INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT (IPOE)

by

MEJAR MOHAMAD HEIKAL BIN MOHAMAD HAIRI

SO 2 JIPB CELL EDUCATION DIVISION

IPOE – Step 3
EVALUATE THE THREAT

STEP 3: EVALUATE THE THREAT

- Identifying the level of threat command that is likely to be faced in the particular op or sit at hand
- Provides the commander with a realistic assessment of the capabilities
- It determines the threat's CV and affects the subsequent development of DP

Acty 1. Identify Level of Threat Comd

Acty 2. Establish Threat Model & Templates

Acty 3. Identify Threat Capabilities

Acty 1. Identify Level Of Threat Comd

- Identify the level of threat comd likely to be opposed
- Prov the focus for further analysis of the designated threat – avoid wasted int effort
- To decide the level of threat comd,derived:
  - Guidance fm Higher Comd intent, msn & task
  - Intelligence estimates and IPOE products fm higher HQ

Acty 1. Identify Level Of Threat Comd

- Identify stakeholder groups include **hostiles**, **adversaries**, **neutrals** and **friendly forces**
- Stakeholder groups subsets:
  - Insurgents
  - The local population (of which there may be multiple factions)
  - Local interest groups
  - Other government agencies
  - Allied military forces
  - Other nations' intelligence and security agencies
  - Non-government organisations

Acty 1. Identify Level Of Threat Comd

- Stakeholder groups subsets (Cont):
  - Political representatives
  - Personnel from supporting combat arms units
  - Military police
  - Civilian police
  - The media
- The level of command of a stakeholder group is normally expressed interms of the organising HQ (eg; mechanised brigade)
- A stakeholder's intent - **OBJ** and its **RELEVANT TIME LINE** (eg; the imm obj is to seize the key bridges across the Pahang River)

