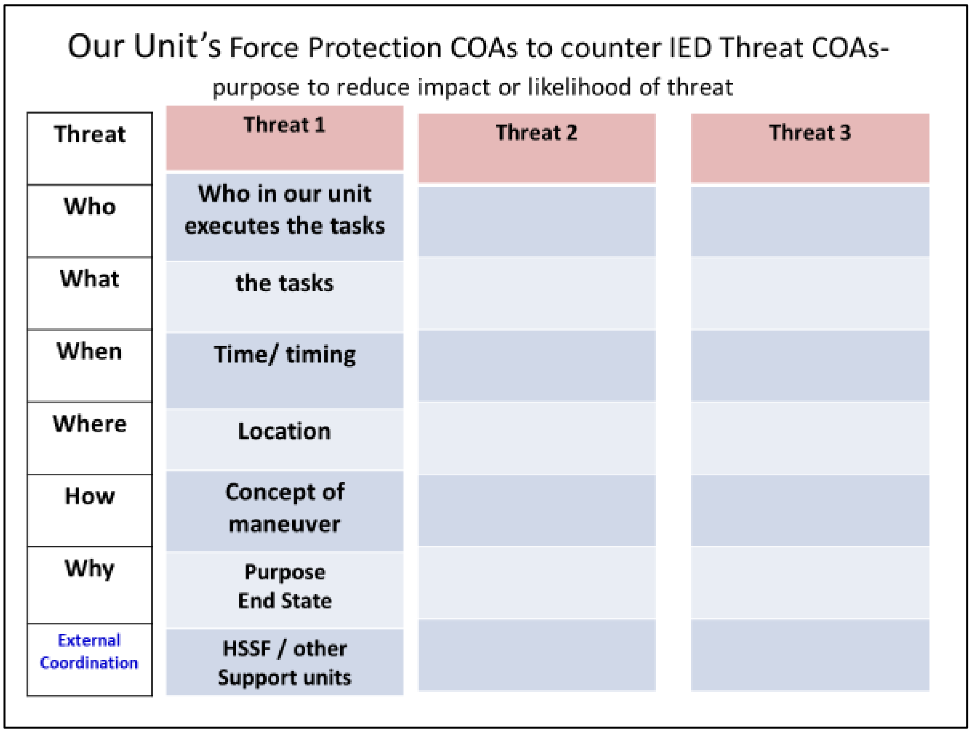
33

Having evaluated the risks linked to each threat, our next step is to prioritise our Force Protection (FP) planning efforts, focusing on the higher-risk threats. We will then proceed to develop plans or unit Courses of Action (COAs) with the aim of mitigating those risks by diminishing, neutralising, or eliminating the identified threats. The COAs will be designed to achieve the following objectives:

- Reduce the likelihood of the threats materialising
- Minimise the potential impact in case a threat does occur
- Disrupt or impede any activity, actor, or phase within the IED Network that contributes to the threat

By implementing these targeted COAs, we can effectively mitigate the risks associated with the higher-priority threats, enhancing the overall security and safety of our operations

Slide 34



Our Unit’s Force Protection COAs to counter IED Threat COAs-

purpose to reduce impact or likelihood of threat

Threat	Threat 1	Threat 2	Threat 3
Who	Who in our unit executes the tasks		
What	the tasks		
When	Time/ timing		
Where	Location		
How	Concept of maneuver		
Why	Purpose End State		
External Coordination	HSSF / other Support units		

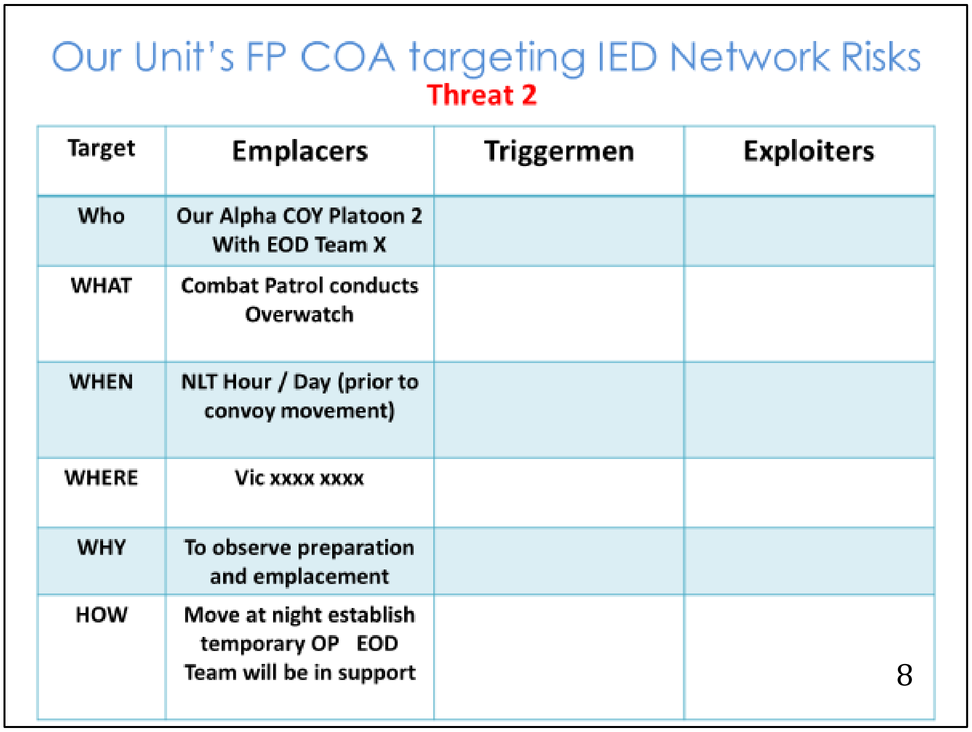
This Chart/Matrix outlines our Unit’s Force Protection Courses of Action designed to counter the IED Threat, with the purpose of reducing the risks, the impact or likelihood of the threat. The COAs include the following elements:

- Who: your Unit or Support Unit that will carry out the mitigating task
- What: The tasks our unit will execute concerning relevant actors and terrain
- When: Critical timing parameters for the operations
- Where: Geographical locations where the effects of our actions will be achieved
- How: The UN unit’s concept of operation, incorporating tasks
- Why: The purpose of the mission, which must align with command levels at least two levels up

Many units depict COAs both visually and in matrix format. A COA board can be expanded to include the mission, commander’s intent, and a scheme of manoeuvre overlaid on a relevant geographic terrain map, encompassing phases of the operation, including any shaping operations.

To adopt a proactive approach to countering IEDs, we must further break down into more specific COAs to mitigate risks by degrading or impacting the network. The upcoming slides will aid in developing auxiliary or supporting COAs that target the actors or activities of the network groups, assisting in mitigating IED risks more effectively.

Slide 35



Our Unit's FP COA targeting IED Network Risks

Threat 2

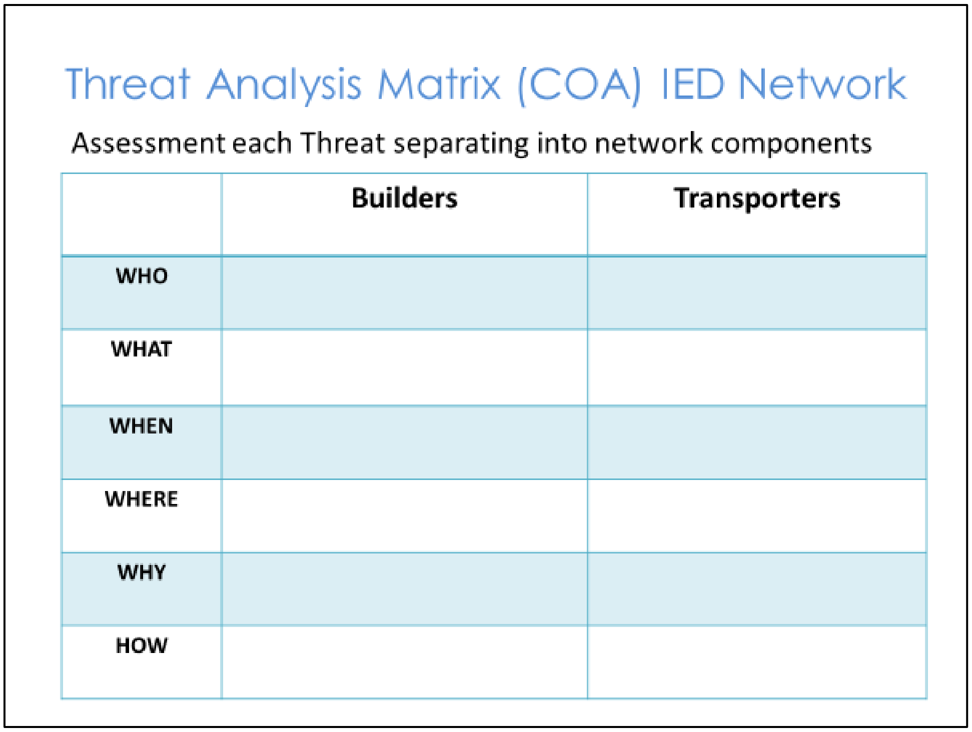
Target	Emplacers	Triggermen	Exploiters
Who	Our Alpha COY Platoon 2 With EOD Team X		
WHAT	Combat Patrol conducts Overwatch		
WHEN	NLT Hour / Day (prior to convoy movement)		
WHERE	Vic xxxx xxxx		
WHY	To observe preparation and emplacement		
HOW	Move at night establish temporary OP EOD Team will be in support		

8

This Chart/Matrix serves as a breakdown of the network components. Shown is an example of a COA targeting the "emplacer" for threat #3. It presents our Unit's Force Protection Courses of Action (COAs), which are tailored to counter the key actors/activities within the IED Network. The primary objective is to adopt a proactive approach to countering and disrupting the network, thereby reducing the risks posed by the network.

To effectively counter IEDs, it is essential to delve into more specific network micro-level COAs. These COAs aim to mitigate risks by degrading or impacting the activities within the network. By focusing on these aspects, we are dedicated to developing effective mitigating COAs that specifically target the actors or activities of the network groups. This approach will significantly enhance our ability to mitigate IED risks more efficiently and proactively.

Slide 36



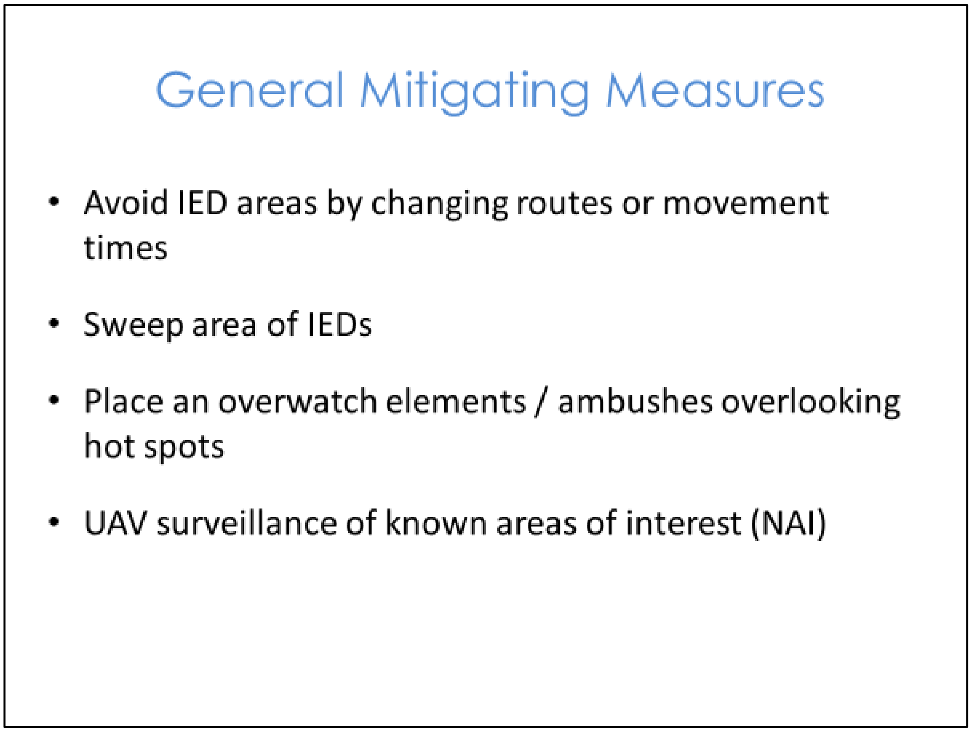
Threat Analysis Matrix (COA) IED Network

Assessment each Threat separating into network components

	Builders	Transporters
WHO		
WHAT		
WHEN		
WHERE		
WHY		
HOW		

Here is a chart/matrix for the breakdown / micro view of the IED building and transporting activities of the IED network.

Slide 37



General Mitigating Measures

- Avoid IED areas by changing routes or movement times
- Sweep area of IEDs
- Place an overwatch elements / ambushes overlooking hot spots
- UAV surveillance of known areas of interest (NAI)

Here are some general mitigating measures that can be implemented to effectively reduce the risks posed by IEDs:

Route and Movement Adaptation: One of the fundamental measures is to avoid known or suspected IED areas by altering routes or adjusting movement times. By staying clear of these high-risk zones, the chances of encountering an IED are significantly minimised.

Area Sweeping: Regular and thorough area sweeps are crucial to identify and detect potential IED threats before they pose a danger. These proactive sweeps involve carefully examining the surroundings, both visually and with specialised equipment, to locate any suspicious objects or indicators of IEDs.

Overwatch and Ambush Tactics: Employing overwatch elements or setting up ambushes at strategic locations overlooking known hot spots can be effective in countering IED threats. Such positions provide valuable vantage points for observation and enable rapid response to potential threats, enhancing the safety of UN units and civilians.

UAV Surveillance: Utilising Unmanned Aerial Vehicles (UAVs) to conduct surveillance over areas of interest (NAIs) is a powerful tool for IED risk reduction. UAVs can cover large areas and collect real-time data, providing valuable peacekeeping-intelligence on potential IED activities or suspicious movements.

Training and Awareness: Proper training for personnel, including both police and military units and civilians, is essential. This involves educating them about IED threats, recognising indicators of potential devices, and adopting the necessary safety precautions.

Robust Intelligence Gathering: Establishing a reliable peacekeeping-intelligence network to gather information on potential IED threats is crucial. This includes collecting data from various sources, such as human peacekeeping-intelligence, signals intelligence, and open-source peacekeeping-intelligence, to gain a comprehensive understanding of the threat landscape.

Counter-IED Technology: Investing in and deploying advanced counter-IED technologies can significantly enhance risk mitigation efforts. These technologies may include electronic countermeasures, remote-controlled robots for IED disposal, and advanced detection systems.

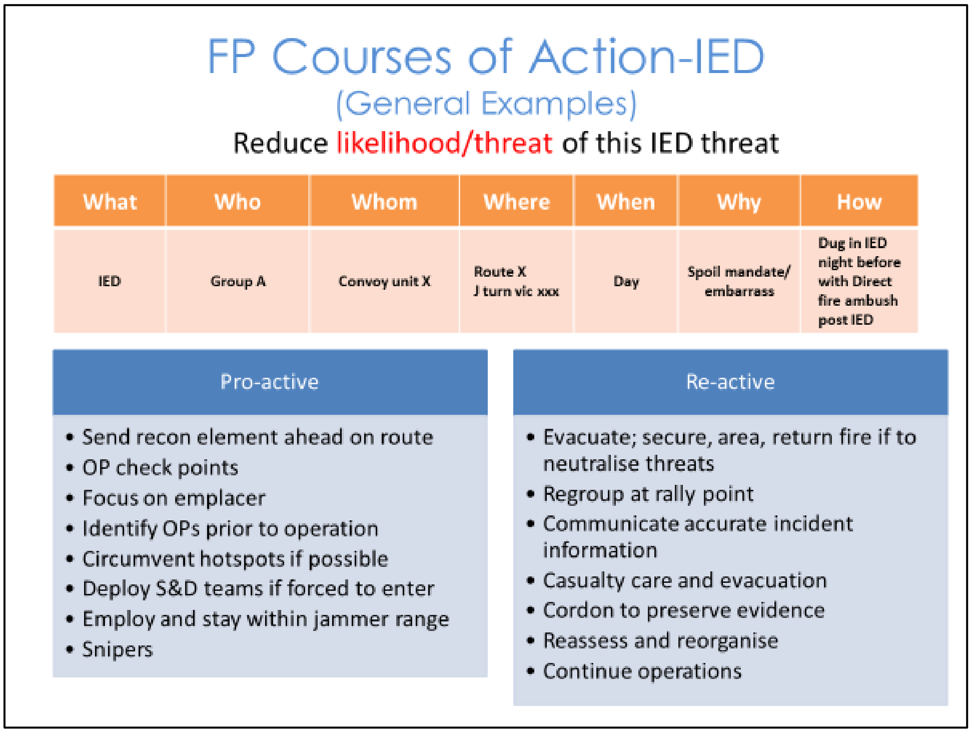
Collaboration and Information Sharing: Effective risk mitigation often involves cooperation between different organisations and agencies. Sharing information and peacekeeping-intelligence with relevant partners can help identify emerging threats and implement collective measures to address them.

Community Engagement: Engaging with local communities can foster trust and cooperation, leading to better information sharing and a deeper understanding of the local threat environment. This collaboration can be instrumental in identifying potential IED threats and preventing their use.

Post-Incident Analysis: Conducting thorough post-incident analyses is vital to learn from past experiences and adapt strategies accordingly. This enables the refinement of existing and future mitigating measures and the development of new tactics to stay ahead of evolving IED threats.

By integrating these comprehensive mitigating measures into security protocols, it becomes possible to mitigate the risks of IEDs effectively, safeguarding personnel and civilian populations from potential harm.

.Slide 38



FP Courses of Action-IED

(General Examples)

Reduce likelihood/threat of this IED threat

What	Who	Whom	Where	When	Why	How
IED	Group A	Convoy unit X	Route X J turn vic xxx	Day	Spoil mandate/ embarrass	Dug in IED night before with Direct fire ambush post IED

Pro-active

- Send recon element ahead on route
- OP check points
- Focus on emplacer
- Identify OPs prior to operation
- Circumvent hotspots if possible
- Deploy S&D teams if forced to enter
- Employ and stay within jammer range
- Snipers

Re-active

- Evacuate; secure, area, return fire if to neutralise threats
- Regroup at rally point
- Communicate accurate incident information
- Casualty care and evacuation
- Cordon to preserve evidence
- Reassess and reorganise
- Continue operations

Here is an example of a threat Course of Action (COA) that falls within a medium to high-risk level, which we discussed earlier:

Proactive Mitigation Measures:

Recon Element Deployment: Send a reconnaissance element ahead on the route to gather peacekeeping-intelligence and identify potential threats before proceeding further.

Implement OP Checkpoints: Set up observation posts (OPs) at strategic locations along the route to monitor and intercept any suspicious activities or emplacements.

Focus on Emplacer Identification: Emphasise the identification of individuals or groups responsible for emplacing IEDs to disrupt their operations before they can execute an attack.

OP Identification: Identify and locate IED group Observation Posts (OPs) prior to conducting operations to maintain situational awareness, attack them with a show of force or avoid the area.

Avoid Hotspots: Whenever possible, circumvent known hotspots or areas of high risk to minimise exposure to potential IED threats.

S&D Teams Deployment: If forced to enter high-risk areas, deploy Search and Destroy (S&D) teams to actively locate and neutralise any potential IEDs.

Use Jammers: Deploy electronic jammers, CREW, and stay within their effective range to disrupt remote detonation signals and reduce the risk of triggering IEDs.

Sniper Overwatch: Position and establish sniper positions to provide overwatch of potential IED locations, deterring potential threats and enhancing force protection.

Reactive Mitigation Measures (Post IED Detonation):

Move out of Kill Zone: Immediately evacuate the area and move out of the kill zone to reduce the risk of further casualties.

Establish Security and Return Fire: Secure the area and return fire if necessary to neutralise any immediate threats.

Disperse to Rally Point: Disperse and regroup at a designated rally point to consolidate forces and maintain situational awareness.

Effective Communication: Communicate accurate information about the distance, direction, and description of the incident to aid in coordinated response efforts.

Initiate Casualty Care (CASEVAC): Immediately initiate casualty care and call for medical evacuation (CASEVAC) to provide prompt medical attention to the injured.

