



## Module 3 Operational Framework for UNFORPRO

# 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



# Lesson 3.1 Military Unit Tactical Planning Considerations for Force Protect (FP)

# Content

- Using the Decision-Making Process for FP tactical planning considerations
- Threat based planning tools
- Threat analysis
- Risk analysis

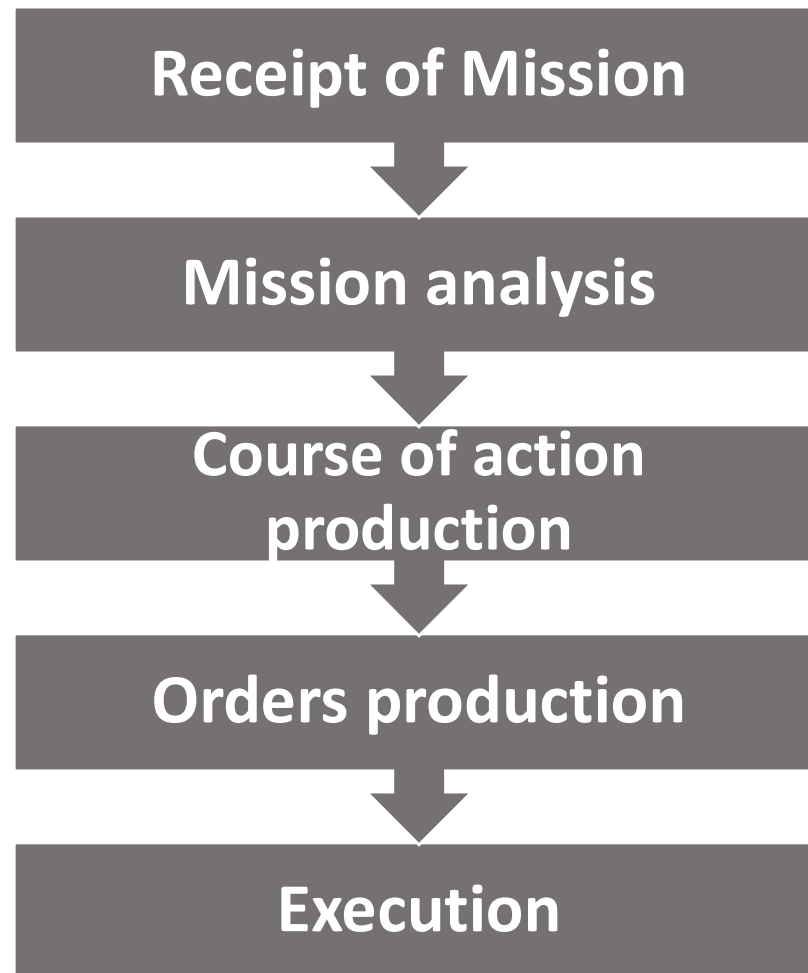
# Learning Objectives

- 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

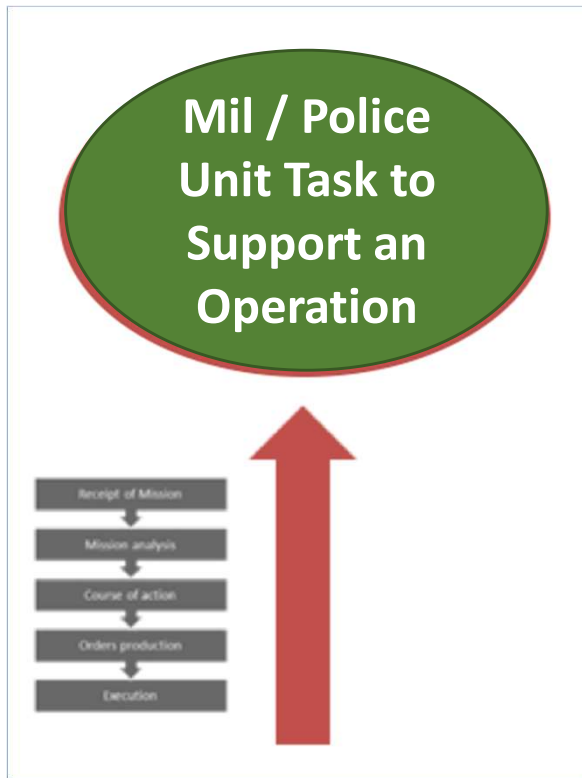
# Key Terms and definitions for FP Planning