Acty 2. Estb Threat Models & Template

Sub Acty A. Produce Doctrinal Overlays

Sub Acty B. Describe Prefered Tactic & Options

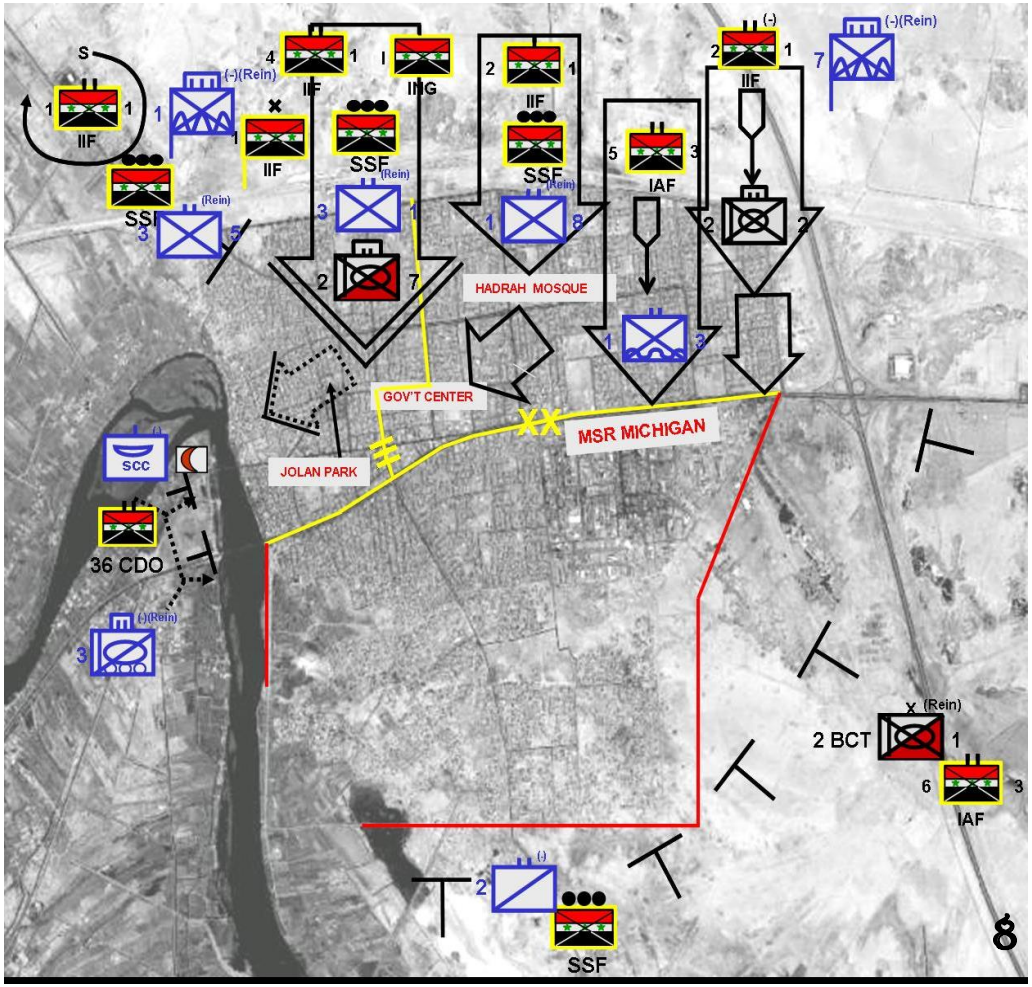
Sub Acty C. Produce HVT Matrix

Sub Acty D. Produce ORBAT File

Sub Acty A. Produce Doctrinal Overlays

- Doctrinal overlays/templates illustrate graphically the deployment pattern & disposn preferred by the threat normal tactics

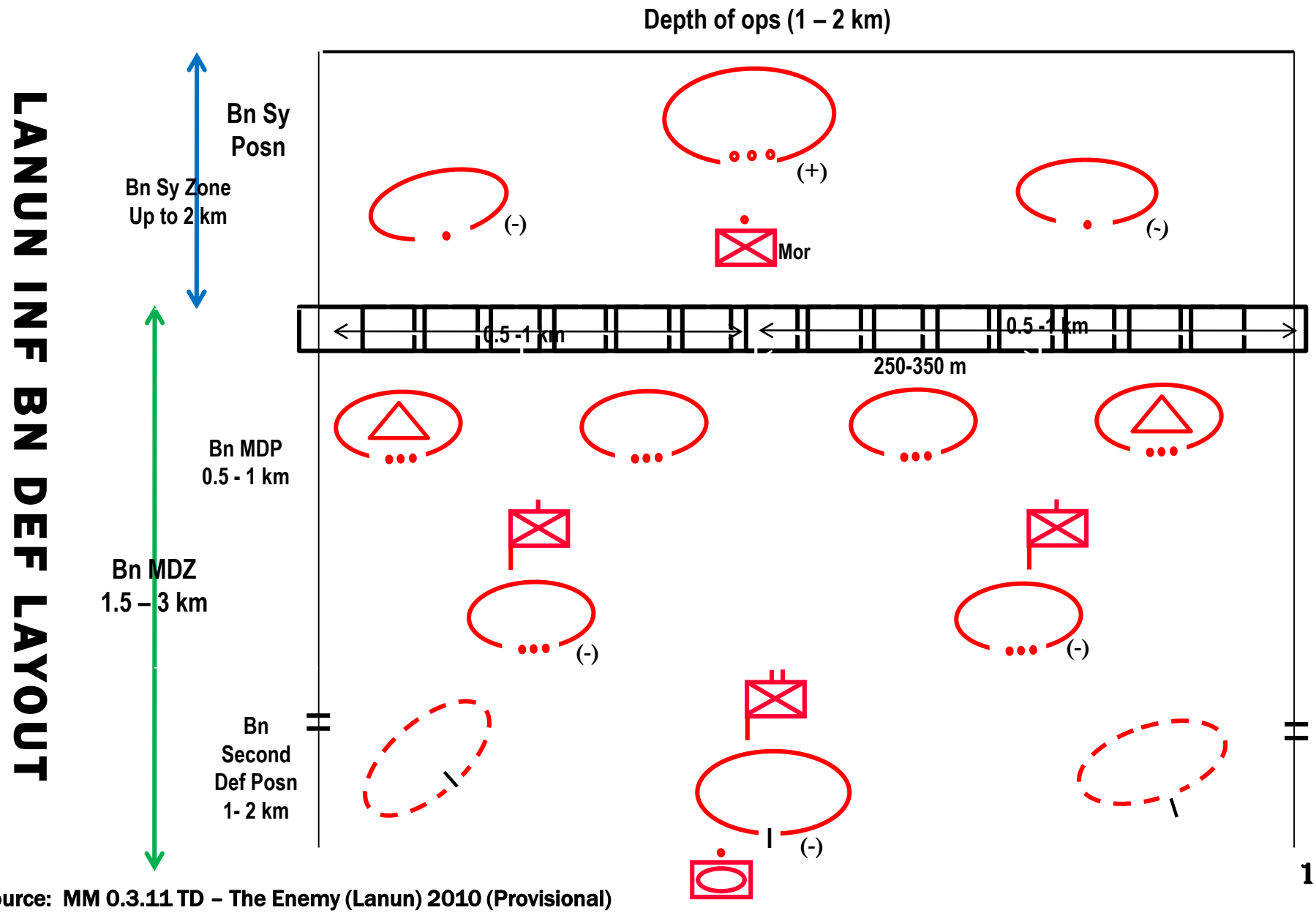
- Scaled graphic depictions of force disposn for standard ops such as:
  - Adv to Contact
  - Attk
  - Exploitation
  - Pursuit
  - Area & Mobile Def
  - Retrograde