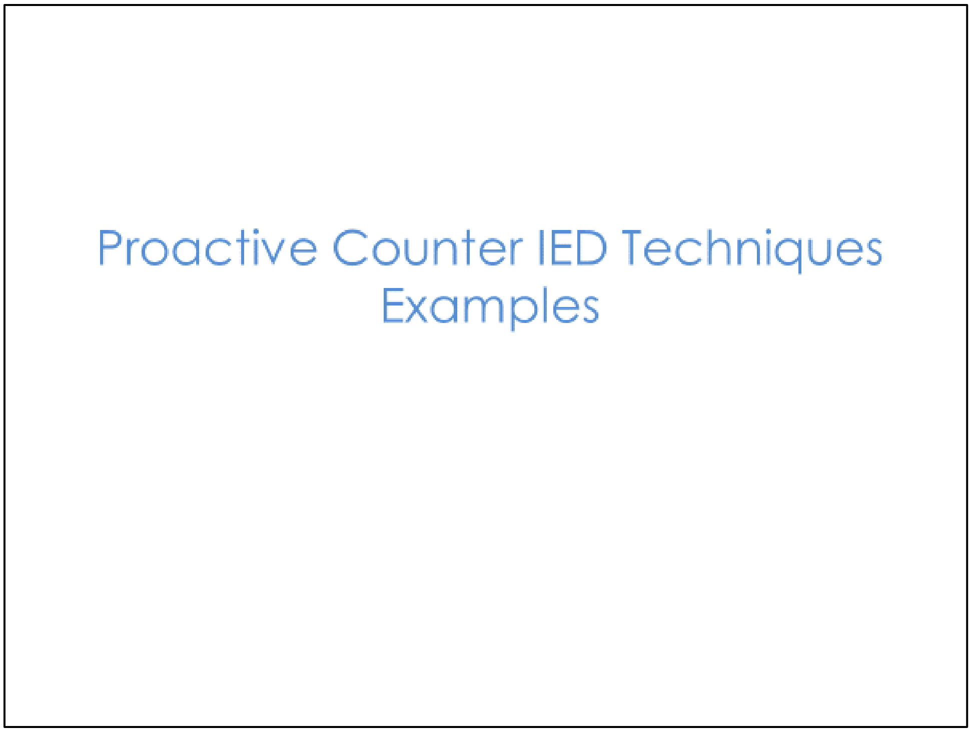
Cordon the Area: Establish a security cordon around the incident site to prevent unauthorised access and preserve potential evidence.

Consolidate and Reorganise: Reassess the situation, consolidate forces, and reorganise to maintain operational effectiveness.

Continue the Mission: After addressing the immediate aftermath of the IED detonation, assess the mission's feasibility and continue.

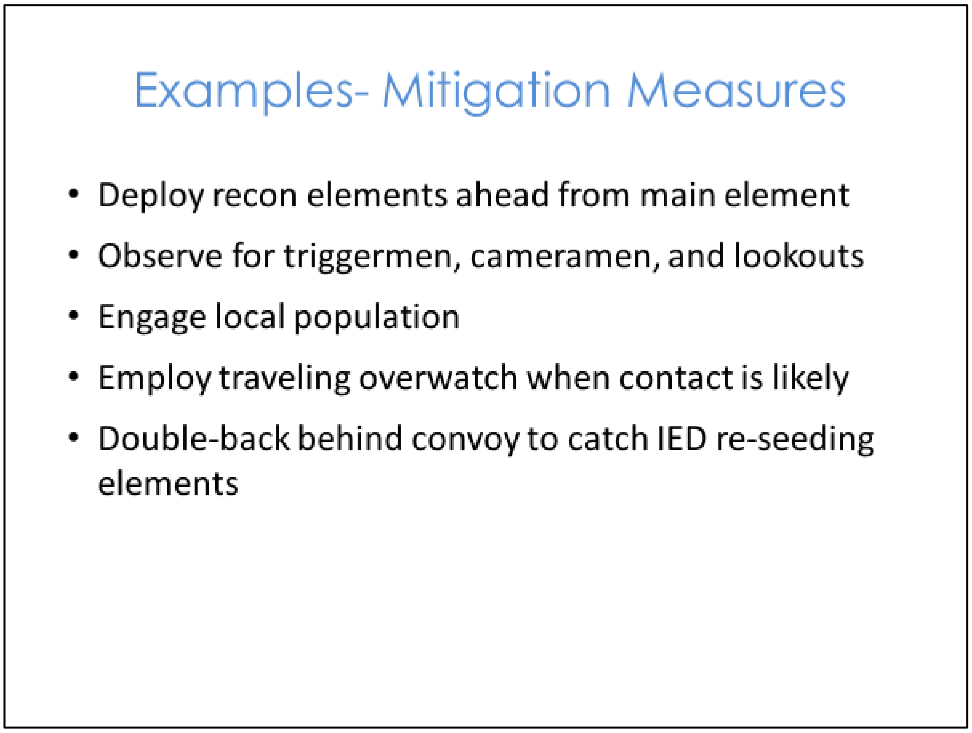
By combining these proactive and reactive measures, we can effectively mitigate the risks posed by this medium to high-risk threat COA. Implementing these measures will enhance force protection, reduce potential casualties, and allow for a swift and organised response to IED incidents.

Slide 39



Proactive Counter IED Techniques Examples

Slide 40



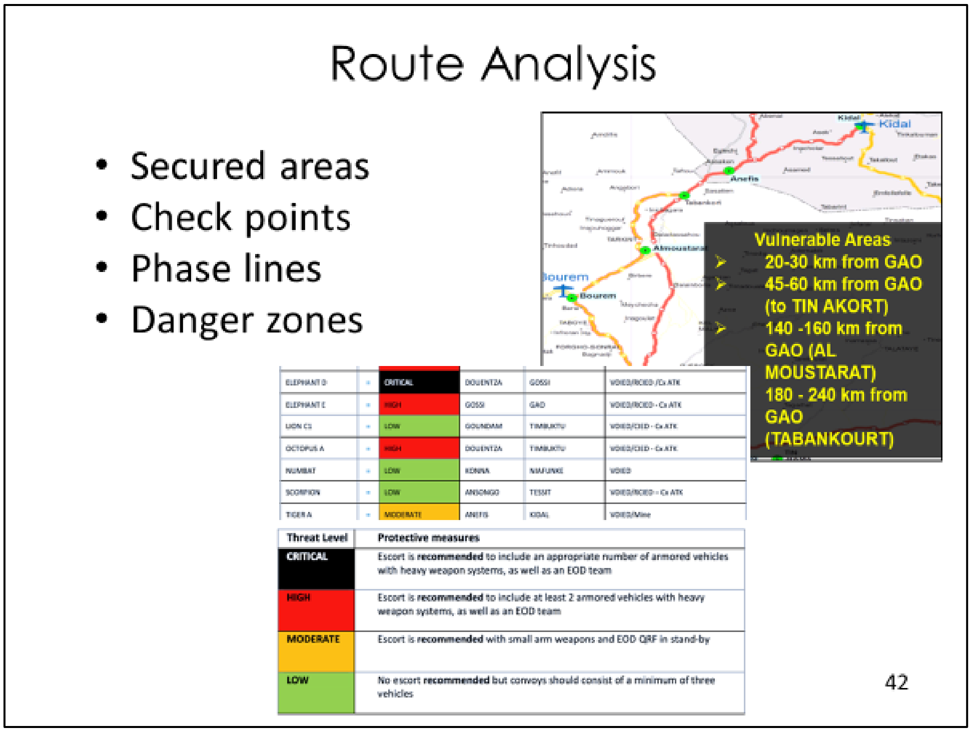
Examples- Mitigation Measures

- Deploy recon elements ahead from main element
- Observe for triggermen, cameramen, and lookouts
- Engage local population
- Employ traveling overwatch when contact is likely
- Double-back behind convoy to catch IED re-seeding elements

Here are examples of possible basic mitigation measures:

- Deploy recon elements ahead of the main element
- Observe for triggermen, cameramen, and lookouts
- Engage the local population for information
- Employ travelling overwatch when contact is likely
- Double back behind the convoy to catch the group that may re-seed an IED

Slide 41



Route Analysis

- Secured areas
- Check points
- Phase lines
- Danger zones

Kidal
Anefis
Tabankort
Almoustarat
Bourem

Vulnerable Areas

- 20-30 km from GAO
- 45-60 km from GAO (to TIN AKORT)
- 140 -160 km from GAO (AL MOUSTARAT) 180 - 240 km from GAO (TABANKOURT)

ELEPHANT D	→	CRITICAL	DOUENTZA	GOSSI	VOIED/RCIED /Cx ATK
ELEPHANT E	→	HIGH	GOSSI	GAO	VOIED/RCIED - Cx ATK
LION C1	→	LOW	GOUNDAM	TIMBUKTU	VOIED/CIED - Cx ATK
OCTOPUS A	→	HIGH	DOUENTZA	TIMBUKTU	VOIED/CIED - Cx ATK
NUMBAT	→	LOW	KONNA	NIAFUNKE	VOIED
SCORPION	→	LOW	ANSONGO	TESSIT	VOIED/RCIED - Cx ATK
TIGER A	→	MODERATE	ANEFIS	KIDAL	VOIED/Mine

Threat Level	Protective measures
CRITICAL	Escort is **recommended** to include an appropriate number of armored vehicles with heavy weapon systems, as well as an EOD team
HIGH	Escort is **recommended** to include at least 2 armored vehicles with heavy weapon systems, as well as an EOD team
MODERATE	Escort is **recommended** with small arm weapons and EOD QRF in stand-by
LOW	No escort **recommended** but convoys should consist of a minimum of three vehicles

42

Effective route reconnaissance and analysis play a crucial role in enhancing IED situational awareness and counter-IED operations. To aid in codifying the level of risk associated with certain routes in the area of operations, a valuable tool can be employed by all mission components. This tool utilises red, yellow, and green assignments to indicate the risk level of routes, which may vary over time due to changing circumstances. Additionally, to facilitate IED risk mitigation, routes should be designed and designated to incorporate the following elements:

Risk Level Assignments: Implement a clear and standardised system for assigning risk levels (red, yellow, and green) to different routes. This enables personnel to quickly assess the relative dangers associated with each route before proceeding.

Secured Areas: Designate and maintain secured areas along routes to provide safe zones where UN personnel, UN units, and civilians can assemble away from potential IED threats. These areas can be regularly monitored and cleared to ensure their effectiveness.

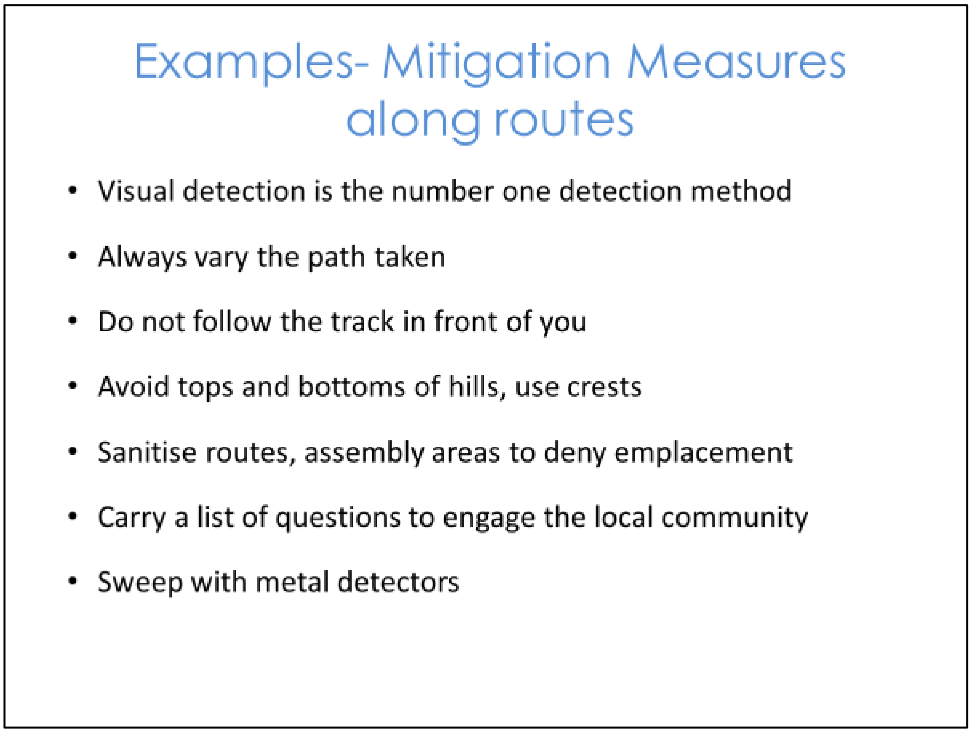
Checkpoints: Strategically place checkpoints along the routes to monitor and regulate vehicle and personnel movement. These checkpoints serve as critical locations for inspections and can help detect potential threats.

Phase Lines: Establish phase lines along the routes to divide the area of operations into different zones. These phase lines act as checkpoints for progress during missions, allowing for better control and situational awareness.

Danger Zones: Identify and clearly mark danger zones along the routes where there is a higher likelihood of encountering IEDs or hostile activity. Effective signage and communication are essential to alert personnel and civilians about the increased risk in these areas.

By integrating these measures into route planning and operations, missions can significantly enhance their ability to mitigate IED risks. Regular updates and assessments of the risk level assignments will ensure that the latest peacekeeping-intelligence and threat assessments are considered, allowing for dynamic and adaptable route planning. Additionally, clear communication and training for personnel on the significance of the risk level assignments and the incorporation of designated elements will further strengthen the effectiveness of IED risk mitigation efforts.

Slide 42



Examples- Mitigation Measures along routes

- Visual detection is the number one detection method
- Always vary the path taken
- Do not follow the track in front of you
- Avoid tops and bottoms of hills, use crests
- Sanitise routes, assembly areas to deny emplacement
- Carry a list of questions to engage the local community
- Sweep with metal detectors

Improving IED Mitigation Measures along Routes:

Visual Detection Priority: Visual detection should be given the highest priority as the primary method for identifying potential threats along the route. Vigilant observation by trained personnel is essential to spot any suspicious objects or indicators of IEDs.

Path Variation: Always vary the path taken along the route to avoid predictability. This unpredictable movement helps reduce the risk of potential ambushes and IED attacks targeting repetitive routes.

Avoid Following Tracks: Refrain from following the track immediately in front of you, as this could lead to falling into a potential IED trigger pattern. Maintaining distance and avoiding the same path as preceding vehicles enhance safety.

Utilise Crests on Hills: When traversing hilly terrain, use crests rather than tops and bottoms of hills. Crests provide better visibility and reduce the risk of hidden threats on the other side.

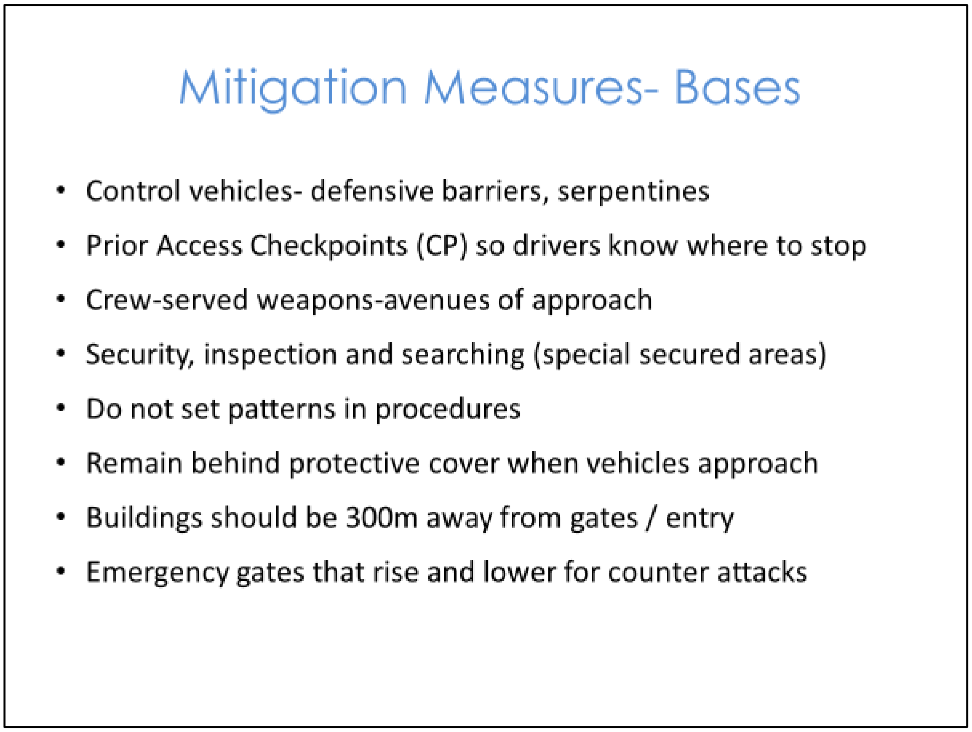
Sanitise Routes and Assembly Areas: Regularly sanitise routes and assembly areas to deny potential emplacement sites for IEDs. This proactive measure aims to minimise opportunities for adversaries to plant devices.

Engage Local Community: Carry a list of questions to engage with the local community during operations. Building rapport and gathering information from locals can provide valuable insights into potential threats in the area.

Sweep with Metal Detectors: Equip personnel with metal detectors to sweep the area ahead of them, especially in high-risk zones. This additional layer of detection can help identify metallic components of potential IEDs.

By incorporating these improved mitigation measures into route planning and operations, the risks of encountering IEDs can be significantly reduced. A combination of visual detection, path variation, and strategic avoidance of potential threats, along with engaging the local community and employing specialised equipment, enhances overall safety and effectiveness during missions.

Slide 43



Mitigation Measures- Bases

- Control vehicles- defensive barriers, serpentines
- Prior Access Checkpoints (CP) so drivers know where to stop
- Crew-served weapons-avenues of approach
- Security, inspection and searching (special secured areas)
- Do not set patterns in procedures
- Remain behind protective cover when vehicles approach
- Buildings should be 300m away from gates / entry
- Emergency gates that rise and lower for counter attacks

Improving IED Mitigation Measures in and around UN Unit Bases:

Mitigating the threats of suicide vehicles and personnel IEDs is of paramount importance, as these attacks have resulted in significant casualties among peacekeepers in recent years. To effectively safeguard our bases, we must be meticulous planners and maintain constant vigilance. Implementing the following measures, with proper planning, resources, and execution, can be highly effective:

Vehicle Control Measures: Employ defensive barriers and serpentine layouts to control vehicle access points to the base. These measures help slow down potential threats and create chokepoints for inspection and searching.

Prior Access Checkpoints (CP): Clearly mark and establish prior access checkpoints so drivers know where to stop and undergo scrutiny before entering the base. This helps prevent unauthorised vehicles from approaching critical areas.

Crew-Served Weapons and Avenues of Approach: Strategically position crew-served weapons to cover potential avenues of approach towards the base. This creates a deterrent for potential attackers and enhances the base's perimeter defence.

Security, Inspection, and Searching: Designate special secured areas for security, inspection, and thorough searching of vehicles and personnel entering the base. Rigorous checks in these areas help detect and intercept potential threats.

Avoid Predictability: Avoid setting patterns in procedures to prevent adversaries from predicting our actions. Implement randomised security measures and patrol patterns to keep potential attackers off-guard.

Safety Behind Protective Cover: Instruct personnel to remain behind the protective cover when vehicles approach access points. This minimises exposure to potential threats and provides added protection.

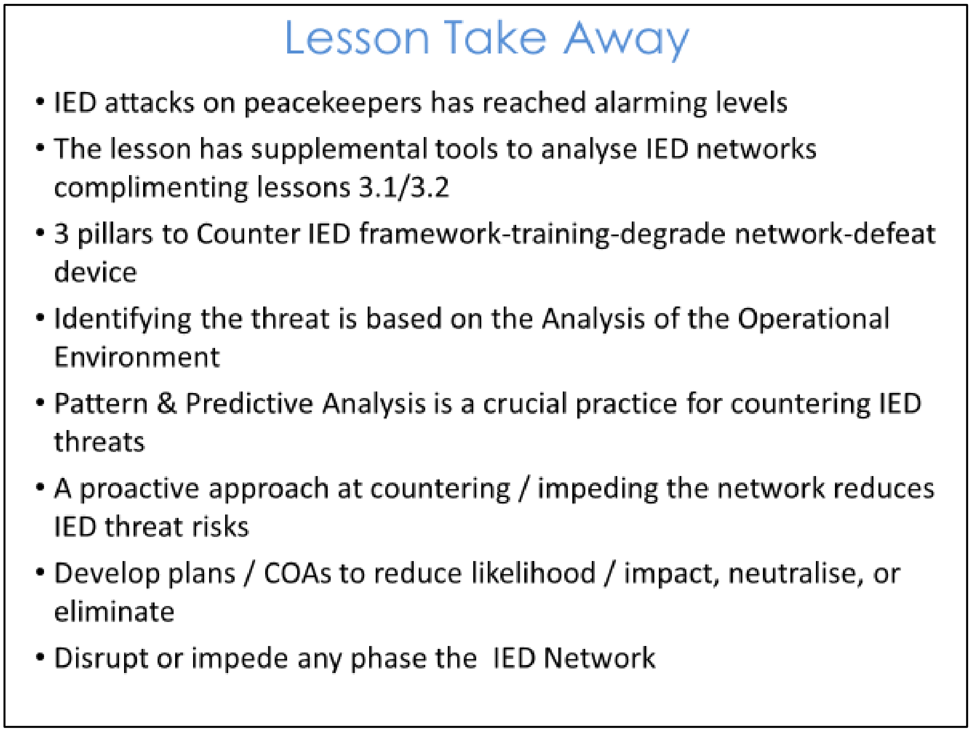
Safe Building Distance: Ensure that buildings are at least 300 meters away from the gates or entry points to mitigate the damage caused by IED attacks. This distance creates a safer buffer zone for the base's infrastructure.

