IED and Sniper Defeat:

The Battle Staff Operations Process in a COIN Environment

Base Battle Staff Training Support Package

Version 4 – 13 April 2007

(Proponent: CAC-T)

Administrative Data

- There are no safety requirements
- The risk assessment level is low
- There are no environmental considerations
- Student checks

Purpose

To examine Battle Staff techniques for the defeat of the IED system

References:

- CENTCOM Commander's Counter-Improvised Explosive Device (C-IED) Training Guidance, dated Sep 05
- Center for Army Lessons Learned (CALL), Handbook Number 05-23, Counter IED Tactics, Techniques, and Procedures (TTP), dated Jul 05
- FMI 2-91.4, Intelligence Support to Operation in the Urban Environment, dated Mar 05
- FM 3-0, Operations, dated Jun 01
- FM 3-06, Urban Operations, dated Jun 03
- FM 3-24, Counterinsurgency (Draft, June 06)
- FM (Interim) 3-34.119, IED Defeat, dated Sep 05
- (Draft) Field Manual (FM) 3-90.11 (3-34.112), Combined Arms Mobility, dated Sep 05
- FM 5-0, Army Planning and Orders Production, dated Jan 05
- FM 6-0, Mission Command: Command & Control of Army Forces, dated Aug 03
- FM 3-06.11 Combined Arms Operations in Urban Terrain, 01 Feb 2002

Objectives

Terminal Learning Objective (TLO): Perform Brigade / Battalion Battle Staff operations in a COIN environment

Enabling Learning Objectives (ELO):

- **ELO1:** Apply the principles and techniques of pattern analysis to the operations of an active insurgent cell
- **ELO2:** Explain the operation and function of a Brigade Combat Team (BCT) emerging insurgent TTP's ('IED/Sniper') Working Group
- **ELO3:** Determine targeting priorities, process methods and effects for insurgent operations using predictive tools & methodologies
- **ELO4:** Plan for the use of integrated enablers in support of COIN operations (IED/Sniper)

Outline

- **Defining the Problem**
  - COIN Warfare & Characteristics
  - The Enemy
  - The IED
  - The Insurgent Sniper
- **The Operational Situation and Battle Staff Framework**
- **Role of the Battle Staff in COIN Operations**
  - Observations on Battle Staffs
  - Battle Staffs Organization
- **IED Defeat Tenets Related to Battle Staffs**
- **Analyzing the IED Threat**
  - Models and Applied Analysis
  - Principles & Tools
- **Staff Process and Resources**
  - COIN Enablers
- **Coordinating Offensive Operations**
  - Targeting the insurgent System
- **Gathering Intelligence and Data**

Defining the Problem

COIN Warfare and its Characteristics

COIN Paradoxes

- The more you protect your force, the less secure you are.
- The more force you use, the less effective you are.
- Sometimes doing nothing is the best reaction.
- The host nation doing something poorly is sometimes better than CF doing it well.
- If a tactic works this week, it may not work next week.
- If a tactic works in this province, it may not work in the next.
- Tactical success guarantees nothing.
- The more successful you are, the less force you can use – and the more risk you must accept.
- Most of the important decisions are not made by generals.

FM 3-24 Counterinsurgency
(Draft, June 06)

COIN Imperatives

- Manage information and expectations
- Use measured force
- Learn and adapt
- Empower the lowest levels
- Support the Host Nation

FM 3-24 Counterinsurgency
(December 06)

Defining the Problem

The Enemy

The Enemy

Increased Violence

Islamic Symbolism

Loose Leadership

External Facilitators

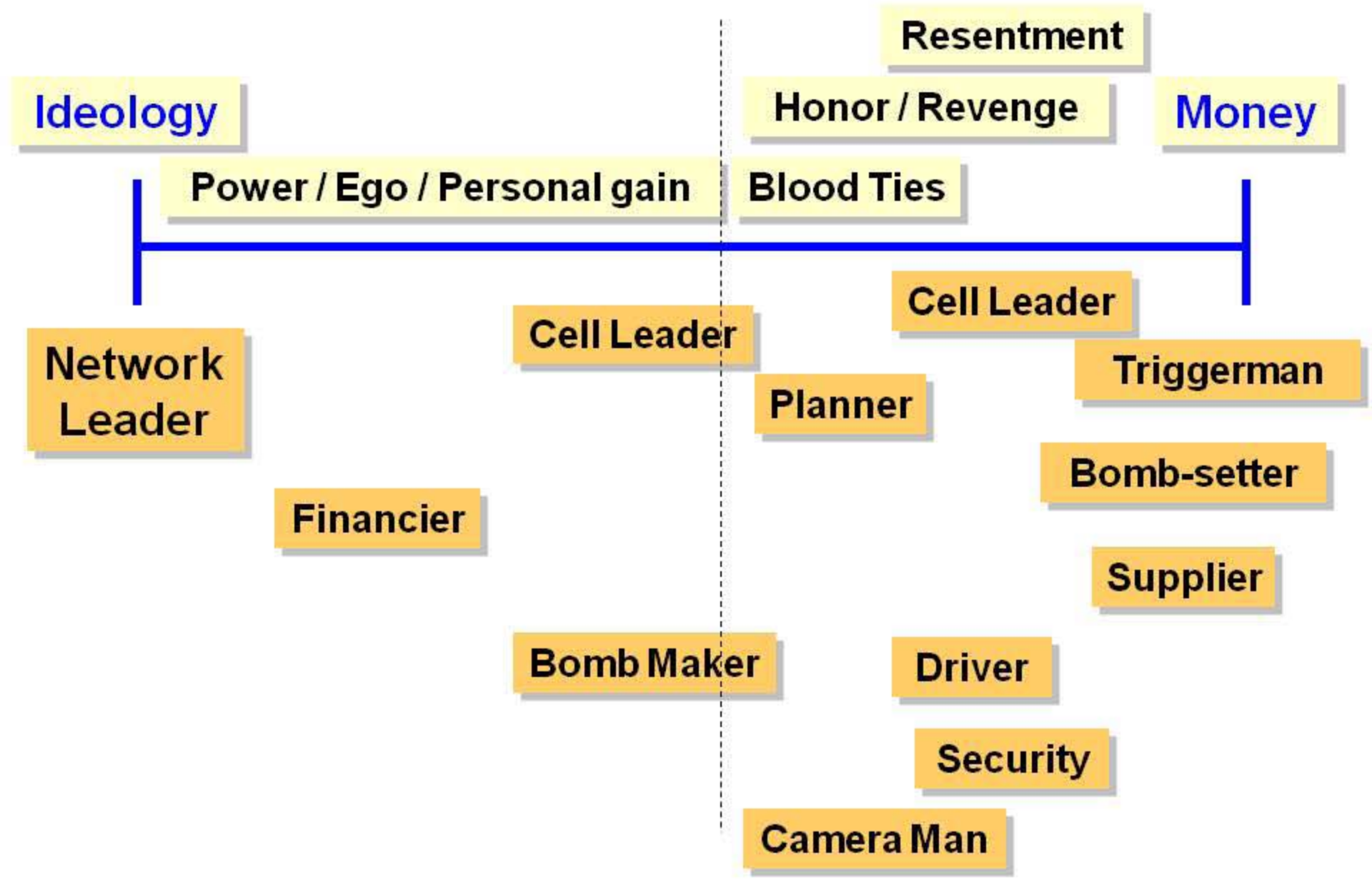
Enemy Qualities Enabling Success

- Has innate understanding of environment
- Moves freely and blends within the population
  - Hides easily from us but not his neighbors
- Has the ability to claim or play upon cultural and religious homogeneity and the natural suspicion of the motives of outsiders that we cannot
- Is restricted only by his own ingenuity and has the freedom to change his definition of success
- Is not bound or restricted by law or social barriers to behavior
- Goes where he has been successful
- Has favorite areas of operation
- Will continue to use favorite areas until they are killed (we control) or simply change their mind (they control)
- Uses probability analysis (result of his reconnaissance to commit resources) against specific targets on days or times of most likely occurrence

Enemy Tactics

- Create tension between civilians, government, and indigenous security forces
- Identify & exploit friendly patterns
- Conduct harassing attacks against Forward Operating Bases (FOB)
- Conduct increasingly complex attacks
- Employ continuous, patient action
- Form temporary alliances with other groups
- Capitalize on attacks by 'out-of-towners'
- Target units appearing intimidated or weak

Enemy Motivations



Understanding the Threat in Order to Anticipate

Groups

- FRMs
- Militant Islamists
- Foreign Jihadists
- Tribal groups
- **Angry / Aggressive populace**
- **Gangs / Thugs**

Motives

- Subvert or overthrow Government
- Establish an Islamic state
- Resist occupation
- Achieve status associated with martyrdom
- **Power, money, pleasure, excitement**
- **Sense of gaining localized prestige or power**

Power Base

- Political ideology
- Religious ideology
- Shared solidarity
- **Personal relationships**
- **Resources gained through embezzlement, coercion or theft (money, weapons & material)**

Defining the Problem

The IED

Improvised Explosive Device (IED)

Definition

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 non-military components.

JP 1-02 Department of Defense Dictionary of Military and Associated Terms
AAP-6 (2006) - NATO Glossary of Terms and Definitions

IEDs: An Evolving Threat

Command Wire IEDs

Radio Controlled IEDs

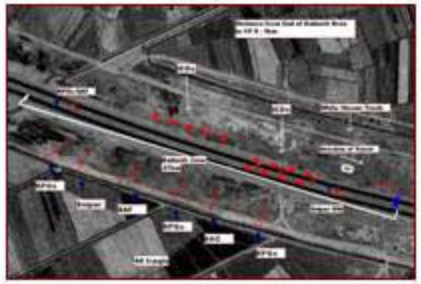
Icon Vehicle Attacks

Vehicle Borne IEDs (VBIED)

- Evolving
  - Learning
    - Innovating

Explosively Formed Projectiles (EFP)

Improved Concealment



Complex Ambushes

Targeting First Responders

IED Process

Bomb Maker

Mule

Mule

IED Components

Execution Support

Site Recon

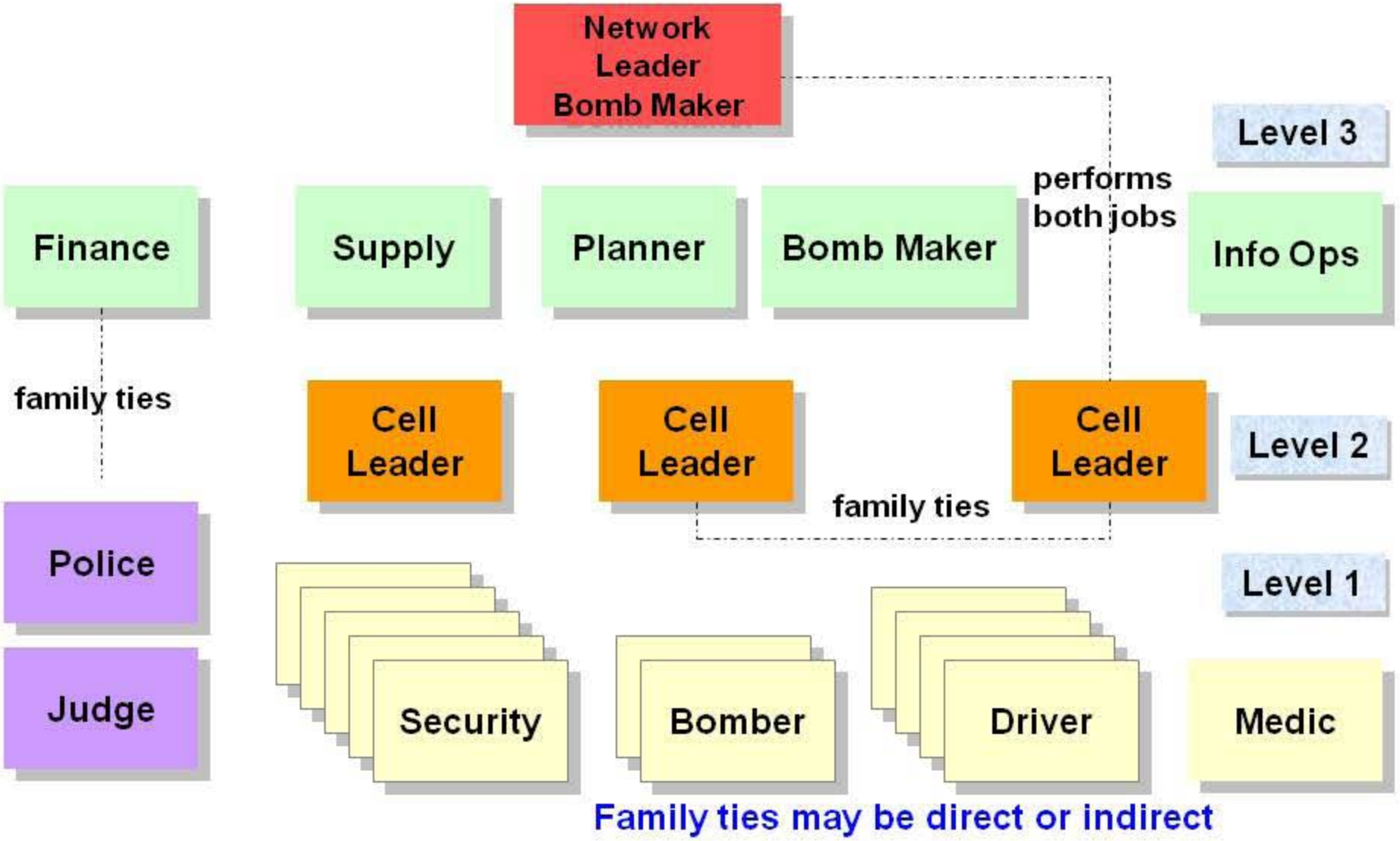
Site Prep

Placement

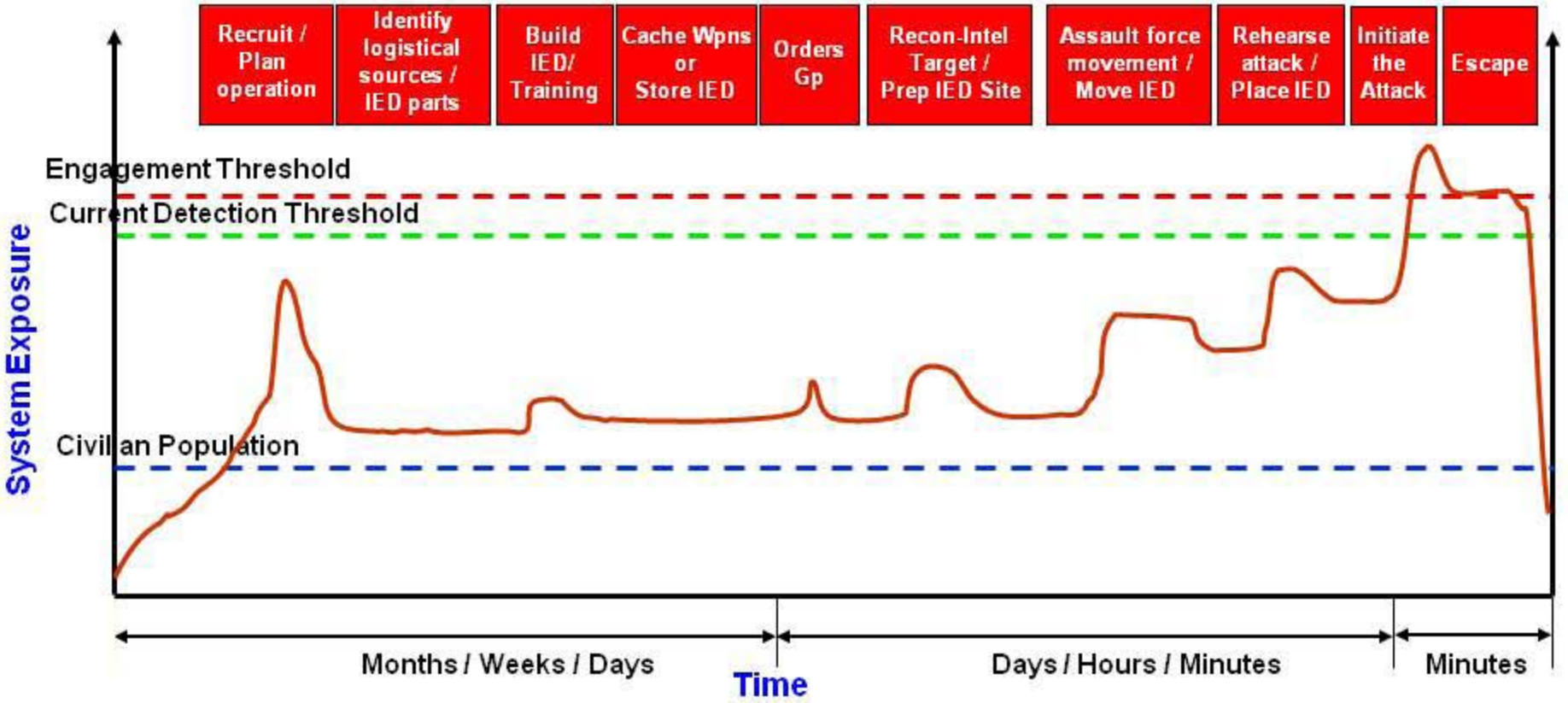
Triggerman

- Organized into cells
- Dependent on group structure, emplacers may be specialists or multi-rolled

Typical IED Cell Structure

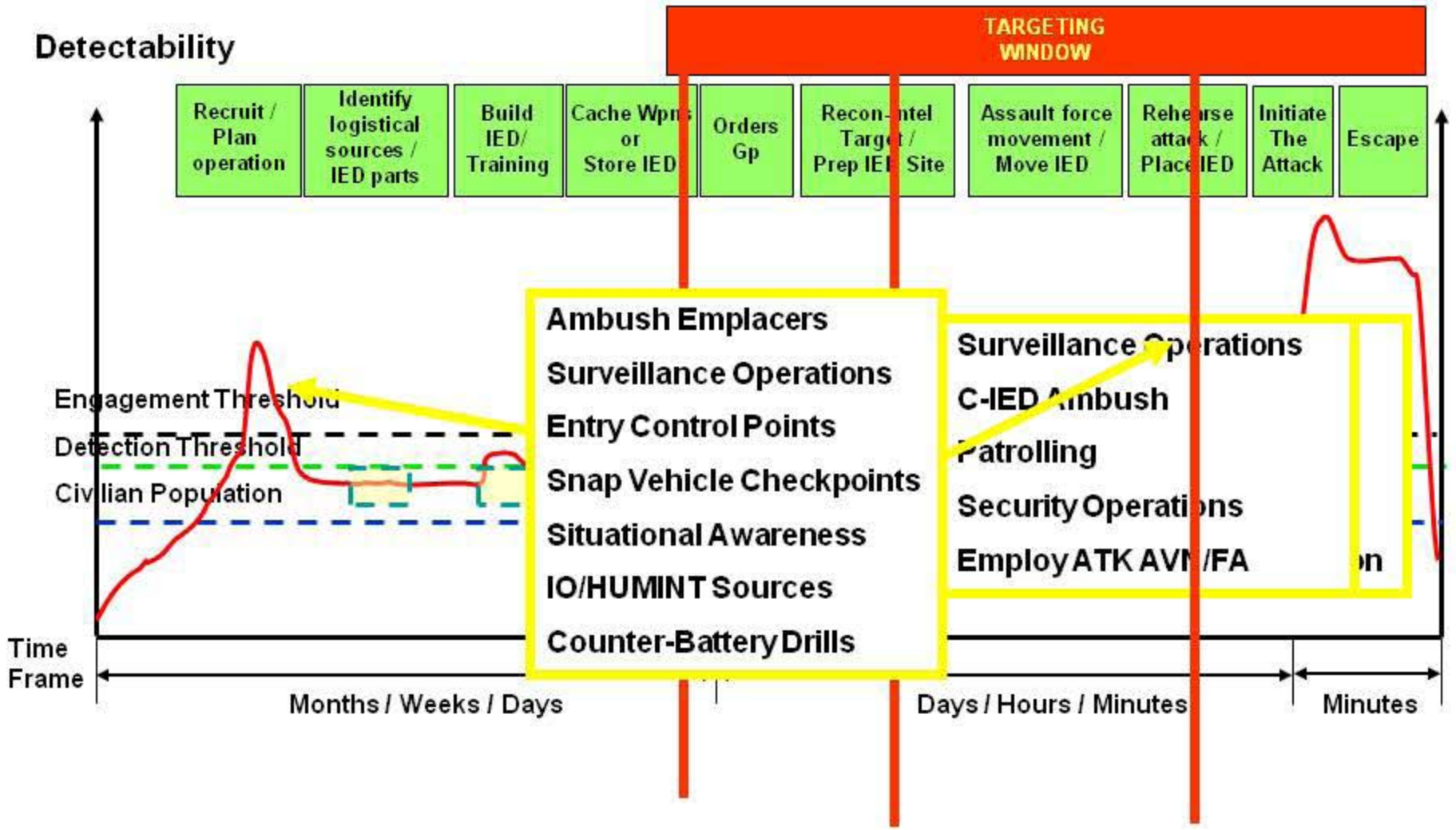


Chronology Model of IED System

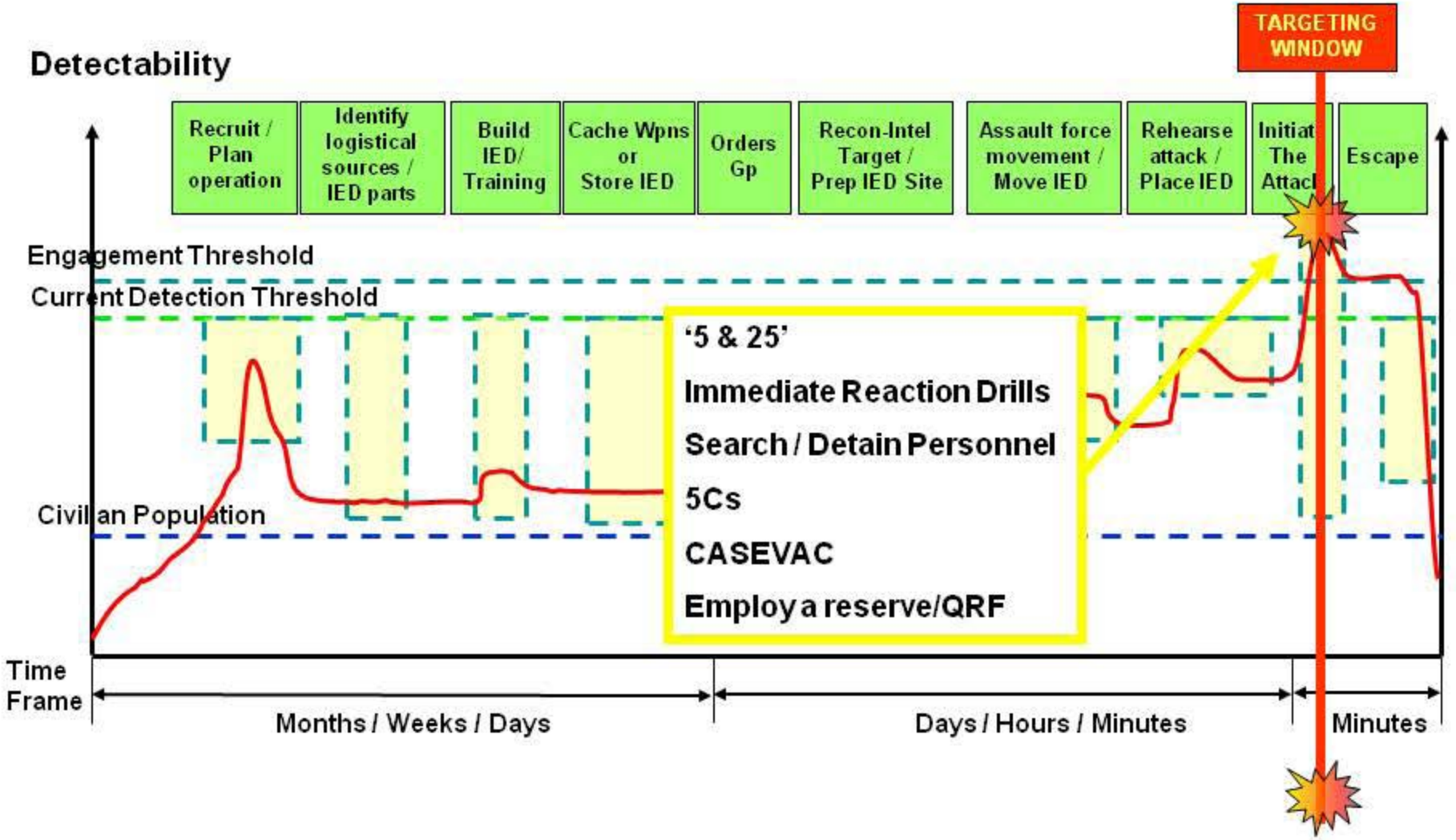


This model illustrates the sequence of the IED System operation in relation to time. The chart illustrates the visibility of the IED system in relation to the civilian population, the point at which our units currently encounter the system, and the point at which we take action.