Sub Acty A. Produce Doctrinal Overlays

- Threat doctrine is used to determined:
  - How they normally organise
  - How they deploys & employs units incl various BOS assets for cbt
- Not possible to dev doctrinal overlays in the course of lack of info

A Produce Doctrinal Overlays



Source: MM 0.3.11 TD – The Enemy (Lanun) 2010 (Provisional)

Sub Acty B. Describe Prefered Threat Tactic & Option

Description should consist of:

- Doctrinal SOM for each major threat elm
- Doctrinal acty of threat BOS SOM
- The normal doctrinal planning timings for the ops & synchronizing BOS acty that sp the SOM

Techniques

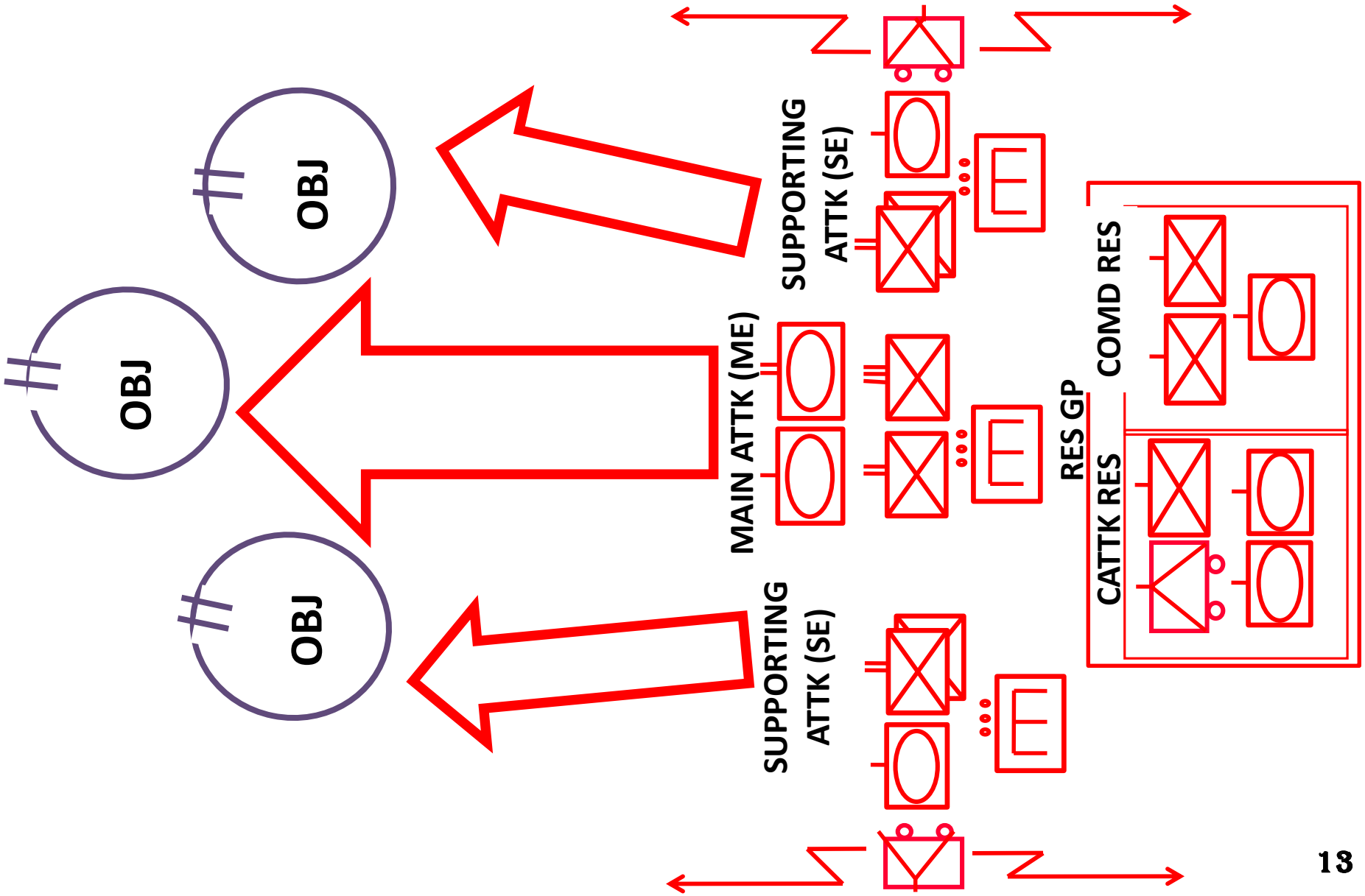
1. Start with SOM & examine how the Threat BOS sp the SOM