Emergency Gates: Install gates that can be raised or lowered quickly to facilitate counterattacks in the event of an incident. These emergency gates enhance the base's ability to respond swiftly to threats.

Separate Holding or Load Transfer Area for Commercial/Vendor Vehicles: Establish a separate holding or load transfer area away from the main facility for commercial or vendor vehicles. This area should be equipped with defensive barriers to ensure that these vehicles undergo thorough inspection and screening before entering the main base. Creating this distinct area helps reduce the risk of potential threats from commercial or vendor vehicles and adds an extra layer of security to the base's perimeter.

By adopting these comprehensive measures and ensuring their proper implementation, UN Unit Bases can significantly reduce the risk posed by suicide vehicles and personnel IEDs. Continuous evaluation, adaptation, and training are essential to maintain a robust defence posture and protect the safety of peacekeepers and personnel within the base.

Slide 44



Lesson Take Away

- IED attacks on peacekeepers has reached alarming levels
- The lesson has supplemental tools to analyse IED networks complimenting lessons 3.1/3.2
- 3 pillars to Counter IED framework-training-degrade network-defeat device
- Identifying the threat is based on the Analysis of the Operational Environment
- Pattern & Predictive Analysis is a crucial practice for countering IED threats
- A proactive approach at countering / impeding the network reduces IED threat risks
- Develop plans / COAs to reduce likelihood / impact, neutralise, or eliminate
- Disrupt or impede any phase the IED Network

Summary

Key takeaways from the lesson:

The frequency of IED attacks on peacekeepers is a cause for concern.

The lesson offers supplemental tools to analyse IED networks, complementing lessons 3.1 and 3.2.

The Counter IED framework relies on three pillars: training, degrading networks, and defeating devices.

Identifying the threat requires a thorough analysis of the Operational Environment.

Employing Pattern & Predictive Analysis is crucial for effectively countering IED threats.

Taking a proactive approach to impede the network reduces the risks posed by IED threats.

Develop plans and courses of action to minimize the likelihood and impact of IED attacks and neutralize or eliminate the threat.

Disrupt or impede any phase of the IED Network is a proactive strategy to mitigate the risks of IED threats

Learning Activities 3.3

RESOURCES
Situations- Slide LA Slide 45 as a Handouts; chalkboard or butcher paper and markers

TIME
Suggested time 30 min to one hour (depending on the discussions).

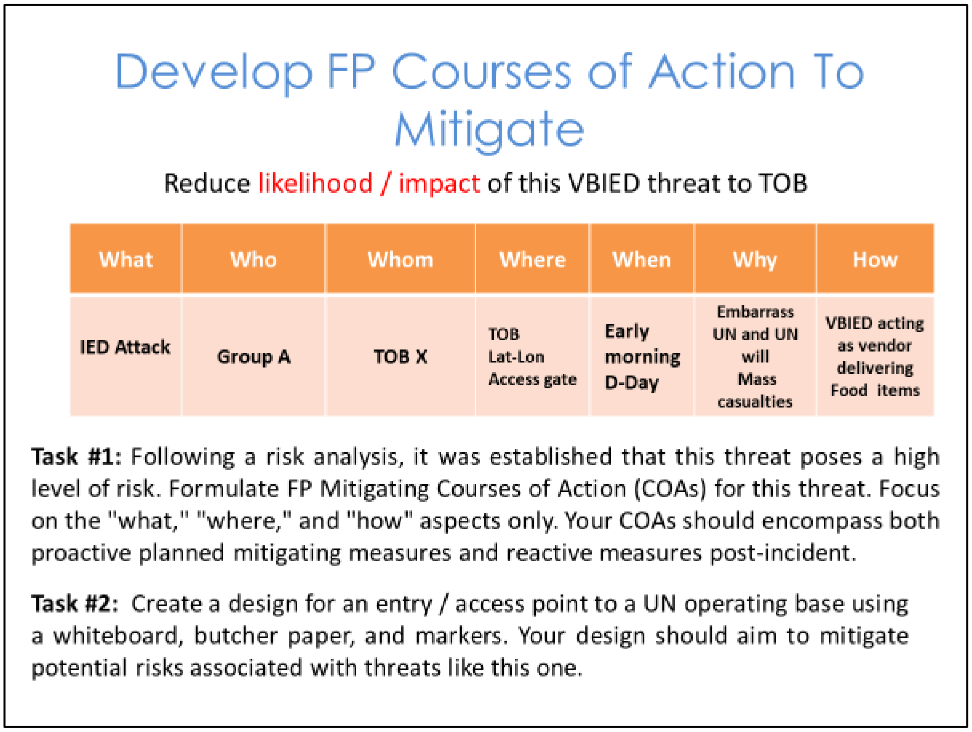
PREPARATION
Divide the class into groups and give them the necessary time to review the LA Slide 45. Ask the students to accomplish the two tasks, discuss and report back to the plenary.

TASKS:

Task #1: Following a risk analysis, it was established that this threat (shown on LA Slide 45) poses a high level of risk. Formulate FP Mitigating Courses of Action (COAs) for this threat. Focus on the "what," "where," and "how" aspects only. Your COAs should encompass both proactive planned mitigating measures and reactive measures post-incident.

Task #2: Create a design for an entry/access point to a UN operating base using a whiteboard, butcher paper, and markers. Your design should aim to mitigate potential risks associated with threats like this one.

LA Slide 45



Develop FP Courses of Action To Mitigate

Reduce likelihood / impact of this VBIED threat to TOB

What	Who	Whom	Where	When	Why	How
IED Attack	Group A	TOB X	TOB Lat-Lon Access gate	Early morning D-Day	Embarrass UN and UN will Mass casualties	VBIED acting as vendor delivering Food items

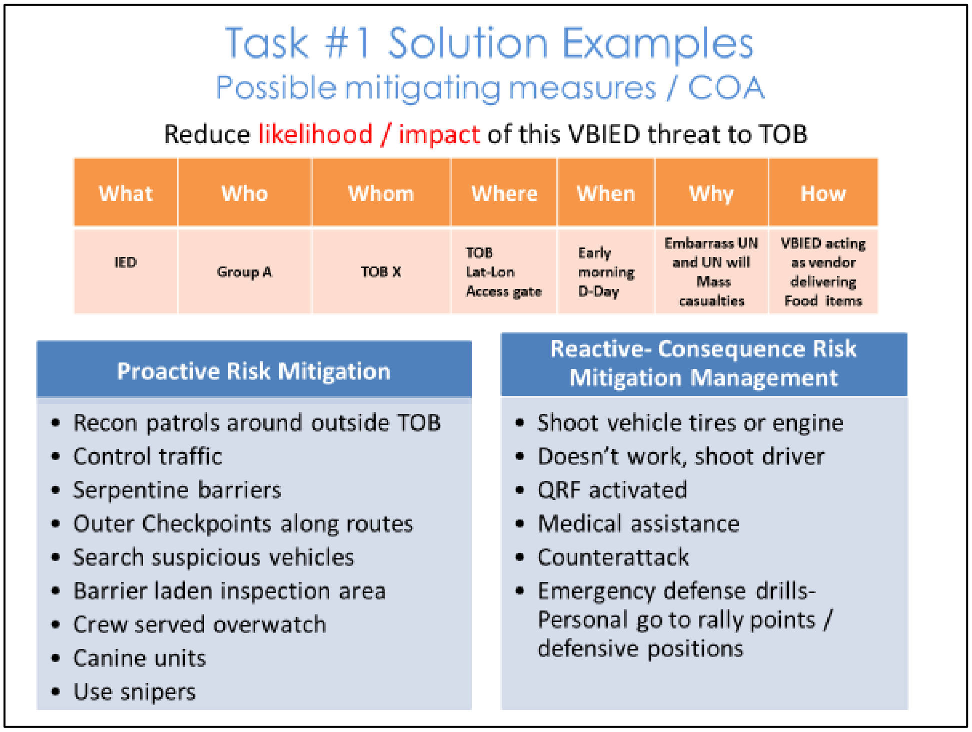
Task #1: Following a risk analysis, it was established that this threat poses a high level of risk. Formulate FP Mitigating Courses of Action (COAs) for this threat. Focus on the "what," "where," and "how" aspects only. Your COAs should encompass both proactive planned mitigating measures and reactive measures post-incident.

Task #2: Create a design for an entry / access point to a UN operating base using a whiteboard, butcher paper, and markers. Your design should aim to mitigate potential risks associated with threats like this one.

INSTRUCTOR NOTES:

After the groups have presented their solution sets to the plenary, use the provided example solution slides (LA Slides 46 / 47) to help facilitate further discussions. Displaying these slides visually will enable the students to review their work and compare it to the possible solutions. This exercise will help reinforce the key framework for FP planning and encourage constructive discussions among the participants.

LA Slide 46



Task #1 Solution Examples

Possible mitigating measures / COA

Reduce likelihood / impact of this VBIED threat to TOB

What	Who	Whom	Where	When	Why	How
IED	Group A	TOB X	TOB Lat-Lon Access gate	Early morning D-Day	Embarrass UN and UN will Mass casualties	VBIED acting as vendor delivering Food items

Proactive Risk Mitigation

- Recon patrols around outside TOB
- Control traffic
- Serpentine barriers
- Outer Checkpoints along routes
- Search suspicious vehicles
- Barrier laden inspection area
- Crew served overwatch
- Canine units
- Use snipers

Reactive- Consequence Risk Mitigation Management

- Shoot vehicle tires or engine
- Doesn't work, shoot driver
- QRF activated
- Medical assistance
- Counterattack
- Emergency defense drills- Personal go to rally points / defensive positions

Here are additional expanded talking points to help you facilitate the discussions. Our primary emphasis is on proactive measures; however, we will also include reactive consequence mitigation measures that should be planned and rehearsed to effectively reduce post-IED incidents, casualties, and negative effects on our operations.

Proactive Risk Mitigation:

Conducting regular recon patrols around the perimeter of the base enables early identification of potential threats and suspicious activities, preventing them from getting closer to the facility undetected.

Implementing comprehensive traffic control measures within and around the TOB helps regulate vehicle movement and prevents unauthorised or suspicious vehicles from entering the area.

Deploying serpentine barriers at key entry points to the TOB forces vehicles to follow a zig-zag pattern, reducing their speed and making it more difficult for potential Vehicle-Borne IEDs (VBIEDs) to approach at high speeds.

Establishing outer checkpoints along routes leading to the TOB allows for thorough inspections of vehicles and cargo, effectively preventing VBIEDs from entering unnoticed.

Regularly searching suspicious vehicles, both at checkpoints and during patrols, enhances the capability to identify and intercept potential VBIED threats before they pose a danger.

Setting up a barrier-laden inspection area at the TOB entrance subjects incoming vehicles to thorough scrutiny, providing an opportunity to neutralise potential threats from a safe distance.

Utilising crew-served overwatch positions ensures continuous surveillance and a robust defence against potential VBIED threats, improving the overall security posture.

Deploying highly trained canine units specialised in explosive detection enhances the ability to identify concealed explosives and prevent VBIED attacks.

Employing skilled snipers as part of the proactive measures allows for the neutralisation of threats at a distance, especially during the approach to the TOB.

Reactive- Consequence Risk Mitigation Management:

In case a suspicious vehicle poses an immediate threat, authorised personnel are prepared to disable the vehicle by shooting its tires or engine, rendering it immobile and reducing the risk it poses.

If the above action proves ineffective, personnel are trained and authorised to target the driver, preventing the vehicle from reaching its intended target.

A Quick Reaction Force (QRF) is readily activated to rapidly respond to any incidents, neutralising threats and providing immediate assistance and support.

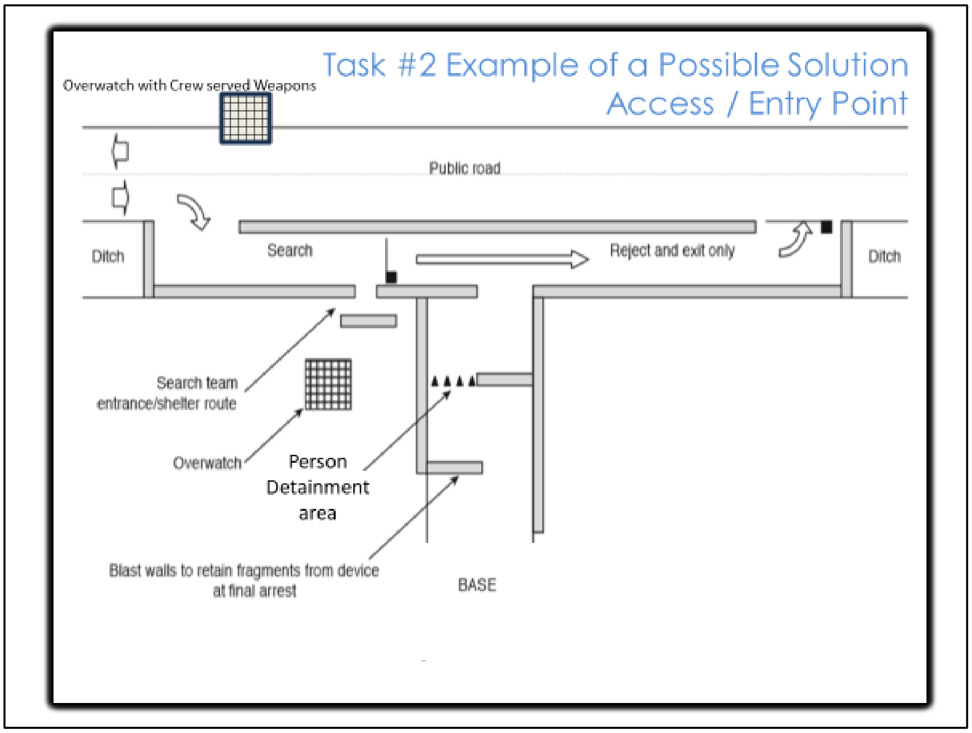
Dispatching medical assistance promptly to the affected area ensures the timely treatment of casualties and minimises the impact of the attack.

Having well-rehearsed counterattack plans ensures a swift and effective response to any IED-related incidents, mitigating the consequences and enhancing operational resilience.

Regularly conducting emergency defence drills trains personnel to take immediate action, such as proceeding to rally points or defensive positions, in the event of an IED attack.

By effectively integrating these proactive and reactive measures into operational planning and training, the likelihood and impact of VBIED threats to the base can be significantly reduced. This approach fosters a safer and more secure environment for personnel and operations, enhancing overall mission success and personnel.

LA Slide 47



Task #2 Example of a Possible Solution
Access / Entry Point

Here is an example of a possible solution set for the design of a UN Unit Base entry point.

Lesson 3.4

Cyber Threat Mitigation

The Lesson

Starting the Lesson

Overview

Engage the participants by eliciting their views and thoughts on the direct and collateral impact of cyber-attacks on tactical unit operations. Explore various perspectives and insights. Consider the following discussion points: Direct Impact: Discuss how cyber-attacks can directly disrupt tactical units, including unauthorised system access, denial-of-service attacks on communication networks, or malware compromising critical equipment. Collateral Impact: Explore the ripple effects of cyber-attacks on tactical unit operations, such as disruptions to logistics, intelligence gathering, and command and control networks, affecting the unit's overall effectiveness and readiness.

☞ ***Note to instructor*** *IT Equipment refers to physical devices used in information technology systems, such as computers, peripherals, networking equipment, storage devices, communication equipment, and servers. Networks are interconnected systems that allow devices to communicate and share resources. It is suggested that the instructor for this lesson have some technical knowledge of IT or communication systems.*

This lesson expands on the previous module focusing on cyber and misinformation/disinformation. Its objective is to provide participants with strategies for mitigating the risks associated with cyber threats. The instructor should possess a foundational understanding of IT and communication networks/equipment.

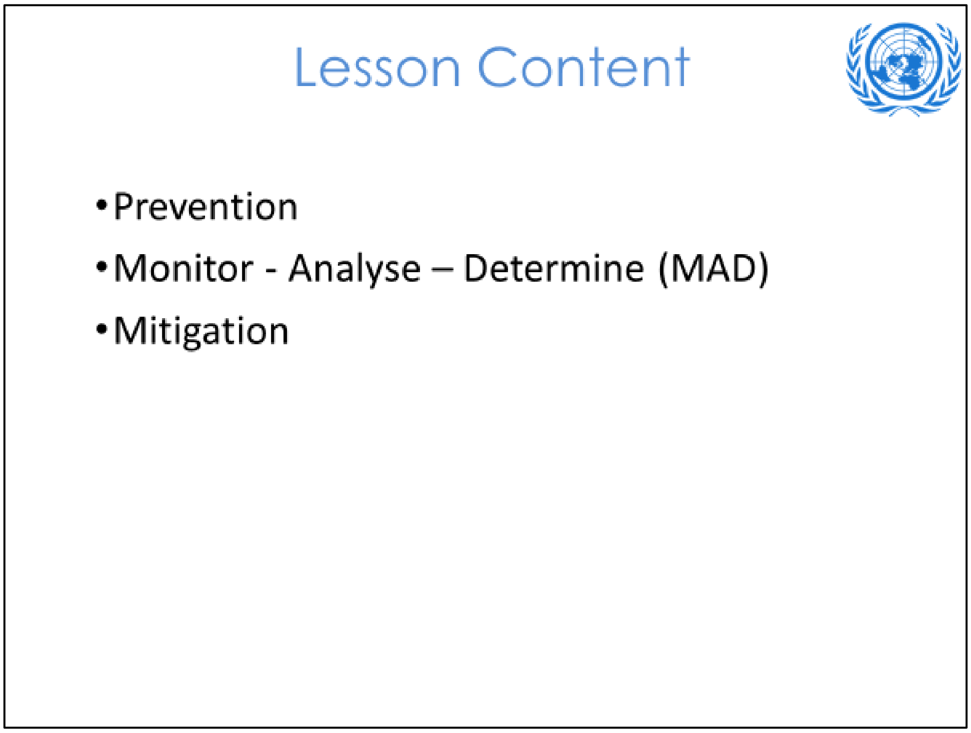
Slide 1

Lesson 3.4
Cyber Threat Mitigation

In today's interconnected world, cyber threats are a growing concern for organisations worldwide, including the United Nations (UN) and its peacekeeping operations. Cyber-attacks targeting the UN or tactical units engaged in peacekeeping operations can have far-reaching consequences, impacting the organisation's and UN units' ability to carry out its mandates effectively and compromising the safety and security of personnel in the field. To address this challenge, a proactive and comprehensive approach to risk mitigation is necessary.

Cyber-attack risk mitigation involves implementing strategies and measures to minimise the chances of cyber-attacks and their negative impact on an organisation or system. In this lesson, we aim to familiarise you with a method for monitoring, analysing, and determining whether a cyber-attack could compromise or adversely affect a tactical operation. This will enable you to conduct force protection planning and implement measures to mitigate those risks.