Offensive Counter Insurgent Operations



Reacting to the Insurgents



Defining the Problem

The Enemy Sniper

Enemy Sniper

Definition

An individual skilled in field-craft and marksmanship who provides precision fires at selected targets from concealed positions.

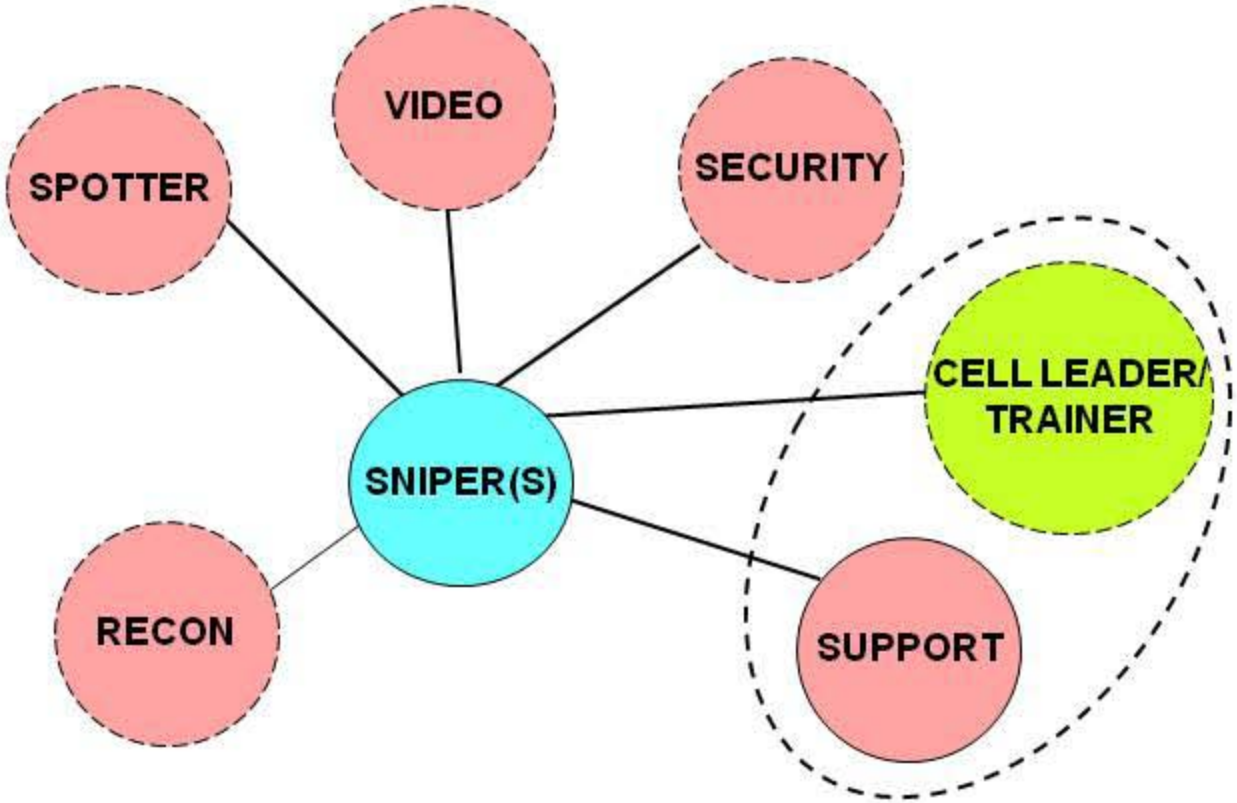
FM 3-06.11 (Combined Arms Operations in Urban Terrain)

Classifications:

1. Well Trained Sniper
2. Trained Marksmen
3. Armed Irregulars

Typical Sniper Cell Structure

Concept sketch for illustrative purposes



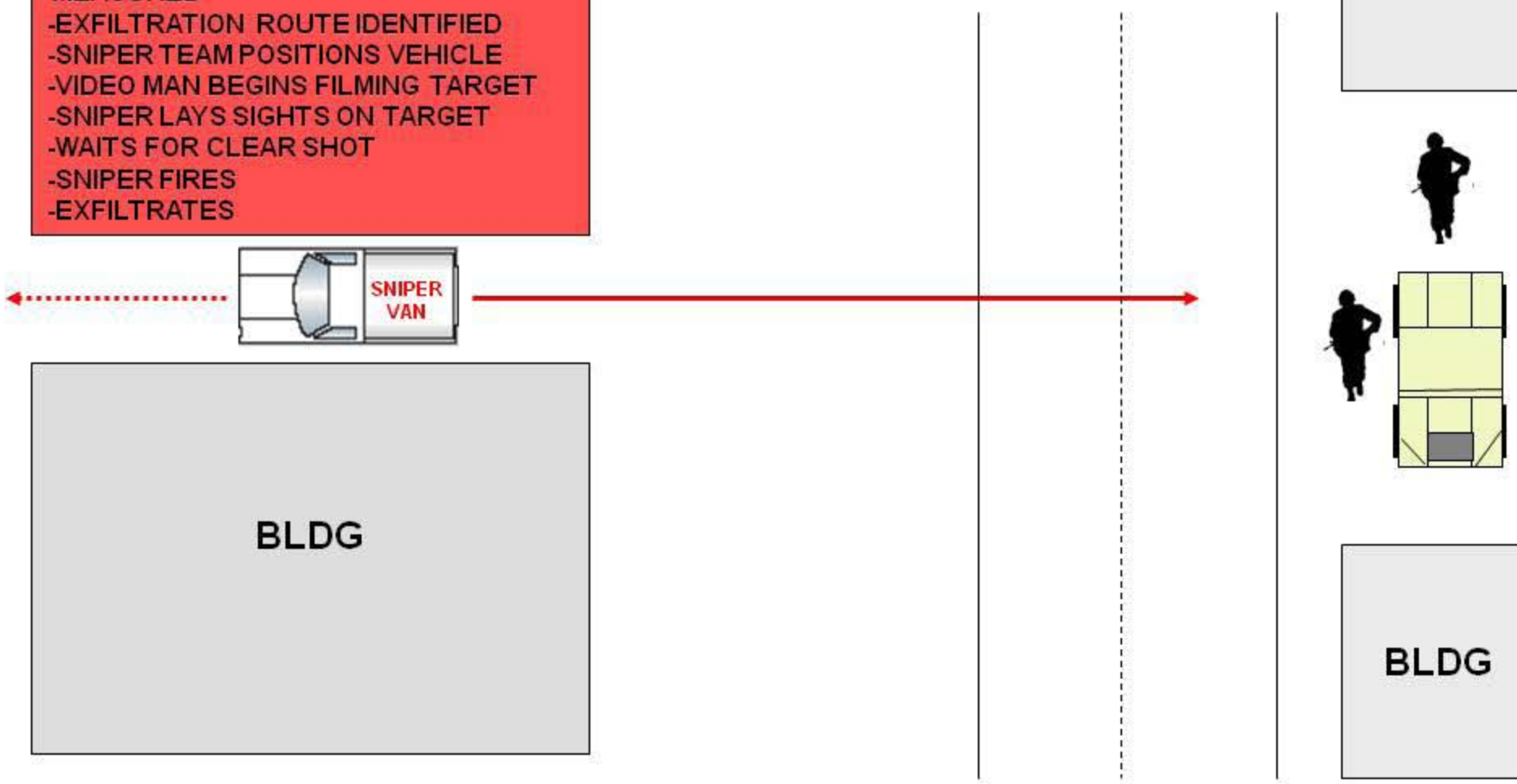
Leader/Trainer usually an experienced sniper. Thought to perform most support functions and coordinate multiple sniper action elements.

Example Enemy Sniper Employment

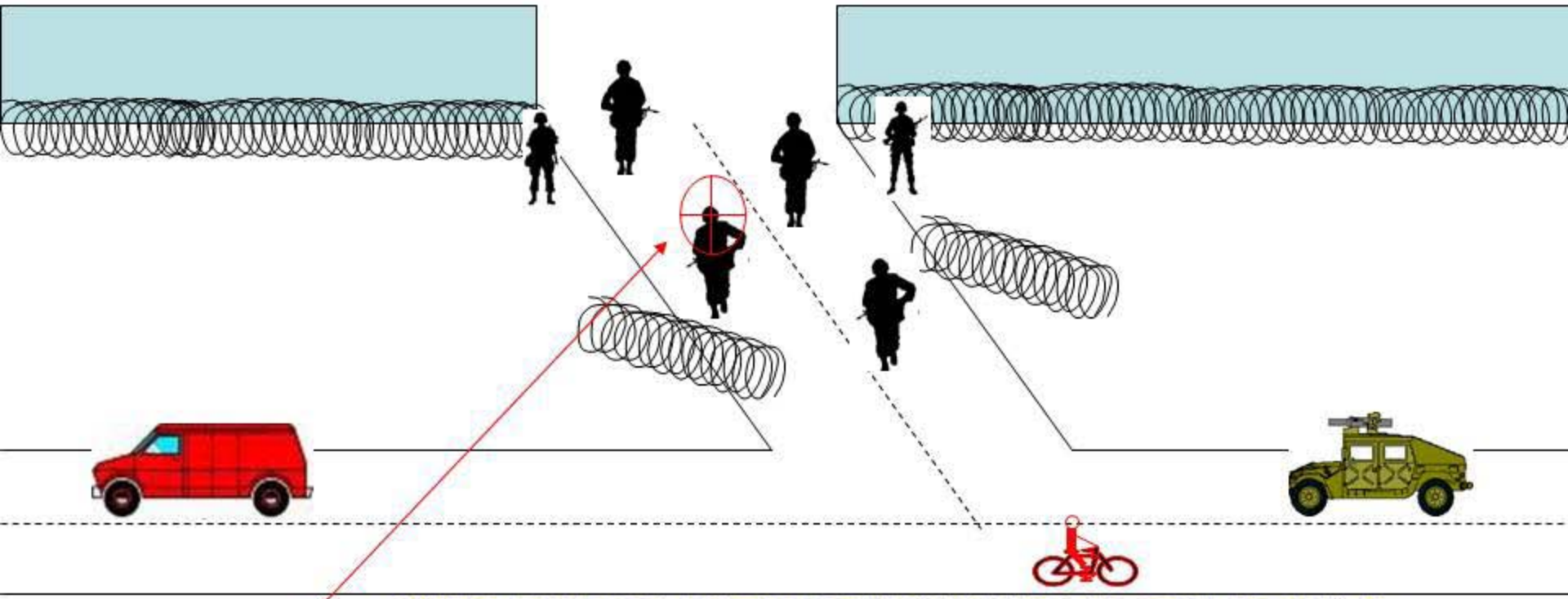
Example Enemy Sniper Employment

US CHECKPOINT

-PRE-SELECTED TARGET
  -KNOWN CHECKPOINT LOCATION
  -INTERSECTION
-RANGE TO TARGET ESTIMATED OR MEASURED
-EXFILTRATION ROUTE IDENTIFIED
-SNIPER TEAM POSITIONS VEHICLE
-VIDEO MAN BEGINS FILMING TARGET
-SNIPER LAYS SIGHTS ON TARGET
-WAITS FOR CLEAR SHOT
-SNIPER FIRES
-EXFILTRATES



DISMOUNTED PATROL RETURNING THROUGH GATE

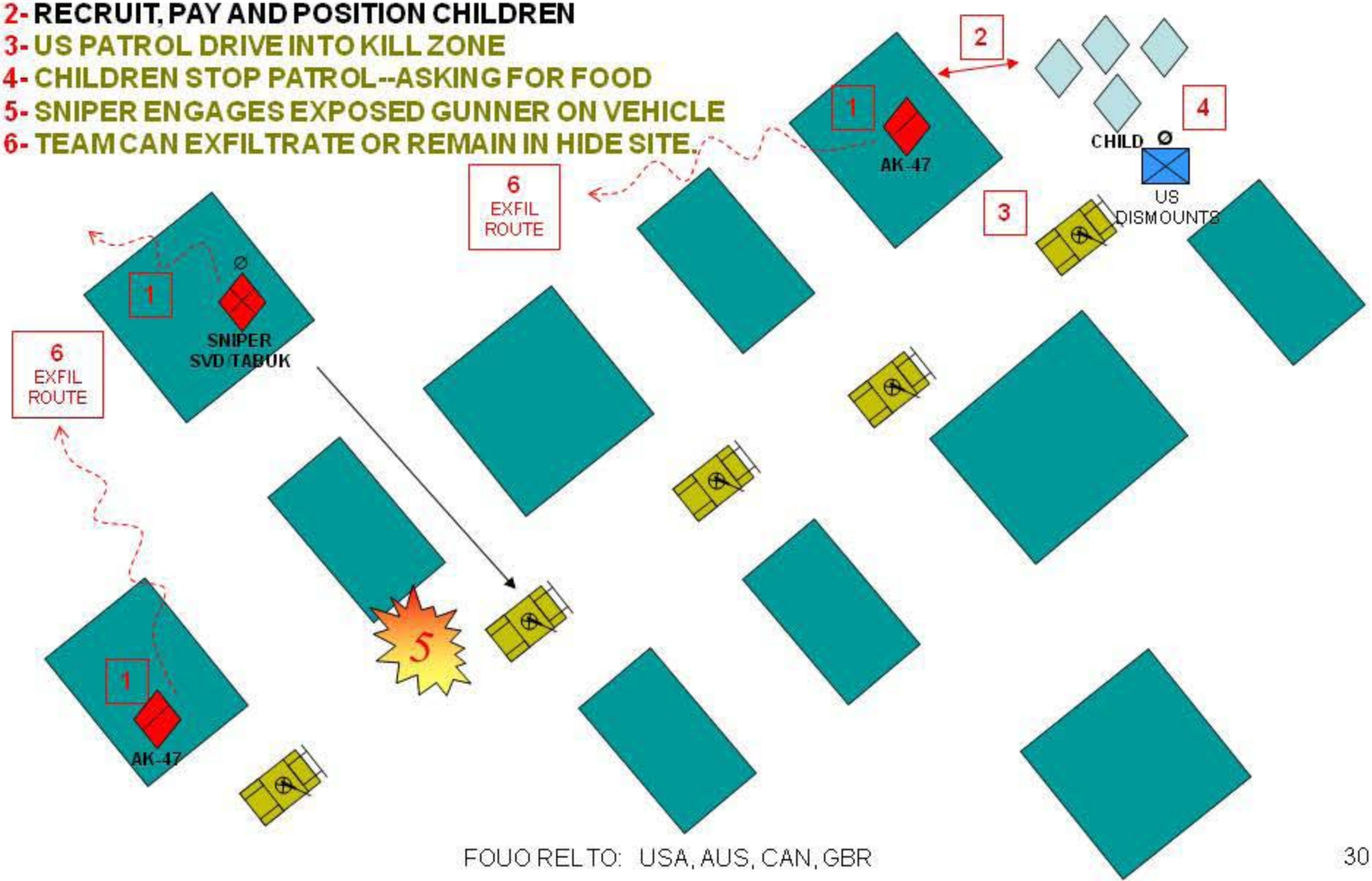


- SNIPER TEAM LOCATED IN BACK OF VEHICLE (SHOOTER, SPOTTER, DRIVER).
- MOTOROLA RADIO USED TO COMMUNICATE WITH MOBIL OBSERVATION POSTS (OPs)--BIKE, VAN, WHO ALSO SET PACE OF TRAFFIC.
- SHOTS ARE TIMED BETWEEN VEHICLES.
- OP VAN STOPS TO BLOCK LINE-OF-SIGHT TO SHOOTER.
- OP VAN CREATES NOISE TO MUFFLE SHOTS (HORN, ACCELERATOR, BRAKE).
- SNIPER WILL TAKE MULTIPLE SHOTS AT FIRST RESPONDERS--SNIPER IS CONFIDENT IN HIS HIDE SITE AND HIS SKILLS--DOES NOT IMMEDIATELY WITHDRAW.

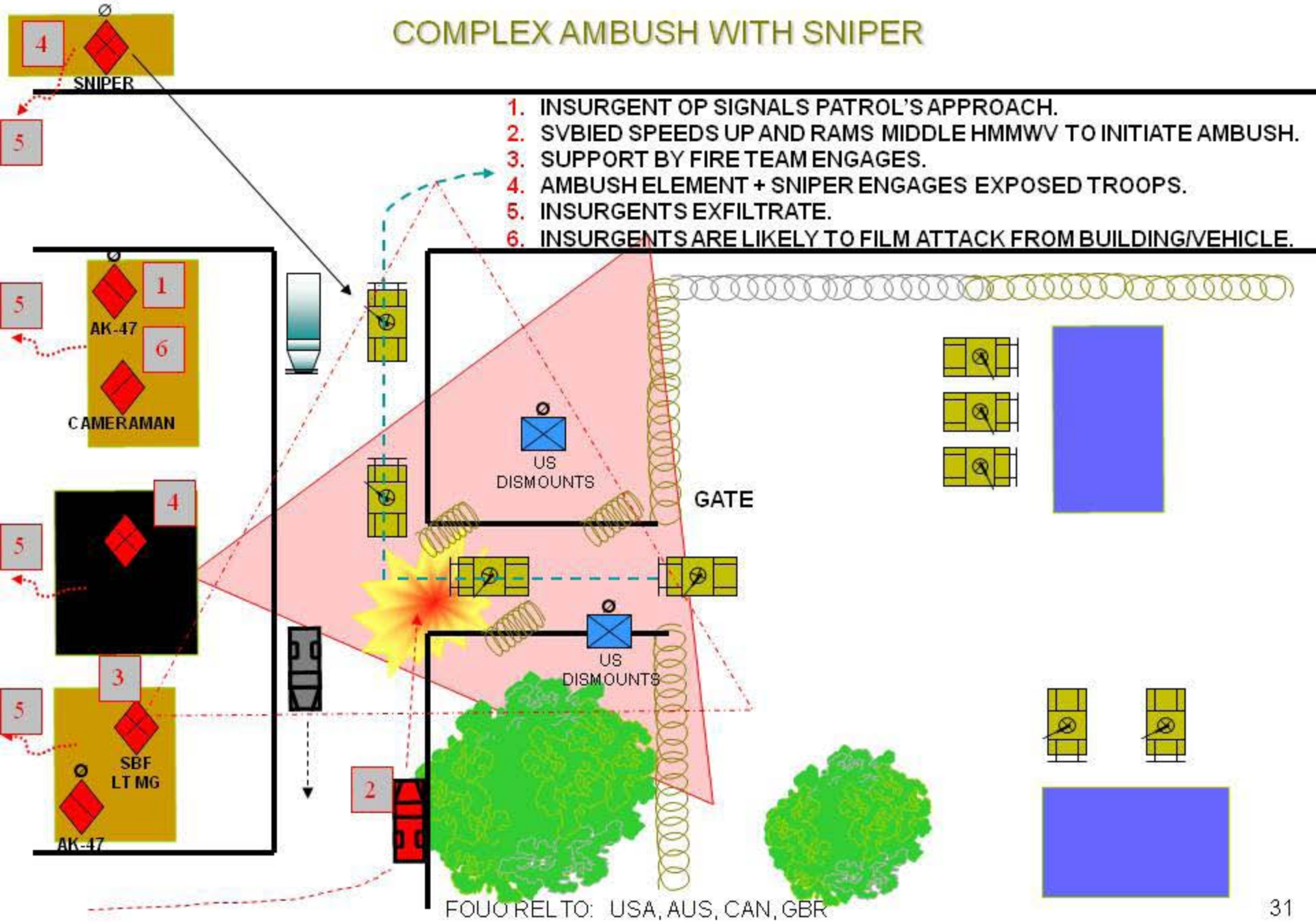
MOUNTED PATROL HALTED BY CHILDREN

(WITTING)

1- SNIPER TEAM & SECURITY POSITIONED
2- RECRUIT, PAY AND POSITION CHILDREN
3- US PATROL DRIVE INTO KILL ZONE
4- CHILDREN STOP PATROL--ASKING FOR FOOD
5- SNIPER ENGAGES EXPOSED GUNNER ON VEHICLE
6- TEAM CAN EXFILTRATE OR REMAIN IN HIDE SITE.

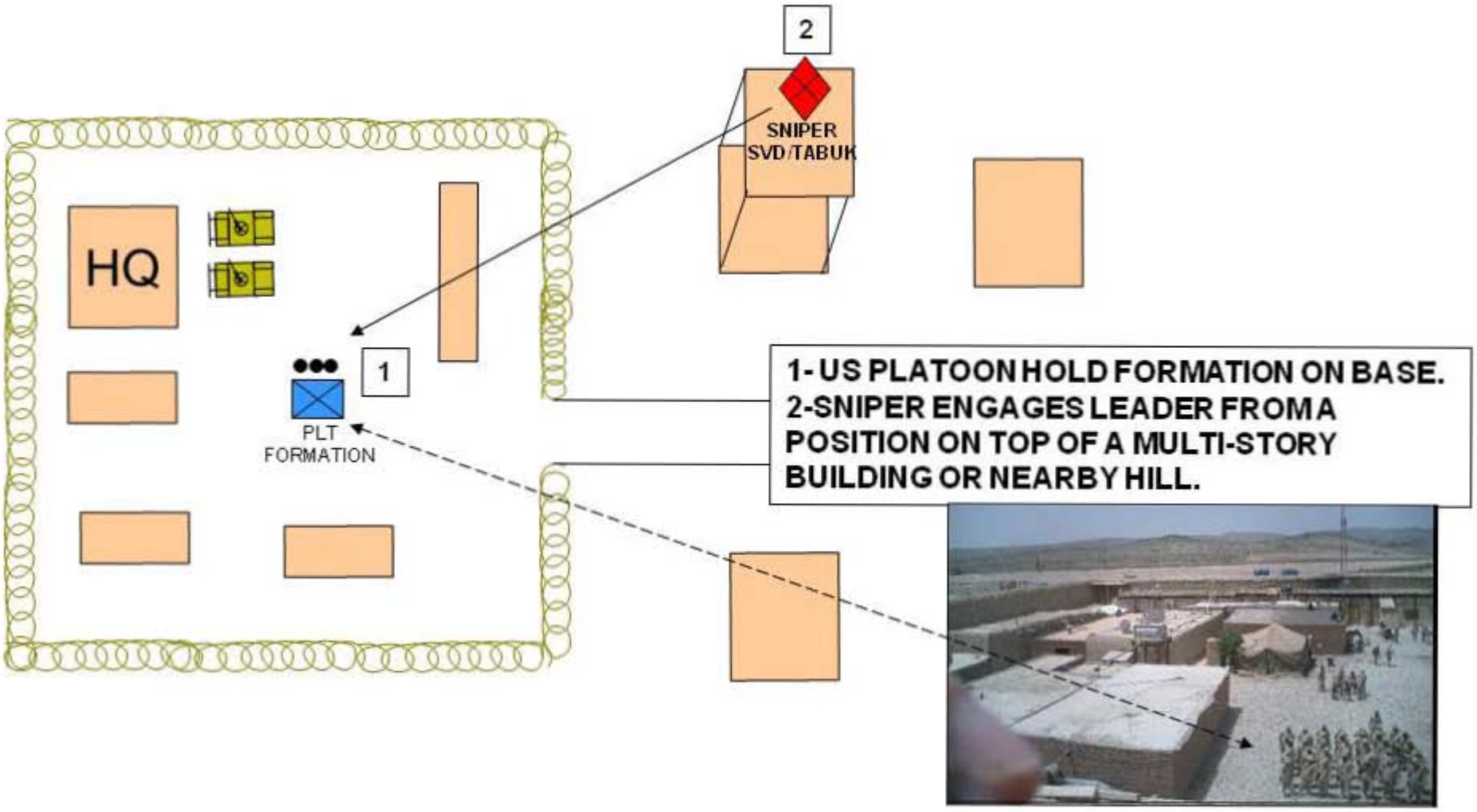


COMPLEX AMBUSH WITH SNIPER



1. INSURGENT OP SIGNALS PATROL'S APPROACH.
2. SVBIED SPEEDS UP AND RAMS MIDDLE HMMWV TO INITIATE AMBUSH.
3. SUPPORT BY FIRE TEAM ENGAGES.
4. AMBUSH ELEMENT + SNIPER ENGAGES EXPOSED TROOPS.
5. INSURGENTS EXFILTRATE.
6. INSURGENTS ARE LIKELY TO FILM ATTACK FROM BUILDING/VEHICLE.

TROOP FORMATION



Why Snipers?