2. Time event charts to describe how Threat normally conduct an ops

3. Marginal notations on the graphic template are effective – especially when the notes are tagged to key pt or posn on the template

DOCTRINAL SCHEME OF MANOEUVER

LANUN INF DIV IN ATTK : SINGLE PENETRATION



Techniques

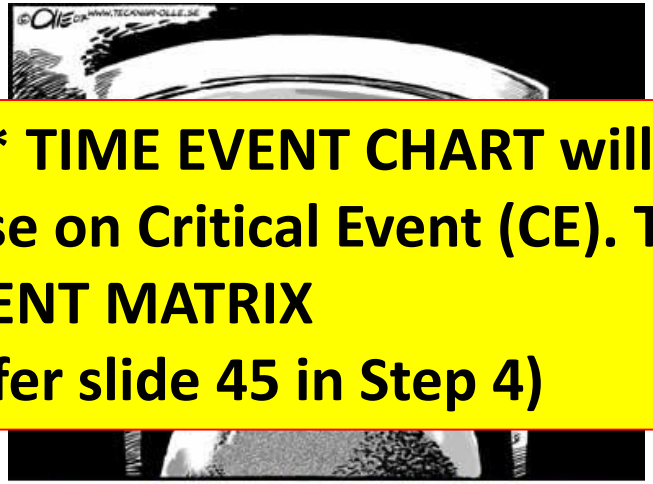
1 Start with SOM & examine how the Threat BOS sp the SOM

2 Time event charts to describe how Threat normally conduct an ops

3 Marginal notations on the graphic template are effective – especially when the notes are tagged to key pt or posn on the template

Time Event Chart

Time		BOS Activity	Remarks
Earliest	Latest		
H-120	**H-70**	**Threat Air Strike**	
H-68	**H-1**	**Threat FS Masses Fire to assist Attk on obj**	
H-60	**H hr**	**Threat Engr breach obs to assist Tk mov**	



***** TIME EVENT CHART will be refined in latter steps base on Critical Event (CE). The output will become EVENT MATRIX**
(refer slide 45 in Step 4)