Slide 2



Lesson Content

- Prevention
- Monitor - Analyse – Determine (MAD)
- Mitigation

This lesson will cover the following key topics:

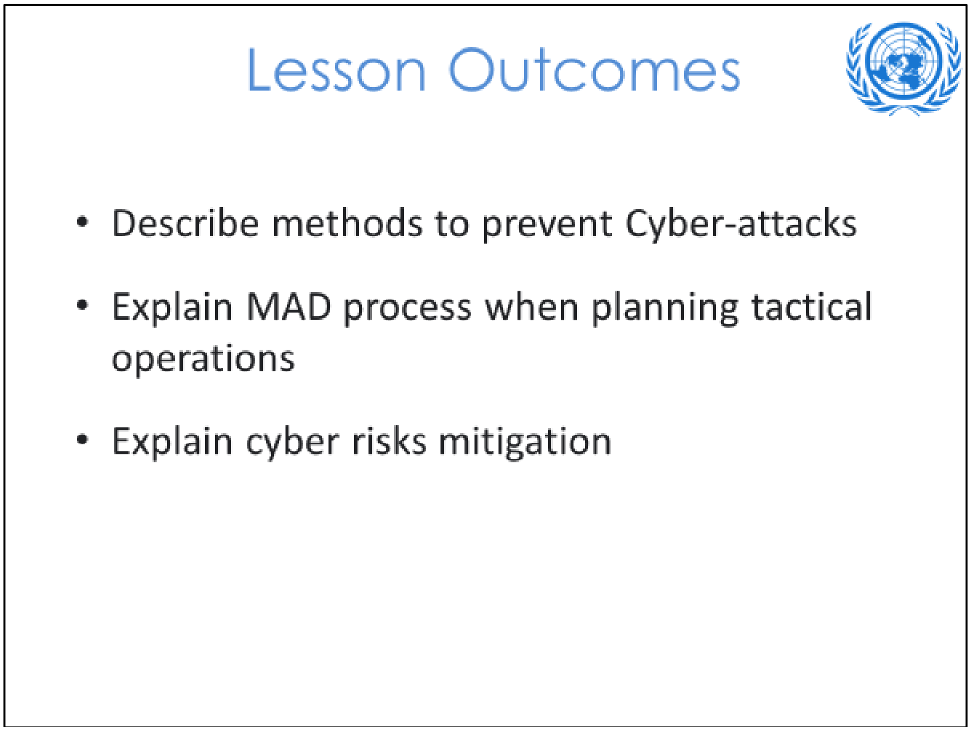
Prevention: Strategies and measures aimed at preventing cyber-attacks from occurring in the first place. This includes implementing strong security measures, conducting regular assessments, and educating employees about cybersecurity best practices.

Monitor - Analyse - Determine (MAD): An approach for actively monitoring and analysing cyber threats, determining/ assessing their potential impact on operations, and developing appropriate response actions. This method enables timely detection and decision-making in the face of cyber-attacks.

Mitigation: Techniques and practices to mitigate the risks and minimise the impact of cyber-attacks. This includes implementing response and FP plans.

By covering these topics, participants will gain a comprehensive understanding of prevention strategies, the "MAD" approach for threat analysis, and effective mitigation techniques to protect against cyber-attacks and safeguard organisational operations.

Slide 3



Lesson Outcomes

- Describe methods to prevent Cyber-attacks
- Explain MAD process when planning tactical operations
- Explain cyber risks mitigation

These are the lesson objectives for this session. Please take a moment to review them. By the end of this lesson, you will be able to:

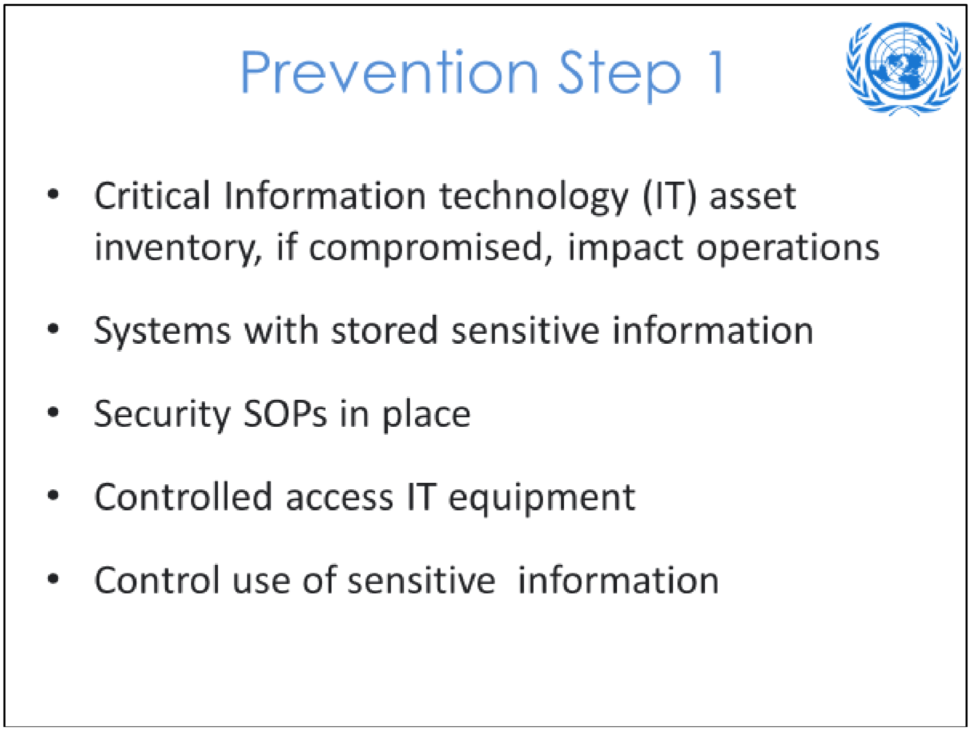
Describe methods for preventing cyber-attacks and safeguarding against potential threats.

Explain the MAD process (Monitor-Analyse-Determine) and its application in planning tactical operations, enabling effective FP planning to mitigate risks.

Explain the concept of cyber risk mitigation and identify strategies and measures to minimise the impact of cyber-attacks on unit operations.

By achieving these objectives, you will gain the necessary knowledge and skills to proactively prevent cyber-attacks, assess threats using the MAD process, and implement effective mitigation strategies to protect tactical operations from potential risks.

Slide 4



Prevention Step 1

- Critical Information technology (IT) asset inventory, if compromised, impact operations
- Systems with stored sensitive information
- Security SOPs in place
- Controlled access IT equipment
- Control use of sensitive information

Prevention is the foremost step in stopping an attack before it occurs. The upcoming slides will present suggested techniques and processes to assist in preventing attacks. Here are some key points to consider:

Completion of Critical Asset Inventory: It is essential to compile a comprehensive inventory of critical assets within the unit. This includes identifying IT and communication systems that, if compromised, could have a significant impact on operations. By recognising these assets, focused protective measures can be implemented.

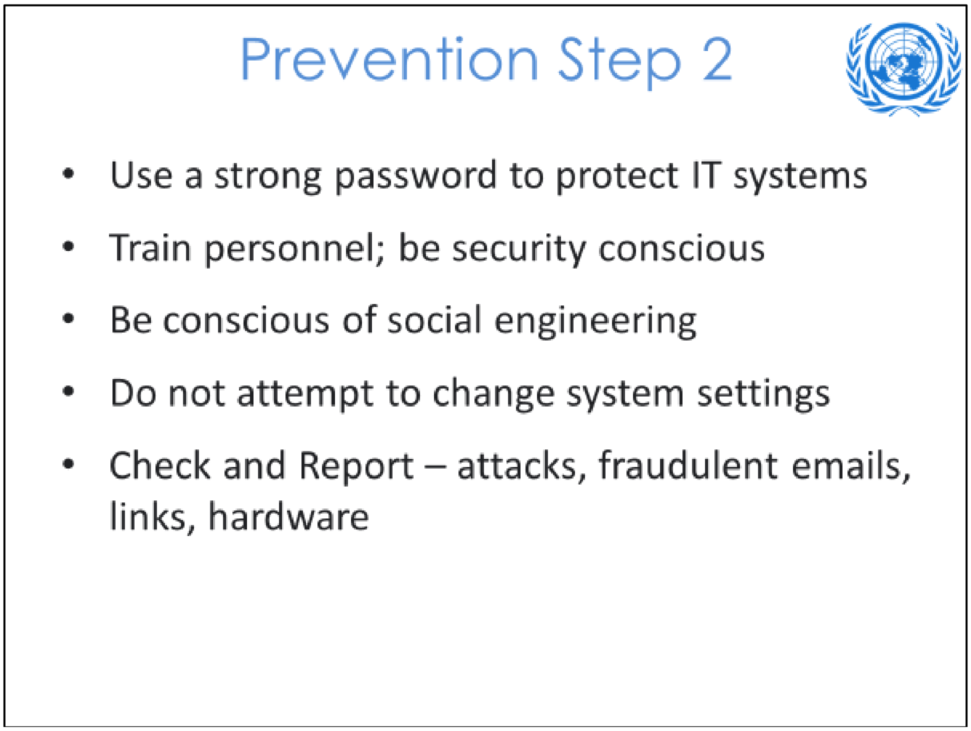
Storage and Control of Sensitive Digital Documents/Information: Proper storage and control mechanisms should be in place for sensitive digital documents and information. This ensures that access to such information is limited to authorised personnel and minimises the risk of unauthorised exposure.

Security Measures and Standard Operating Procedures (SOPs): Organisations / Units should establish and enforce security measures and SOPs for the use and access of IT equipment.

Controlled Access to Sensitive IT Equipment and Networks: To mitigate risks, controlled access should be enforced for sensitive IT equipment and networks. This involves implementing authentication mechanisms, access controls, and monitoring systems to ensure that only trained authorised individuals can access these resources.

By emphasising these preventive measures, organisations/ tactical units can significantly reduce the likelihood of successful cyber-attacks. It is crucial to proactively protect critical assets, control access to sensitive information, and establish secure practices for the use and management of IT equipment and networks.

Slide 5



Prevention Step 2

- Use a strong password to protect IT systems
- Train personnel; be security conscious
- Be conscious of social engineering
- Do not attempt to change system settings
- Check and Report – attacks, fraudulent emails, links, hardware

To further expand on the preventive measures for cyber-attack mitigation, consider the following points:

Use Strong Passwords: Enforce the use of strong, unique passwords for IT systems and accounts. Passwords should be complex, incorporating a combination of letters, numbers, and special characters. Regularly updating passwords and avoiding password reuse across multiple accounts is also essential.

Personnel Training and Security Consciousness: Conduct regular training sessions to educate unit personnel/users about cybersecurity best practices. This includes raising awareness about common attack vectors, such as phishing and social engineering, and teaching them to be vigilant in identifying and reporting suspicious activities or potential security breaches.

Beware of Social Engineering: Stress the importance of being cautious about social engineering tactics.

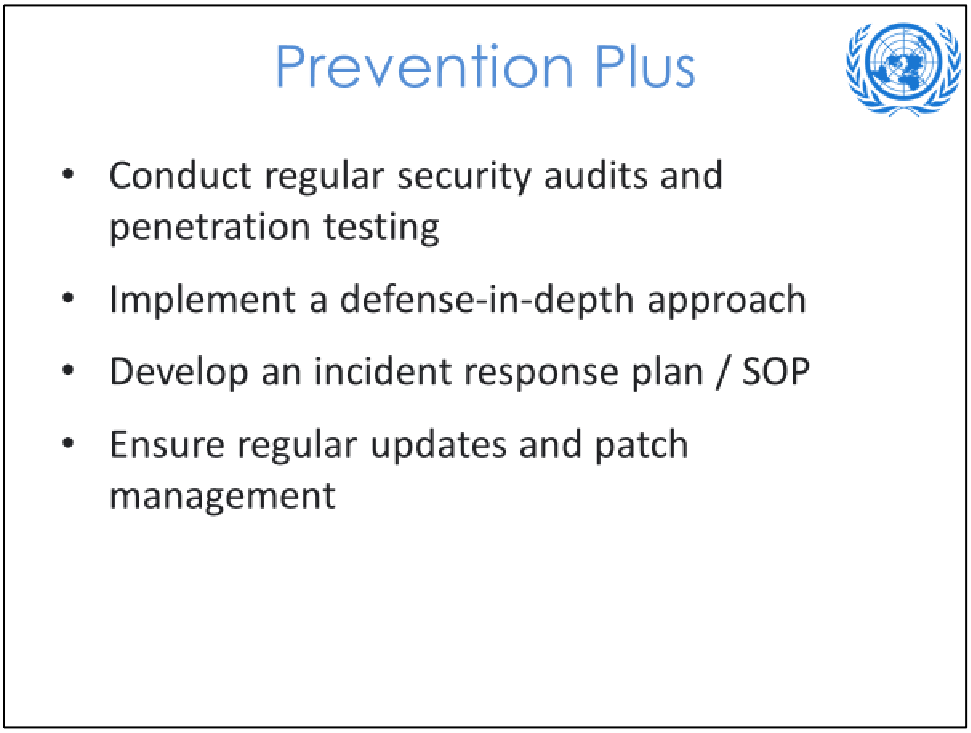
Avoid Changing System Settings: Emphasise that personnel should not attempt to change system settings or modify configurations without proper authorisation. Unauthorised changes can introduce vulnerabilities and compromise the security of IT systems.

Check and Report Suspicious Activities: Encourage personnel to regularly check for signs of cyber-attacks, including monitoring for unusual system behaviour, unexpected pop-ups, or suspicious emails. Any suspicious activity or potential security incidents should be reported promptly to the designated person/cell for investigation and appropriate action.

Attacks, Fraudulent Emails, Links, and Hardware: Instruct personnel to remain vigilant regarding potential cyber threats. They should be cautious when interacting with emails, links, or attachments from unknown or untrusted sources. Additionally, personnel should report any suspected attacks, fraudulent emails, or suspicious hardware, such as USB drives found in the workplace, to the IT security team for further analysis.

By promoting these preventive measures and fostering a security-conscious culture, units/organisations can significantly reduce the risk of successful cyber-attacks. It is crucial to prioritise training, awareness, and reporting mechanisms to empower personnel in actively protecting IT systems and networks from potential threats.

Slide 6



Prevention Plus

- Conduct regular security audits and penetration testing
- Implement a defense-in-depth approach
- Develop an incident response plan / SOP
- Ensure regular updates and patch management

These preventive (plus) measures against cyber-attacks may involve outside or additional technical expertise, specialised equipment, and software implementation. While these measures may require IT professionals, it is essential to be familiar with them and consider their implementation in your unit's cyber-attack prevention programmes. The following strategies should be explored and considered:

Conduct Regular Security Audits and Penetration Testing: To identify vulnerabilities and weaknesses in the system, periodic security audits and penetration testing should be performed. These assessments simulate cyber-attacks to pinpoint potential entry points and vulnerabilities within the network infrastructure. By addressing the identified weaknesses, the overall security posture is strengthened.

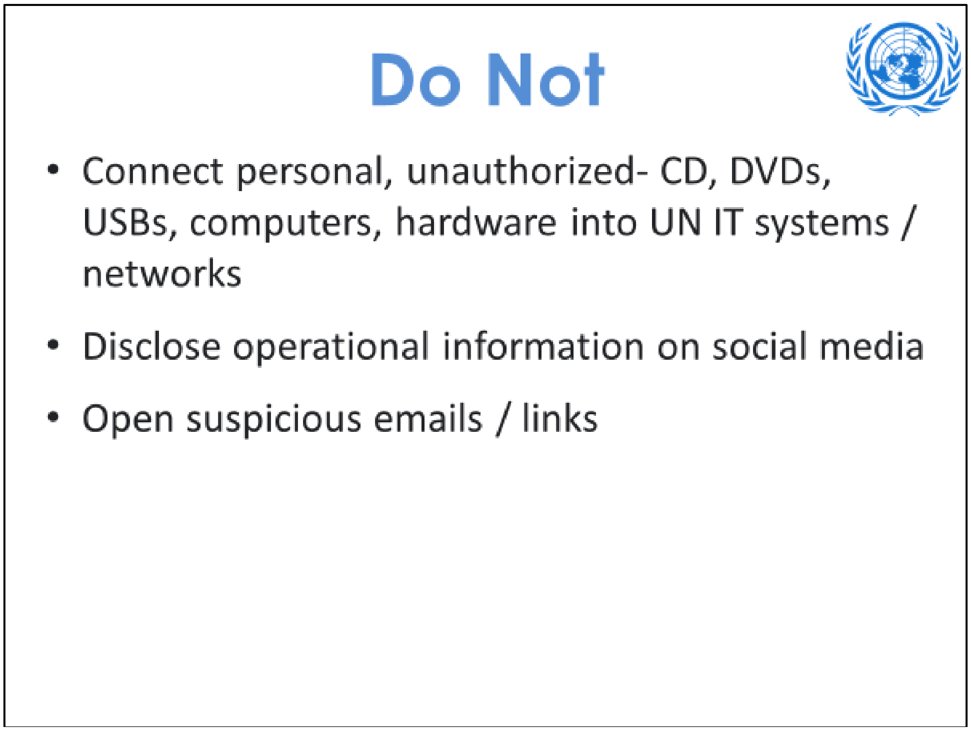
Implement a Defence-in-Depth Approach: A defence-in-depth strategy should be adopted, which involves implementing multiple layers of security controls. These include firewalls, intrusion detection systems, access controls, encryption, and user awareness training. Each layer adds an additional barrier against cyber threats, providing a more robust defence against potential attacks.

Develop an Incident Response Plan and SOP: An incident response plan should be developed and implemented to effectively respond to and mitigate cyber incidents. This plan outlines the necessary steps to be taken in the event of a cyber-attack, including incident identification, containment, eradication, recovery, and lessons learned. Regular testing and updates of the plan are crucial to ensure its effectiveness in handling security incidents.

Ensure Regular Updates and Patch Management: It is essential to keep all systems and software up to date by applying the latest security patches and updates. Regularly applying these updates helps address known vulnerabilities and enhances the overall security of the systems. Effective patch management reduces the risk of exploitation by cyber attackers.

By incorporating these technical measures and best practices into your unit's cyber-attack prevention programmes, you can enhance the resilience of your systems and minimise the potential impact of cyber threats. While some measures may require specialised expertise, it is crucial to prioritise their implementation to safeguard your unit's critical IT assets and information.

Slide 7



Do Not

- Connect personal, unauthorized- CD, DVDs, USBs, computers, hardware into UN IT systems / networks
- Disclose operational information on social media
- Open suspicious emails / links

“Do not do this” points for cyber-attack prevention and risk mitigation:

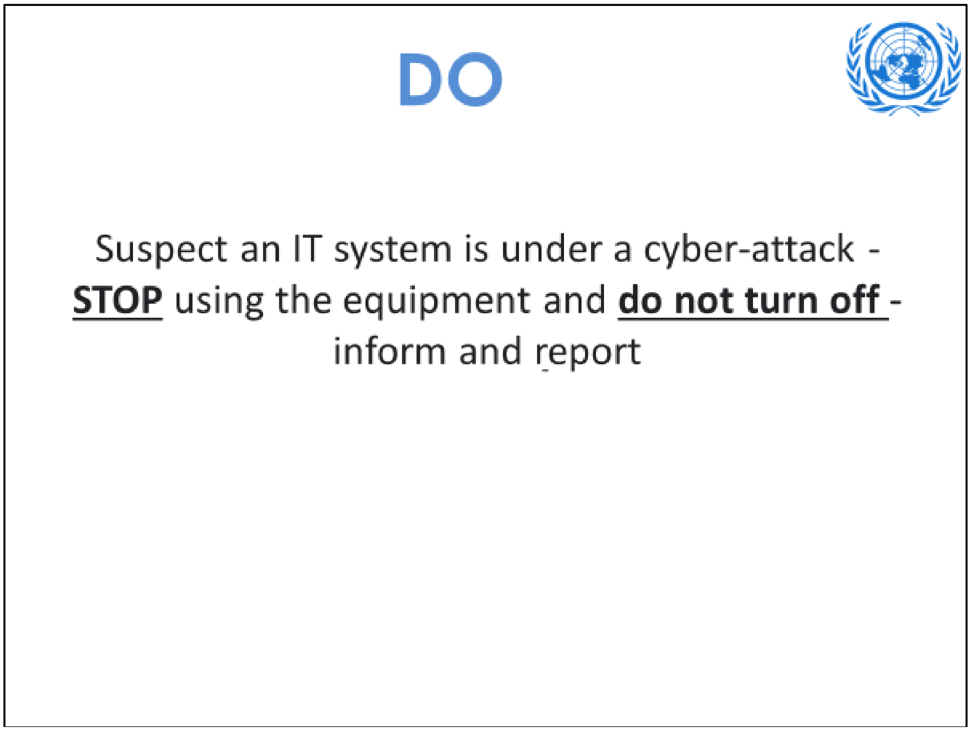
Do not connect Untrusted/Unauthorised or Personal USB Devices or CD/DVDs: Instruct personnel to strictly refrain from connecting untrusted or unauthorised USB devices, CD/DVDs, or personal devices to the organisation’s IT systems. Explain that these external devices can introduce malware or compromise network security. It is crucial to use only approved and trusted devices to minimise potential vulnerabilities. In case of suspected infection, it is recommended to locate and isolate all disks and other input/output media that may have been used on an infected workstation. Do not switch off or reboot the system.

Do Not Disclose Operational Information to Unknown or Suspicious Parties: Stress the importance of not disclosing sensitive operational information to unknown or suspicious individuals or entities. This includes being cautious about sharing operational details, strategies, or internal processes that could be exploited by malicious actors. Encourage personnel to exercise discretion and verify the legitimacy of requests before sharing any sensitive information.