- Strategic IO implications
  - David verses Goliath (Arab warrior vs infidel occupiers)
  - Less Collateral Damage (Precision targeting)
- Cost Effective
- Survivability
- Impacts Morale

The Sniper's Role in Information Operations (Why a tactical event has Strategic implications)

In the 21st century insurgent sniper wars will be fought more with the video camera and information technology than the sniper's rifle.

"The psychological impact of sniping has received little attention in the overall scheme of war. ***The psychological impact can ruin the fiber and morale of an entire army***. ***The U.S. military has only recently recognized*** the ***psychological impact of sustained combat***, although the sniper has always contributed as much to fear as he has to fighting. Operational planners may consider this PSYOP capability when planning sniper missions, especially when using PSYOP in unconventional warfare where it plays a vital role." *FM 3-05.222 (TC 31-32), Special Forces Sniper Training and Employment, April 2003.*

"Why should I hunt lions, when there are so many sheep?"
-- *old Afghan proverb*

The Sniper's Role in Information Operations
(continued)

Iraq

- In a widely disseminated propaganda video of Iraqi sniper attacks on U.S. troops, the narrator (an insurgent) who describes himself as the "brigade commander" states that--

  "The idea of filming the (result of) operations is very important because the scene that shows the falling soldier when hit has more impact on the enemy than any other weapon."

- An insurgent sniper training manual posted on the Internet contained the tips: ***"Killing doctors and chaplains is suggested as a means of psychological warfare."***
- It also calls for targeting enemy snipers and surveillance teams because the lesson was learned "***in Fallujah, where mujahideen were handicapped more by U.S. Marine snipers than by air raids or other artillery or indirect fire."***

Examining the Problem Set

- IEDs and Snipers are a battlefield condition, not the mission.
- We do not own the roads, we share them.
- Setting and triggering IEDs is largely a political, rather than ideological activity and, as such, is a criminal problem.
- Campaign planning and financing of IED operations are ideologically motivated.
- Defeating the insurgent (IED / Sniper) system means identifying the members of a network before they act by dissuading them, eliminating their ability to hide within the population and by killing or capturing them. Intelligence and exploitation lead to this end.
- The operational environment includes the enemy as a discrete part of the population.
- The population is the center of gravity. It provides key terrain for unit effects.
- We gain understanding of the enemy by understanding the operational environment.

Examining the Problem Set II

- IEDs are not just a weapon.
- Conditions and enemy are different in every Area of Operations (AO).
- Enemy Tactics, Techniques, and Procedures (TTPs) migrate and spread throughout the world.
- "We will not eliminate the IED threat until we eliminate the insurgency."

3ID ADC(M)

Sustaining the Effort

- The enemy will continue to exploit observed weakness in our defense.
- Training and incorporating indigenous security forces into IED Defeat Operations and Sniper Defeat Operations can reduce the strain on own forces and enhance chances for mission accomplishment.
- Killing or capturing IED emplacers and Enemy Snipers will not make the threat go away. Such an approach must be supported and exploited with solid CMO and Intelligence Operations.

The Operational Situation and the Battle Staff Framework

CENTCOM Commander's Guidance

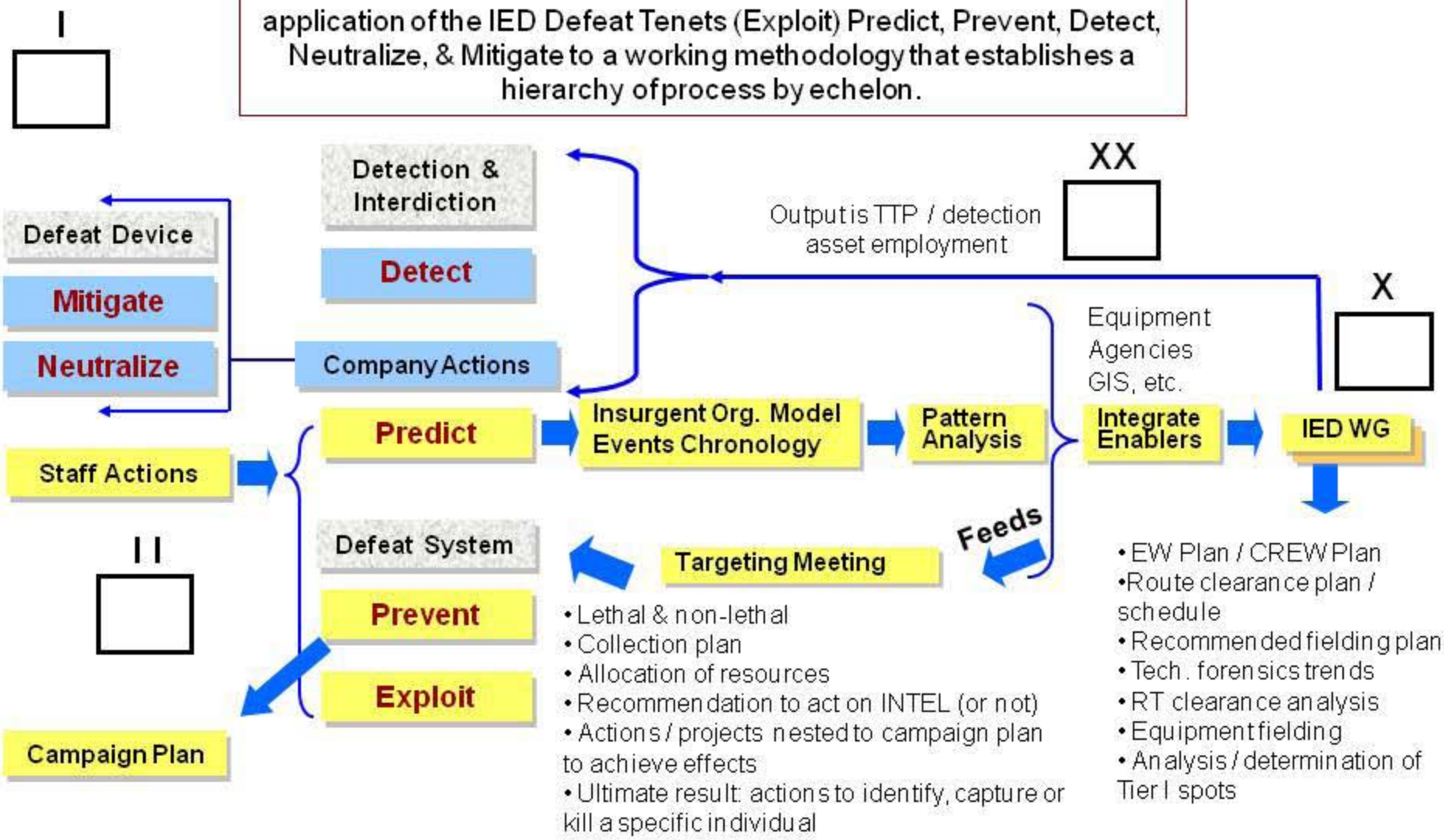
Brigade Combat Team and Higher C-IED Related Battle

Staff tasks:

- Conduct operations to defeat the IED system and to defeat the IED
- Establish an IED defeat task force, cell, or board in every headquarters
- Integrate C-IED enablers into all operations

IED Defeat: Battle Staff Framework

CENTCOM Commander's Guidance – September 2005
resulted in
application of the IED Defeat Tenets (Exploit) Predict, Prevent, Detect, Neutralize, & Mitigate to a working methodology that establishes a hierarchy of process by echelon.



Threat Defeat Tactics

- **Patrols**
  - Reconnaissance patrols to feed intelligence development
  - Sniper and Scout LP/OP
  - Specific objectives: people, places, things, information
  - IED hunting patrols to mitigate risk
- **Ambushes**
  - Turn our patterns to our advantage
  - Make IED emplacement or Sniper employment high risk for insurgents
  - Employ Small Kill Teams (SKT)
- **Raids**
  - Focused on specific targets based on intelligence
  - Insurgents are certain you will act, but uncertain of when & where
- **Information Operations & Civil-Military Operations (CMO)**
  - Lower the detection threshold for identifying insurgents
  - Use cultural awareness to create offensive opportunities

Our Patterns & Vulnerabilities

- Recent, (2006) Operational Analysis: In over 95% of attacks, friendly units had set clear patterns of operation, response, or passive security.
- Units establish patterns, often in the form of Standard Operating Procedures (SOP) and standardized TTPs, and do not recognize when they raise their own risk levels.
- Units have a tendency to not change their favorite TTPs until the enemy forces the issue.

Enemy Patterns and Vulnerabilities

- Too much of our IED / Sniper Defeat emphasis is on reaction to attack or force protection instead of using initiative to reduce number of attacks.
- The enemy also has patterns.
- Emplacement / Employment is the weak link.
  - Fish are vulnerable when out of water.
- Emplacement can be interdicted at unit level.
  - It puts pressure on the enemy network.

Hierarchy of Success

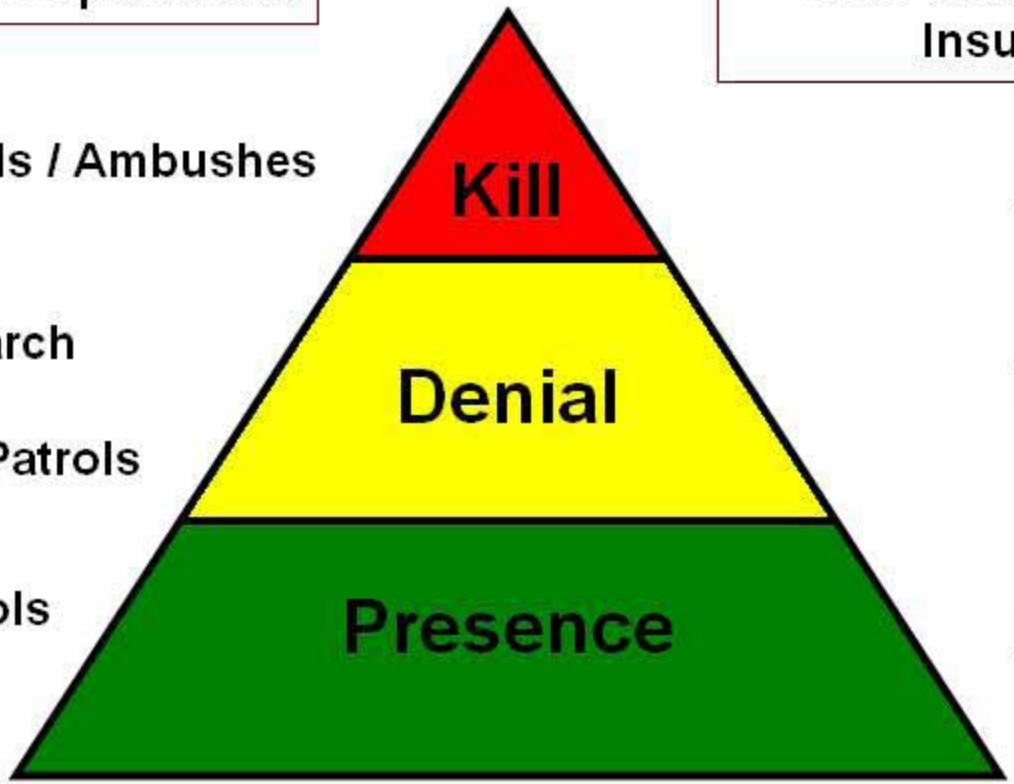
Effect on the Enemy

Type / Volume of Operations

- Snipers / Raids / Ambushes
- Kill / Capture

- Cordon & Search
- TCP / Ops
- Dismounted Patrols

- Mounted Patrols



Own Casualties from Insurgents

Low

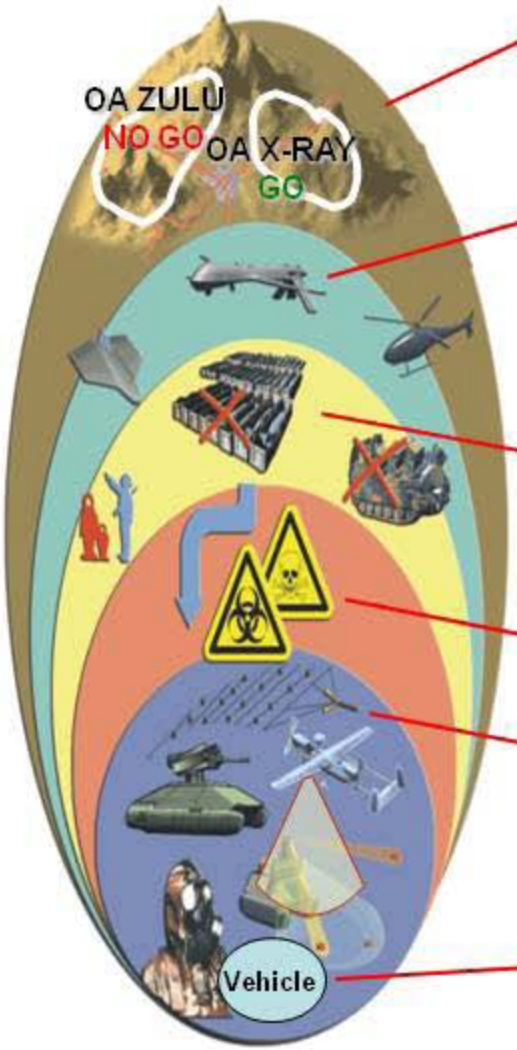
Medium

High

Role of the Battle Staff in COIN (IED Defeat) Operations

Observations on Battle Staffs

IED Defeat Tenets



- **PREDICT** actions and circumstances that could affect the ability of the force to maintain momentum
- **DETECT** indicators of impediments or lack of impediments to battlefield mobility early; identify alternatives and establish surveillance
- **PREVENT** potential impediments to maneuver from affecting battlefield mobility
- **AVOID** impediments to mobility of the force
- **NEUTRALIZE**, reduce, or overcome (breach) impediments to battlefield mobility that cannot be prevented or avoided
- **PROTECT** soldiers and vehicles against effects of explosives

EXPLOIT

ACCURATELY ANTICIPATE IED ACTIVITIES Predict, thru pattern analysis, to position C4ISR to confirm or deny enemy actions. Use the information to interdict and disrupt the IED System

PREDICT

RESTRICT PRODUCTION Deny the bomb maker of sanctuary, guidance, finances, support, targets, supplies and life.

PREVENT

RESTRICT EMPLACEMENT Restrict the ability of enemy combatants to emplace IEDs through the use of right [illegible]ce, active combined [illegible], UAVs, use of sniper [illegible]ED threat areas, control [illegible]emy Ammunition (CEA), intelligence, and CA work with local nationals.

DETECT

NEUTRALIZE

MITIGATE

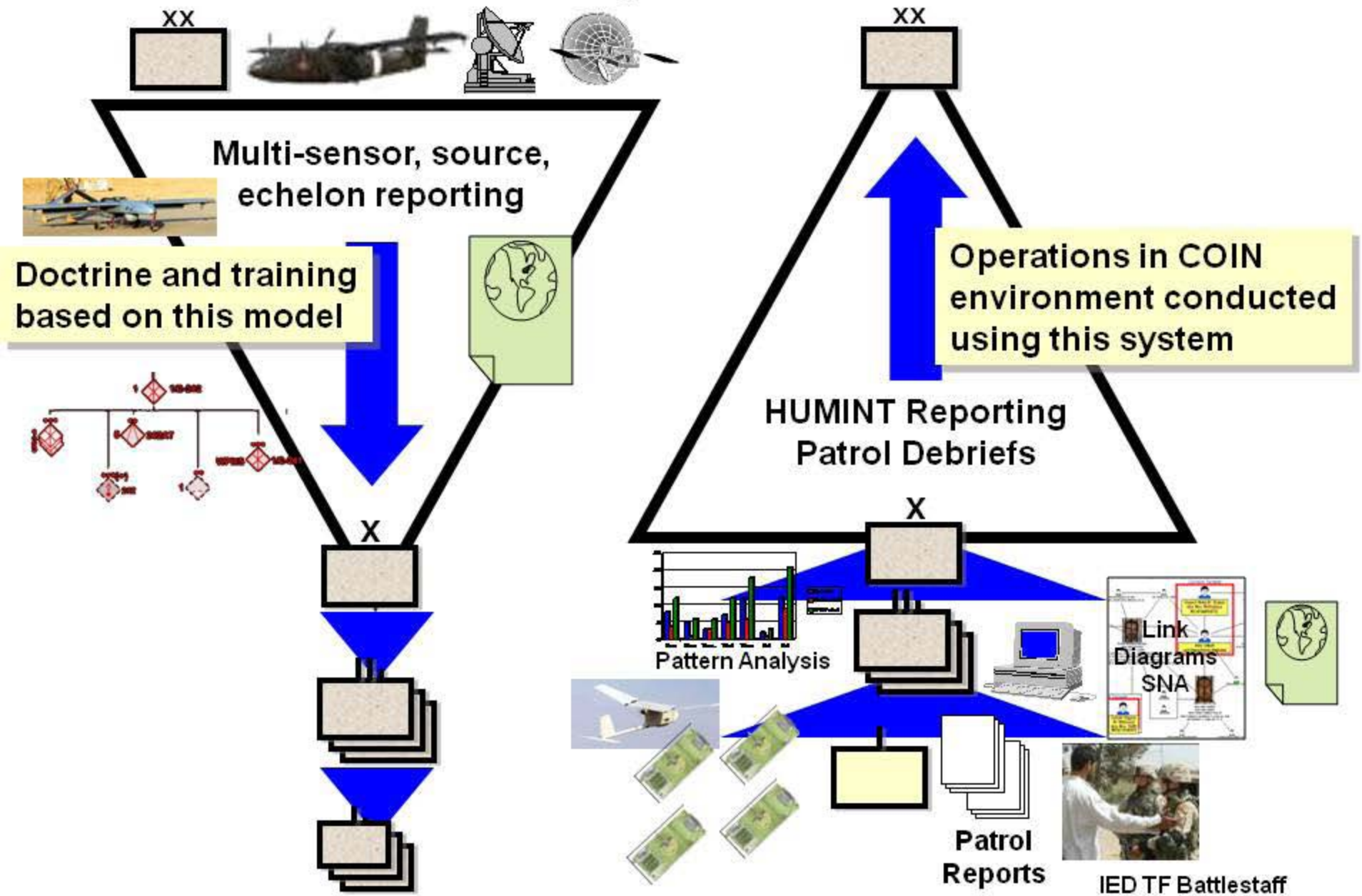
DEFEAT THE DEVICE
Detect and neutralize IEDs through aggressive route clearance and maintenance, a systematic sweep program, and the use of IED jamming devices. Increase Soldier protection through the distribution of hardened vehicles.

Staff's Role

FUNDAMENTALS OF ASSURED MOBILITY | **TENETS OF IED DEFEAT** | **IED DEFEAT OPERATIONS**

REF: JIEDDO & FMs 3-34 / 3-90.11

Intelligence Flow



Sub-unit Expectations

- Provide unity of effort & command
- Assign clear responsibilities
- Allocate resources – especially intelligence
- Delegate responsibility and control
- Timely sharing of information & intelligence
- Assign responsibility for routes
- Anticipate requirements

Higher HQ Expectations

Within an assigned AO:

- Execute transitions with host nation security forces
- Provide unity of effort / offensive focus
- Execute / coordinate Information Operations
- Execute / coordinate CMO
- Control routes in your AO
- Disseminate intelligence
- Anticipate consequences

Tactical Expectations – Battalion (BN)

- Continuous coordination with other units and crosstalk within BDE
- Execute CMO
- Combined operations with indigenous forces
- Collect / process / disseminate intelligence
- Pattern analysis & anticipation
- Transition quickly
- Anticipate requirements
- Anticipate consequences
- Targeting
- Tactical techniques – BN
- Command and Control (C2) distributed operations
- Anticipate requirements
- Intelligence summaries & Fragmentary Order (FRAGO)
- Route reconnaissance
- Reaction force operations
- Contracting – to provide tactical advantage (e.g., roadside clearance or facilitation of information flow)
- Detainees

Commander's Expectations

- Focus on the commander's tactical problem – not staff stovepipes
- Understand and act within the Commander's intent (must be IO focused), objectives, and priorities
- Anticipate decisions and enemy actions
- Recommend feasible options to meet higher / subordinate expectations

What We See in Theater - Staff

- Lack of offensive approach to C-IED operations
- Emphasis is on reaction versus a plan of action
  - Little time spent on what to do next
- Emphasis on staff internal concerns instead of actions outside the wire
- Fixation on process / product instead of communication and intent
- Lack of shared awareness of current / future situation

Observations about Staffs

- The Staff needs to integrate
  - Each staff section has a stovepipe view of the fight
  - Intelligence Officer (S2) & Operations and Training Officer (S3) should integrate
- Targeting must be continuous
  - Not a daily / weekly / monthly meeting
  - Must be a mindset of finding and killing the enemy
  - Applies to friendly interaction as well
  - Act while information is current
  - S3 must leverage assets to make IO happen IAW Commander's intent
- Tactical Operations Center (TOC) layouts do not facilitate proper C2 requirements
- Having the right staff make-up is critical

Why must the staff train differently?

Characteristics - Pre-War Training

- Doctrinally precise tasks and conditions
- Doctrinally based scope & task organization
- Centralized planning & control in response to enemy actions
- Doctrine based opposing force
- Top-down intelligence direction and products
- Detailed planning & preparation for a discrete, short duration, collective unit operation
- Standardized performance of staff process, procedure, and products as the measures of effectiveness

Characteristics - Operations in Iraq

- Nonstandard, ambiguous tasks and conditions
- Expanded mission scope & resource challenges
- Concurrent, decentralized, continuous operations to maintain initiative over enemy
- Adaptive, cellular enemy
- Bottom-up intelligence development and initiative in application
- 24 / 7 / 365 operations requiring rapid decisions and execution information to subordinates
- Staff teamwork and skills at communication, anticipation, judgment, agility, as the measures of effectiveness
- Effective de-briefing format

From a Marine Corps Captain

"Staffs must be able to collect information and turn it into intelligence - fast. Often what we've seen is our Marines are great at killing the enemy but our inefficiencies and sloppiness at the staff planning level (company on up) are not putting them into a situation to exploit opportunities quickly."

Staff Personnel

Command Post (CP) personnel must be able to visualize from radio traffic what is going on, what is likely to occur, what is needed, what must be done, and then have the intelligence, imagination, and initiative to do what is necessary. . . Personnel assigned to the CP must be selected with care. Competent, experienced, mature, intelligent captains and sergeants should comprise the bulk of the CP personnel.

Commander, 1st Bde, 1ID
Vietnam, 1967

Role of the Battle Staff in COIN Operations

Organization of Battle Staffs

COIN (IED Defeat) Operations – Battle Staff Tasks

- Conduct IED-related battle tracking and information management
- Conduct terrain visualization
- Conduct pattern analysis – REDFOR and BLUFOR
- Conduct insurgent network analysis
- Conduct IED technical analysis
- Understand capabilities and integrate joint IED Defeat enablers
- Conduct IED Defeat training
- Conduct IED Defeat Intelligence, Surveillance, and Reconnaissance (ISR) planning

COIN (Sniper Defeat) Operations – Battle Staff Tasks

- Conduct Sniper-related battle tracking and information management to include SKT Tracking
- Conduct terrain visualization
- Conduct pattern analysis – REDFOR and BLUFOR
- Conduct insurgent network analysis
- Conduct Sniper post shot technical analysis
- Understand capabilities and integrate joint Sniper Defeat enablers
- Conduct Sniper Defeat training
- Conduct Sniper Defeat Intelligence, Surveillance, and Reconnaissance (ISR) planning

Sniper Defeat Battle Staff Considerations

Sniper Employment Considerations

- KACTIS-D
  - KNOWLEDGE - of sniper capabilities and limitations.
  - ADVISE - the supported unit commander.
  - COORDINATE - all aspects of the sniper mission.
  - TRAINING - should be realistic, varied, challenging, and mission oriented.
  - ISSUE - combat orders to teams.
  - SUPERVISE - planning, preparation, and rehearsals.
  - DEBRIEF - all members of the team upon completion of the mission.

Sniper Defeat Battle Staff Considerations

Sniper Counter-Measures

- After the enemy Sniper threat has been identified and classified the proper countermeasures must be emplaced. The two types of countermeasures are;
  - **Passive**; Includes all actions taken by the unit to reduce the likelihood of casualties inflicted by the enemy sniper. -Avoid setting routines or patterns.
  - **Active;** Includes all actions taken that directly relate to the elimination of the enemy sniper threat.

Sniper Defeat Battle Staff Considerations

Sniper Employment Officer/NCO

- The Sniper Employment Officer's (SEO) primary responsibility is to act as a liaison between the unit Commander and his Sniper teams. The SEO is responsible for conducting the necessary planning and coordination for each sniper mission, and is over all responsible for the leadership, planning, and conduct of all Sniper operations.

Battle Tracking

Monitoring current location, activity, and combat power of Task Force elements; monitoring the progress of adjacent and supporting units, and updating templates.