- 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

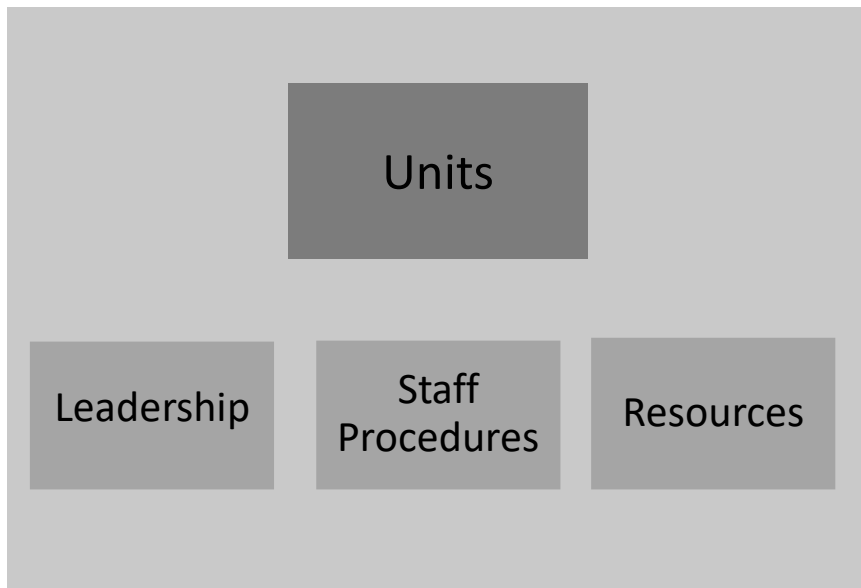
# Conventional decision-making process



# FP Planning Considerations- Uses the same DMP



*Tactical  
decision-  
making  
process*

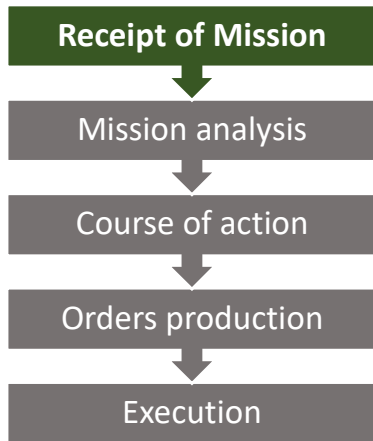


*FP Considerations  
for the tactical  
decision-making  
process focused on  
threats against  
your unit and the  
ability to  
accomplishing the  
operation*





# Receipt of Mission



Mission Mandate  
CONOPS

Mission Concept Strategy

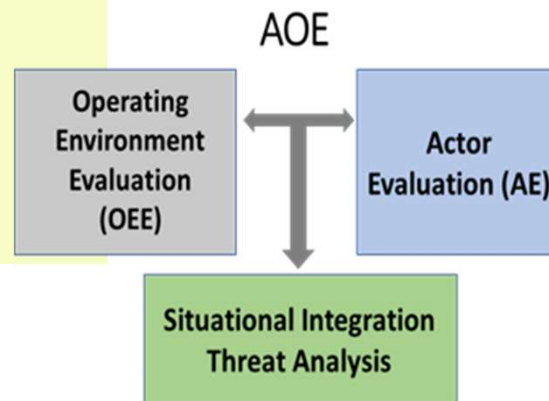
Mission POC  
Plan

Force Commander  
OPORD

Sector Commander  
OPORD

## Start Looking at Missions from a FP viewpoint

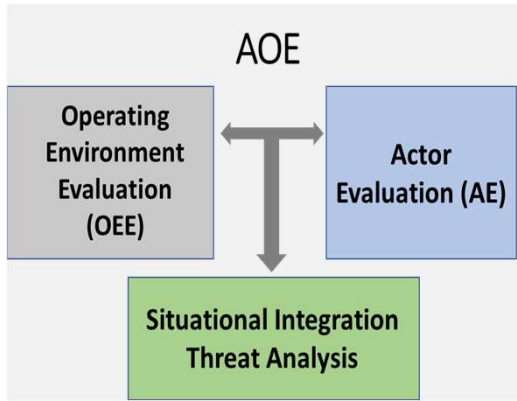
- Your current location / deployment
- Do you need to transit to a new area
- Your Future tactical area of operation
- What assets does higher HQs provide
- Medical facilities / CASEVAC
- Continue to refine Analysis of the Operational Environment (AOE)