Suspicious Email (?) If in Doubt, Do Not Open It: Emphasise the criticality of exercising caution when dealing with suspicious emails. Train personnel to adopt a sceptical approach towards unexpected or unsolicited emails, particularly those containing suspicious attachments or links. Encourage them to prioritise caution and refrain from opening such emails to minimise the risk of malware infection or falling victim to phishing attempts.

By reinforcing these practices, organisations can enhance their cybersecurity posture and reduce the likelihood of malware infections, data breaches, or unauthorised access resulting from untrusted devices or suspicious email interactions.

Slide 8



DO

Suspect an IT system is under a cyber-attack - **STOP** using the equipment and **do not turn off** - inform and report

If a user suspects that their IT system has been subjected to a cyber-attack, it is crucial that they follow these steps:

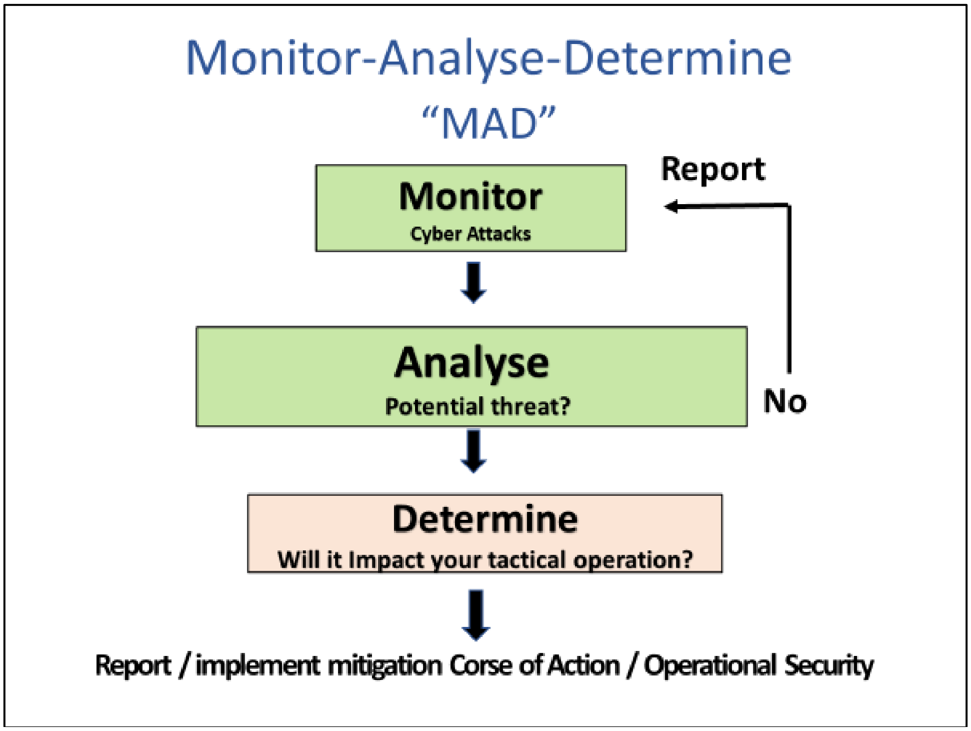
STOP Using the IT Equipment Immediately: The user must cease all activity on the potentially compromised IT equipment without delay. This helps prevent further damage or spread of the attack within the system.

Do NOT Switch Off the Equipment: Advise the user to refrain from shutting down or restarting the equipment on their own. Inform them that it is important to leave the equipment powered on until they receive further instructions from the appropriate expert. Switching off the equipment prematurely may hinder the investigation process or compromise potential evidence.

Inform and Report: Direct the user to promptly report the suspected cyber-attack to their designated reporting point. This might be a cybersecurity incident response team at higher headquarters or a dedicated IT person in the unit. Providing this information ensures that the incident is logged, investigated, and addressed in a timely manner by the responsible personnel.

By following these steps, users can help mitigate the impact of a suspected cyber-attack and enable the organisation’s response individual or team to take appropriate actions to contain and investigate the incident effectively.

Slide 9



Monitor-Analyse-Determine

"MAD"

Monitor

Cyber Attacks

Analyse

Potential threat?

Determine

Will it Impact your tactical operation?

Report

No

Report / implement mitigation Corse of Action / Operational Security

In the event that prevention fails, it becomes imperative to seek a methodology or process for analysing a cyber-attack and assessing the level of harm or damage caused. Once it has been established that a cyber-attack poses a direct threat to the operations of a tactical unit, the need for force protection planning becomes crucial. It is essential to devise action plans aimed at mitigating the risks and consequences faced by tactical units and their operations. By thoroughly evaluating the risks and challenges posed by the cyber-attack, we can implement strategies that bolster the effectiveness and resilience of units engaged in peacekeeping missions.

The UN needs to prioritise cybersecurity and implement force protection plans to ensure the effectiveness and success of its peacekeeping missions in an increasingly interconnected digital landscape. By employing a comprehensive approach known as the Monitor, Analyse, and Determine (MAD) assessment methodology, the UN can effectively identify and respond to cyber threats.

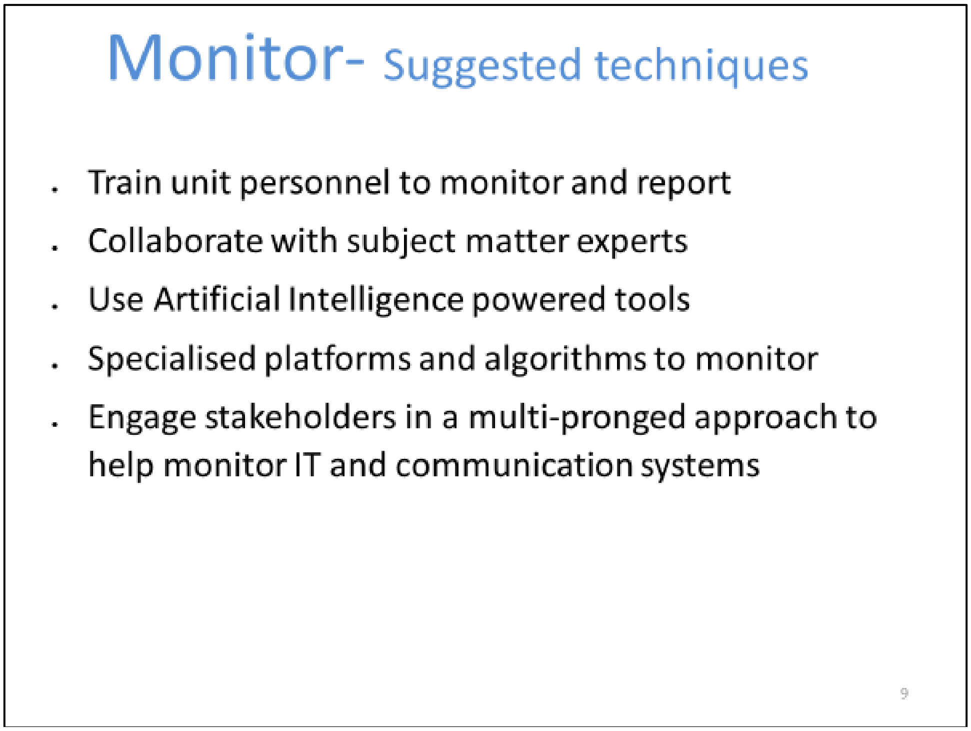
The MAD assessment methodology involves three key phases: monitoring, analysis, and determination. During the monitoring phase, the UN engages stakeholders, including cybersecurity experts and AI/software algorithms, to monitor IT networks, computer systems, communications systems, and equipment of the UN, Troop-Contributing Countries (TCCs), and Police-Contributing Countries (PCCs) involved in peacekeeping operations. This aims to detect cyber threats and understand the methods used by different threat actors.

The analysis phase involves determining the attack’s intent, identifying vulnerabilities within the IT network, and evaluating the impact on the organisation/unit’s systems. Understanding the motives and targets helps inform response and mitigation measures while assessing the scope and severity allows for appropriate responses to minimise damage.

During the Determination Phase, the paramount objective is to meticulously evaluate the immediate and collateral repercussions of the cyber-attack on the operational environment, particularly concerning the tasks, missions, and operations of the tactical unit. This entails a thorough assessment of the extent to which the attack curtails the freedom of action and undermines coordination, communication, and operational security. Grasping the full magnitude of the impact is imperative for pinpointing vulnerabilities and foreseeing potential secondary or collateral ramifications of the attack.

To proactively combat cyber-attacks and ensure successful peacekeeping tactical unit operations in the digital age, we should adopt the MAD assessment methodology. This comprehensive approach entails continuous monitoring, in-depth analysis, and a meticulous evaluation of the direct and indirect impact on unit operations. By implementing FP planning, we can effectively mitigate the risks posed by cyber-attacks, reducing the consequential threat impact and or likelihood. These proactive mitigation measures, represented by FP courses of action, enable the unit to maintain highly effective tactical operations within the evolving technological landscape of peacekeeping.

Slide 10



Monitor- Suggested techniques

- Train unit personnel to monitor and report
- Collaborate with subject matter experts
- Use Artificial Intelligence powered tools
- Specialised platforms and algorithms to monitor
- Engage stakeholders in a multi-pronged approach to help monitor IT and communication systems

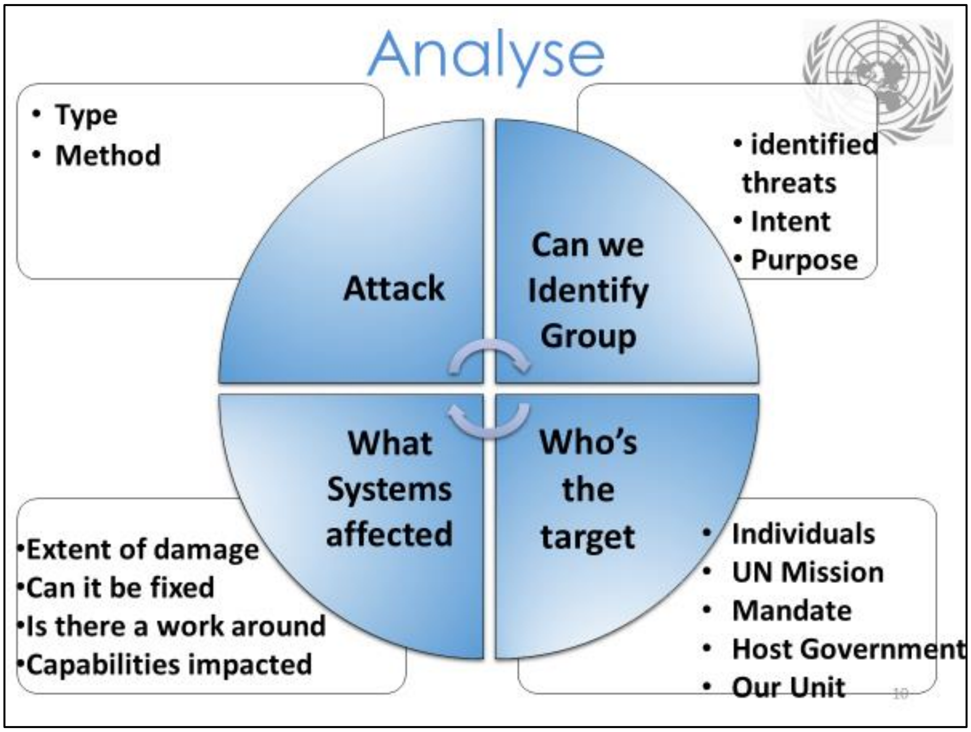
9

Implement robust network monitoring systems that continuously monitor network traffic and detect any unusual or suspicious activities.

- By training users and operators to be vigilant monitors and reporting issues, units can leverage their collective knowledge and awareness to strengthen situational awareness. Users and operators should be trained to identify suspicious activities or indicators of a potential cyber-attack. This proactive approach can significantly reduce the impact of cyber threats and enable faster response and analysis.
- Collaborate with communication and IT network SMEs: Monitoring cyber / IT systems is technical in nature, and most UN military and police tactical units may require additional support or subject matter expertise (SME) at Higher HQs / Mission level to assist and monitor.
- Acquisition collection plan: Include cyber threats in your acquisition collection plan. Mission peacekeeping-intelligence cells can also help identify methods, groups or saboteurs who attack the UN.
- Automated tools: If available, utilise AI-powered tools and software/algorithms that can monitor/analyse large volumes of data and systems. Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools can provide real-time alerts and analysis of potential cyber threats, enabling timely response and mitigation.

- Engagement: Combating cyber-attack efforts that require a multi-pronged approach involving various stakeholders, including civil communities, organisations, Civil Affairs, and Public Relations cells, can be helpful. Establish SOPs to do systematic engagement.

Slide 11



Analyse

- Type
- Method

- identified threats
- Intent
- Purpose

- Extent of damage
- Can it be fixed
- Is there a work around
- Capabilities impacted

- Individuals
- UN Mission
- Mandate
- Host Government
- Our Unit

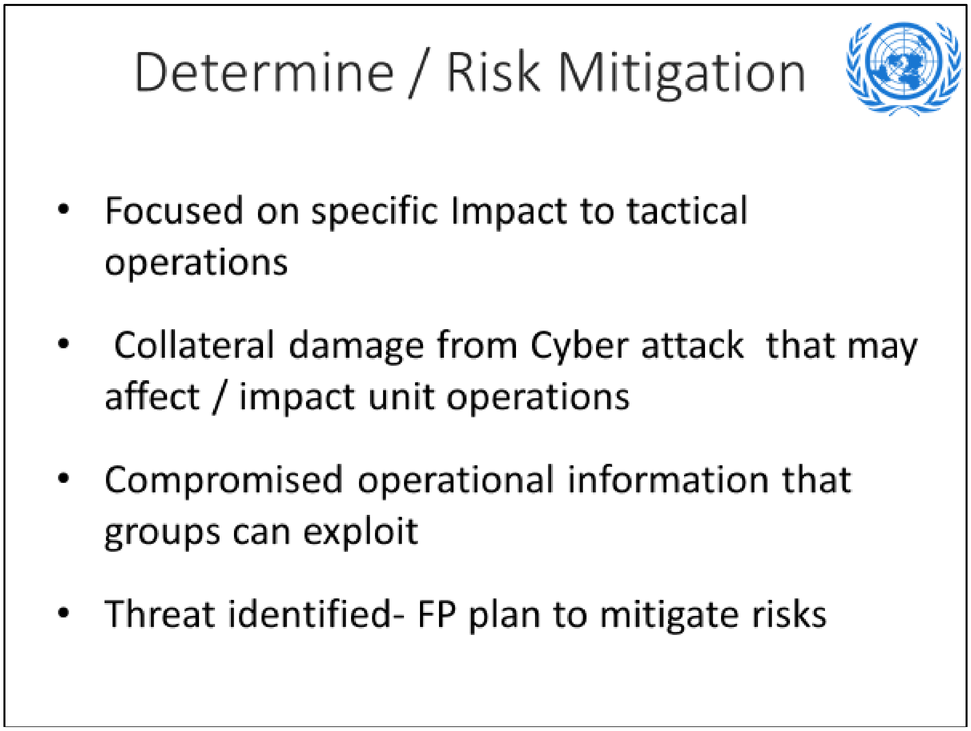
The analysis phase of the MAD assessment methodology is focused on gaining deeper insights into the cyber-attack and its implications. It involves determining the intent behind the attack, identifying our vulnerabilities or IT network casualties, and evaluating the overall impact on the organisation.

Understanding the reason for the attack is vital for gauging the motives of threat actors. Whether the attack is aimed at retaliation, embarrassing the UN, disrupting ongoing operations, or interfering with specific tasks, this knowledge helps inform the response and mitigation measures.

Additionally, determining the specific target of the attack is crucial. It allows us to assess whether the attack is directed at the organisation as a whole or specific tactical units engaged in peacekeeping operations. Factors such as geographical location, involvement in sensitive operations, and the potential disruption they may cause to the interests of threat actors play a role in identifying the target.

The analysis of the impact of cyber-attacks on the IT infrastructure, communications systems, and computer equipment can be profound. Compromised systems can lead to the loss of sensitive information, disruption of command-and-control structures, reduced operational effectiveness, and even render critical equipment unusable. Assessing the scope and severity of the impact is vital for devising appropriate response measures and minimising the damage caused by the attack.

Slide 12



Determine / Risk Mitigation

- Focused on specific Impact to tactical operations
- Collateral damage from Cyber attack that may affect / impact unit operations
- Compromised operational information that groups can exploit
- Threat identified- FP plan to mitigate risks

In the determine phase, the focus shifts to assessing the ramifications of the cyber-attack, specifically on the tactical units' task, mission, or operation. This phase involves a very FP-focused assessment of the extent to which the attack impacts the unit's freedom of action.

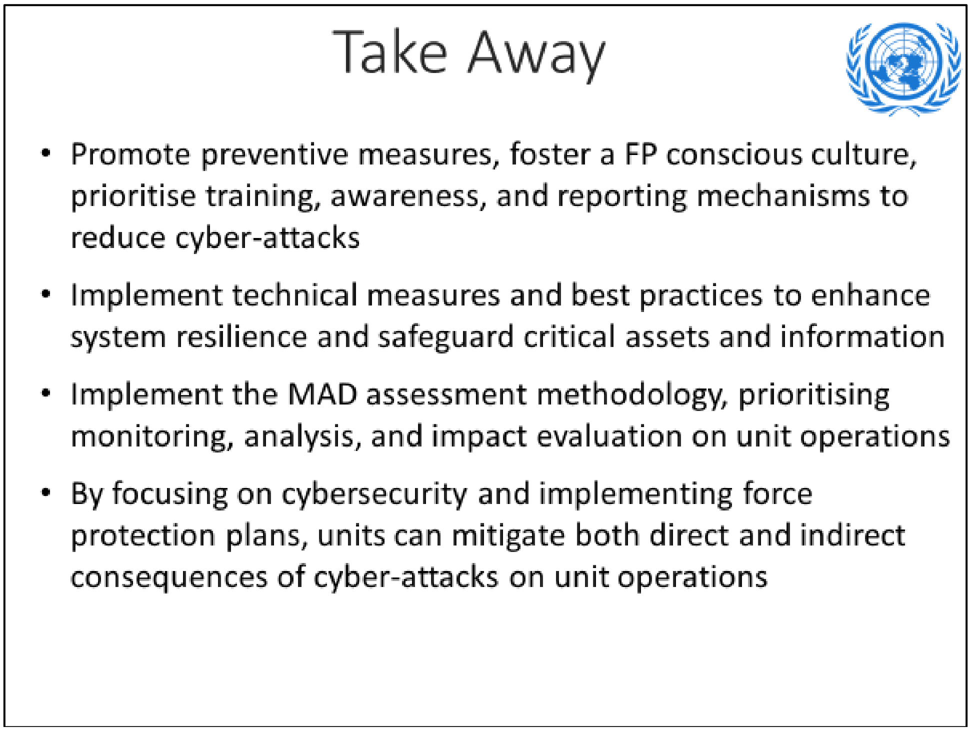
A cyber-attack may impede coordination and communication between sub-elements and hamper situational awareness that can significantly hamper operational effectiveness. Furthermore, compromised IT systems used in planning can undermine peacekeeping-intelligence collection and logistical and tactical information. A cyber-attack can directly or indirectly (collateral damage) affect the success of planned operations and may necessitate adjustments to an original plan to mitigate the impact or likelihood of a direct or secondary consequential threat.

Compromised operational security is another critical consideration during the determine phase. Cyber-attacks that breach sensitive information or provide threat actors with prior knowledge of tactical actions can seriously compromise the operational security of peacekeeping operations. Understanding the extent to which operational security has been compromised allows for appropriate responses to address the vulnerabilities and prevent further exploitation.

Additionally, it's important to recognise that cyber-attacks at the UN mission level can have secondary/auxiliary effects on tactical units initiated by threat actors. These effects may include manipulating local populations, disrupting command and control structures, and creating chaos in the operational area. Understanding these potential secondary effects helps to anticipate and respond to broader challenges that may arise from an initial cyber-attack.