Techniques

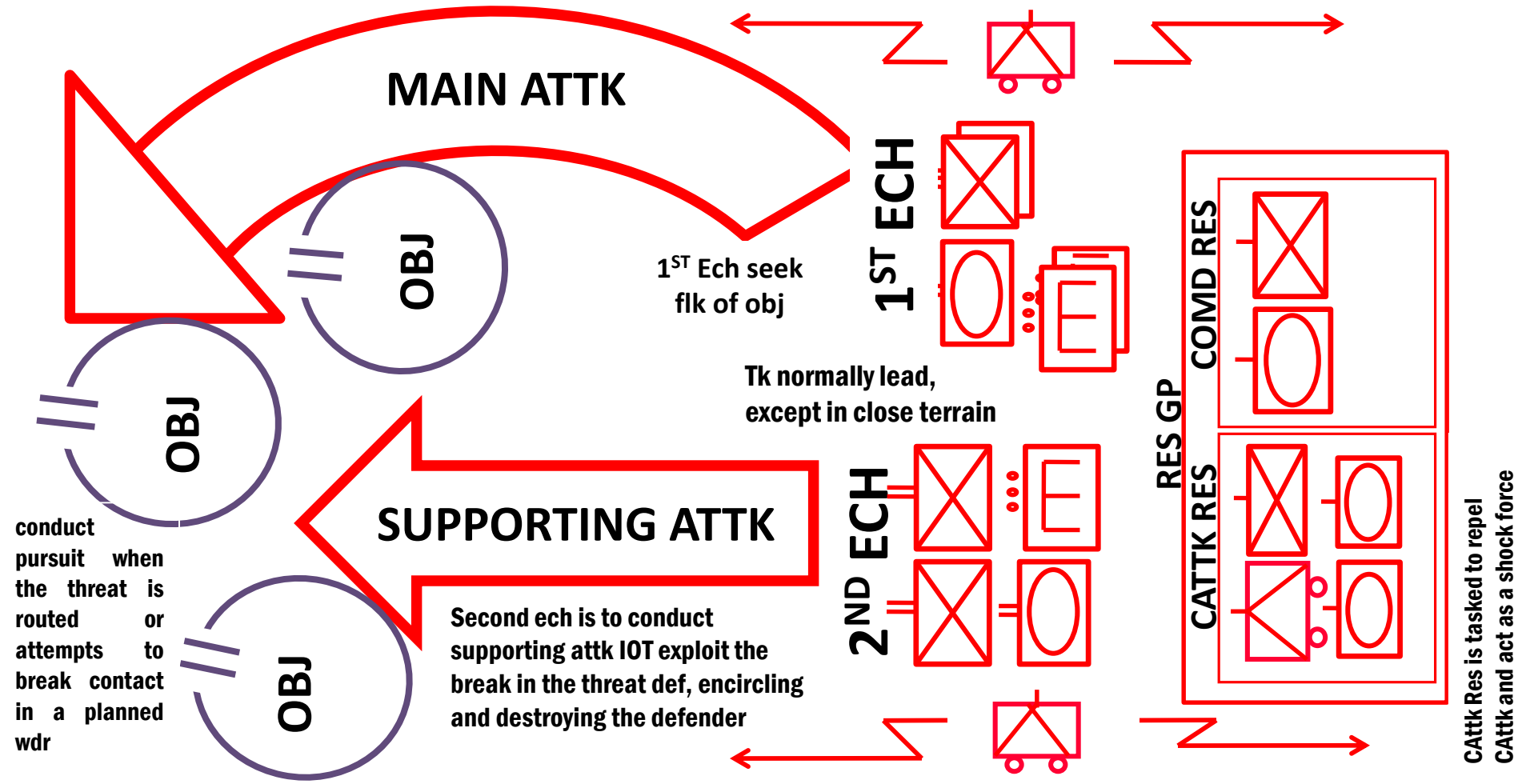
1 Start with SOM & examine how the Threat BOS sp the SOM

2 Time event charts to describe how Threat normally conduct an ops

3 Marginal notations on the graphic template are effective – especially when the notes are tagged to key pt or posn on the template

MARGINAL NOTATIONS

LANUN INF DIV IN ATTK: SINGLE ENVELOPMENT



1. During the prep of the attk, recon will be conducted mostly during ni time
2. DAG to prov max fire sp (i.e. gun, how & mor bn) starting H-68 and protection fm air threat by AD bn.
3. Attk adv rate is 2 – 3 km/h (35-50 m/min) – open country & dismounted or 1 – 2 km/h (15-45 m/min) - close country & dismounted.
4. Time taken to complete the attk is 8 – 16 hrs.