Receipt of mission

FP planning included for all unit missions

# Mission Analysis



*For all static and mobile operations*

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

# Potential Attackers- Groups (Armed / Unarmed )



*Information  
Requirements  
established*

*Recce operations  
conducted*

*Information  
requested from  
and offered to  
intelligence cells*

## 1. Pinpoint location and area of operations

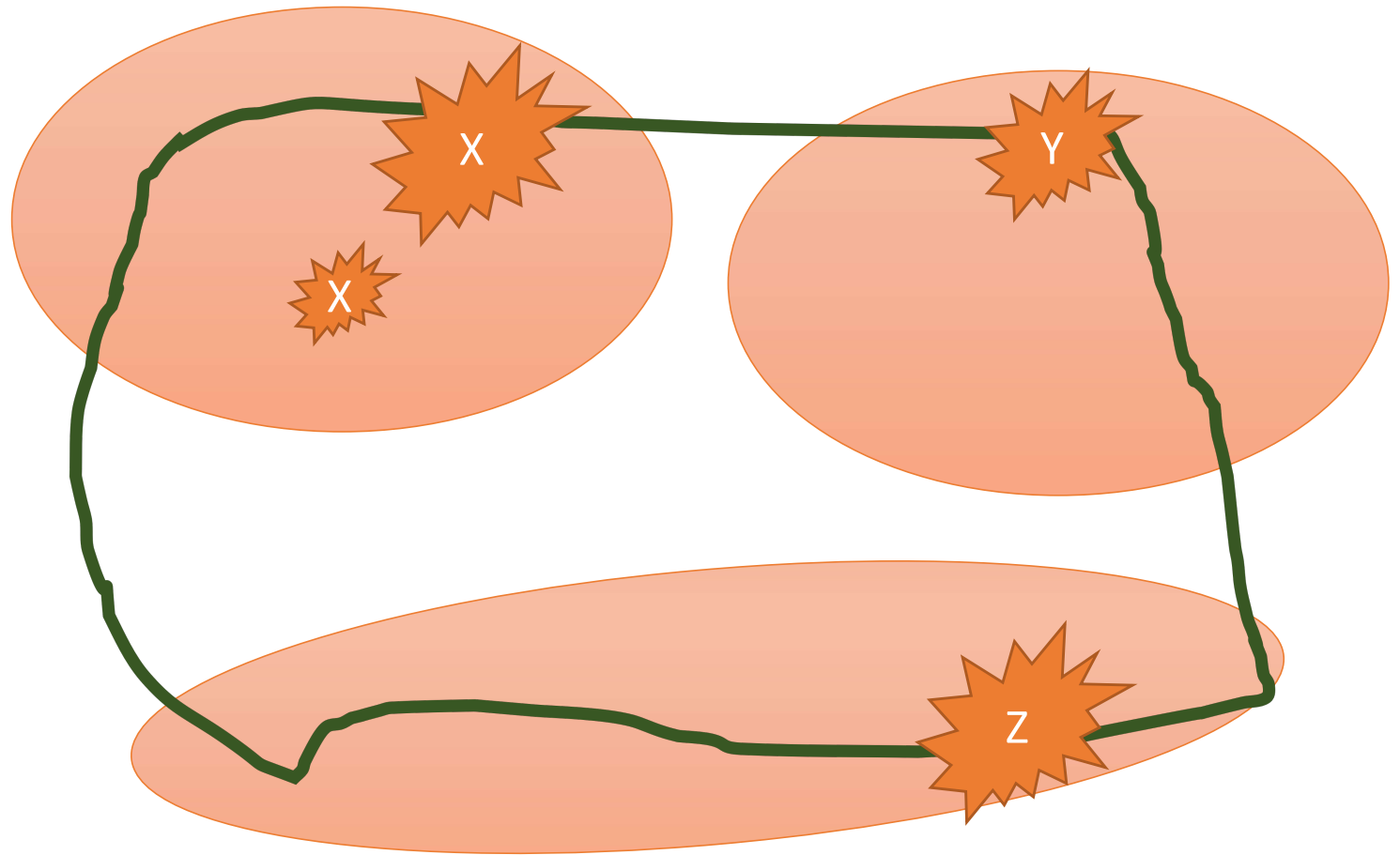
## 2. Determine:

- 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

Key actors

# Potential Attackers- Groups



# Key actors

## Potential Attackers-Groups



*For each  
Armed /  
unarmed  
group within  
the potential  
TAO*

Group	Location	Number	Composition	C2 Commo
X				
Y				
Z				
Compliance	Capabilities	Social Media Access	Historical Background Patterns	Human Rights Record

Key actors

# Civilian Communities- that pose a potential to generate attackers



*Information Requirements are established.  
Patrols and recce operations are conducted.  
Information is requested from intelligence cells*