In conclusion, cyber-attacks targeting the United Nations (UN) or specific tactical units involved in peacekeeping operations pose risks that must be addressed. To effectively mitigate these risks, the implementation of the MAD assessment

Slide 13



Take Away

- Promote preventive measures, foster a FP conscious culture, prioritise training, awareness, and reporting mechanisms to reduce cyber-attacks
- Implement technical measures and best practices to enhance system resilience and safeguard critical assets and information
- Implement the MAD assessment methodology, prioritising monitoring, analysis, and impact evaluation on unit operations
- By focusing on cybersecurity and implementing force protection plans, units can mitigate both direct and indirect consequences of cyber-attacks on unit operations

Summary:

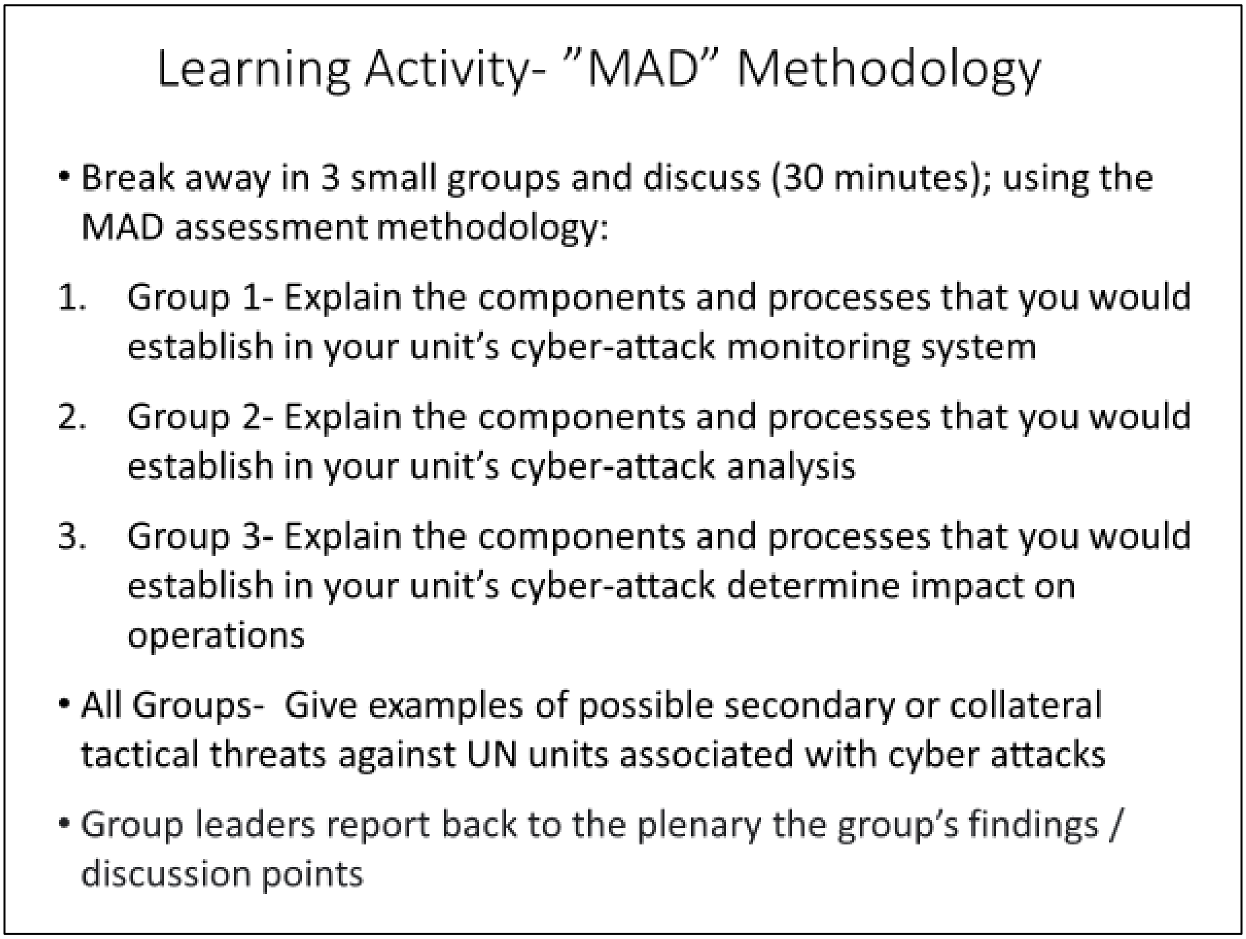
By promoting these preventive measures and fostering a security-conscious culture, units/organisations can significantly reduce the risk of successful cyber-attacks. It is crucial to prioritise training, awareness, and reporting mechanisms to empower personnel in actively protecting IT systems and networks from potential threats.

By incorporating these technical measures and best practices into your unit's cyber-attack prevention programmes, you can enhance the resilience of your systems and minimise the potential impact of cyber threats. While some measures may require specialised expertise, it is crucial to prioritise their implementation to safeguard your unit's critical IT assets and information.

To effectively address cyber-attacks, the UN must implement the MAD assessment methodology, which includes monitoring, thorough analysis, and determination of the impact on unit operations. By prioritising cybersecurity and implementing force protection plans, the UN unit can mitigate the direct and indirect consequences of cyber-attacks, ensuring successful peacekeeping operations in the digital age.

By implementing FP planning, we can effectively mitigate the risks posed by cyber-attacks, reducing the consequential threat impact and or likelihood. These proactive mitigation measures, represented by FP courses of action, enable the unit to maintain highly effective tactical operations within the evolving technological landscape of peacekeeping.

Learning Activity 3.4



Learning Activity- ”MAD” Methodology

- Break away in 3 small groups and discuss (30 minutes); using the MAD assessment methodology:

1. Group 1- Explain the components and processes that you would establish in your unit’s cyber-attack monitoring system
2. Group 2- Explain the components and processes that you would establish in your unit’s cyber-attack analysis
3. Group 3- Explain the components and processes that you would establish in your unit’s cyber-attack determine impact on operations

- All Groups- Give examples of possible secondary or collateral tactical threats against UN units associated with cyber attacks
- Group leaders report back to the plenary the group’s findings / discussion points

Lesson 3.5

The Lesson

Starting the Lesson

To create an engaging start for this lesson, encourage participants to share their experiences and insights on countering Mis/Disinformation strategies during United Nations Peacekeeping Operations (PKOs). Encourage them to discuss the specific challenges the UN encountered and the effective measures they implemented to address these challenges. This interactive discussion will provide valuable real-world perspectives and promote collaborative learning.

☞***Note to instructor*** *– It is recommended that the instructor for this lesson possesses a background in IT and/or communications networks. Additionally, the instructor should review the lessons covered in Module 1 on Cyber and Mis/Disinformation to ensure a comprehensive understanding of the topic."*

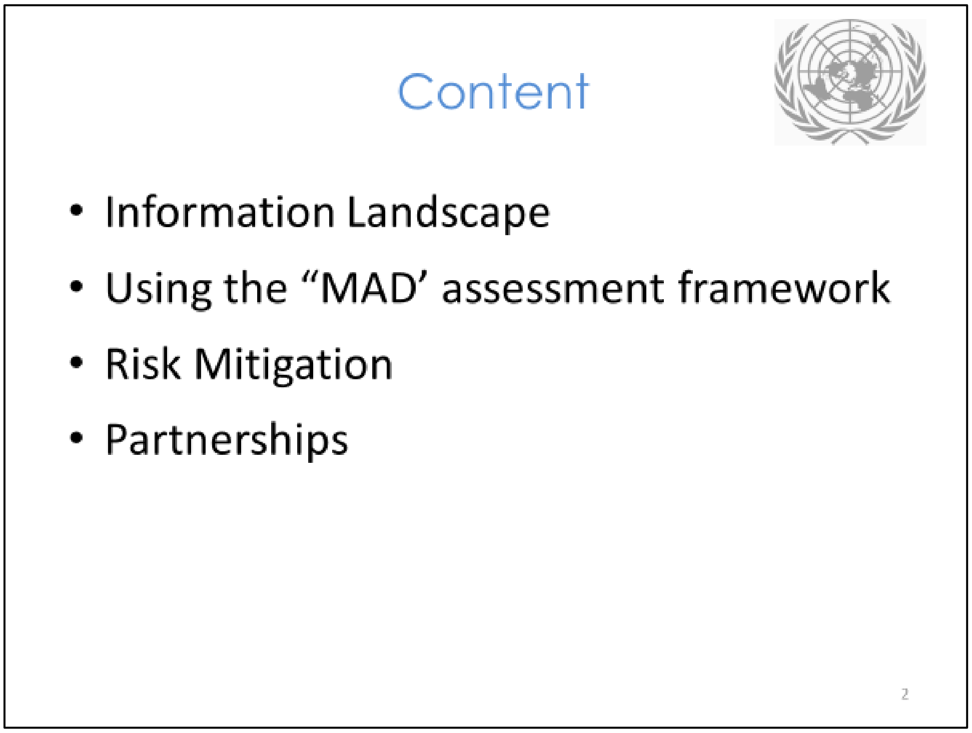
Slide 1

Mitigating
Misinformation / Disinformation
Impacting UN Unit Operations
Lesson 3.5

1

The spread of misinformation and disinformation by various groups or media outlets is a long-standing issue that has consistently been associated with political manipulation and harmful persuasion. However, what sets the current situation apart is the unprecedented virality and widespread sharing of information on social media platforms, fuelled by the rapid development of social networks and diverse communication mediums. The objective of this lesson is to offer a basic understanding of Mis/Disinformation in a PKO, as well as equip you with techniques for monitoring, analysing, and mitigating its impact on UN unit operations.

Slide 2



Content

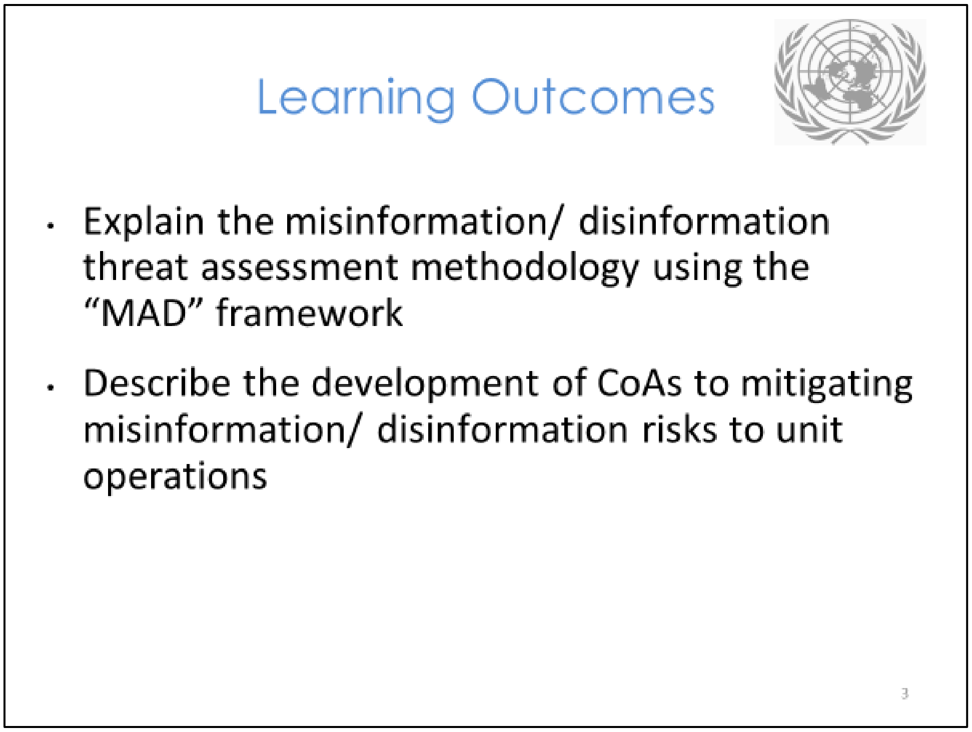
- Information Landscape
- Using the "MAD' assessment framework
- Risk Mitigation
- Partnerships

2

This lesson covers the following topics:

- Information Landscape: Understanding the current state of information dissemination, including the prevalence of misinformation and disinformation in a UN PKO.
- The "MAD" Framework: Learning how to effectively Monitor, Analyse, and Determine the veracity and impact of mis/disinformation circulating in order to make informed decisions on FP planning and risk mitigation.
- Risk Mitigation: Exploring strategies and techniques to mitigate the risks posed by misinformation and disinformation.
- Partnerships: Recognising the importance of collaborative efforts and forging partnerships with relevant stakeholders, such as fact-checking organisations, media outlets, and social media platforms, to combat the spread of misinformation and disinformation effectively.

Slide 3



Learning Outcomes

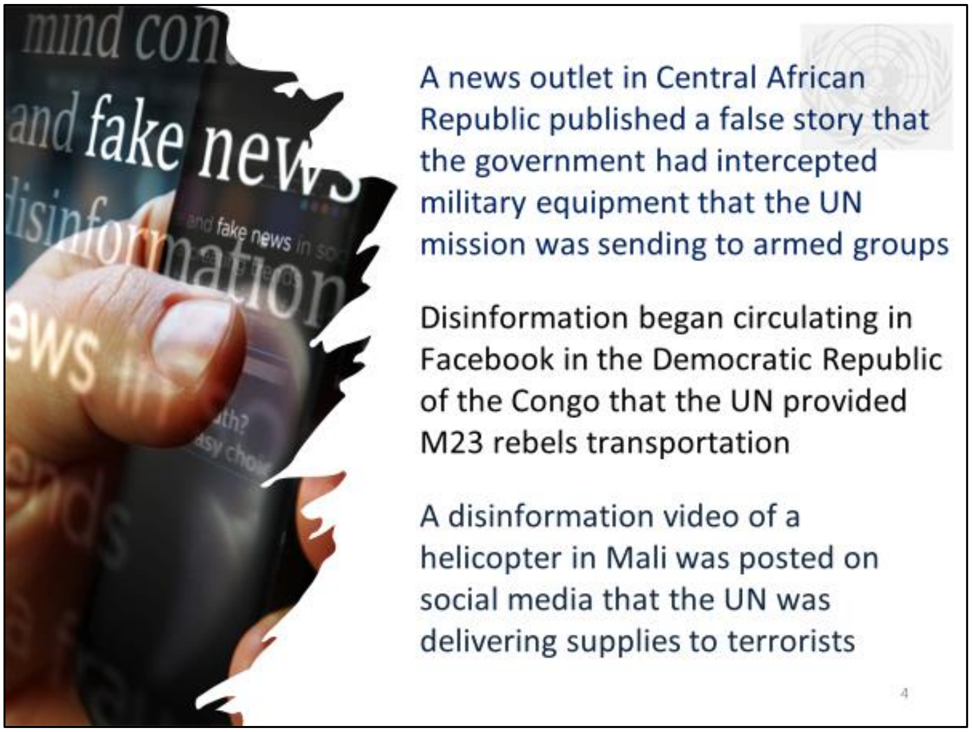
- Explain the misinformation/ disinformation threat assessment methodology using the “MAD” framework
- Describe the development of CoAs to mitigating misinformation/ disinformation risks to unit operations

3

The learning objectives for this lesson are as follows. By the end of the lesson, you should be able to:

- Explain the process of identifying and understanding the threat of misinformation and disinformation, utilising the Monitor, Analysis, and Determine (MAD) framework.
- Describe the steps involved in developing FP planning Courses of Action (CoAs) to effectively mitigate the risks posed by misinformation and disinformation to unit operations. Explain how to develop and implement proactive strategies and actions to minimise the risks of misinformation and disinformation in unit operations.

Slide 4


mind con
and fake news
disinformation
and fake news in so
news

A news outlet in Central African Republic published a false story that the government had intercepted military equipment that the UN mission was sending to armed groups

Disinformation began circulating in Facebook in the Democratic Republic of the Congo that the UN provided M23 rebels transportation

A disinformation video of a helicopter in Mali was posted on social media that the UN was delivering supplies to terrorists

4

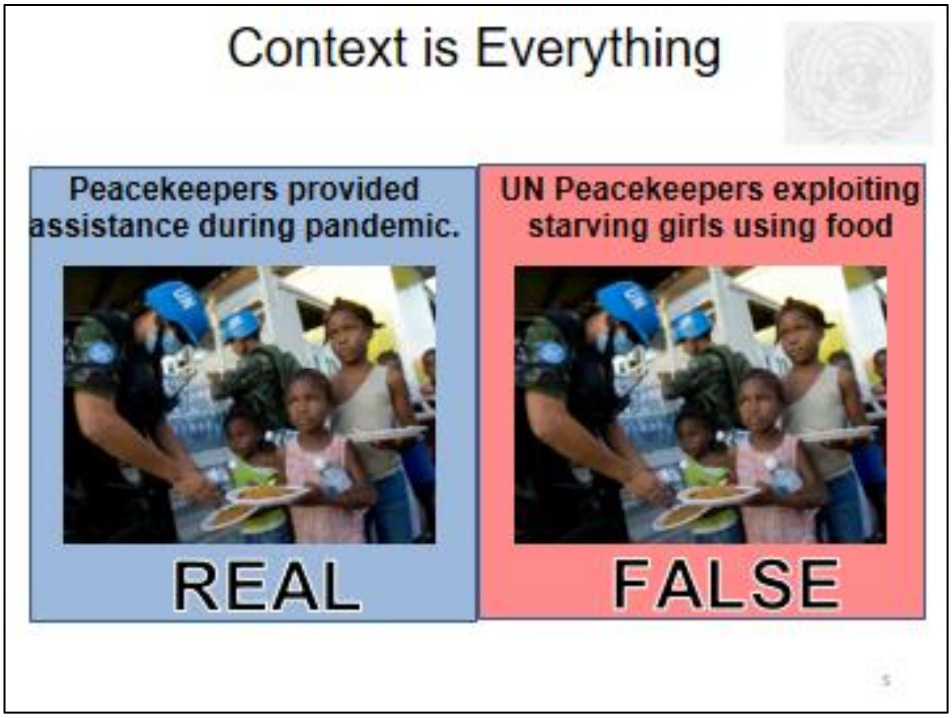
Below are real-world examples of disinformation attacks targeted at the United Nations, which had profound impacts on peacekeeping operations and public opinion. These attacks directly influenced the UN mandate and the ability of UN units to carry out their operations effectively in the field. One of the key objectives of UN missions is to protect civilians, but this becomes increasingly challenging when disinformation spreads and taints civilian opinions. Consequently, there is a risk of creating a crisis of legitimacy for the UN, as local populations may become unwilling to accept the presence of the UN in their area.

- A news outlet in the Central African Republic published a false story that the government had intercepted military equipment that the UN mission was sending to armed groups.

- Disinformation began circulating on Facebook in the Democratic Republic of the Congo that the UN provided M23 rebels with transportation.

- A disinformation video of a helicopter in Mali was posted on social media that the UN was delivering supplies to terrorists.

Slide 5



Context is Everything

Peacekeepers provided assistance during pandemic.

REAL

UN Peacekeepers exploiting starving girls using food

FALSE

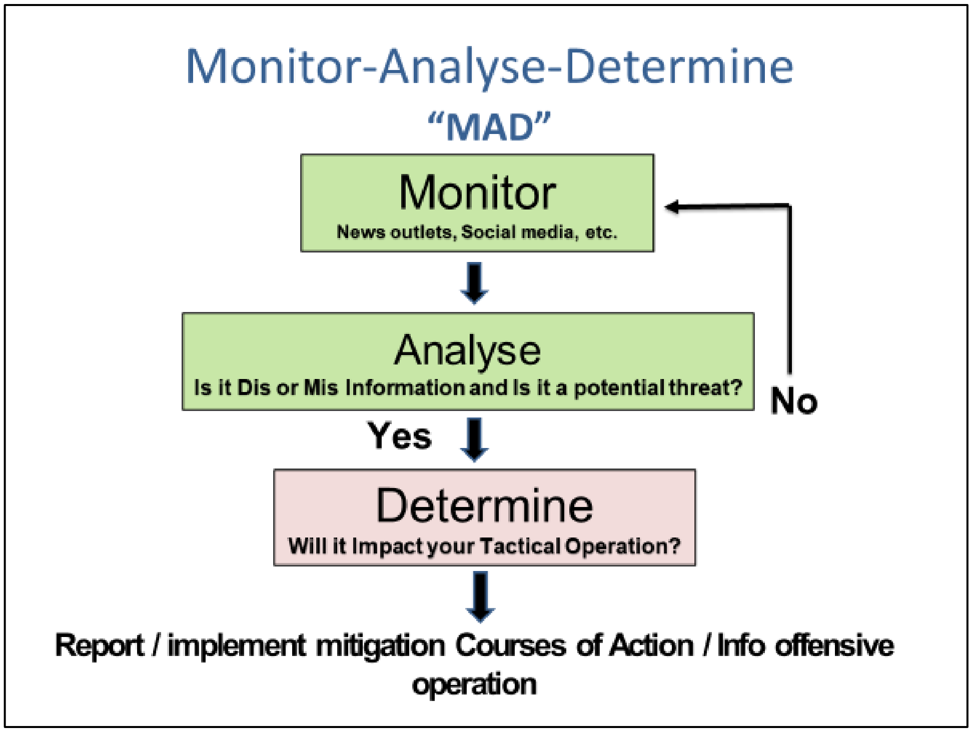
5

Let's consider another example of how news or social media platforms can manipulate the context of a photograph to influence public opinion or elicit a specific reaction. Here are two photographs that can include captions to drive different narratives and meanings. Such actions can have both direct and indirect consequences, including collateral effects on the United Nations (UN) and its ability to effectively carry out unit operations.