Sub Acty C. Produce HVT MATRIX

- Rank in order of their relative worth to the threat op
- Gp into appropriate categories in Tgt Value Matrix (TVM)
- The TVM forms the basis of the friendly forces targeting process

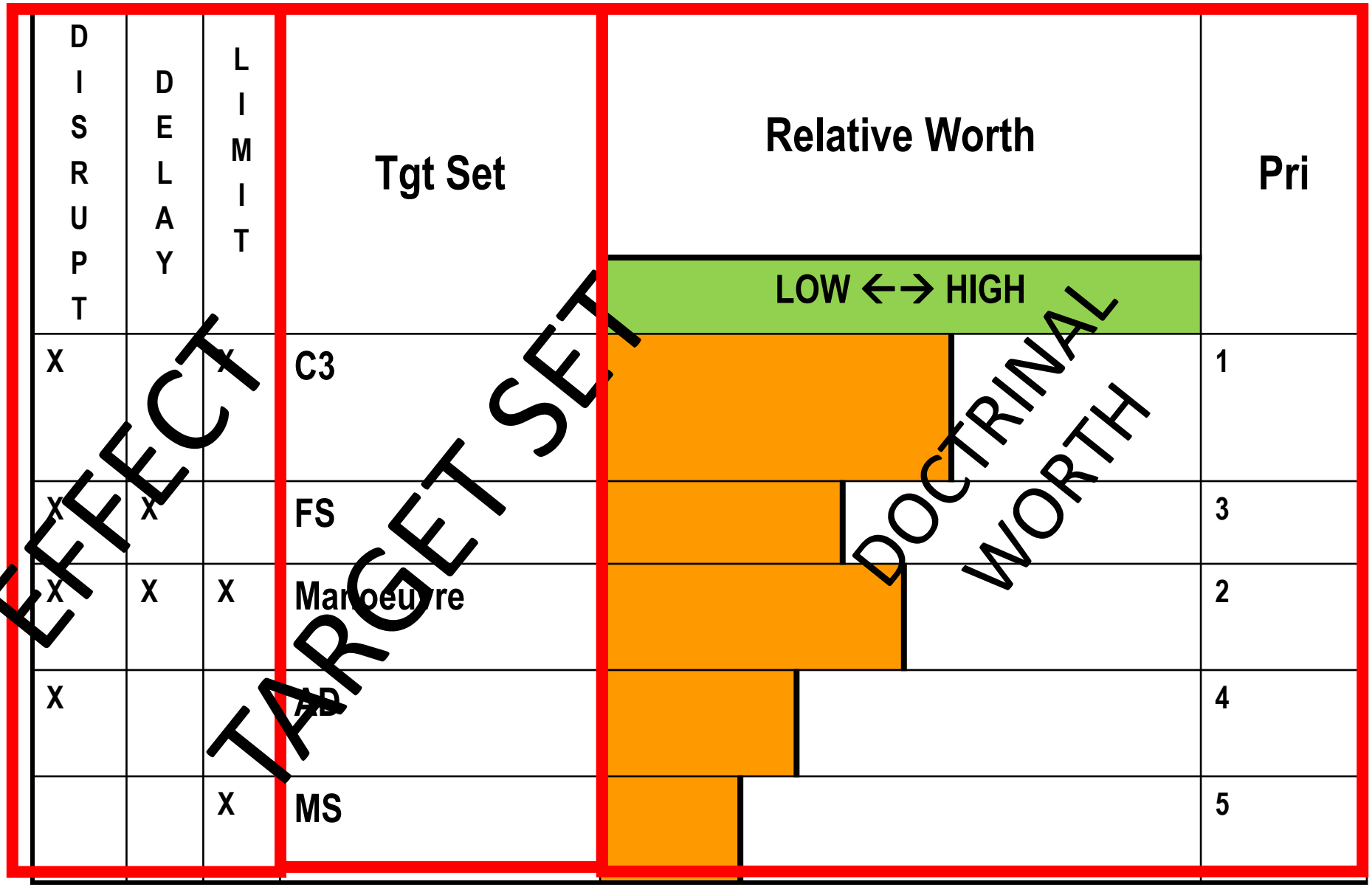
HVT. Assets that the threat comd req for the successful completion of his msn