## 1. Pinpoint locations

## 2. Determine:

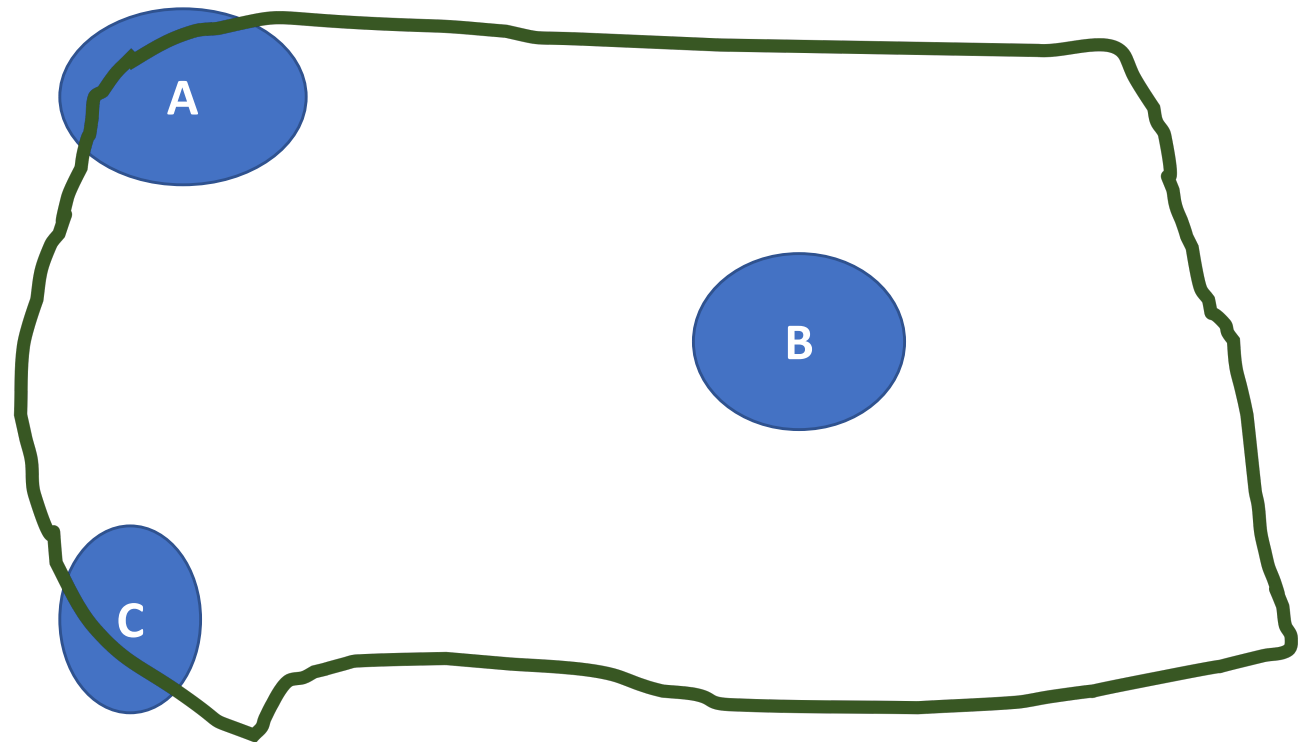
- Number of civilians (gender and age breakdown)
- Historical background for civil unrest / violence
- Compliance
- Exposure to Mis/disinformation, cell phones, internet access, internet cafés, etc.
- Access to weapons, explosives

## 3. Identify leaders

Key actors

# Civilian Communities-

that pose a potential to generate attackers



# Key actors

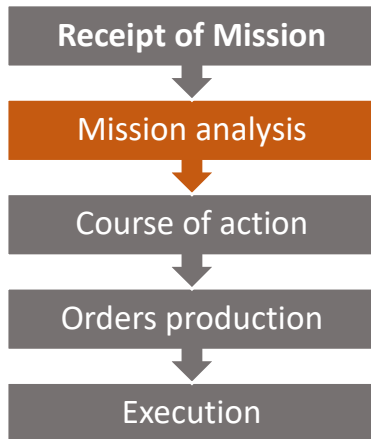