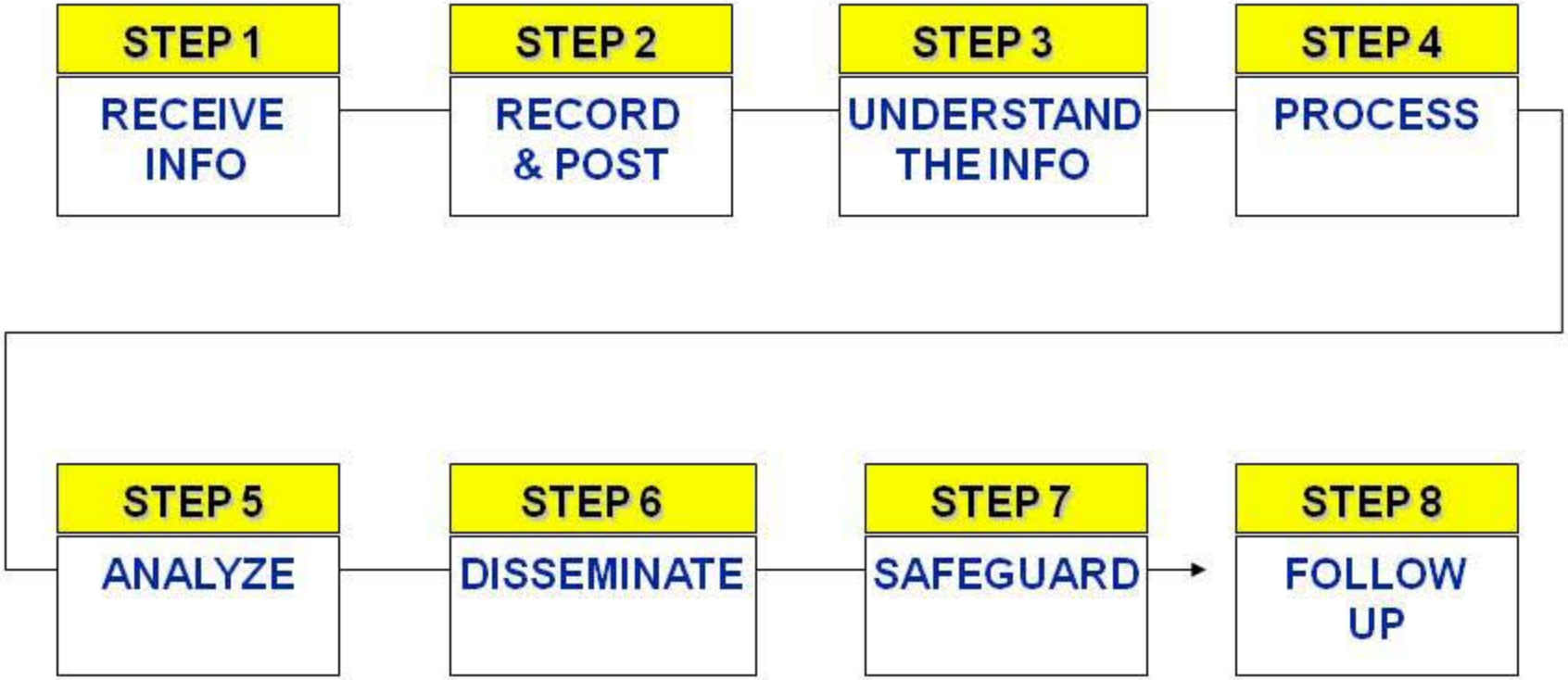
- The Battle Staff Officer processes all reports and information entering the CP
- Maintains and monitors:
  - Situation Map
  - Adjacent unit and JIIM activities
  - Status Charts
  - Emerging enemy TTPs
- Coordinates activities of all CP sections.

Information Management

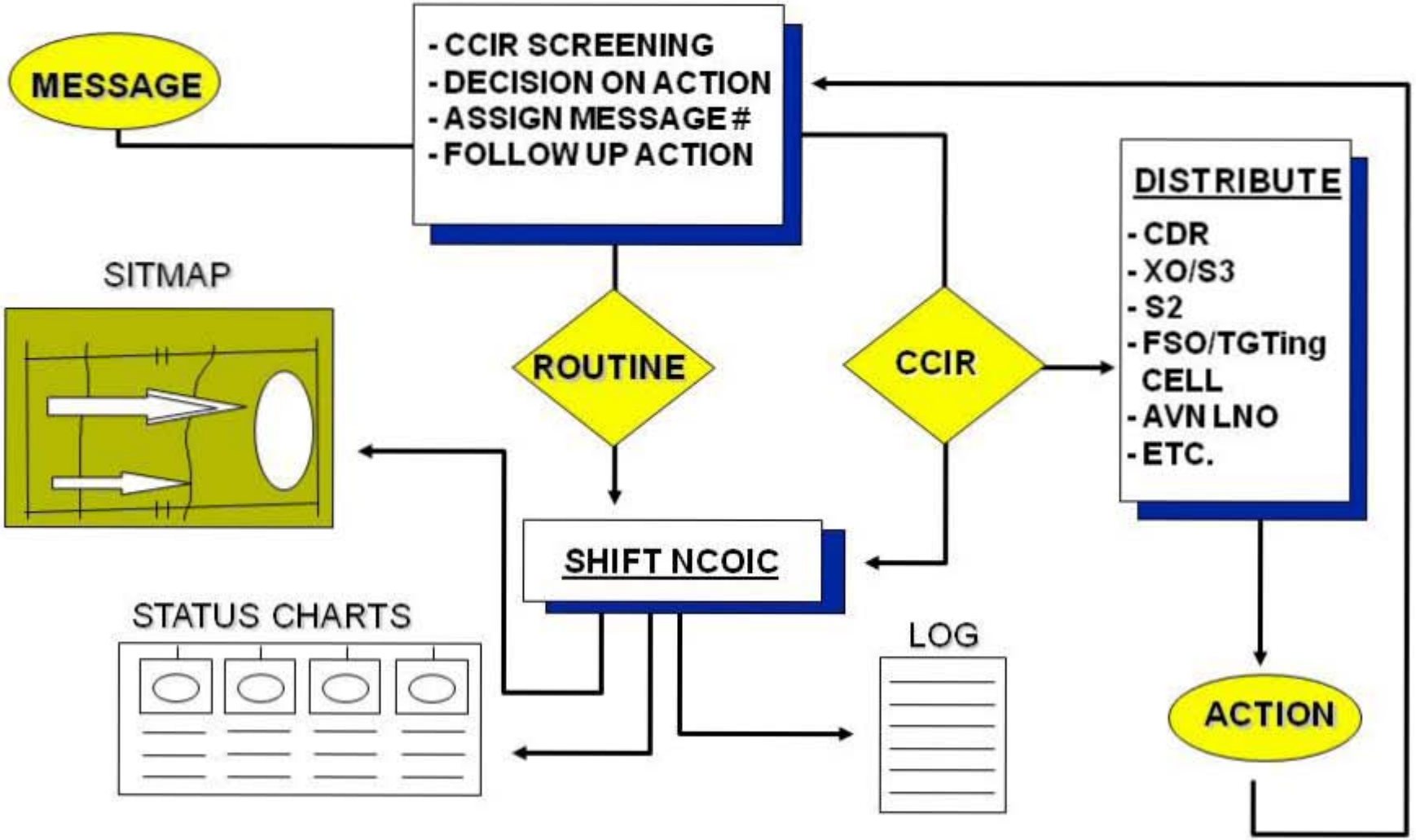
- **Image Building Information**
  - Define the tactical problem
  - Understand requirements, capabilities, and shortfalls, both current and future
  - Provide feasible options
  - Recognize the time for decision
- **Execution Instructions**
  - Articulate commander's decisions to subordinates
  - Allocate resources to subordinates
  - Develop technical and tactical instructions to implement commander's vision

Information Management

The Eight Steps to Managing Information



Information Process

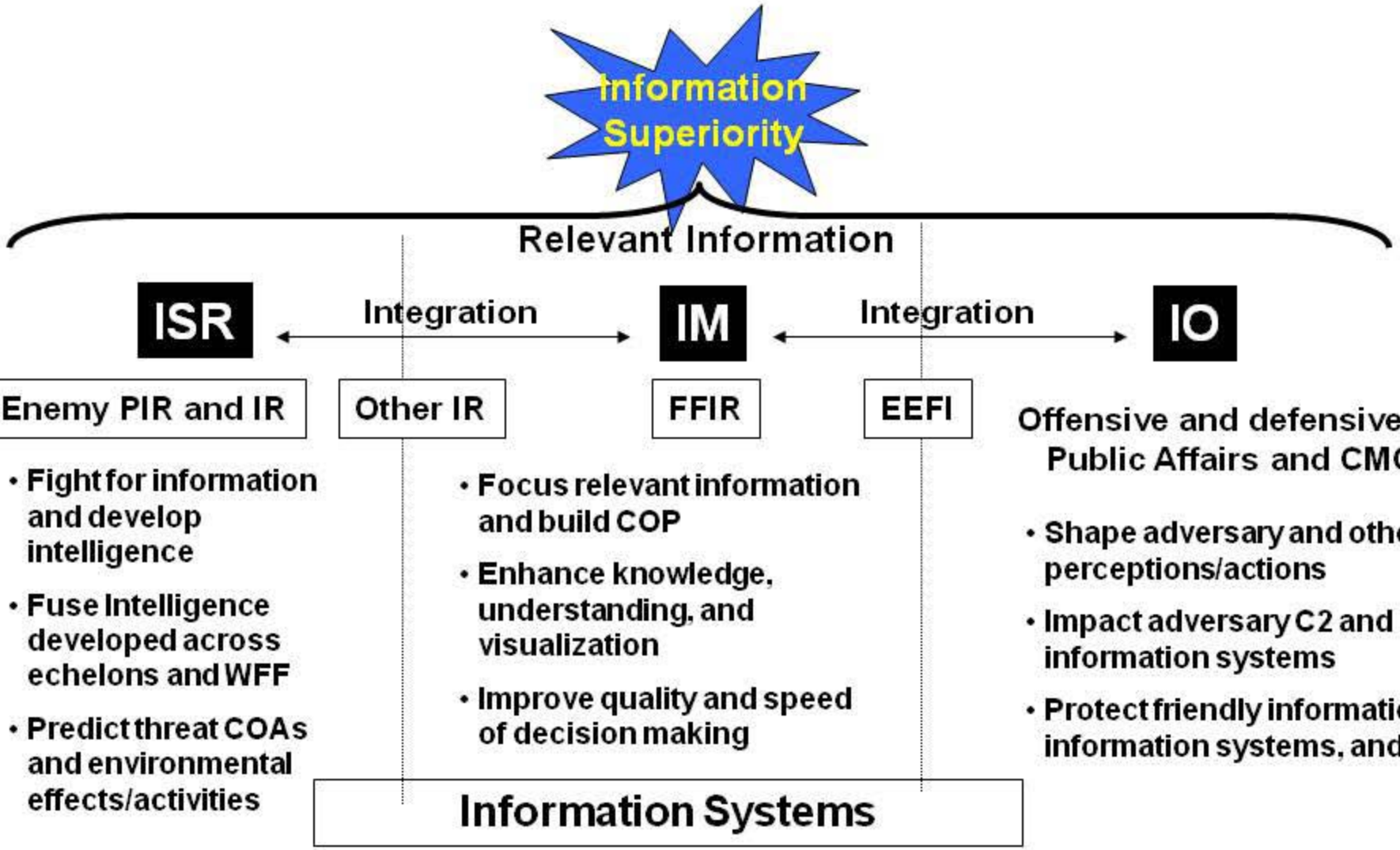


Information

"Information is an element of combat power. It is a powerful operational and tactical multiplier. It enhances leadership and magnifies the effects of maneuver, firepower, and protection. In the past, commanders made enemy contact, developed the situation, and gained information. Today, Army leaders increase their situational understanding before maneuvering forces and engaging the enemy."

FM 3-0

Information Superiority_



FM 3-0 Fig 11-1

Doctrinal Keys to Achieving IS

- Develop and maintain a comprehensive picture of enemies and adversaries; forecast their likely actions.
- Deny enemies and adversaries information about friendly forces and operations. Influence enemy and adversary leader perceptions, plans, actions, and will to oppose friendly forces.
- Influence noncombatants and neutrals to support friendly missions or not to resist friendly activities.
- Inform noncombatant and neutral organizations so they can better support friendly policies, activities, and intentions.
- Protect friendly decision making processes, information, and information systems.
- Continually provide relevant information (including intelligence) to the commander and staff in a useable form.
- Destroy, degrade, disrupt, deny, deceive, and exploit enemy decision making processes, information, and information systems, and influence those of adversaries and others.

FM 3-0

Intelligence, Surveillance and Reconnaissance (ISR)

Reconnaissance:

Area
Zone
Route

Security Missions:

Screen
Area
Route
Convoy

Reconnaissance Operations:

"Those operations undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy, or to secure data concerning the meteorological, hydrographical or geographical characteristics and the indigenous population of a particular area." FM 3-90 G22

"Reconnaissance collects information and can validate current intelligence of predictions. Reconnaissance units, unlike other units, are designed to collect information." FM 3-0, p11-9

A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. FM 1-02 SEP 2004

Surveillance Operations:

"Surveillance involves continuously observing an area to collect information. It is the systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means." FM 3-0 11-9

"Reconnaissance elements *may* have to fight for information. However, the purpose of reconnaissance is to gain information through stealth, not initiate combat." FM 3-0, p11-10

ISR Mission Sets

Reconnaissance:

- Area
- Zone
- Route

Security Missions:

- Screen
- Area
- Route
- Convoy

AREA RECONNAISSANCE:

A directed effort to obtain detailed information concerning society, infrastructure, terrain or enemy activity within a prescribed area such as a town, ridge line, woods or other feature critical to operations.

IED / Sniper Considerations:

Social demographics and breakdown by religious sect, clan, and tribe

- Key infrastructure within the area of operations which would lend itself to IED or Sniper attacks- corner buildings, open spaces, intersections etc…
- Identify terrain which insurgents can use to emplace IEDs or employ Snipers and exfiltration routes

ISR Mission Sets

Reconnaissance:

Area
Zone
Route

ZONE RECONNAISSANCE:

The directed effort to obtain detailed information concerning all threat forces, routes, obstacles, and terrain within a zone defined by boundaries. The reconnaissance may be enemy oriented, terrain oriented, or a combination of the two.

IED Considerations:

- Identify insurgent groups and their areas of operation
- Identify areas around key infrastructure in which insurgents can place IEDs
- Use the infiltration and exfiltration routes that insurgents use to conduct counter-IED efforts

Sniper Considerations:

- Identify insurgent groups and their areas of operation
- Identify areas around key infrastructure in which insurgents can employ snipers
- Possible sniper final firing positions – FFPs (enemy and friendly).
- Possible infiltration and exfiltration routes (enemy and friendly).
- Street angles, intersections, corner buildings, open spaces, and line of sight studies.
- Effective ranges for first round reduction and identification capabilities of optics (enemy and friendly).
- Possible engagement areas (enemy and friendly)

ISR Mission Sets

Reconnaissance:

- Area
- Zone
- Route

Security Missions:

- Screen
- Area
- Route
- Convoy

ROUTE RECONNAISSANCE:

Directed effort to gain detailed information about a specific route and the terrain on either side of the route the threat could use to influence movement along the route.

Critical Tasks:

- Determine trafficability
- Find/ report any threat that can influence movement
- Reconnoiter all lateral routes
- Inspect/ classify bridges, over and underpasses, culverts, defiles
- Locate bypass around built-up areas, obstacles, barriers
- Clear defiles along route within capabilities or find a suitable bypass

Principles for ISR Success

1. **Prioritization** – Determining the relative importance of each Information Requirement (IR)

2. **Redundancy** – Ensuring multiple assets can observe critical Named Areas of Interest (NAI)

3. **Focus of effort** – Using Priority IRs and NAIs to narrow the requirements for ISR assets

4. **Flexibility of assets** – Adopting a plan that allows for the repositioning of assets to cover critical NAIs

ISR Operations

Why ISR?

- Fill Voids in Information
- Enable Targeting
- Answer the CCIR

How ISR?

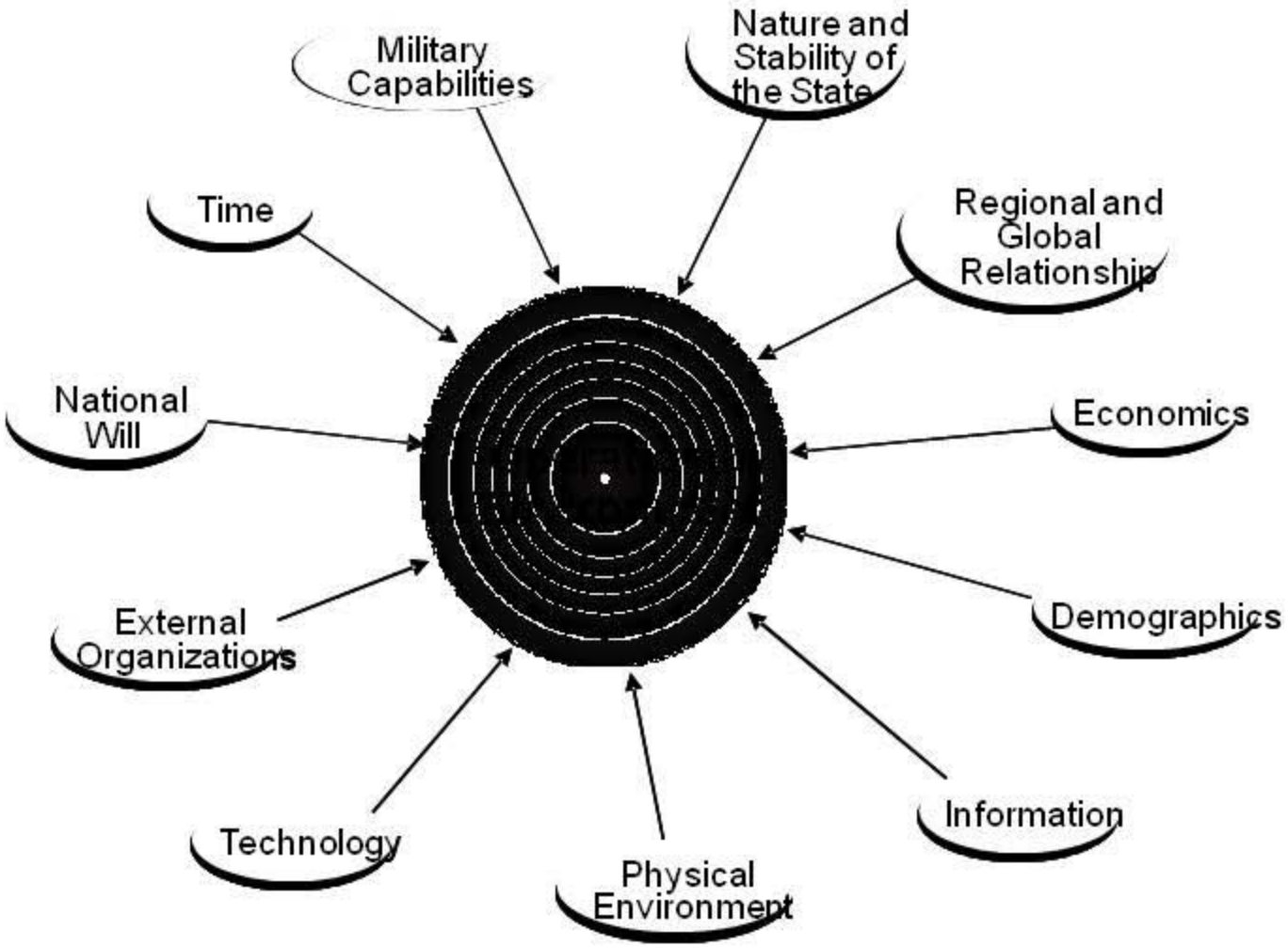
- Reconnaissance
- Surveillance
- Methods of R & S
- Fundamentals of Surveillance
- Fundamentals of Reconnaissance
- Forms of Reconnaissance
- Reconnaissance Guidance

Intelligence Preparation of the Battlefield (IPB)

A Four Step Process

1. Define the Operational Environment
2. Describe the Environmental Effects
3. Evaluate the Threat
4. Determine threat Course of Action

The Operational Environment



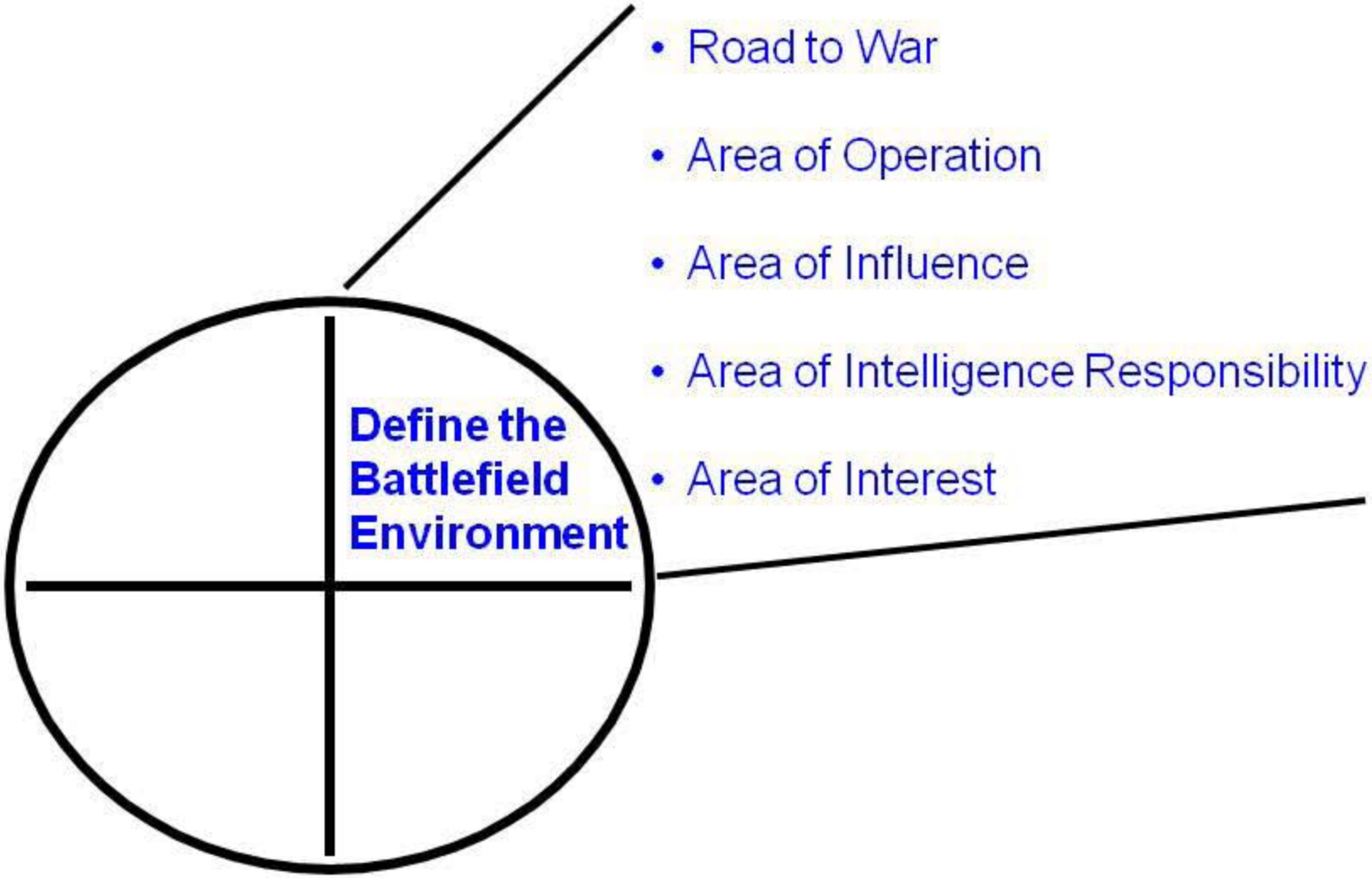
Summarized Analysis of the OE (PMESI)

- ***Political***:
  - Sniper operations (little collateral damage) easy to overlook by political leadership
  - Demonstrates government is powerless to eradicate sniper threat
- ***Military***:
  - Ministry of Defense trained snipers
  - Cellular makeup of AIF sniper
- ***Economic***:
  - Most sniper activity conducted on freelance, for hire basis
- ***Social***:
  - Paints picture of the lone Arab warrior, larger than life mystique
- ***Information***:
  - IO effect of snipers well established/capitalized upon (USSR/German sniper war, Russian battles for Grozny, DC sniper, Juba sniper of Baghdad)
  - Allows the enemy to spin outcomes for effects; Enemy gets his message out first
  - Attacks centered on areas with high level of media (Baghdad, Ramadi, Mosul)
  - Snipers enhance recruiting, financing, propaganda
  -