Sub Acty C. Produce HVT MATRIX

- Suggested categories for the HVT matrix:
  - C3
  - Fire support (including target acquisition, ammunition, aircraft and fire control)
  - Manoeuvre
  - AD (including radar, processing centres and HQ)
  - Engineers

HVT. Assets that the threat comd req for the successful completion of his msn

HVT Matrix Example



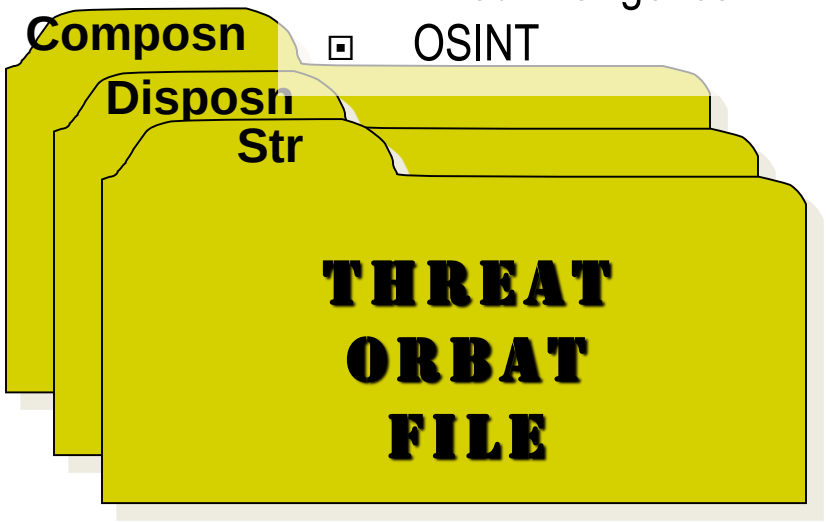
Sub Acty D. Produce ORBAT File

Where can I find such Information?

- Our database
- Our intelligence
- Allied intelligence
- OSINT

- Use all avail int sources to update threat ORBAT

- ORBAT Component:
  - Composn
  - Disposn
  - Str
  - Tactics/Modus Operandi
  - Trg Status
  - Log
  - Effectiveness
  - Electronic/ tech data
  - Misc data



- The threat file should include an assessment of the combat weighting of the threat forces to allow force ratio analysis later in the MAP

Acty 3. Identify Threat Capabilities

- Threat Capabilities - The broad threat's COAs & supporting ops which can influence our msn/ops
- 4 broad tactical COAs:
  - A - Attack
  - D - Defend
  - R - Reinforce
  - R – Retrograde

- Supporting ops incl threat capabilities that are providing sp to the broad COA or may be a specific type of ops; i.e. as fol:
  - Airborne Op
  - Amph Op
  - Int Collection/EW

EXAMPLES:BROAD THREAT CAPABILITIES STATEMENT:

- " THE THREAT HAS THE CAPABILITY TO ATTK WITH UP TO 3 REGT SP BY DAG & 50 SORTIES OF FIXED WING AC "
- "THE THREAT MECH DIV HAS THE CAPABILITY TO SEIZE OBJ NO DEEPER THAN THE LINE AWAN – BARU BECAUSE OF INSUFFICIENT FUEL RES"

EXAMPLES OF BROAD THREAT CAPABILITIES STATEMENT:

"The 204 Mechanised Division is currently located in Kota Bahru, consolidating after securing the Bandar Kota Bahru. The division is at 90 per cent combat effectiveness and is capable of breaking out to resume the offensive in seven days after resupply and detailed reconnaissance. The division is capable of advancing on three axes to contact friendly force defences prior to conducting a deliberate attack using either a penetration or a single envelopment. This may be supported by deep operations using reconnaissance forces, an airmobile battalion and offensive fire."

STEP 3 OUTPUT

- Threat Doctrinal Overlay
- Threat Preferred Tactics & Option
- HVT Matrix
- Broad Threat Capabilities Statements

HOW to conduct IPOE?

1. Define the Operational Environment
2. Describe the Operational Environment Effects
3. Evaluate the Threat
4. Determine Threat COAs

Clarification and Questions