## Civilian Communities- that pose a potential for generating attackers



Civilian Community	Location	Numbers & Gender	Compliance	Historical Background	Social Media Access	Access to weapons

*Communities ,  
groups  
identified  
within the unit  
areas of  
operations  
(current and  
future)*





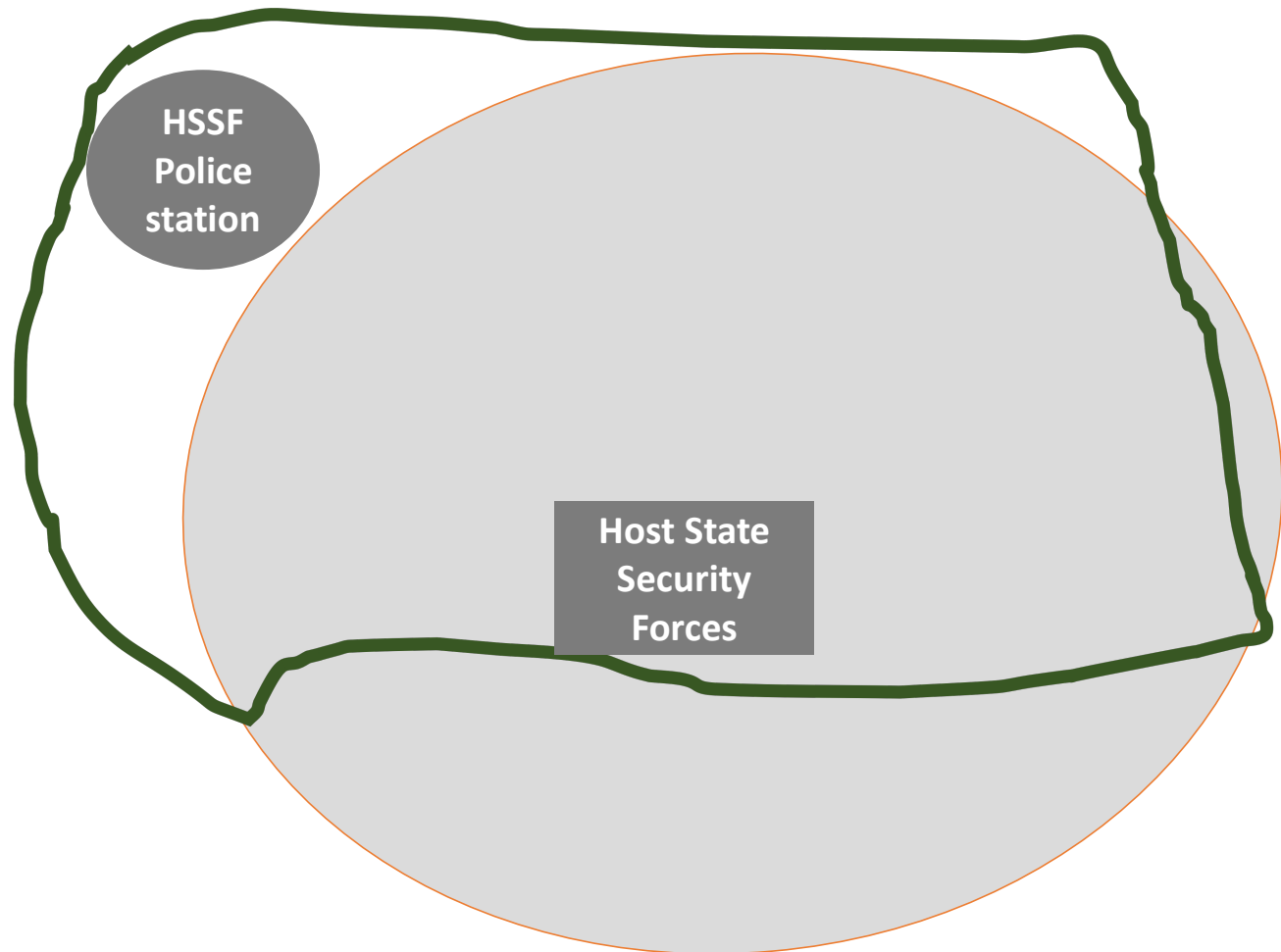
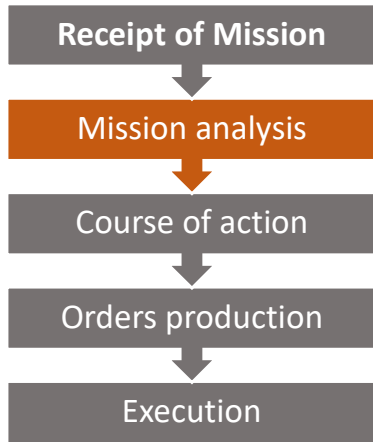
## Host State Security Forces (HSSF)- for potential assistance / support