Summarized COE Analysis (PMESII+PT)

- ***Infrastructure***:
  - Urban density enables ingress/egress, cover/concealment
  - Road networks "bait" target to shooter, enable hasty sniper operations by enabling "trolling" for targets of opportunity
  - Prior regime produced and cached sniper weapons and equipment
- ***Physical Environment***:
  - Urban settings promote short range shots; mask sounds
  - Rural setting promote long range shots
  - Limited visibility attacks
- ***Time***:
  - Recruiting, training, employment of sniper is cyclic and difficult to sustain

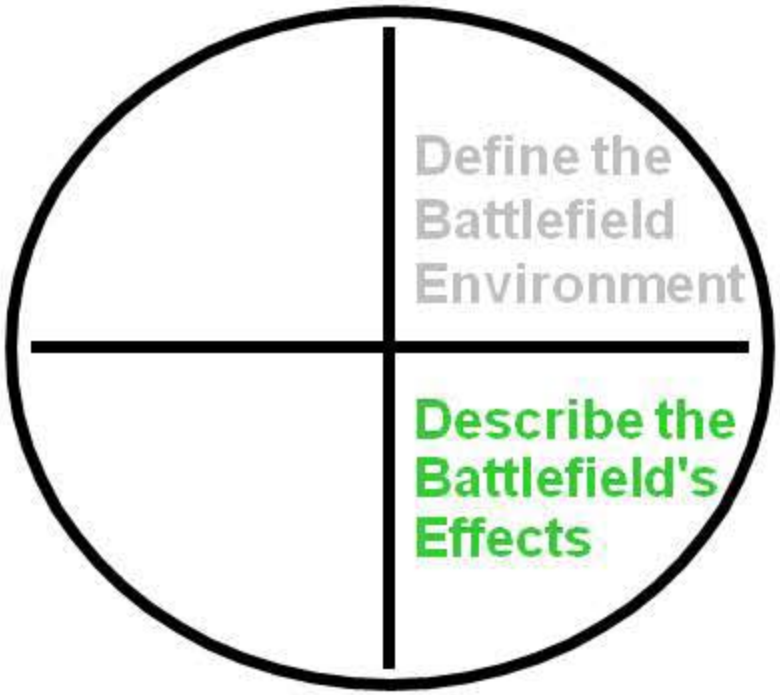
Step 1 - Define the Operational Environment



Identify the Physical Environment

- Area of Operation
- Area of Influence
- Area of Intelligence Responsibility
- Area of Interest

Step 2 - Describe the Environmental Effects



- Terrain Analysis (OACOK)
- Effects of Terrain on Operations
- Civil Considerations (ASCOPE)
- Weather Forecast (and Lunar Data)
- Effects of Weather on Operations
- Overall Assessment

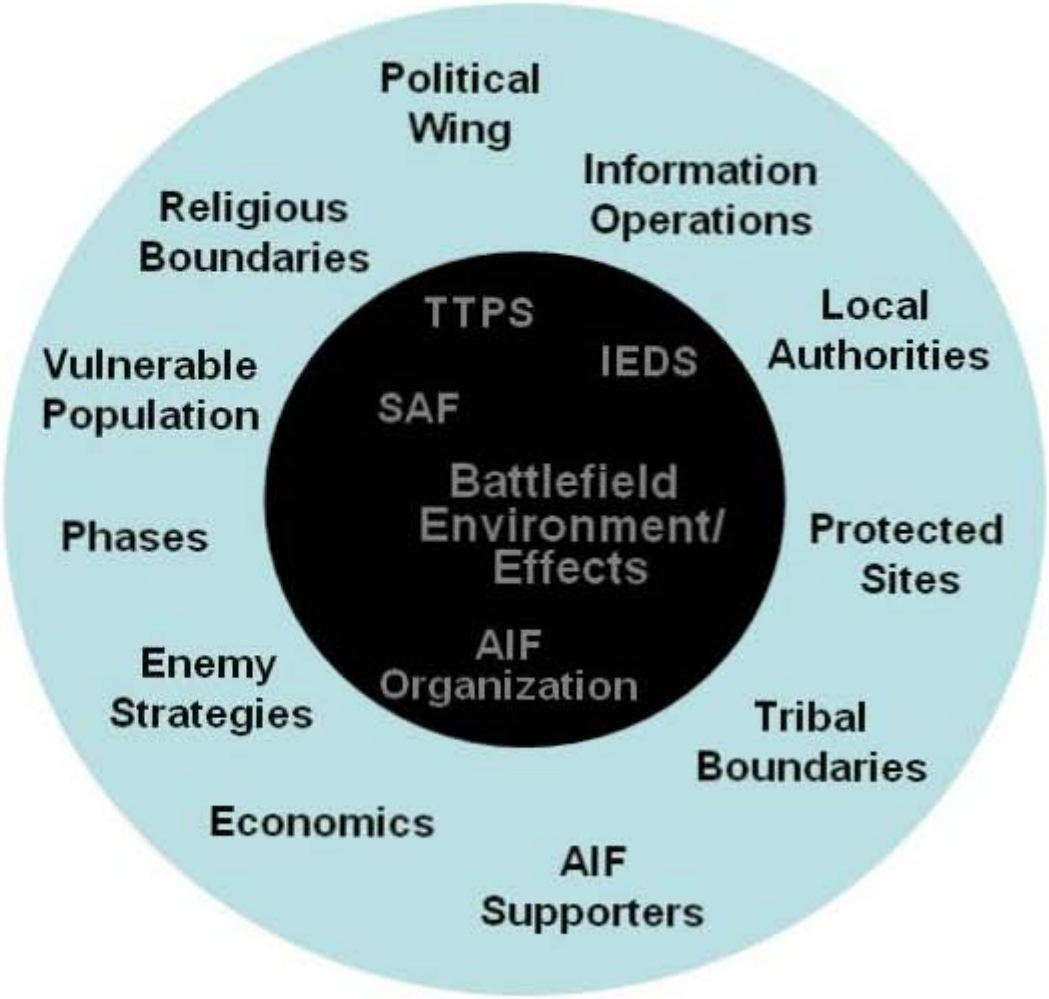
Terrain Analysis

- How will the terrain affect the enemy's COAs?
- How can friendly forces best exploit opportunities provided by the terrain?
- How will the terrain & weather affect friendly and enemy systems?

•Terrain Analysis can be used to maximize friendly opportunities and minimize enemy exploitation.

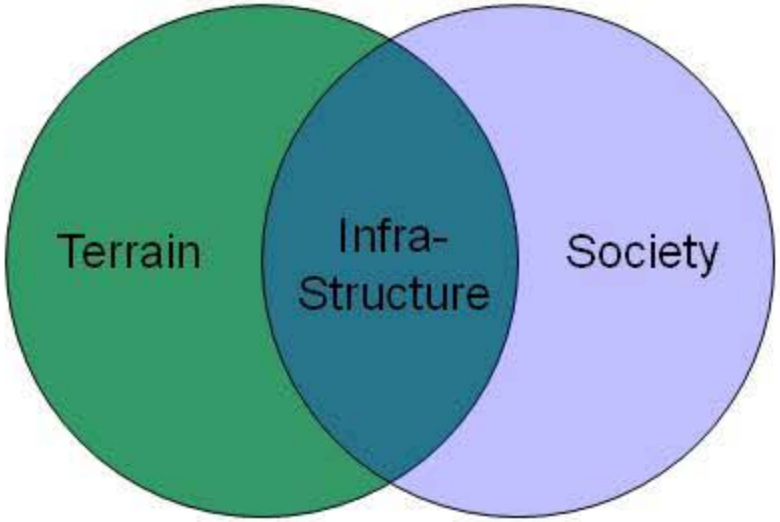
ASCOPE

- **A**reas.
- **S**tructures.
- **C**apabilities.
- **O**rganizations.
- **P**eople.
- **E**vents.



ASCOPE Interpreted

"To help analyze many civil considerations, commanders and staffs can provide structure to their assessments by categorizing according to six characteristics: areas, structures, capabilities, organizations, people, and events (ASCOPE)."



Areas/Structures
Buildings
Blue Prints
DC Camps
Street Patterns
Urban Patterns
Criminal Enclaves
Underlying Terrain
Construction Materials
Key Commercial Zones
Subterranean Passages
Political Precincts and Districts

Capabilities
Fuel
Fire/Rescue
Electrical Power
Transportation
Communications
Health Services

Orgs/People/Events
NGOs
Media
Culture
Loyalties
Authority(s)
Perceptions
Relationships
Labor Unions
Demographics
Groups & Sub-groups
Religious Holidays

FM 3-06, Ch 9

Step 3 - Evaluate the Threat

- Disposition (2 levels up min)
- Composition (OB) (Line & Block Chart)
- Strength (Enemy Unit Strength – %)
- Enemy Key Systems Capabilities
- Enemy Unit Capabilities by Battlefield Operating System (WFF)
- Enemy System Capabilities by WFF
- Blue Systems vs. Red Systems Capabilities
- Blue Artillery vs. Red Artillery Ranges
- Force Ratios
- Enemy Threat Model

Attributes of The Threat

Identify the Threat

- Why do insurgents fight?
  - Patriotism
  - Ideology
  - Religion
  - Financial Gain
- Study the Insurgency
  - Origin & History
  - Support among populace
  - Organization
  - Inter-Operative Networks
  - Operational Tactics

Step 3 - Evaluate the Threat

Enemy Analysis

Where do we start?

Requirements

What must the enemy do/have to accomplish his objectives?

Examples:
Money
Technical know-how
Bomb making supplies
Vehicles
Compliant population
Suicide bombers
Weapon system

Capabilities

What resources does the enemy have available?

Examples:
Information dissemination
VBIEDs
External support
Hide within population
Knowledge of location

Vulnerabilities

What shortfalls does the enemy have between capabilities and his requirements?

Examples:
Key individuals
Caches
VBIED Factories
Counter Sniper Ops

Step 3 - Evaluate the Threat

Enemy Analysis

Another method…

Who

Is attacking?
Organizing?
Directing?

Examples:

Emplacers
Builders
Financiers
Triggermen
Shooters
Security
Cell Leader

What

Are their objectives?
Methods?
Techniques?

Examples:

RCIED
Complex
Baited ambush
Patterns

When

Do they emplace?
Attack?

Examples:

Day/Night
Before/During/After
Clearing

Where

Have they attacked?
Will they attack in the future?
Do they store?
Assemble?
Get supplies?

Examples:

Previous attacks

Why

Do they Attack coalition?
Locals?

Examples:

Personal gain
Money
Power
Revenge

Step 4 - Determine Threat COAs

- Most Likely (MLECOA)
- Most Dangerous (MDECOA)
- All Additional ECOA
- Final Assessments

Changing Threat COAs

Conventional Focus Requirement

- Identify the Threat's likely and desired End State.
- Identify the full set of COAs available to the threat.
- Evaluate and prioritize each COA.
- Develop each COA in the amount of detail time allows.
- Identify initial collection requirements.

COIN Environment Considerations

- COA development becomes MUCH more complex due to:
- Available maneuver options.
- 3-D battlefield
- Increase in friendly vulnerabilities.
- Limited attack options
- Increased Fratricide Risk
- Event-based vs. Maneuver-based COAs.
- Collection requirements are difficult to focus until patterns develop.

Evaluate Threat COAs

Most Likely Enemy Course of Action (MELCOA)

- COA Sketch & Statement (Includes T, P, M, E, DP, CP)
- SITEMP (brief T/P by subunit and/or WFF)
- OBJ Blowup Sketch
- High Value Targets (HVT)

Most Dangerous Enemy Course of Action (MDECOA)

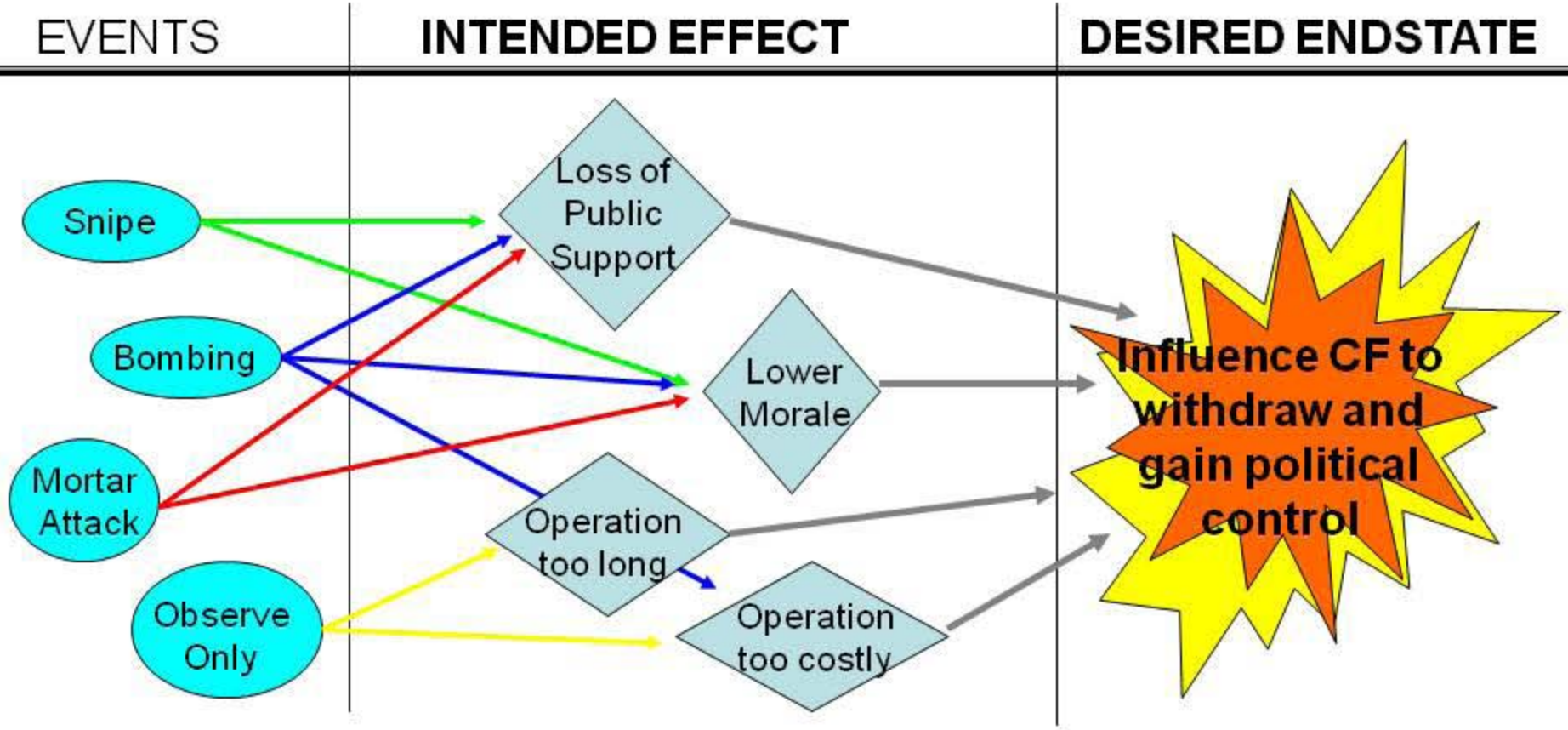
- Same as for MLECOA
- Explain differences between MDECOA, MLECOA, and additional ECOAs

<u>FINAL ASSESSMENTS</u>

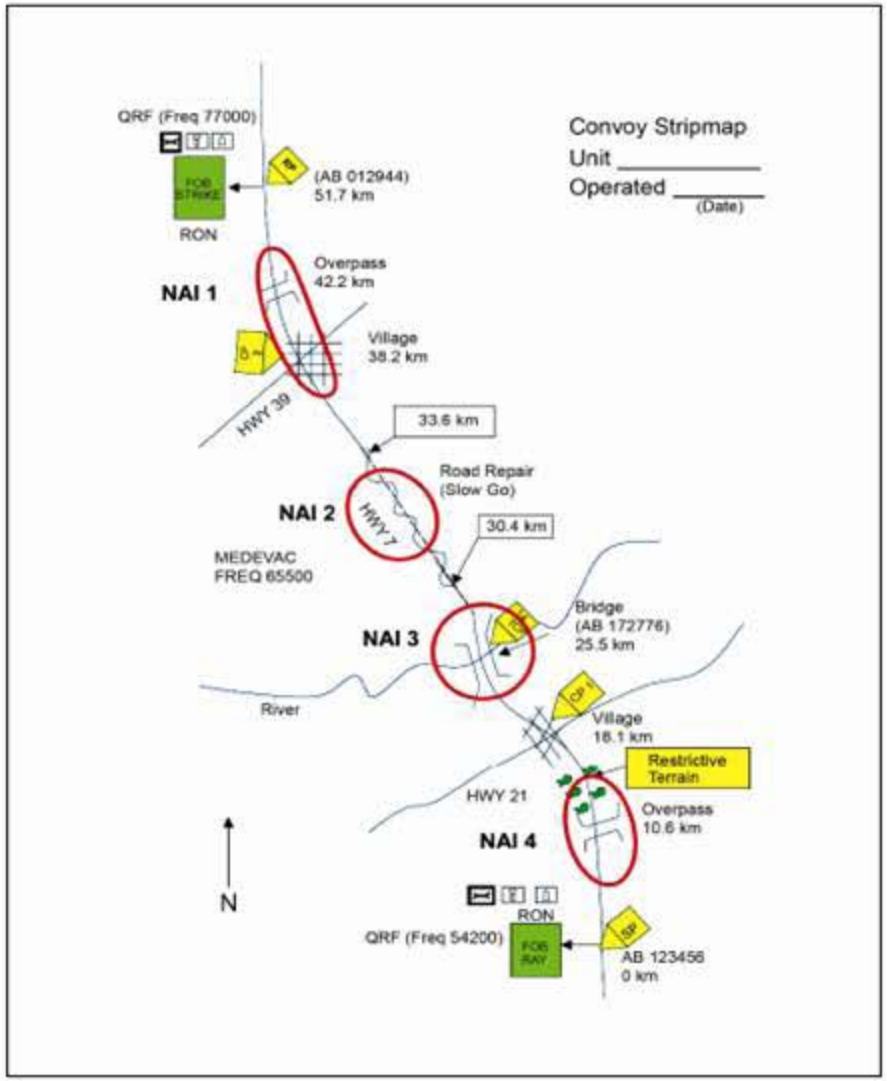
- Enemy Strengths & How to Overcome
- Enemy Weaknesses & How to Exploit
- How Best to Assault the OBJ
- Weaknesses of the Enemy at the OBJ
- Best Use of Terrain to Assault the OBJ
- Where should we attack/assault from, and why?

Event-based vs. Maneuver-based COAs

ISSUE - COAs may consist of linked singular events to reach a desired end-state vice conventional maneuver operations to destroy enemy forces and seize terrain.



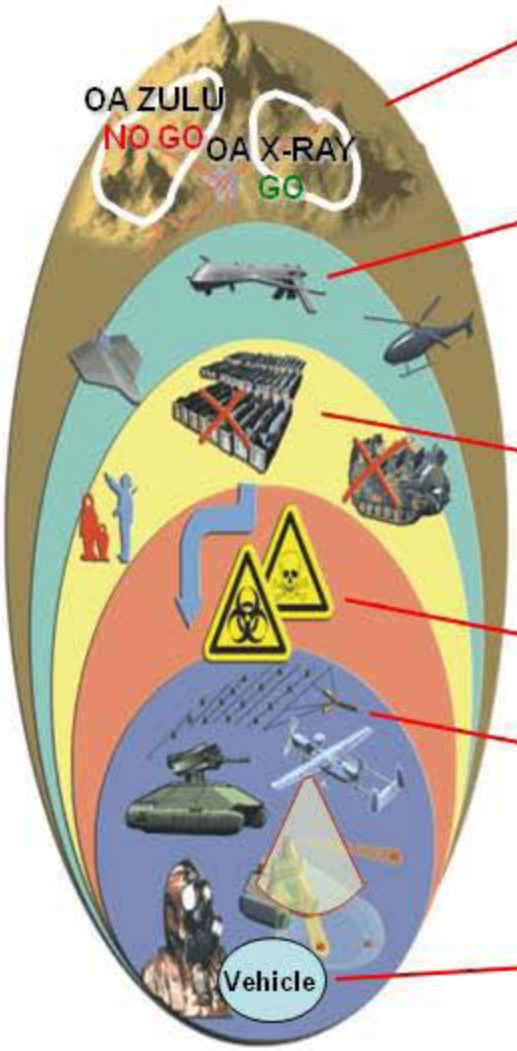
Example of an Event Template



IED Defeat Tenets Related to Battle Staffs

Exploit – Predict – Prevent

IED Defeat Tenets



- **PREDICT** actions and circumstances that could affect the ability of the force to maintain momentum.
- **DETECT** indicators of impediments or lack of impediments to battlefield mobility early; identify alternatives and establish surveillance.
- **PREVENT** potential impediments to maneuver from affecting battlefield mobility of the force.
- **AVOID** detected impediments to battlefield mobility of the force.
- **NEUTRALIZE**, reduce, or overcome (breach) impediments to battlefield mobility that cannot be prevented or avoided.
- **PROTECT** soldiers and vehicles against effects of explosives.

EXPLOIT

PREDICT

PREVENT

DETECT

NEUTRALIZE

MITIGATE

ACCURATELY ANTICIPATE IED ACTIVITIES Predict, thru pattern analysis, to position C4ISR to confirm or deny enemy actions. Use the information to interdict and disrupt the IED System.

RESTRICT PRODUCTION Deny the bomb maker of sanctuary, guidance, finances, support, targets, supplies and life.

RESTRICT EMPLACEMENT Restrict the ability of enemy combatants to emplace IEDs through the use of right of way clearance, active combined arms patrolling, UAVs, use of sniper teams in high IED threat areas, control of Captured Enemy Ammunition (CEA), intelligence, and CA work with local nationals.

DEFEAT THE DEVICE Detect and neutralize IEDs through aggressive route clearance and maintenance, a systematic sweep program, and the use of IED jamming devices. Increase soldier protection through the distribution of hardened vehicles.

FUNDAMENTALS OF ASSURED MOBILITY | **TENETS OF IED DEFEAT** | **IED DEFEAT OPERATIONS**

REF: JIEDDO & FMs 3-34 / 3-90.11

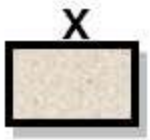
Defeating the System

Exploit

Predict

Prevent

Analysis and technical means synchronized to support concise targeting objectives



Defeating the System

Actions taken or planned by staff

Staff-centric

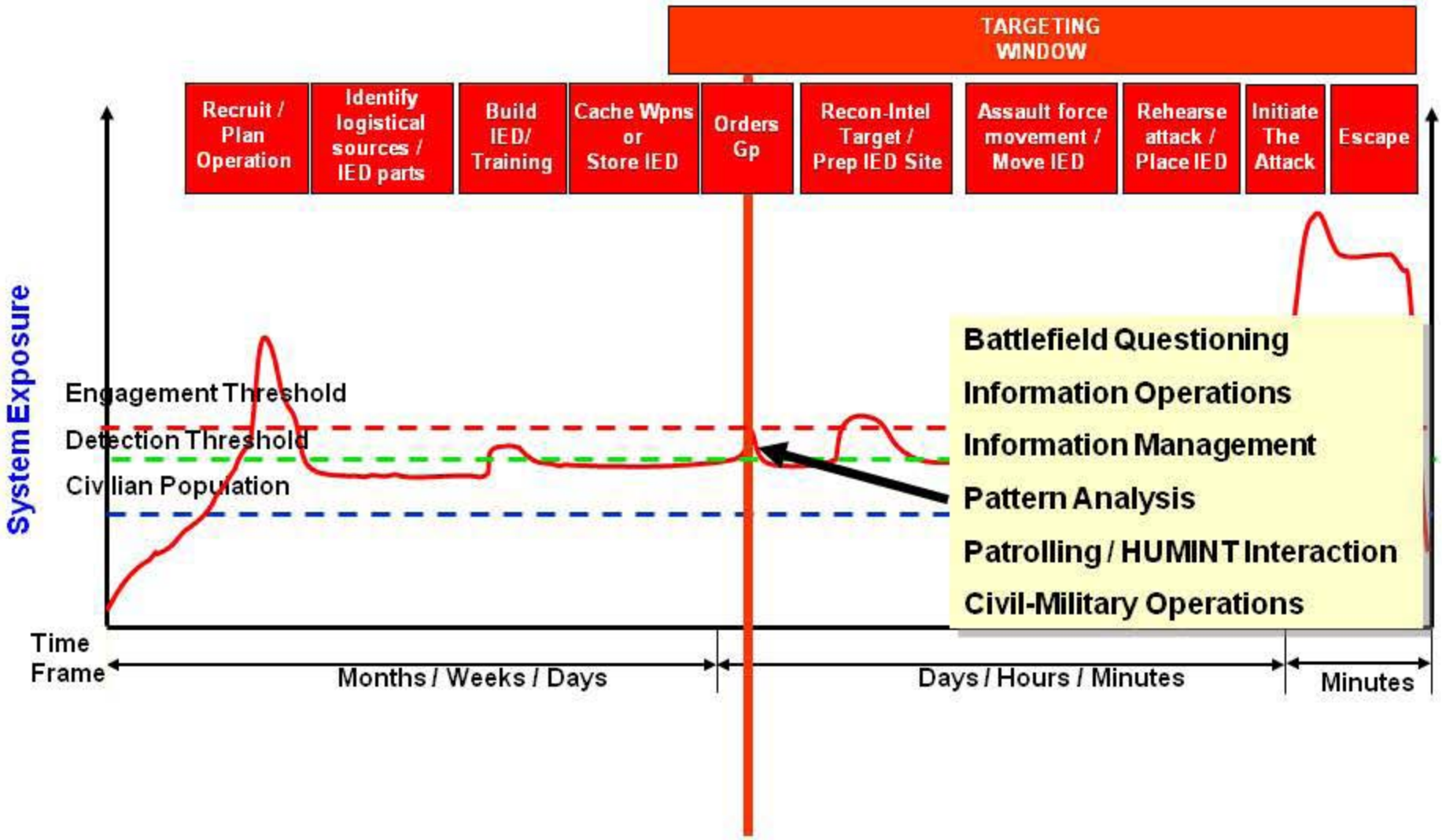
Focused effort should be directed to identify and neutralize individuals

Analysis, allocation of resources, and the focus of effort combine to identify and eliminate the individuals and groups using IEDs or the elimination of their ability to use IEDs.