By strategically framing or presenting a photograph in a particular context, the media or social media platforms can shape the narrative surrounding a situation. This can result in a skewed perception among the public, potentially leading to misinformation or misinterpretation of events. Consequently, the UN may face challenges in its operations as public sentiment is influenced by these distorted portrayals.

It is crucial to recognise the impact that contextual manipulation of visual content can have on public opinion and subsequent support for UN missions. Addressing these challenges becomes imperative for the UN to maintain its effectiveness and credibility in carrying out unit operations.

Slide 6



Monitor-Analyse-Determine

"MAD"

Monitor

News outlets, Social media, etc.

Analyse

Is it Dis or Mis Information and Is it a potential threat?

No

Yes

Determine

Will it Impact your Tactical Operation?

Report / implement mitigation Courses of Action / Info offensive operation

It becomes imperative to seek a methodology or process for analysing mis/disinformation and assessing the level of potential harm or damage caused. Once it has been established that a mis/disinformation attack poses a direct or indirect threat to the operations of a tactical unit, the need for force protection planning becomes crucial. It is essential to devise action plans aimed at mitigating the risks and consequences faced by tactical units and their operations. By thoroughly evaluating the risks and challenges posed by the mis/disinformation, we can implement strategies that bolster the effectiveness and resilience of units engaged in peacekeeping missions.

The UN needs to prioritise mis/disinformation security and implement force protection plans to ensure the effectiveness and success of its peacekeeping missions in an increasingly interconnected digital landscape. By employing a comprehensive approach known as the Monitor, Analyse, and Determine (MAD) assessment methodology or framework, the UN can effectively identify and respond to mis/disinformation threats.

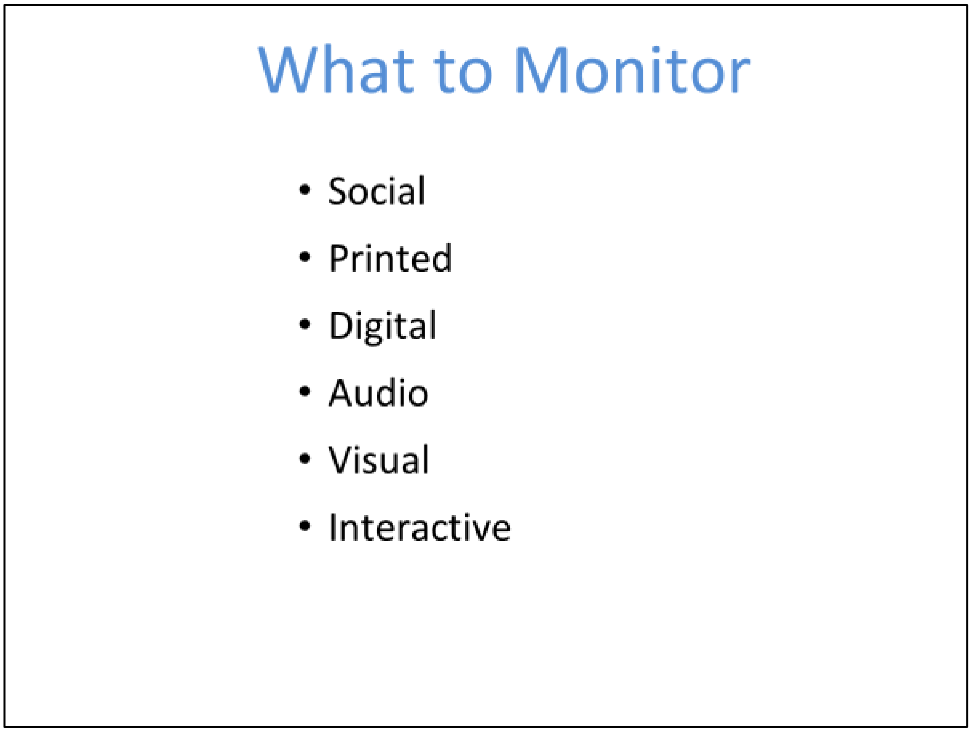
The MAD assessment methodology involves three key phases: monitoring, analysis, and determination. During the monitoring phase, the unit engages user stakeholders, including mis/disinformation experts and AI/software algorithms, to help monitor social networks and the media; this aims to detect mis/disinformation threats and understand the methods used by different threat actors.

The analysis phase involves determining the actor's intent and evaluating the impact on the organisation. Understanding the motives and targets helps inform response and mitigation measures while assessing the scope and severity allows for appropriate responses to minimise impacts.

During the determination phase, the primary focus is to assess the immediate and collateral effects of the mis/disinformation on the operational environment, specifically on the unit tasks, missions, and operations. This involves evaluating the degree to which the attack impedes freedom of action compromises planning and tactical coordination, communication, and operational security. Understanding the full impact is crucial for identifying vulnerabilities and anticipating potential secondary/collateral consequences of the false information being public.

To proactively combat mis/disinformation and ensure successful peacekeeping tactical unit operations in the social media age, we can adopt the MAD assessment methodology. This comprehensive approach entails continuous monitoring, in-depth analysis, and a meticulous evaluation of the direct and indirect impact on unit operations. By implementing FP planning, we can effectively mitigate the risks posed by mis/disinformation -attacks, reducing the consequential threat impact and or likelihood. These proactive mitigation measures, represented by FP courses of action, enable the unit to maintain highly effective tactical operations within the evolving technological landscape of peacekeeping.

Slide 7



What to Monitor

- Social
- Printed
- Digital
- Audio
- Visual
- Interactive

When considering the information landscape, it is important to monitor the various information platforms and mediums to gain a comprehensive understanding of the current state of information dissemination. Here are example areas to monitor:

Social Media: The rise of social media platforms has significantly impacted the spread of information. Monitoring social media platforms such as Facebook, Twitter, Instagram, and others is crucial to keep track of trending topics, viral content, and potential disinformation campaigns.

Printed Media: Traditional printed media, including newspapers, magazines, and newsletters, still play a significant role in shaping public opinion. Monitoring print media allows for the identification of narratives, biases, and potential mis/disinformation within these sources.

Digital Media: This encompasses online news websites, blogs, and other digital publications. Monitoring digital media provides insights into the articles, reports, and opinions that are shaping public discourse.

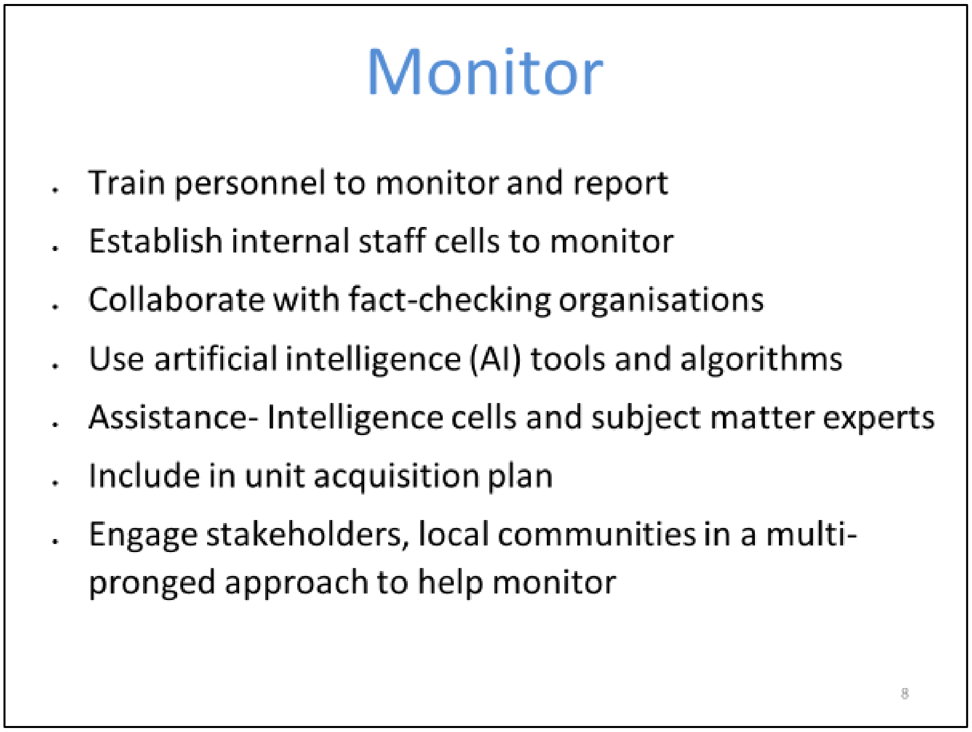
Audio Media: Radio broadcasts, podcasts, and other audio-based platforms can disseminate information to a wide audience. Monitoring audio media ensures that narratives and messages conveyed through these mediums are accurate.

Visual Media: Television broadcasts and video-sharing platforms like YouTube play a vital role in shaping public opinion. Monitoring visual media allows for the identification of visual content, including images and videos, which can be manipulated or contextually distorted.

Interactive Media: With the advent of interactive platforms, such as forums, comment sections, and online communities, monitoring user-generated content and discussions is essential to identify misinformation and disinformation campaigns.

Effectively monitoring information across these diverse areas of the information landscape is crucial for understanding the scope and impact of misinformation and disinformation campaigns.

Slide 8



Monitor

- Train personnel to monitor and report
- Establish internal staff cells to monitor
- Collaborate with fact-checking organisations
- Use artificial intelligence (AI) tools and algorithms
- Assistance- Intelligence cells and subject matter experts
- Include in unit acquisition plan
- Engage stakeholders, local communities in a multi-pronged approach to help monitor

8

To effectively monitor misinformation and disinformation across information mediums and media, several strategies and measures can be implemented:

Train Personnel: Provide comprehensive training to personnel on recognising and monitoring misinformation and disinformation. Educate them on the various techniques used, common sources, and indicators of false information. Train them to report potential threats to the UN and the unit.

Establish Internal Staff Cells: Create dedicated internal staff cells responsible for monitoring and analysing misinformation and disinformation campaigns. These cells can focus on monitoring social media platforms, news outlets, and other relevant sources. They should be equipped with the necessary resources and tools to identify and track potential threats.

Collaborate with Fact-Checking Organisations: Establish partnerships with reputable fact-checking organisations. Collaborate closely with these organisations to verify the accuracy of information and debunk false narratives.

Utilise Artificial Intelligence (AI) Tools and Algorithms: Leverage AI-powered tools and algorithms to monitor and analyse large volumes of data across various media channels. These tools can help identify patterns, detect fake accounts, track the spread of misinformation, and provide real-time alerts.

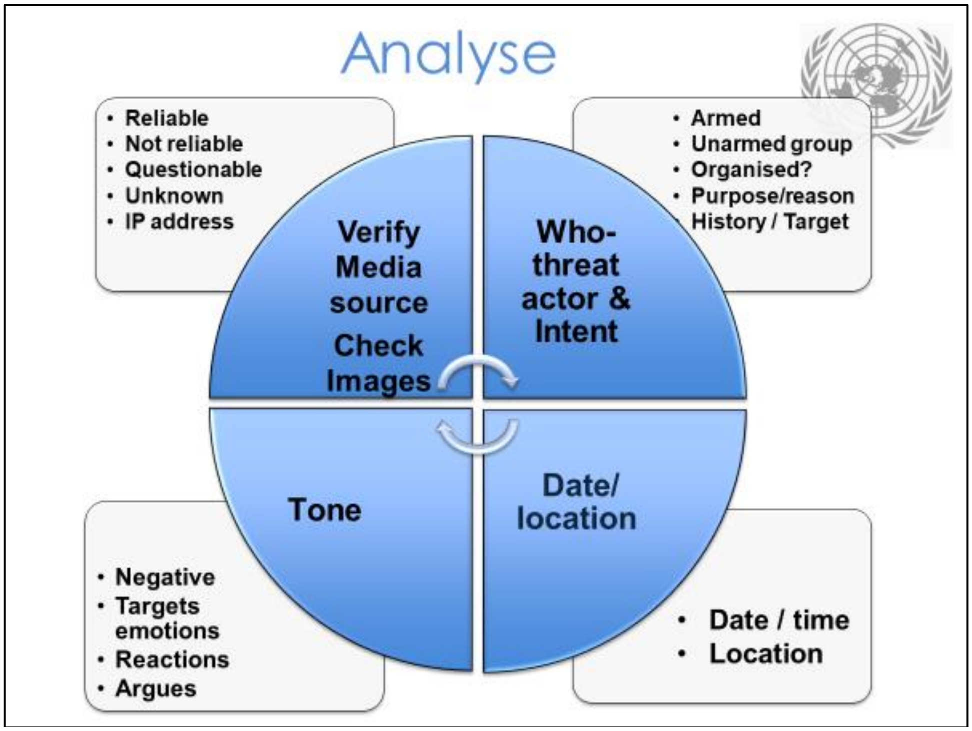
Seek assistance from external peacekeeping-intelligence Cells and Subject Matter Experts: Engage peacekeeping-intelligence cells and subject matter experts within the Mission organisation to provide valuable insights and analysis. Their expertise can help in understanding the broader context of misinformation and disinformation campaigns.

Include in Unit Acquisition Plan: Ensure that the unit acquisition plan includes resources and technologies dedicated to monitoring misinformation and disinformation and the groups that manifest the false information.

Engage Stakeholders and Local Communities: Foster a multi-pronged approach by actively engaging stakeholders, including local communities, in the monitoring process. Encourage them to report suspicious information and collaborate in identifying and countering misinformation and disinformation. Establish open lines of communication and share accurate information to build trust and resilience against false narratives.

By implementing these measures, organisations can enhance their ability to effectively monitor and detect misinformation and disinformation attacks across various mediums and media channels. This multi-faceted approach ensures a comprehensive defence against the harmful effects of false information on public opinion and operational effectiveness.

Slide 9



To effectively analyse misinformation and disinformation attacks, consider the following factors:

Verify Media Sources and Check Images: Assess the reliability and credibility of media sources used to disseminate information. Verify the authenticity of images and other visual content. Determine if the sources and images come from reputable or unknown origins. Verify the legitimacy of IP addresses associated with the sources.

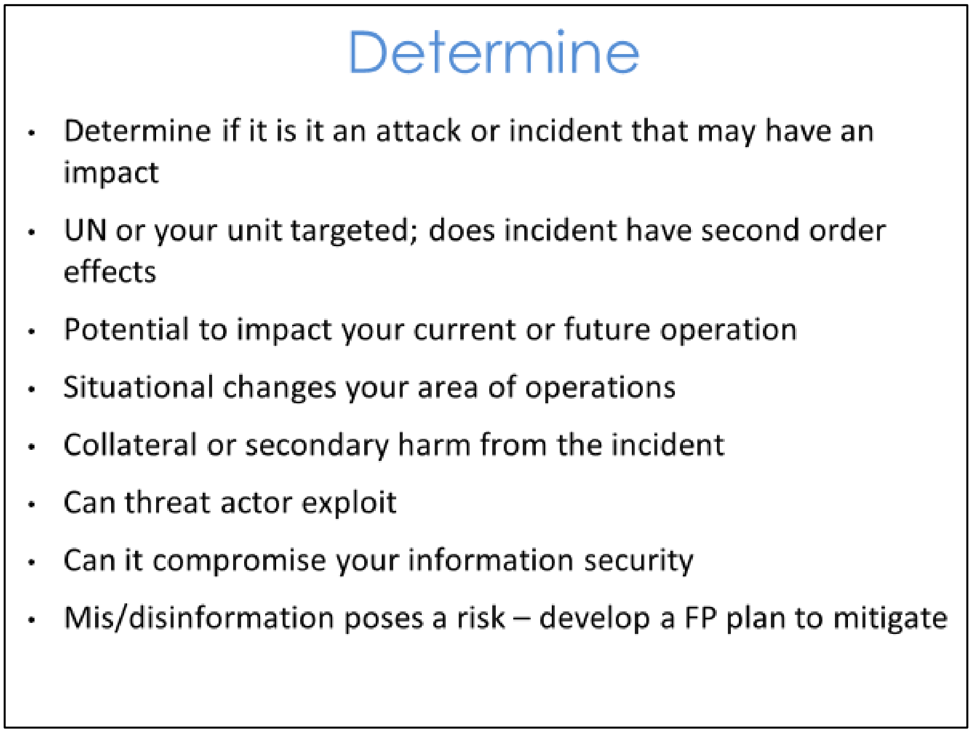
Identify the Initiator and Target: Determine who initiated the misinformation or disinformation campaign and identify the target. Analyse if the attack is specifically directed towards the United Nations (UN), your unit or vulnerable populations. Assess if the actor or group responsible has a history of harmful or violent attacks against the UN, your unit, civilians, the international community, or the government. Access their motives, whether it is to cause harm, retaliate, embarrass the UN, or gain power and influence.

Assess Tone, Emotion, and Balance: Analyse the tone of the misinformation or disinformation. Assess if it employs humour or uses manipulative tactics to incite violent emotions or reactions. Determine if the content presents a fair and balanced argument or if it is one-sided and biased.

Consider Date and Location: Evaluate the significance of the date and location where the misinformation or disinformation is circulating. Determine if it is part of a localised campaign targeting your area of operations or if it has broader implications. Assess the timing and if it is part of a larger, more complex strategy, whether short-term or long-term.

By systematically analysing these factors, you can gain a deeper understanding of the nature and impact of misinformation and disinformation campaigns. This analysis helps in formulating and determining the impacts and the appropriate countermeasures, enhancing awareness, and mitigating the effects of false narratives.

Slide 10



Determine

- Determine if it is it an attack or incident that may have an impact
- UN or your unit targeted; does incident have second order effects
- Potential to impact your current or future operation
- Situational changes your area of operations
- Collateral or secondary harm from the incident
- Can threat actor exploit
- Can it compromise your information security
- Mis/disinformation poses a risk – develop a FP plan to mitigate

The next step in the Monitor, Analyse, and Determine a framework for assessing misinformation and disinformation is to determine the impact and potential implications. For your unit. Here are the key components to consider:

Identify if it is an Attack or Incident: Determine whether the situation at hand constitutes a deliberate action, attack or incident related to misinformation or disinformation. This distinction helps in understanding the intent and nature of the threat.

Assess the Targeting of the UN or your Unit: Analyse if the misinformation or disinformation incident specifically targets the United Nations (UN) or your unit. Consider whether the attack aims to undermine the unit's operations or credibility. Assess if there are second-order effects, such as damage to reputation or strained relationships with stakeholders.

Evaluate Operational Impact: Determine the potential impact on your current and future operations. Analyse whether the incident has the potential to disrupt ongoing activities or hinder the achievement of mission objectives. Consider the implications for resource allocation, operational planning, and your decision-making processes.

Consider Situational Changes: Assess how the incident may lead to changes in the operational environment within your area of operations. Analyse whether it could alter public perception, influence local dynamics, or impact the overall security situation.

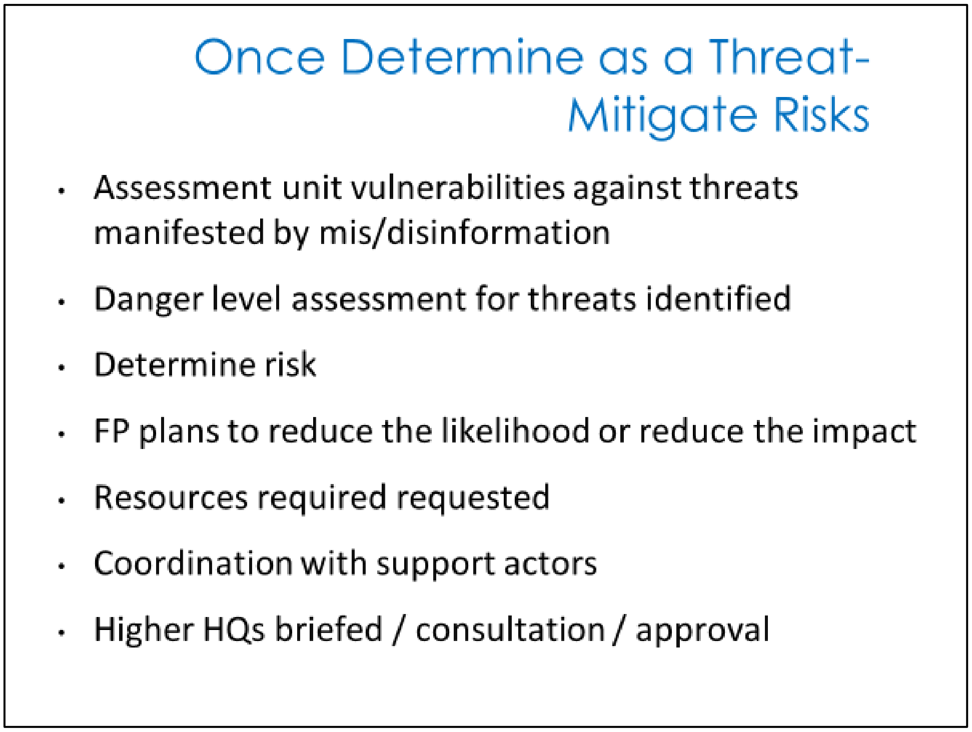
Evaluate Collateral or Secondary Harm: Assess the potential for collateral or secondary harm resulting from the incident. Analyse if the misinformation or disinformation could cause harm to individuals, communities, or your organisation indirectly, either through social tensions, conflict escalation, or other negative consequences.