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

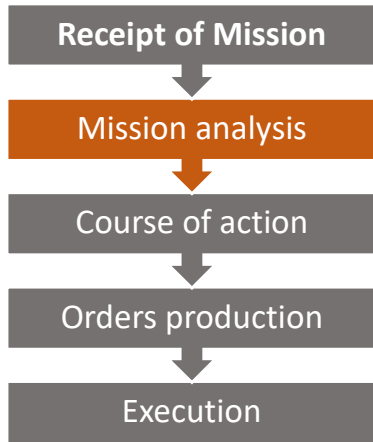
Key actors

# Host State Security Forces



# Key actors

## Host State Security Forces- for potential assistance / support



HSSF	Location	Number	Composition	C2
HSSF X				
HSSF Y				
HSSF Z				
Political	Capabilities	Will	HR Violations	Other

*For each Host State security forces unit deployed within the unit's area of deployment*

**Note:** If HSSF –groups / units are assessed as potential attackers targeting UN units- use the Potential Attackers matrix tools



*May include UN,  
non-UN actors,  
units, int'l or UNSC  
mandated  
international forces*

*Existing  
coordination  
mechanisms will  
facilitate acquisition  
of relevant  
information*

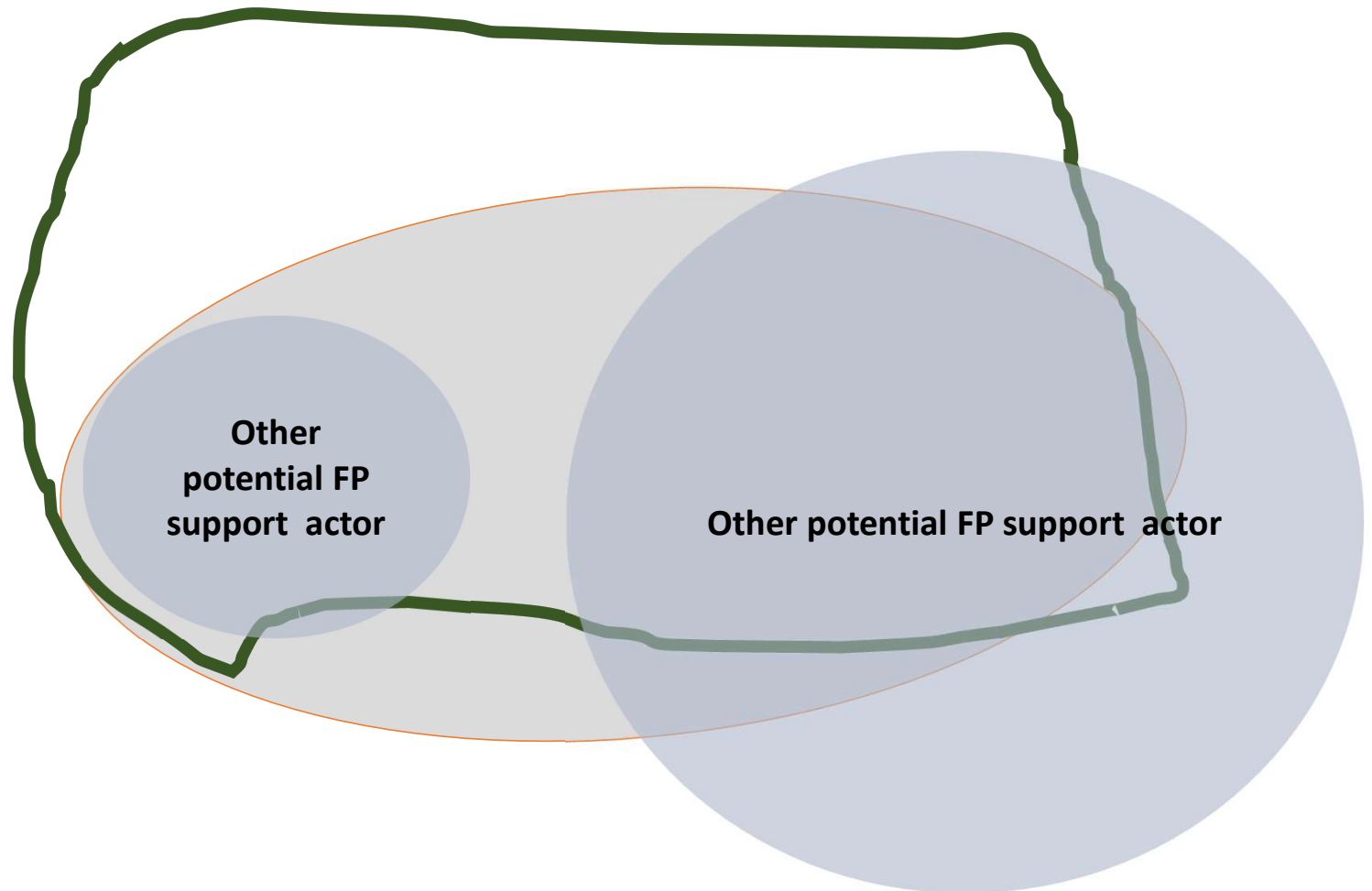
Key actors

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

Key actors

# Other FP Support Actors



Key actors

# Other Support Actors



Other potential FP support actors	Location	Mandate	Capabilities	Support capacity
Unit A				
Unit B				
Actor C				