- Pattern analysis
- Targeting process
- Establishing priorities
- Integration of ISR assets
- Prioritization of funding
- Coordination for ISR assets
- Analysis of HUMINT / Exploitation
- Analysis of sources
- Leveraging UAV & aviation assets

By taking action to defeat the system responsible for IED attacks we regain the initiative.

Prevent

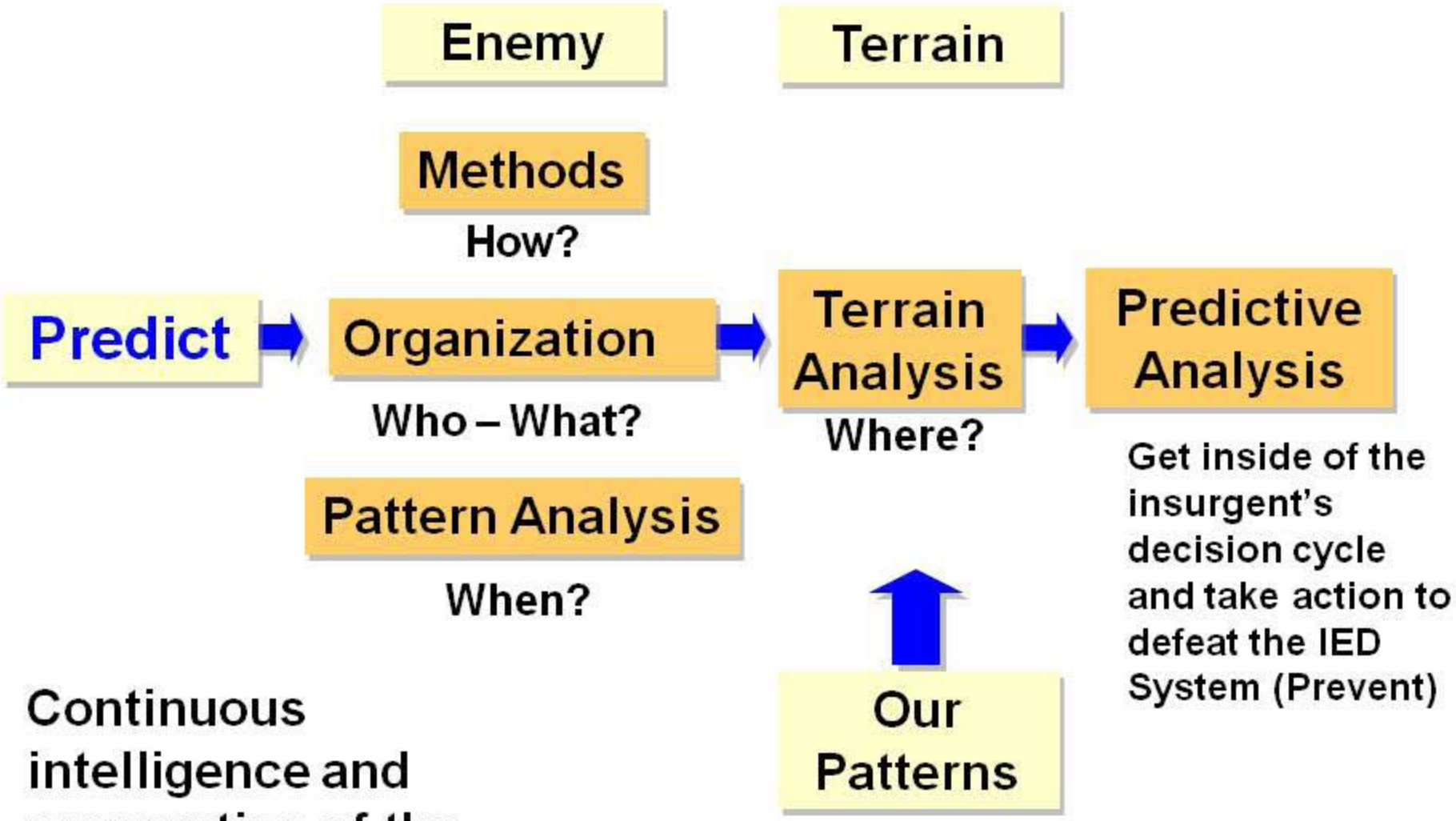

TARGETING WINDOW
Recruit / Plan Operation
Identify logistical sources / IED parts
Build IED/ Training
Cache Wpns or Store IED
Orders Gp
Recon-Intel Target / Prep IED Site
Assault force movement / Move IED
Rehearse attack / Place IED
Initiate The Attack
Escape
System Exposure
Engagement Threshold
Detection Threshold
Civilian Population
Battlefield Questioning
Information Operations
Information Management
Pattern Analysis
Patrolling / HUMINT Interaction
Civil-Military Operations
Time Frame
Months / Weeks / Days
Days / Hours / Minutes
Minutes

Predict & Exploit

- "IEDs are a product of human ingenuity and human social organization. If we understand the social context in which they are invented, built and used we will have an additional avenue for defeating them."
- "Commanders should focus less on the bomb than the bomb maker." (BG Votel, Joint IED Task Force)
- "Identifying the bomb makers should be an absolute priority, and the best way to identify them is through intelligence provided by the bomb maker's customers."
- "IED deployment also depends on the existence of an organization dedicated to this task."
- Social Network Analysis (SNA) provides valuable tools for understanding tribal organization and charting the links between tribes and insurgents. SNA is the mapping of relationships between people, groups and organizations.

From McFate article, Mil Review, Jun 05

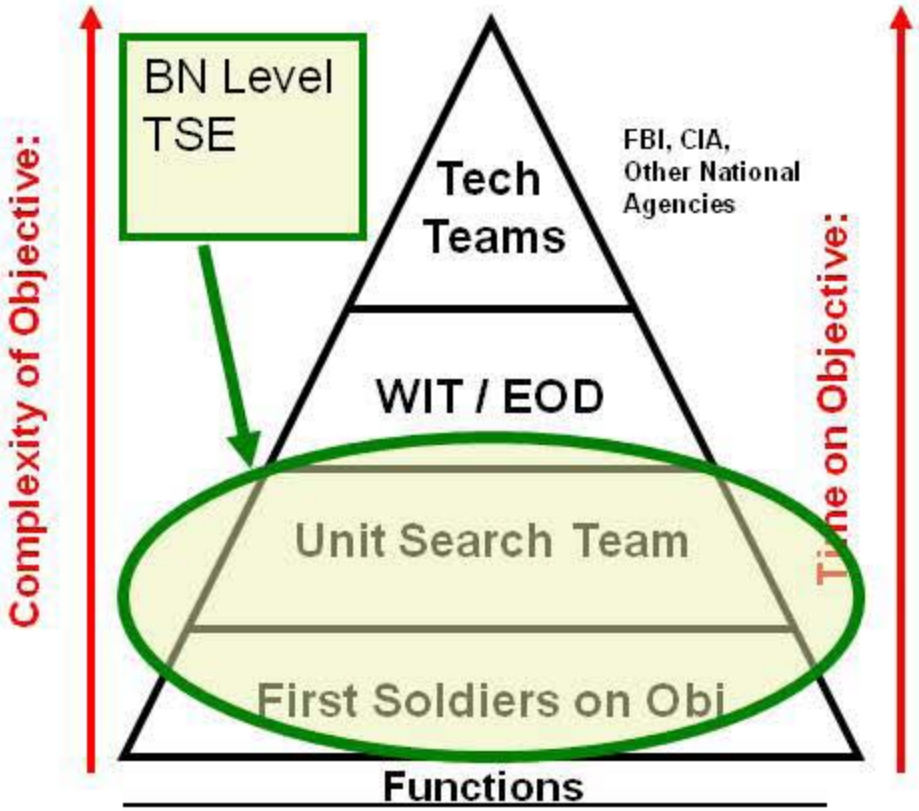
Predict: Staff Process



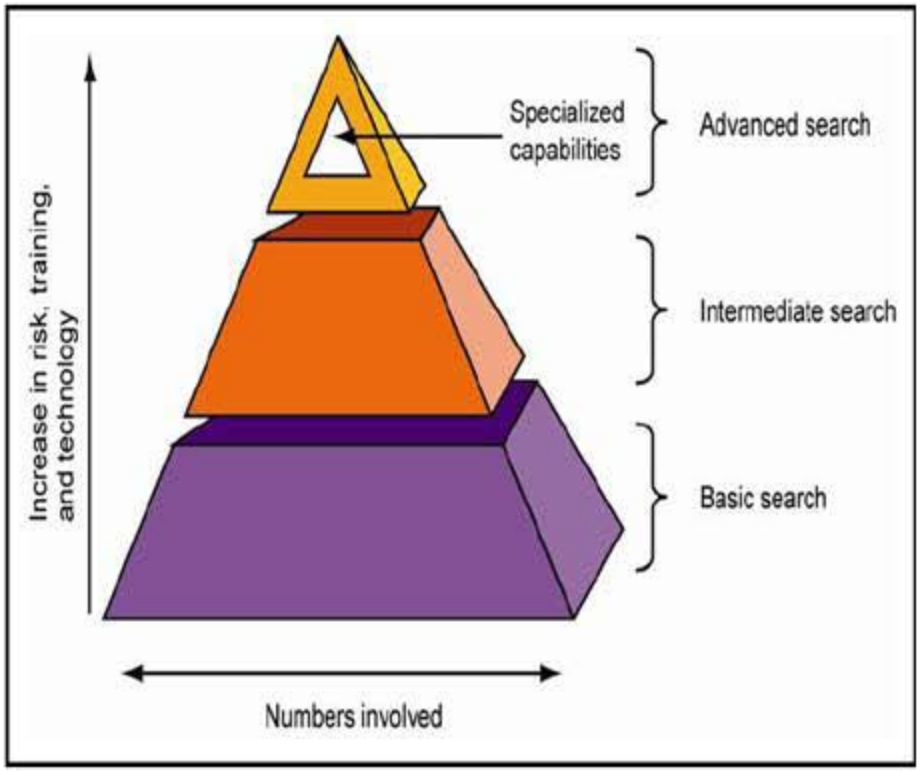
Exploitation Concepts

- **Site Exploitation** (SE) Defined
  - Related series of activities and actions initiated and conducted by Allied/Joint/Army forces to include OGA, for the purpose of exploiting personnel, documents, electronic data, and materiel.
- **Tactical Site Exploitation** (TSE) Defined
  - The actions taken to ensure that documents, materiel, and personnel are identified, collected, protected, and evaluated IOT facilitate follow-on actions.
- **Sensitive Site Exploitation** (SSE) Defined (JP 1-02)
  - A related series of activities inside a captured sensitive site to exploit personnel, documents, electronic data, and materiel captured at the site, while neutralizing any threat posed by the site or its contents
  - FM 3-90.15 SSE OPNS
    - "*A sensitive site is a geographically limited area with special diplomatic, informational, military, or economic* ***sensitivity to the United States***."
    - Examples include WMD and Mass Grave Sites where special teams and considerations are required.
    - Generally not within the capability of a BN or BCT to execute independently

Levels of SE



From Engineer School



Planning the level of TSE for a mission depends on the complexity of the objective and the METT-TC factors.

Exploitation Cycle

Explosives

Biometrics

Link evidence to detainees

Electronics

CEXC

Expose signatures

Identify

Tactical Exploitation

Event

Technical/ Human Exploitation

End State

WIT

Determine enemy TTP

Unit post-blast analysis

- Investigate event
- Categorize device
- Determine lessons learned

Catalog

Analyzing the Threats

Models, Applied Analysis,
Principles and Tools

IED Defeat Analysis

Enemy Patterns

Enemy Tactics

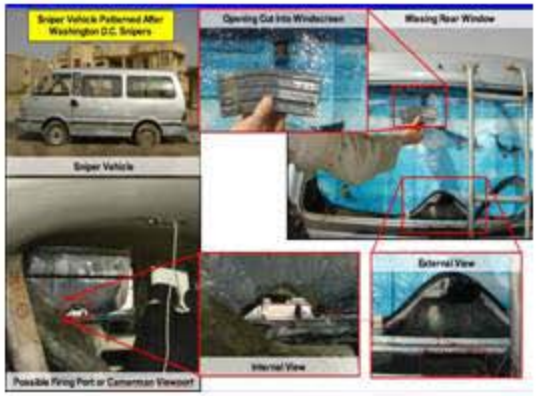
High Risk Terrain

Friendly Tactics

Friendly Patterns

Sniper Defeat Analysis

Enemy Patterns



Enemy Tactics

High Risk Terrain

Friendly Tactics

Friendly Patterns

Using Analysis to Predict

- The enemy repeats attacks in the same area if successful; attack frequency is dependant on the enemy attack cycle.
- The target area is selected for a reason. It may be chosen due to convenience or our patterns in that area.
- Favorite attack area will generally be used until emplacer is killed or an event or action occurs to force a change of target area.
- If the enemy moves his attack area, cyclic analysis will eventually cause the new pattern to emerge.
- Analysis of the patterns allows prediction of the enemy's events and therefore, set the conditions to trap him in his target area.
- Interval analysis allows estimation of when the enemy will strike again at a specific location.

Pattern Analysis Plotting

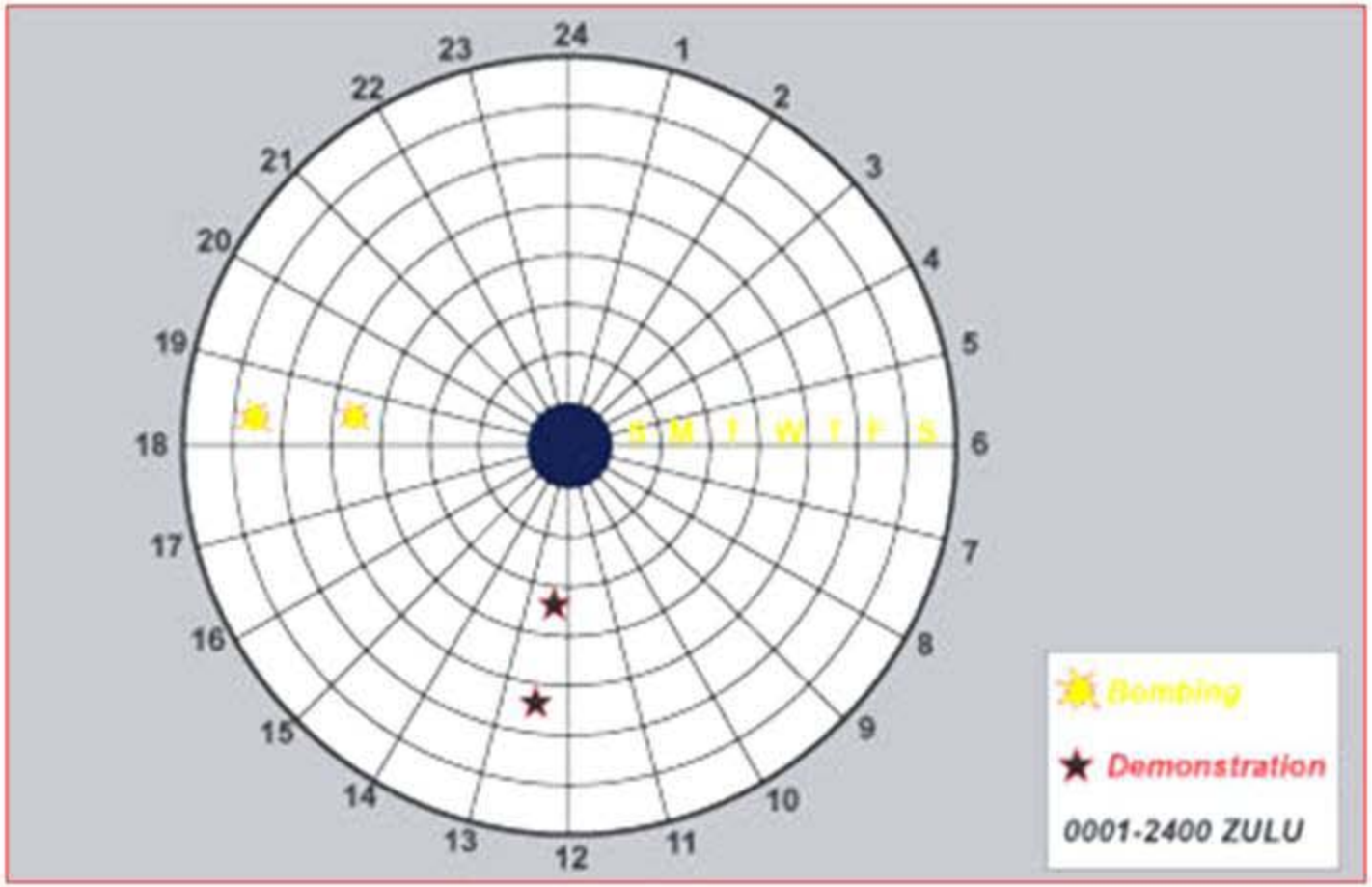
Determine the Baseline

AKA: Benchmarking or Comparative Modeling

Methods of establishing a baseline:

- Historical Comparison
- Compare to Ideal
- Compare to Similar
- Compare to Goal

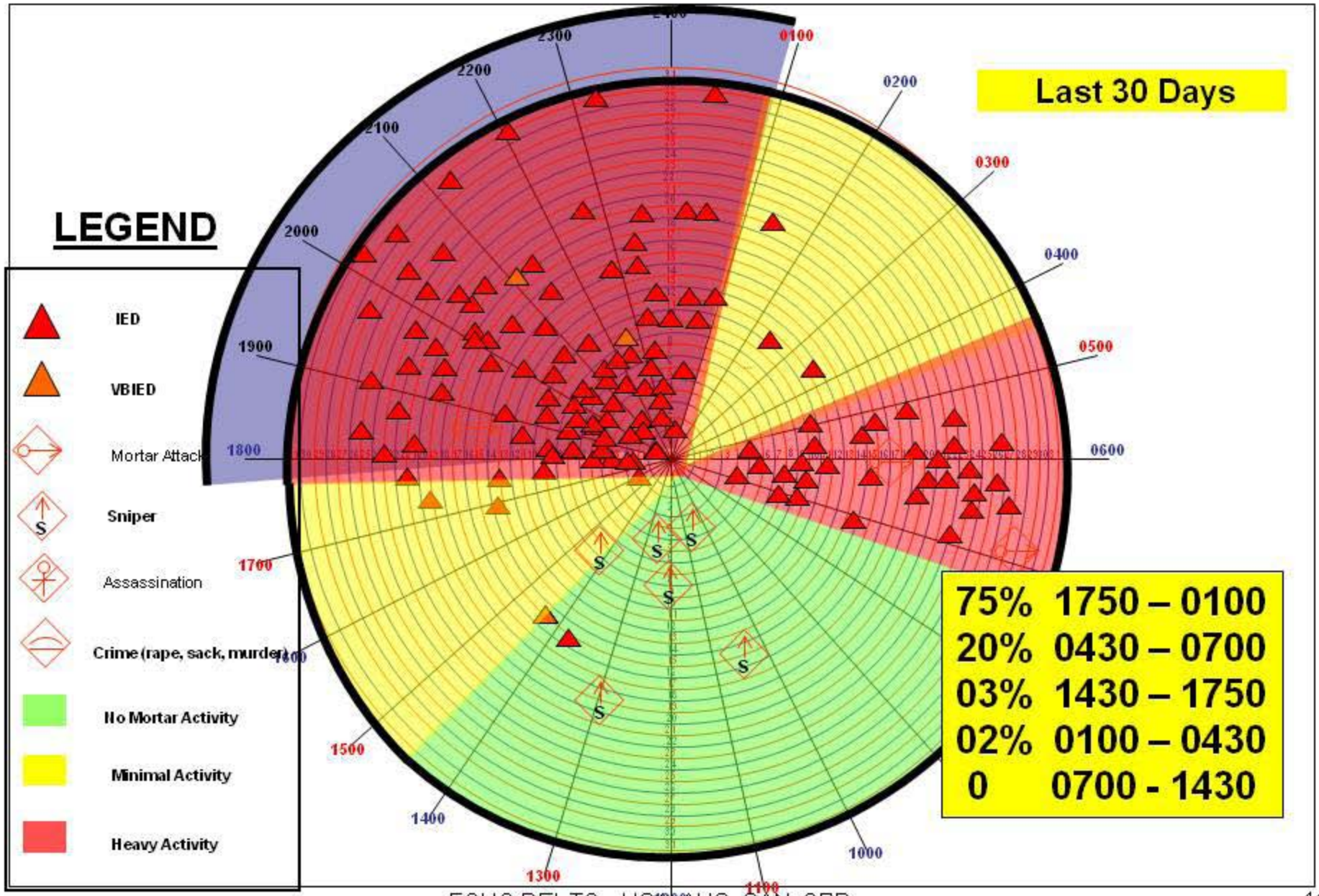
Pattern Analysis Circle Plot Chart



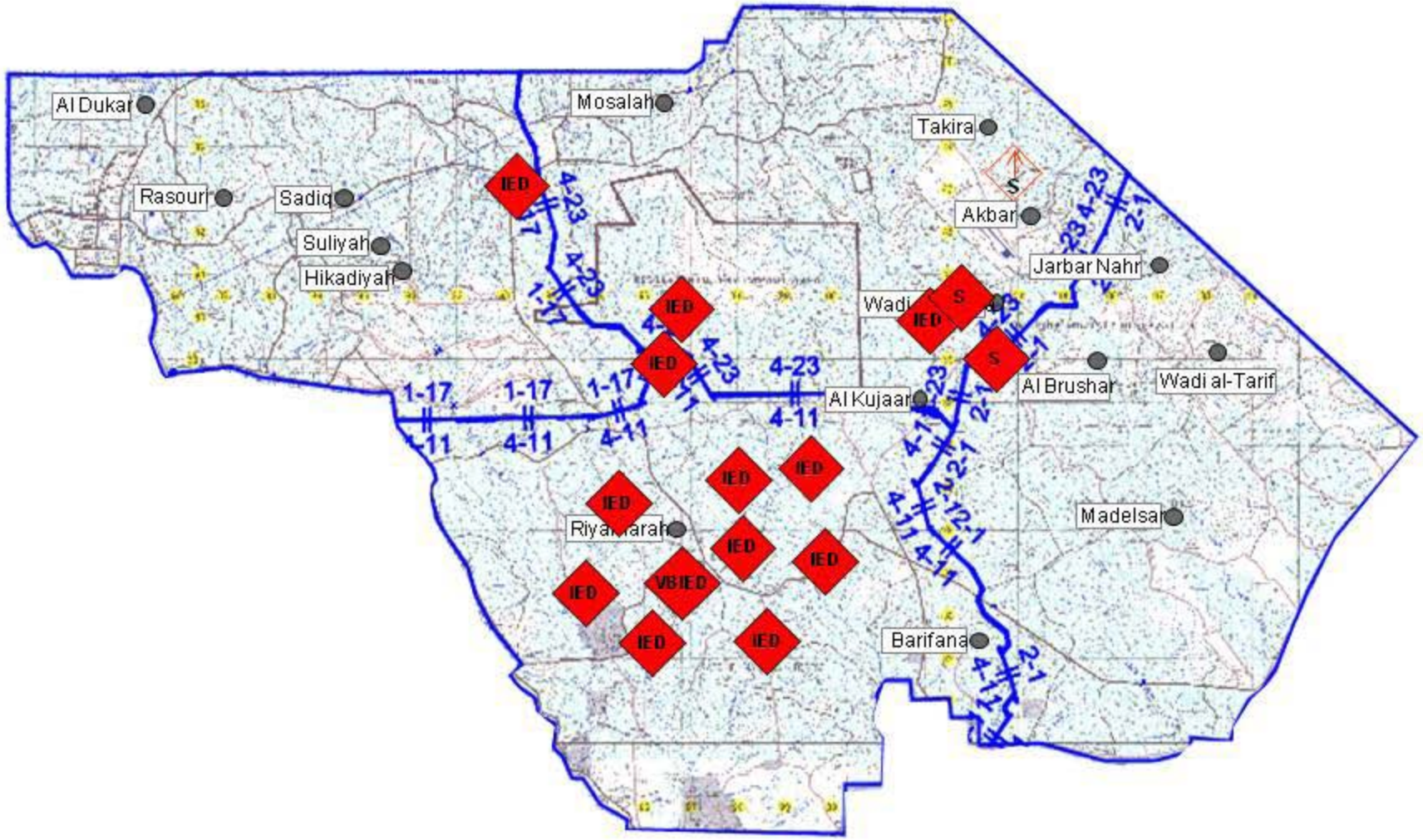
Activity Analysis

JP 2-01.3

Pattern Analysis



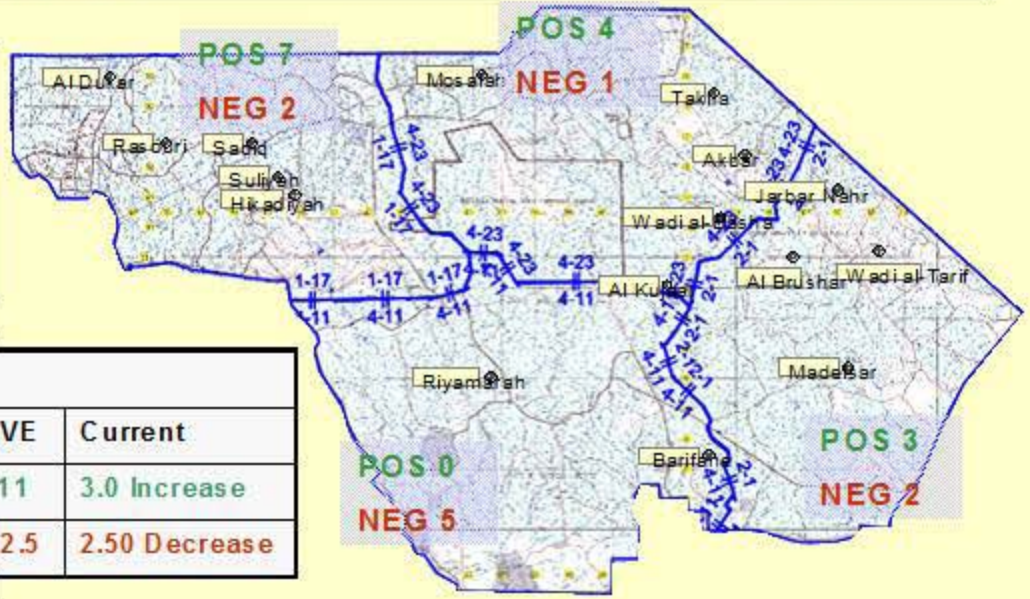
Where is he attacking from and what is he focusing on?