Determine Threat Actor Exploitation: Evaluate whether the threat actors behind the misinformation or disinformation incident could exploit the situation further. Consider if they may attempt to leverage the incident for broader strategic objectives, such as gaining influence, spreading discord, or inciting violence.

Assess Information Security Compromise: Determine if the incident poses a risk to your unit’s information security. Analyse whether the misinformation or disinformation could compromise sensitive data, lead to operational vulnerabilities, or enable unauthorised access to critical systems.

By systematically considering these components during the determination phase, you can better understand the impact and potential risks associated with misinformation and disinformation incidents. This enables the development of targeted strategies and measures to effectively mitigate their effects or impact on unit operations.

Slide 11



Once Determine as a Threat-Mitigate Risks

- Assessment unit vulnerabilities against threats manifested by mis/disinformation
- Danger level assessment for threats identified
- Determine risk
- FP plans to reduce the likelihood or reduce the impact
- Resources required requested
- Coordination with support actors
- Higher HQs briefed / consultation / approval

Once the determination has been made that misinformation or disinformation poses a threat, the next step is to mitigate the risks. This involves several key actions:

Assess Unit Vulnerabilities: Conduct a thorough assessment of unit vulnerabilities in the context of the threats posed by misinformation and disinformation. Identify potential weaknesses in procedures that could be exploited. This assessment helps in understanding the specific risks and devising targeted mitigation strategies.

Evaluate Danger Level: Assess the severity and potential impacts identified. Categorise the danger level associated with each threat to prioritise mitigation efforts. This evaluation assists in allocating appropriate resources and determining the urgency of response.

Determine Risk: Analyse the overall risk posed by the threat. Consider the likelihood of occurrence and the potential impact on unit operations, mission success, and the UN’s objectives. This risk assessment provides a foundation for developing effective mitigation measures.

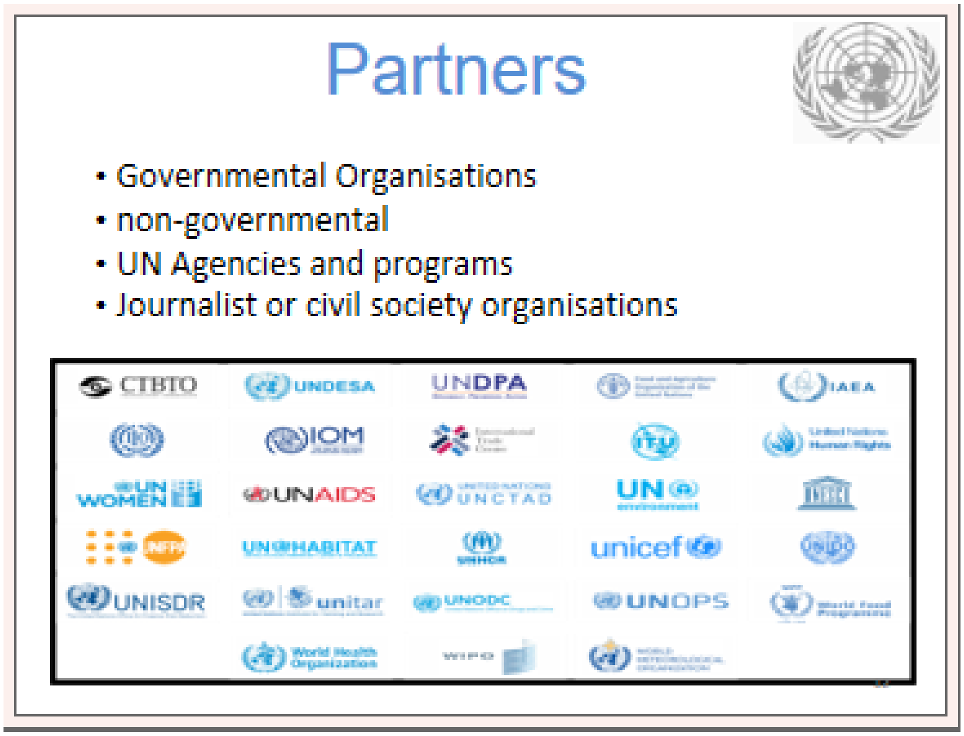
Request Required Resources: Identify the resources necessary for implementing the FP plans effectively. Request the required resources through appropriate channels, ensuring they align with the mitigation strategies proposed.

Coordinate with Support Actors: Collaborate and coordinate with support actors, both internal and external to the unit. Engage with relevant components, agencies, or organisations that can assist, engage groups, and counter-misinformation and disinformation efforts/campaigns. Seek their expertise, assistance, and collaboration in implementing the FP mitigation plan effectively.

Brief Higher Headquarters: Provide briefings to higher headquarters, ensuring they are well-informed of the associated risks and mitigation strategies. Seek consultation, input, and necessary approvals to proceed with the implementation of the FP plans. Foster open lines of communication to facilitate support and guidance throughout the process.

By following these steps, units can proactively mitigate the risks posed by misinformation and disinformation. By assessing vulnerabilities, evaluating danger levels, determining risks, developing FP plans, requesting resources, coordinating with support actors, and briefing higher headquarters, units can enhance their readiness to combat misinformation and disinformation effectively.

Slide 12



Partners

- Governmental Organisations
- non-governmental
- UN Agencies and programs
- Journalist or civil society organisations

CTBTO
UNDESA
UNDPA
IAEA
IOM
ITU
UN WOMEN
UNAIDS
UNCTAD
UN environment
UNFPA
UN-HABITAT
UNHCR
unicef
UNIDO
UNISDR
unitar
UNODC
UNOPS
World Food Programme
World Health Organization
WIPO

When combating false information and manipulation, it is crucial to identify and collaborate with relevant partners. Consider the following key partners who can contribute to countering information manipulation:

Governmental Partners: Identify government agencies or departments that specialise in information security, communication, or counter-disinformation efforts. Collaborate with them to share information, coordinate strategies, and leverage their expertise and resources. Engage with relevant ministries, such as public affairs or communication, to align efforts and ensure a coordinated response.

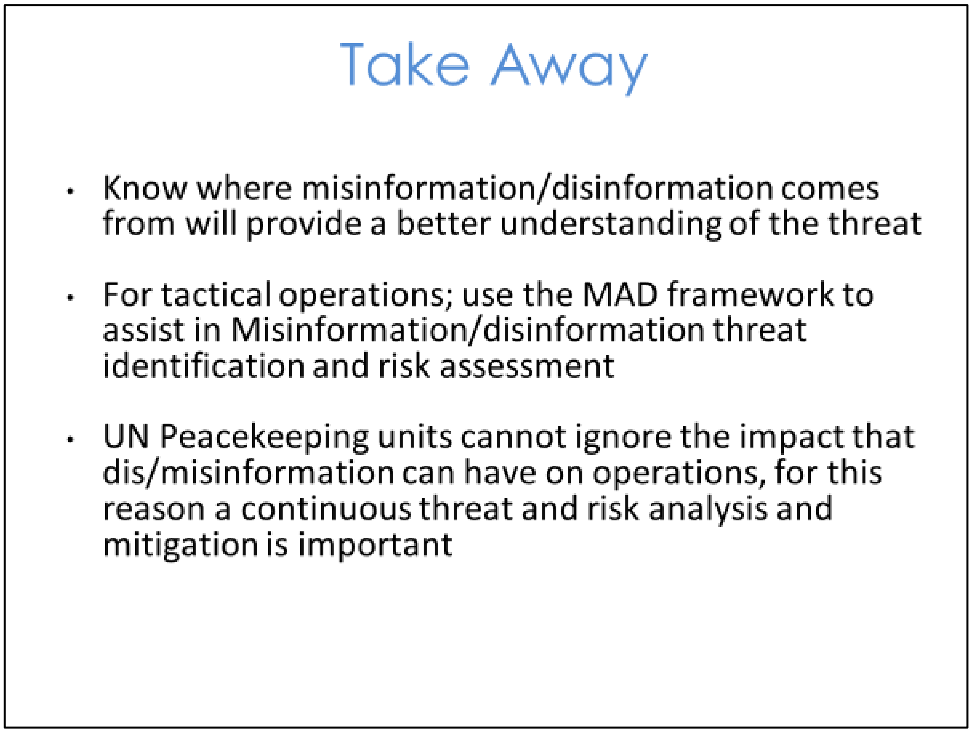
Non-Governmental Organisations (NGOs): Collaborate with NGOs specialising in media literacy, fact-checking, and combating misinformation and disinformation. These organisations often have expertise in monitoring information landscapes, conducting investigations, and exposing falsehoods. Partner with them to leverage their resources, network, and knowledge in countering information manipulation.

Journalists and Media Outlets: Establish partnerships with journalists and media outlets operating within your area. Engage them in fact-checking initiatives, sharing verified information, and amplifying accurate narratives. Work together to combat false information and promote responsible journalism practices.

Civil Society Organisations: Identify civil society organisations that focus on human rights, transparency, or media integrity. Collaborate with them to raise awareness about information manipulation, engage local communities, and develop initiatives to counter false narratives. These organisations can contribute valuable insights, advocacy efforts, and community engagement to build resilience against information manipulation.

It is important to note that the relevance of partners may vary based on the specific context and objectives. Prioritise those who bring relevant skills, resources, or capacity to help respond effectively to information manipulation. Collaborative efforts with diverse partners can strengthen resilience, promote accurate information, and contribute to countering the negative impact of false information.

Slide 13



Take Away

- Know where misinformation/disinformation comes from will provide a better understanding of the threat
- For tactical operations; use the MAD framework to assist in Misinformation/disinformation threat identification and risk assessment
- UN Peacekeeping units cannot ignore the impact that dis/misinformation can have on operations, for this reason a continuous threat and risk analysis and mitigation is important

Summary

Here are the key take-aways from this lesson:

- By identifying the sources, we can better assess the credibility and intent behind false narratives
- The MAD framework, consisting of Monitor, Analyse, and Determine, is a valuable tool for identifying and assessing the threat of misinformation and disinformation on your unit. Applying this framework can contribute to the development of a risk mitigation plan
- Mis/disinformation can be the catalyst for manifesting threats. Ongoing threat and risk analysis and mitigation efforts are essential to ensure unit operational success and maintain the integrity of UN missions

Learning Activity 3.5

Notes to Instructor:

By breaking into smaller groups and using the MAD assessment framework, the participants can access the potential impacts of disinformation, brainstorm monitoring mechanisms, and develop engagement plans to help mitigate risks associated with the collateral harm from disinformation campaigns. This exercise encourages collaborative thinking and problem-solving skills and promotes a better understanding of the complexities associated with disinformation and its potential consequences on unit operations.

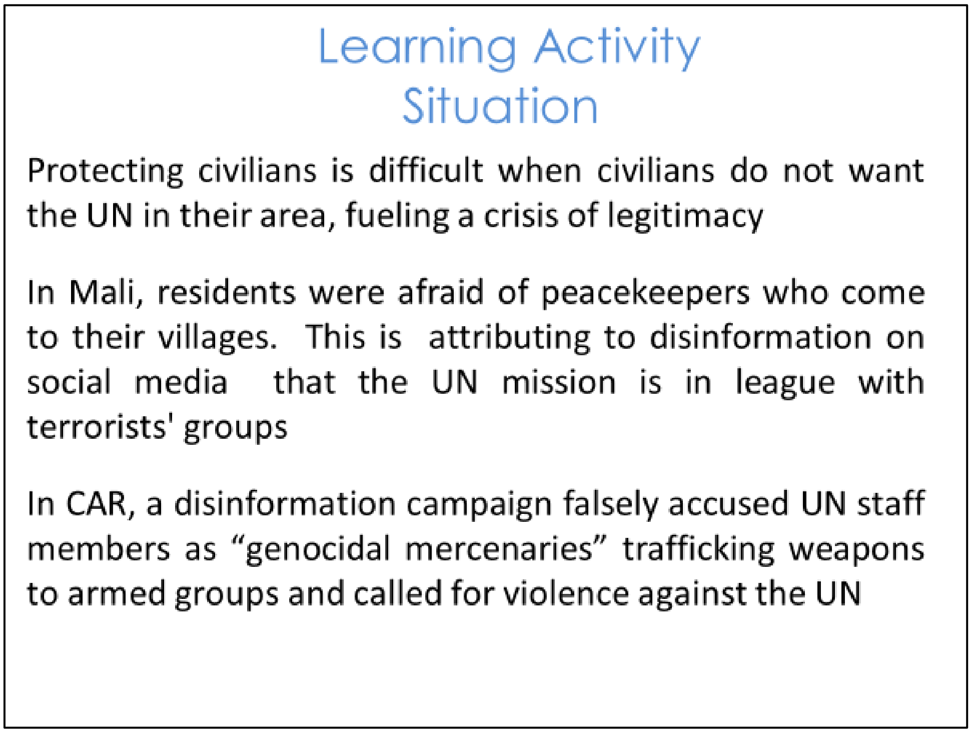
Display or hand out the Situation Slide and Task Slide (LA Slides 14/15): At the beginning of the learning activity session, share two slides with the participants, providing the necessary context and information about the scenario and the assigned tasks. The situation slide will outline the scenario, which likely involves a disinformation campaign with potential impacts on unit operations. The task slide will clearly state a topic that each group will discuss.

Each group gets 30 Minutes to discuss their topics using the MAD assessment framework. After receiving the situation and task details, the participants will break into three smaller groups, each assigned to one of the three discussion topics related to the disinformation campaign. Each group will have a dedicated 30-minute timeframe to explore their respective topics thoroughly.

Group Leaders Report Findings to the Plenary Session: Each group will appoint a leader or spokesperson responsible for summarising the group's discussions and findings. After the allotted time, all groups will reconvene in the plenary session, and each leader will present their group's key insights, conclusions, and solutions to the audience.

Facilitate Summarising Their Findings and Takeaways: After all the presentations, help summarise the key points, highlighting the recurring themes, significant insights, and potential actions.

LA Slides 14 / 15

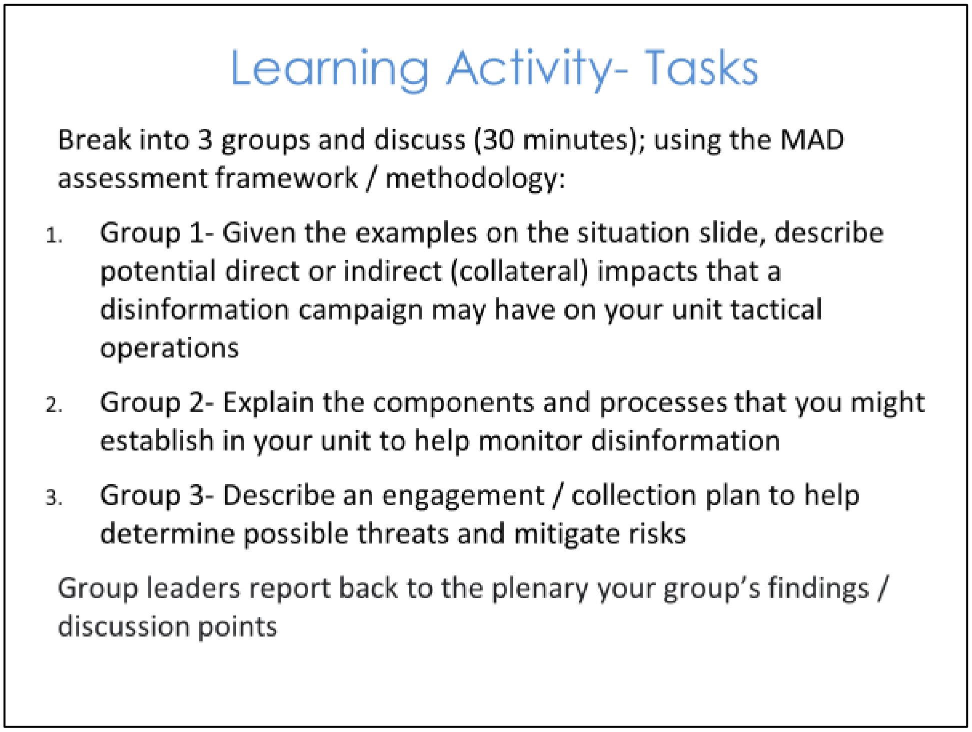


Learning Activity Situation

Protecting civilians is difficult when civilians do not want the UN in their area, fueling a crisis of legitimacy

In Mali, residents were afraid of peacekeepers who come to their villages. This is attributing to disinformation on social media that the UN mission is in league with terrorists' groups

In CAR, a disinformation campaign falsely accused UN staff members as “genocidal mercenaries” trafficking weapons to armed groups and called for violence against the UN



Learning Activity- Tasks

Break into 3 groups and discuss (30 minutes); using the MAD assessment framework / methodology:

1. Group 1- Given the examples on the situation slide, describe potential direct or indirect (collateral) impacts that a disinformation campaign may have on your unit tactical operations
2. Group 2- Explain the components and processes that you might establish in your unit to help monitor disinformation
3. Group 3- Describe an engagement / collection plan to help determine possible threats and mitigate risks

Group leaders report back to the plenary your group’s findings / discussion points

Module 3

Operational Framework Wrap Up

At the conclusion of Module 3, some key elements should have become clear:

Increasing Attacks on UN Personnel: The escalation in attacks on UN personnel poses a significant challenge to our operations. It not only threatens the security of our personnel but also hampers our ability to carry out our mandated tasks effectively. This issue demands attention and proactive measures to ensure the protection of our peacekeeping units.

Diverse Threats Faced by UN Units: UN units are encountering a range of threats that demand comprehensive risk management strategies. From traditional threats to Improvised Explosive Devices (IEDs) and modern challenges such as cyber-attacks and the spread of misinformation/disinformation, the operational landscape has become more complex and unpredictable. These threats require a multidimensional response to our strategies.

Mission Analysis as the Key to Success: Effective mission analysis is at the core of successful peacekeeping operations. By thoroughly understanding the local context, political dynamics, cultural intricacies, and potential threats, we can develop informed and strategic approaches to address the challenges on the ground. It enables us to make well-informed decisions that contribute to achieving our mission goals.

Threat-Based Approach to Force Protection Tactical Planning: Adopting a threat-based approach to Force Protection Tactical Planning is crucial. It involves breaking down the Analysis of the Operation Environment (AOE) into different elements like Physical, Human, and Information Terrain. Additionally, Actor Evaluations (AE) play a pivotal role in identifying Key Actors in the area of operation. This comprehensive analysis forms the foundation for Threat Analysis and ensures that we are prepared to counter potential threats effectively.

Addressing Intelligence Gaps: Intelligence gaps, or missing information, are common in any operation. To overcome these gaps and build situational awareness, a well-structured collection plan or Information Acquisition Plan is necessary. Collecting relevant data and peacekeeping-intelligence enables us to stay ahead of the evolving security landscape and make informed decisions based on accurate information.

Risk Assessment for Prioritisation: Identifying threats is just the beginning; we must assess their potential impact on our operations. Conducting a risk assessment allows us to prioritise our planning efforts and allocate resources wisely. By understanding the level of risk associated with each threat, we can tailor our strategies to address the most critical challenges effectively.

Mitigation Strategies: Once we have identified the potential threats and conducted a risk assessment, we can focus on developing mitigation strategies. These strategies aim to reduce the impact of identified threats or minimise the potential for those threats to materialise. Effective mitigation measures enhance the safety of our personnel and improve mission success.

In the decision-making process, FP plans require the next higher headquarters' approval and support; therefore, all tactical unit plans need to be briefed and endorsed by their higher HQs.

References annexes can be found in separate folders to aid in the delivery of the modules and TTX:

- **Annex A:** Lessons- PowerPoint Slide Presentations
- **Annex B:** Tabletop Exercise (TTX); Scenario-based Exercise (SBE)
- **Annex C:** Additional Lessons in Support of UNFORPRO

[End of document)