# Our Unit and Mission

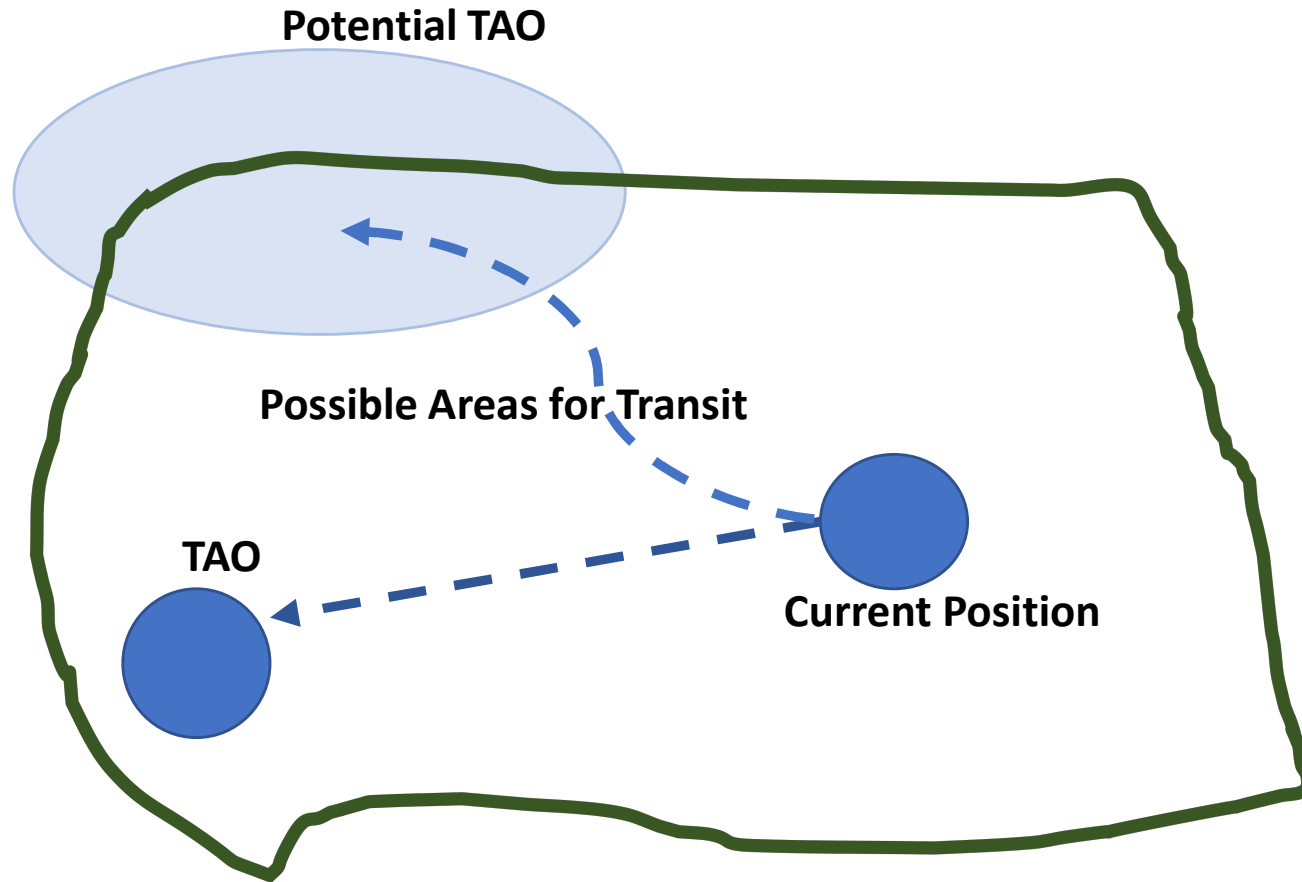


1. Current and future locations (static and mobile)
2. Determine:
  - Number, composition
  - C2 / Communications
  - Armored
  - Mobility
  - Firepower
  - Intelligence / reconnaissance capabilities
  - Cyber Security Capabilities
  - Medical capacity / capabilities (Day , Night CASEVAC)
  - Time Distances for support to unit (QRF, medical, Indirect fire)
3. Attached, non-organic units, assets provided

# Our Unit and Mission



*Consider all phases of an operation / mission both static and mobile*



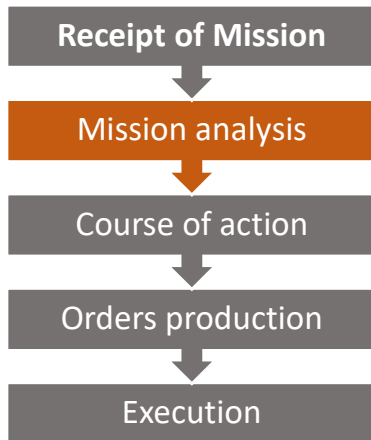




# Assets / Attachments for operation (Nonorganic)

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

# 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)**

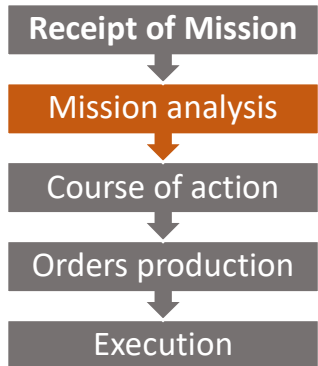
*Attacks include  
direct fire, indirect  
fire, IEDs, Assaults,  
Cyber, Sabotage*

*Mis/Disinformation  
offensives included  
in Cyber*

# 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	<b>Concern</b>	<b>Concern</b>	----	
Group Y	<b>Concern</b>	----	<b>Concern</b>	----
Group Z	----	----	----	----



# Threat analysis Matrix

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

*Develop a predictive threat CoA for each threat identified*

*Note: the same group (A) can pose several different threats*

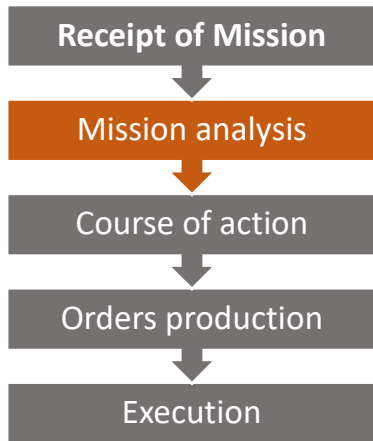
 **Type of attacks** - direct fire, indirect fire, IED, Assault, sabotage, cyber