Trend Analysis (Informational)

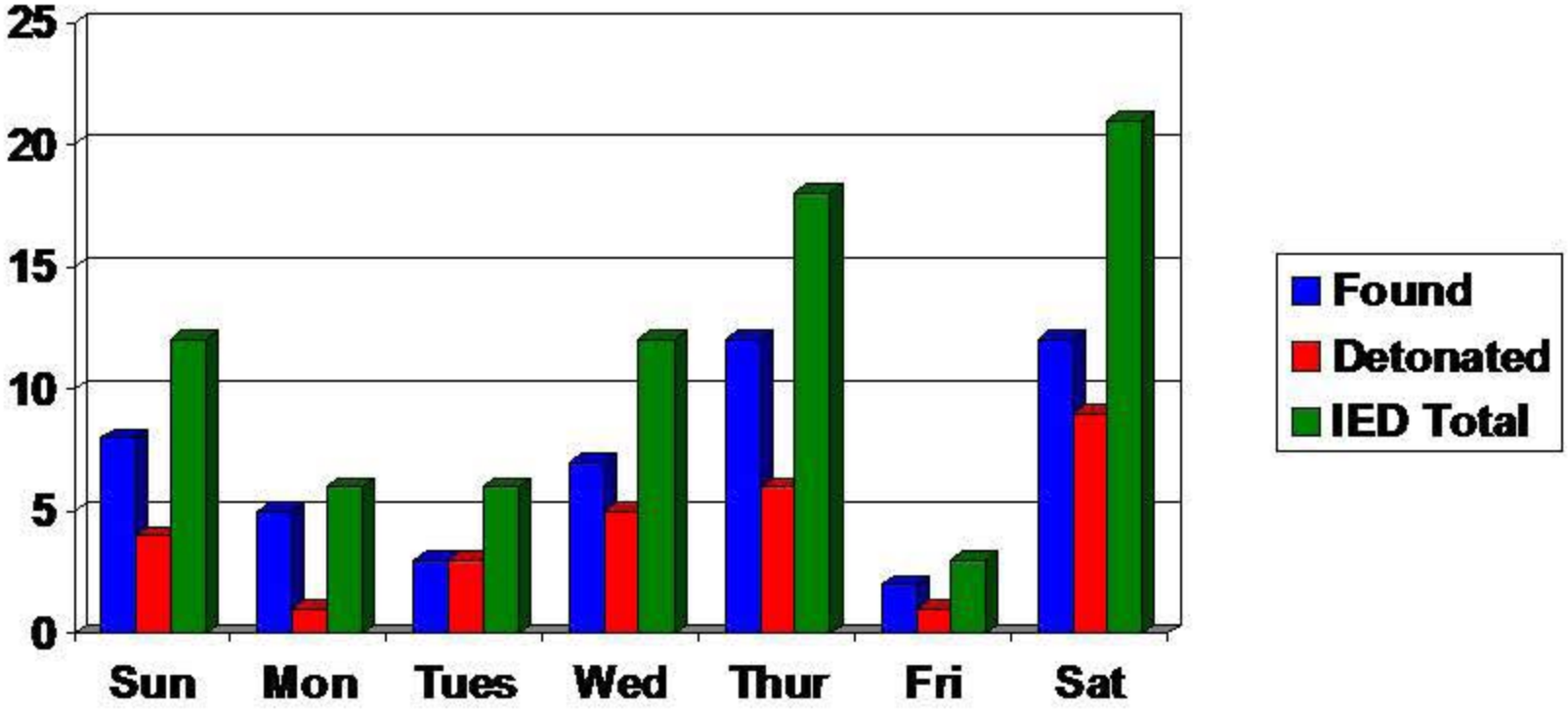
Negative Incidents		Positive Incidents	
• Negative Rhetoric	2	Peaceful Demonstrations	1
• Hostile Propaganda	5	Pro-Coalition Graffiti	0
• Ethnic Violence	2	Populace Cooperation	2
• Threats of Violence	2	Other Positive Incidents	3
• Civil Disobedience	0		
• Other Incidents	1		
	Total 12		Total 6

Summary: Trend analysis indicates a 4 week high in positive indicators and a continued low in negative indicators. [Green]



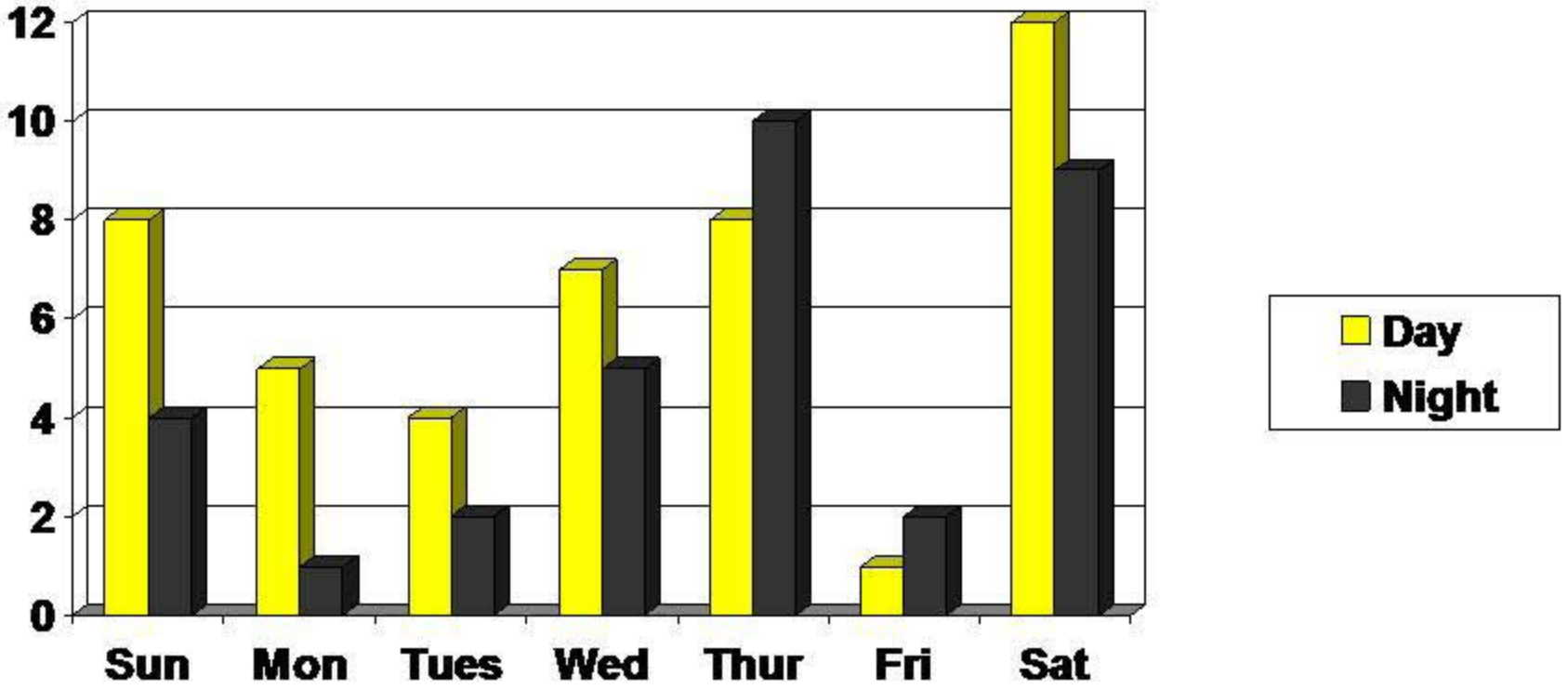
Four Week Analysis						
	ETO B	ETO C	ETO D	ETO E	AVE	Current
POS	12	9	9	14	11	3.0 Increase
NEG	14	16	10	10	12.5	2.50 Decrease

Pattern Analysis of IED Events



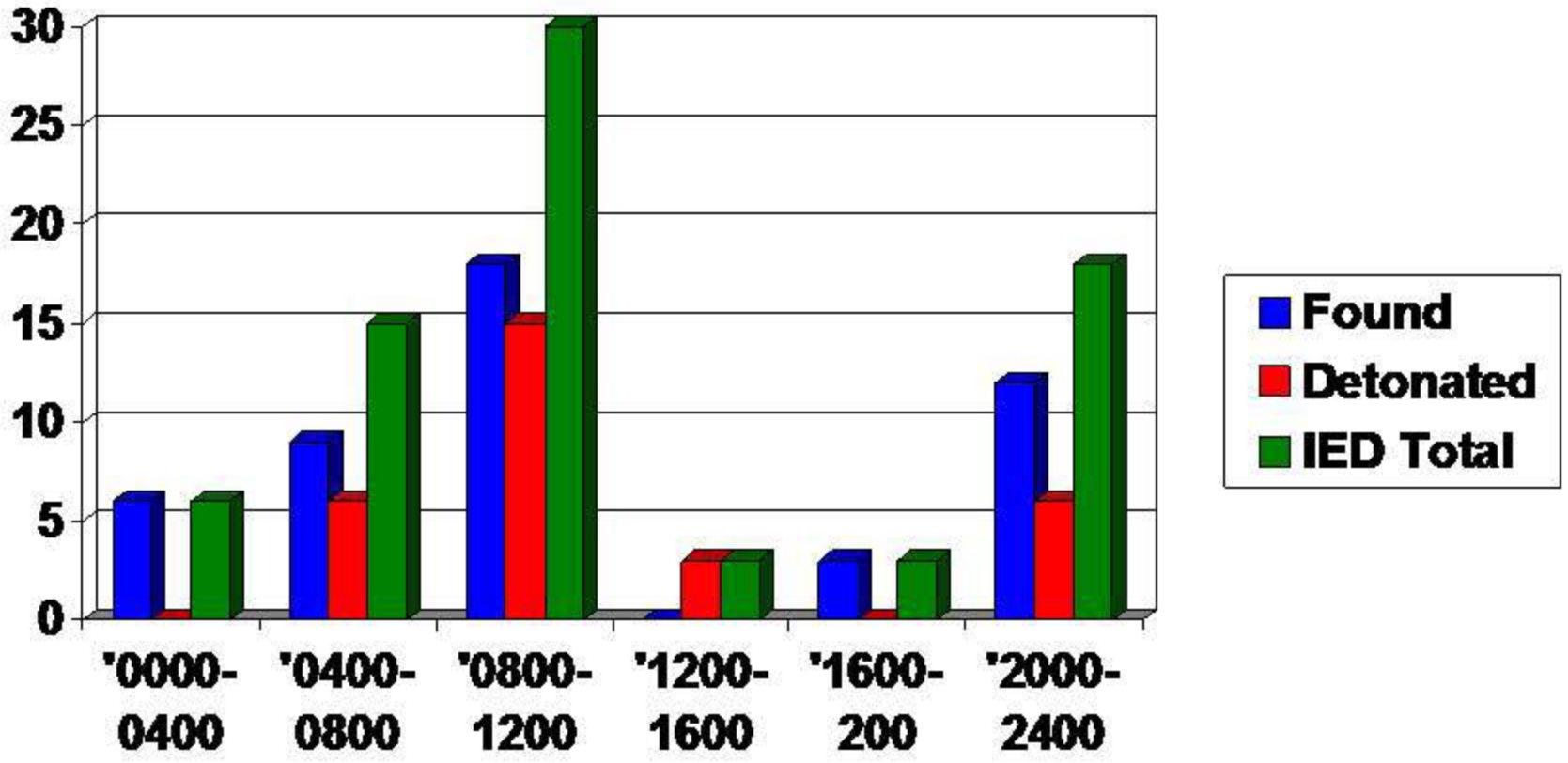
IED Attacks Charted by Day of Week

Pattern Analysis of IED Events



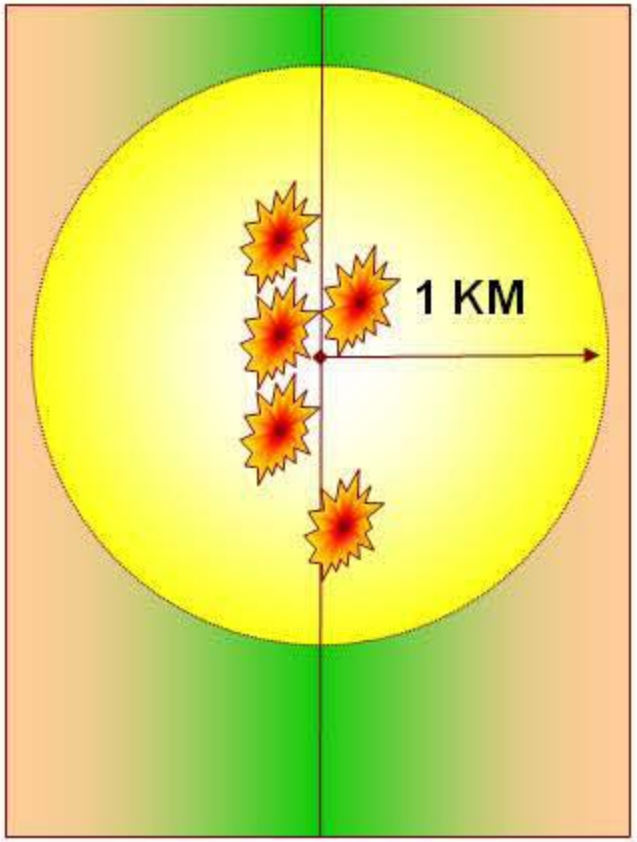
IED Attacks Charted by Day and Night

Pattern Analysis of IED Events



IED Attacks Charted by Time of Day

Definition: Tier 1 Hot Spot



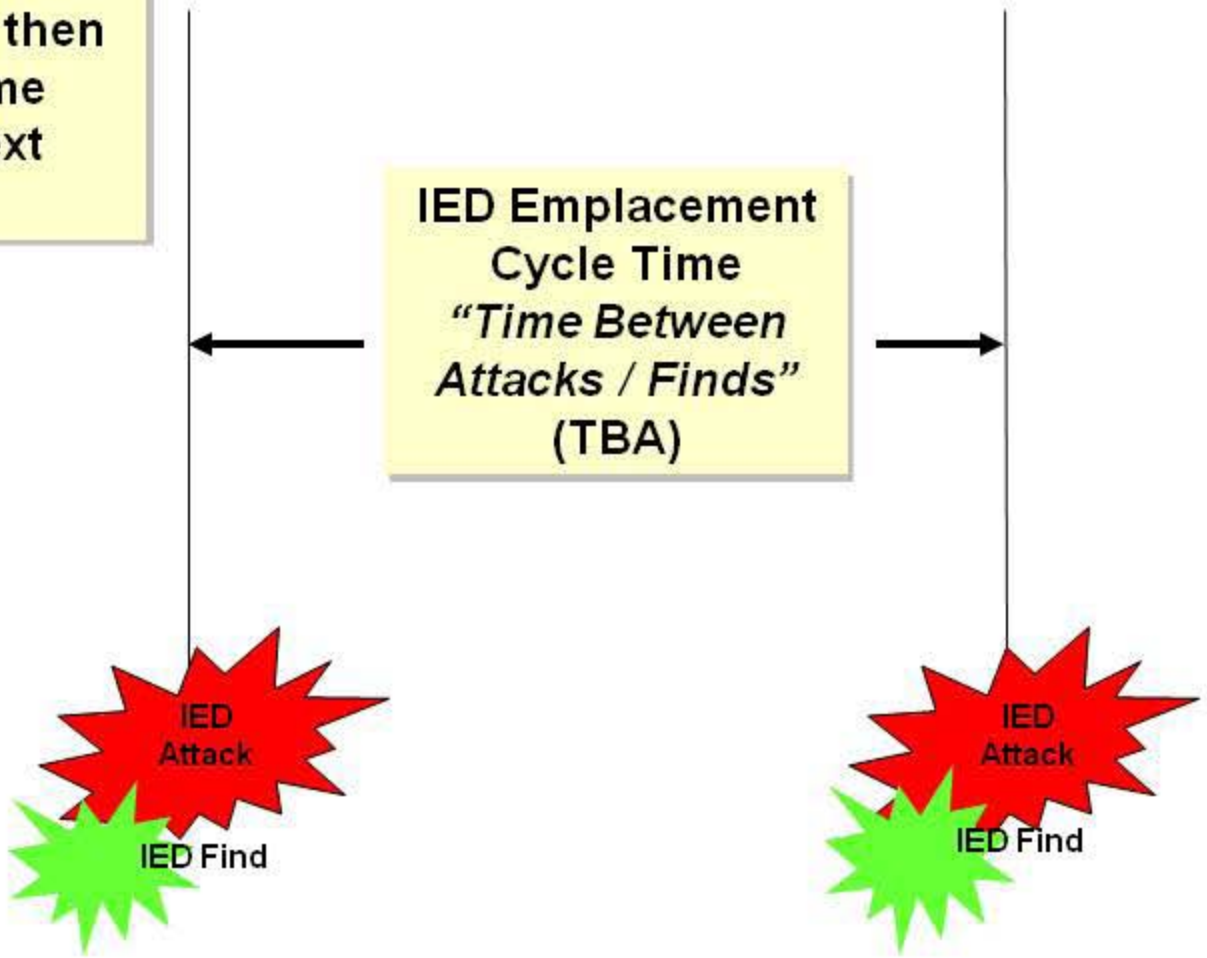
A Tier 1 Hot Spot is a location where there have been 5 or more IED attacks within a 1 kilometer radius in a four week period.

NAI

TAI

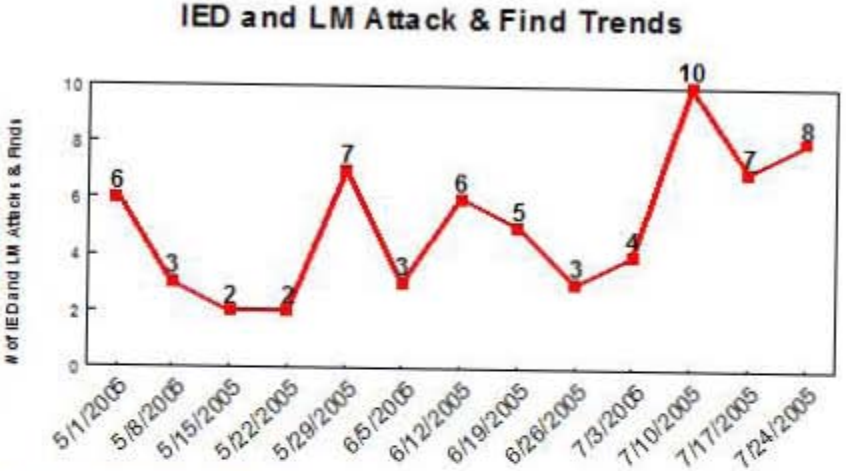
Interval Analysis

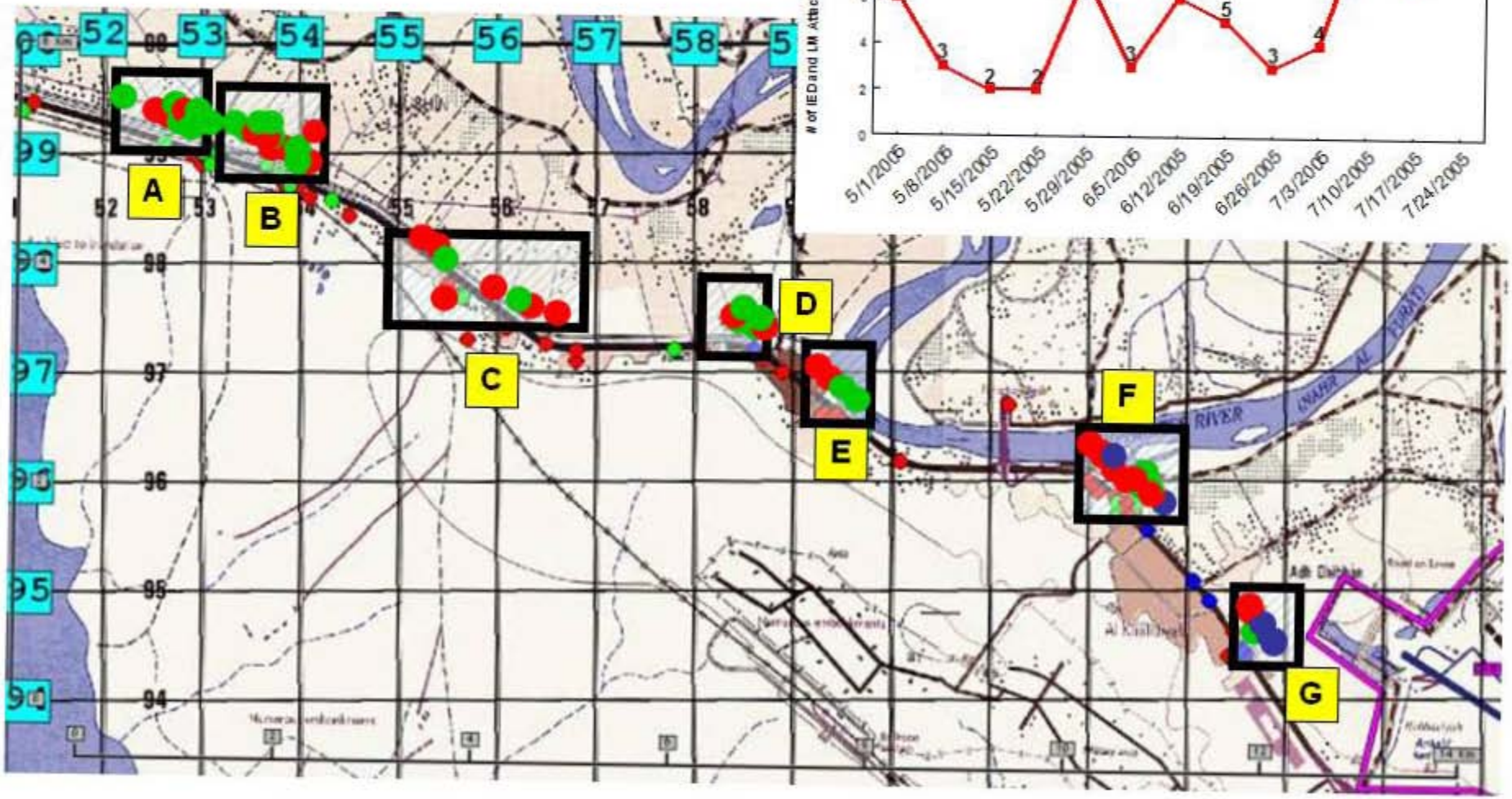
By analyzing the interval between attacks at a specific location, we can identify a pattern and then predict the general time and location of the next attack.