# 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





Risk analysis

# 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



Risk analysis

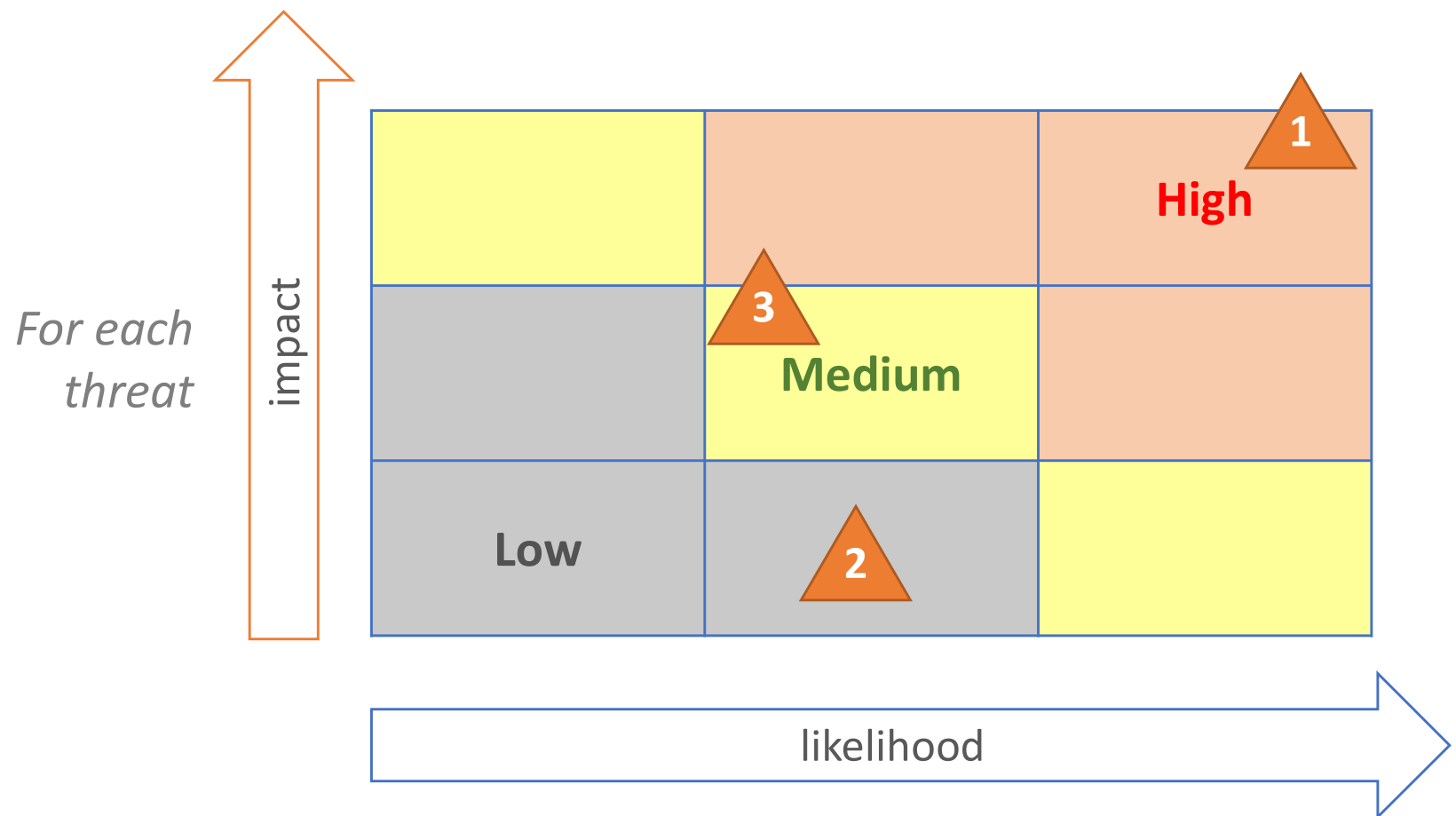
# Danger level assessment



*For each  
Threat*

Threat	Intent	Threat vs Unit Capabilities	Historical	Other (Commander concerns)
Threat 1	<b>High</b>	<b>High</b>	<b>High</b>	<b>High</b>
Threat 2	<b>Low</b>	<b>High</b>	<b>Medium</b>	<b>Low</b>
Threat 3	<b>Medium</b>	<b>Low</b>	<b>Medium</b>	<b>Low</b>

# Risk analysis Matrix





# Unit Course of Action (CoA)

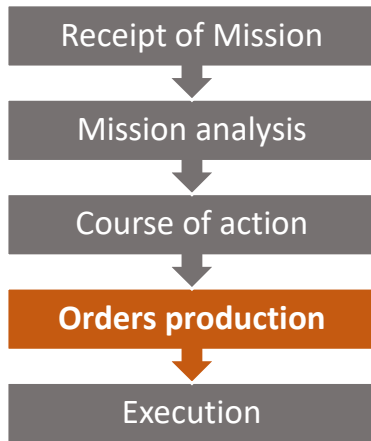
1. Counters threat COA
2. Plans to reduce the likelihood
3. Plans to reduce the impact
4. Resources required requested
5. Coordination with FP Support actors
6. Higher HQs briefed / consultation / approval
7. In consultation with Higher HQs, a priority designation on the criticality of mission- high, medium, low priority

*Development of CoAs are considered for the 3 phases- current deployment, transit, and future*

# Our Unit's Force Protection COAs-

purpose to reduce impact or likelihood of threat

Threat	Threat 1	Threat 2	Threat 3
<b>Who</b>	<b>Who in our unit executes the tasks</b>		
<b>What</b>	<b>the military tasks</b>		
<b>When</b>	<b>Time/ timing</b>		
<b>Where</b>	<b>Location</b>		
<b>How</b>	<b>Concept of maneuver</b>		
<b>Why</b>	<b>Purpose End State</b>		
<b>External Coordination</b>	<b>HSSF / other Support units</b>		



*Plans must be approved by the higher HQs*

# Order Production

1. Approval of plans
2. FRAGO sent
3. Production- Annex to OORDER or Separate FP Order
4. Subordinate units given time for planning
5. Rehearsals
6. Adjustments and updates to original plan

# 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

# 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

Questions