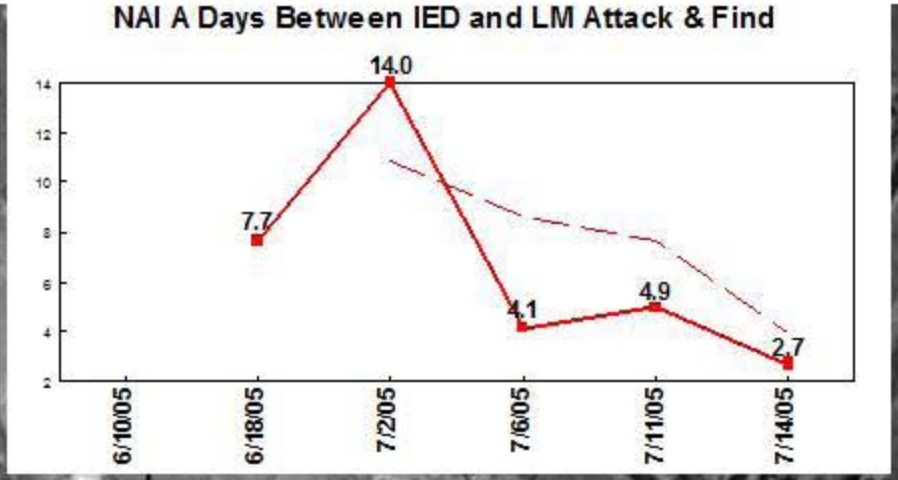
Interval Analysis

Notional date: 28 Jul 05



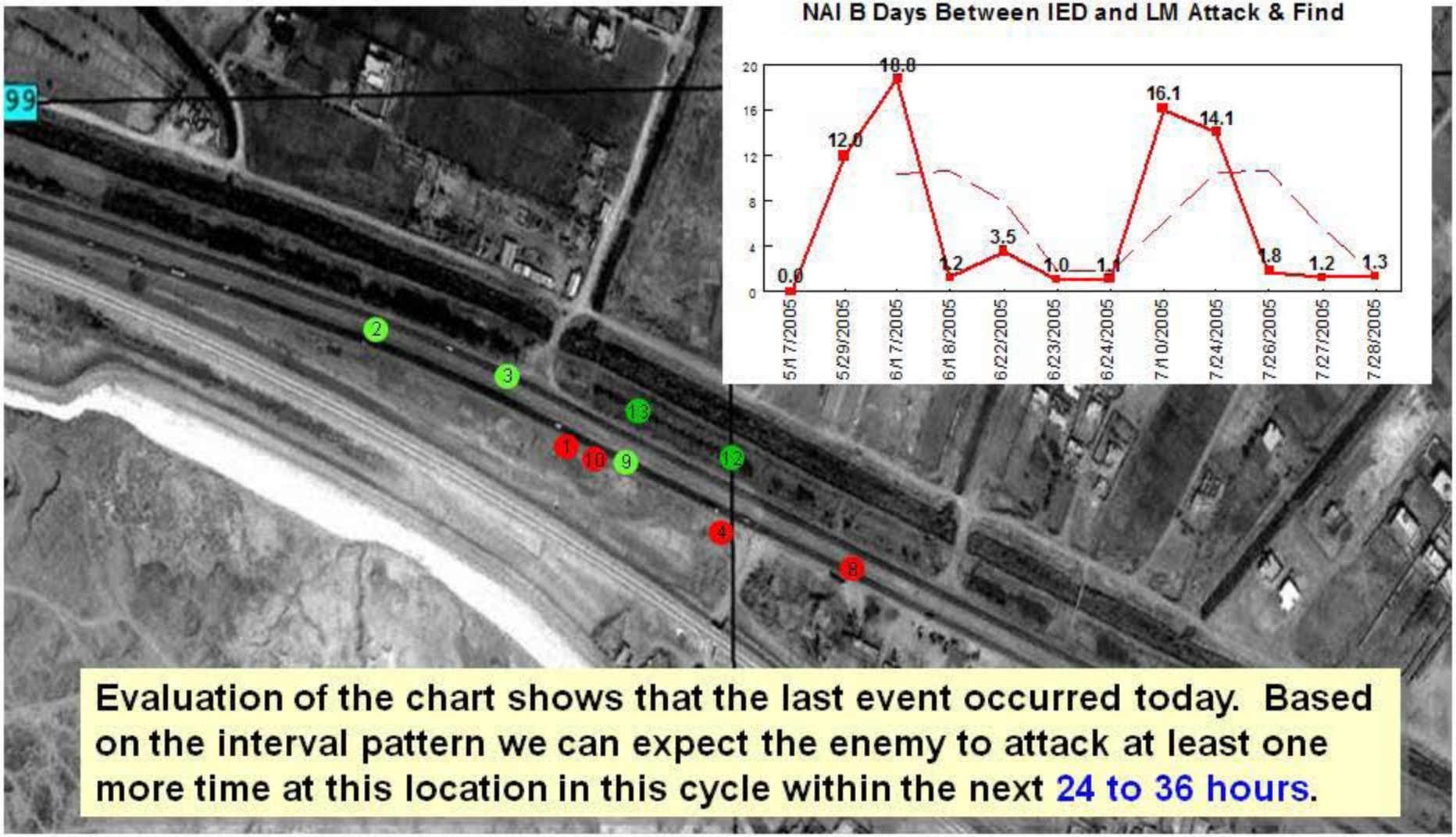


Target A



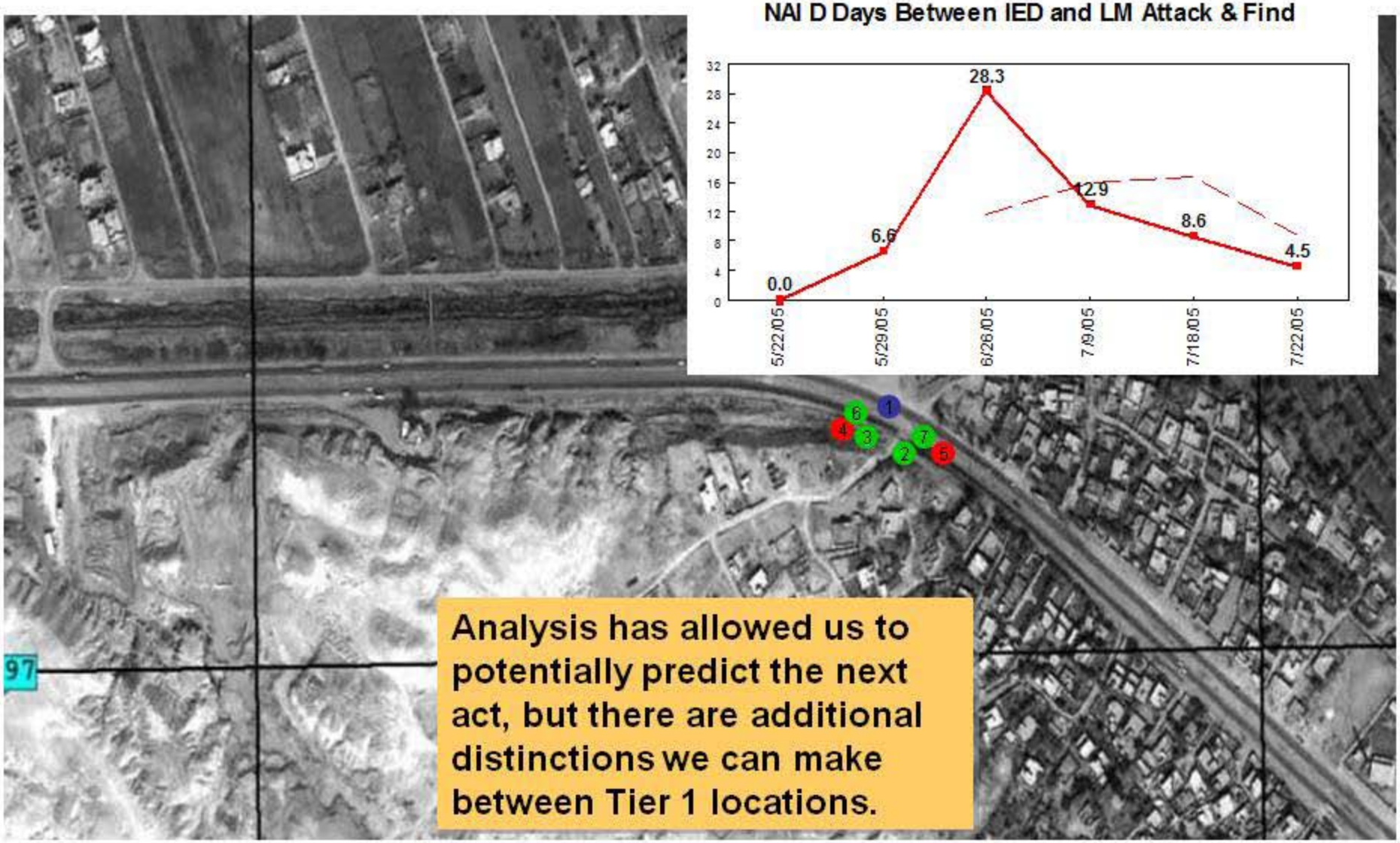
Evaluation of the chart shows that the last event was 14 Jul 05. Activity is dormant, but we do not have enough data to predict a return to activity. This is not a good area to focus currently.

Target B

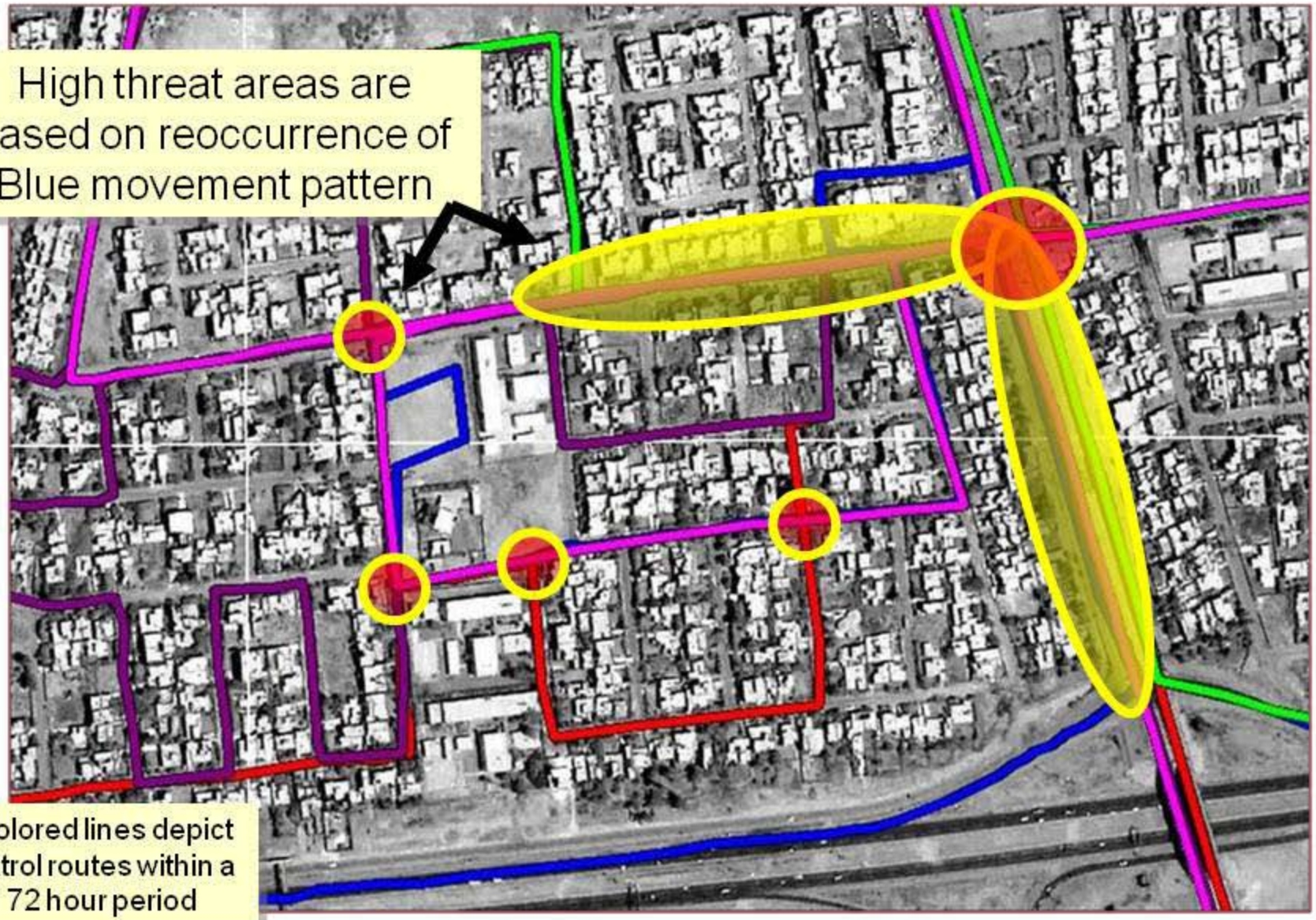


Evaluation of the chart shows that the last event occurred today. Based on the interval pattern we can expect the enemy to attack at least one more time at this location in this cycle within the next 24 to 36 hours.

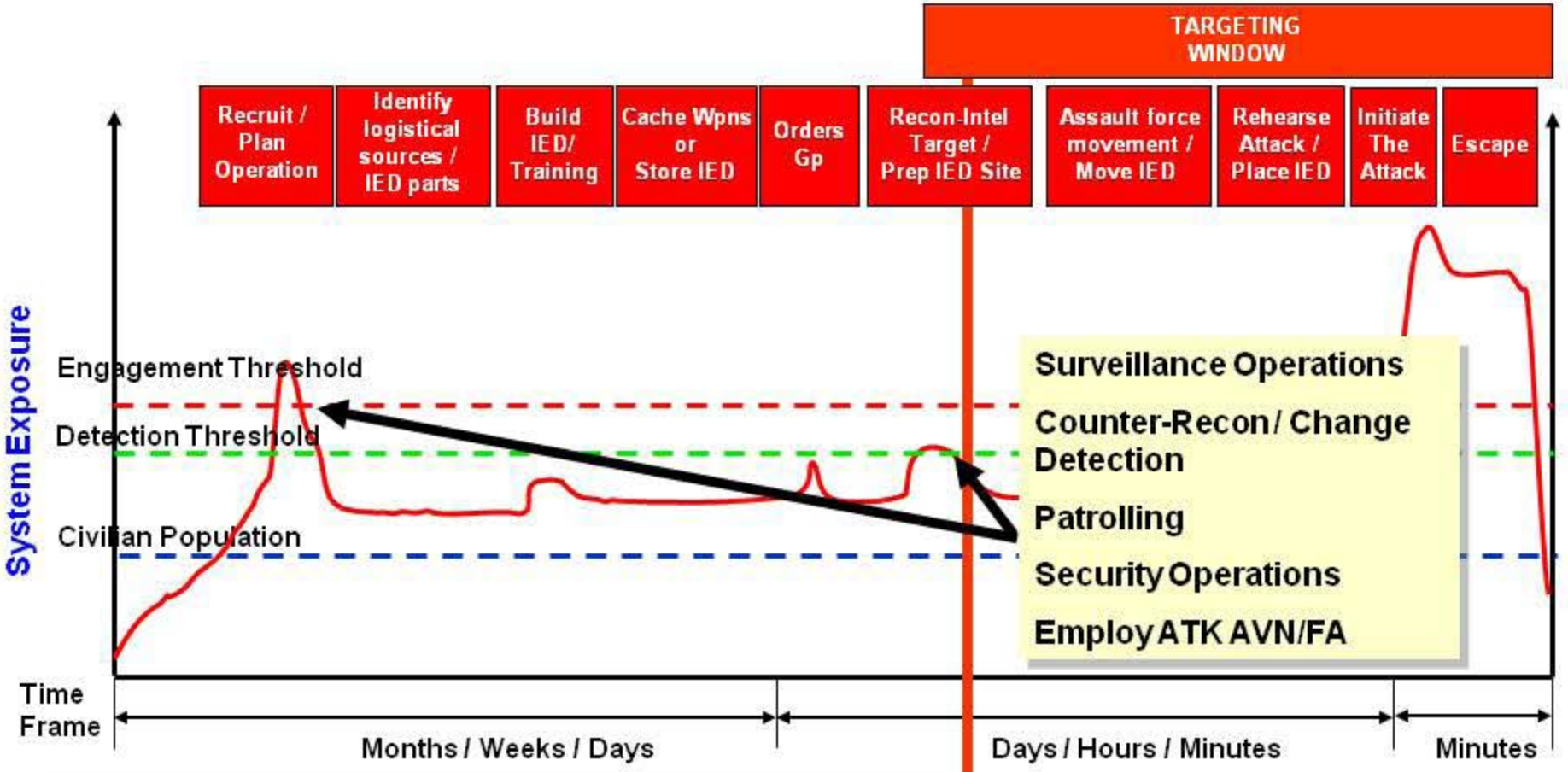
Target D


NAI D Days Between IED and LM Attack & Find
32
28
24
20
16
12
8
4
0
28.3
12.9
8.6
6.6
4.5
0.0
5/22/05
5/29/05
6/26/05
7/9/05
7/18/05
7/22/05
1
2
3
4
5
6
7
97
Analysis has allowed us to potentially predict the next act, but there are additional distinctions we can make between Tier 1 locations.

Blue Pattern Analysis



Predict: Applying Analysis



More refined analysis, particularly the application of SNA will allow us to initiate additional operations to further widen the targeting window and increase the IED System exposure.

Network Analysis

Center of Gravity (COG) Analysis

Carl von Clausewitz was the first to apply the term "center of gravity" to warfare. He described a center of gravity as;

> *"the hub of all power and movement, on which everything depends."*

Clausewitz clarifies this description by stating that:

> *"the ultimate substance of enemy strength must be traced back to the fewest possible sources, and ideally to one alone."*

A COG is the source of power that creates a force or a critical capability that allows an entity to act or accomplish a task or purpose

Other Terms for COG: Key Nodes, Decisive Points, Critical Vulnerabilities

COG Analysis

How to Determine a COG

1. ID adversary's **critical requirements**
2. Determine adversary's **critical capability** to achieve these requirements
3. ID **source of power** for the adversary's critical capability
4. ID critical **functional needs** of adversary's critical capability
5. Where are adversary's **security measures** are focused

Once COG is Determined – ID its Critical Vulnerabilities to Attack or Disruption

COG Analysis

Methods to Assess a COG

- Gravity Model Analysis
- Critical Capabilities Analysis
- Needs/Requirements Analysis
- Critical Processes Analysis
- Vulnerabilities Analysis
- Network Nodal Analysis
- Communications Analysis

COG Analysis

Main Questions to Answer

- Criticality (How critical is it to success of adversary operations?)
- Adversary Focus (Where is his attention focused?)
- Security (Is it well protected?)
- Complexity & Resiliency (Is it part of a complex network?)

COG Analysis

Two Ways to Engage and Target a COG:

1. **Directly**

   A direct attack on an identified COG can prove to be a decisive point in a battle

2. **Indirectly**

   Aimed at those processes that support the COG

   Very often the only available choice in asymmetric COE

   Usually used to disrupt the process—rarely succeeds in destroying the COG itself

Emergent Networks

Emergence:

The process of complex pattern forming and emerging from simpler rules and structures

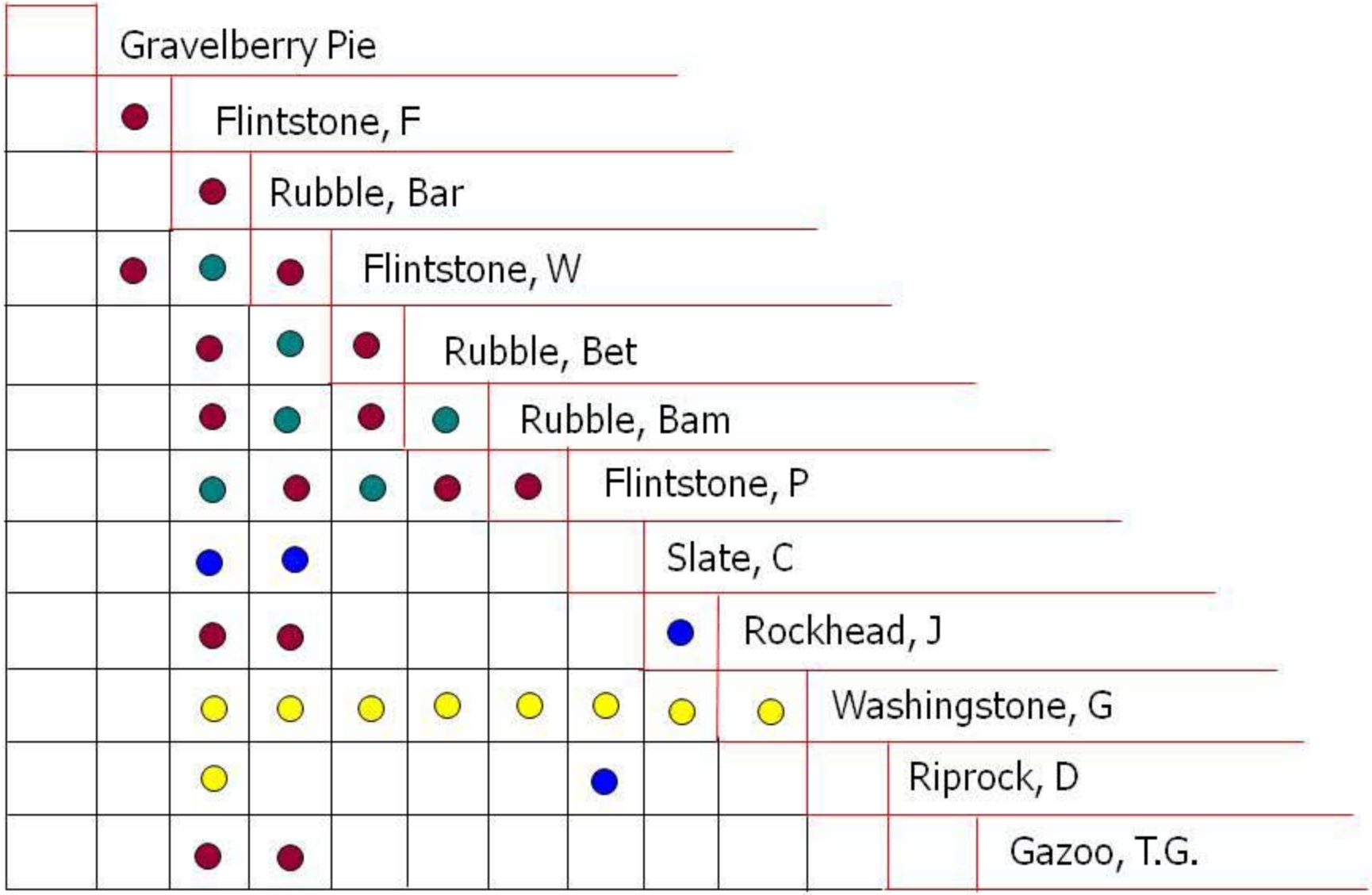
- Also refers to the arising reorganizational structure of existing networks as they evolve and shift

Link Analysis

Highlights associations and contacts between persons, events, activities and organization. Four techniques used in link analysis to cross reference information are:

- Association Matrix (understand the cell)
- Activities Matrix (insurgent vs. criminal)
- Time Event Charts
- Link Diagrams

Association Matrix



Activities Matrix

Time Event Charts

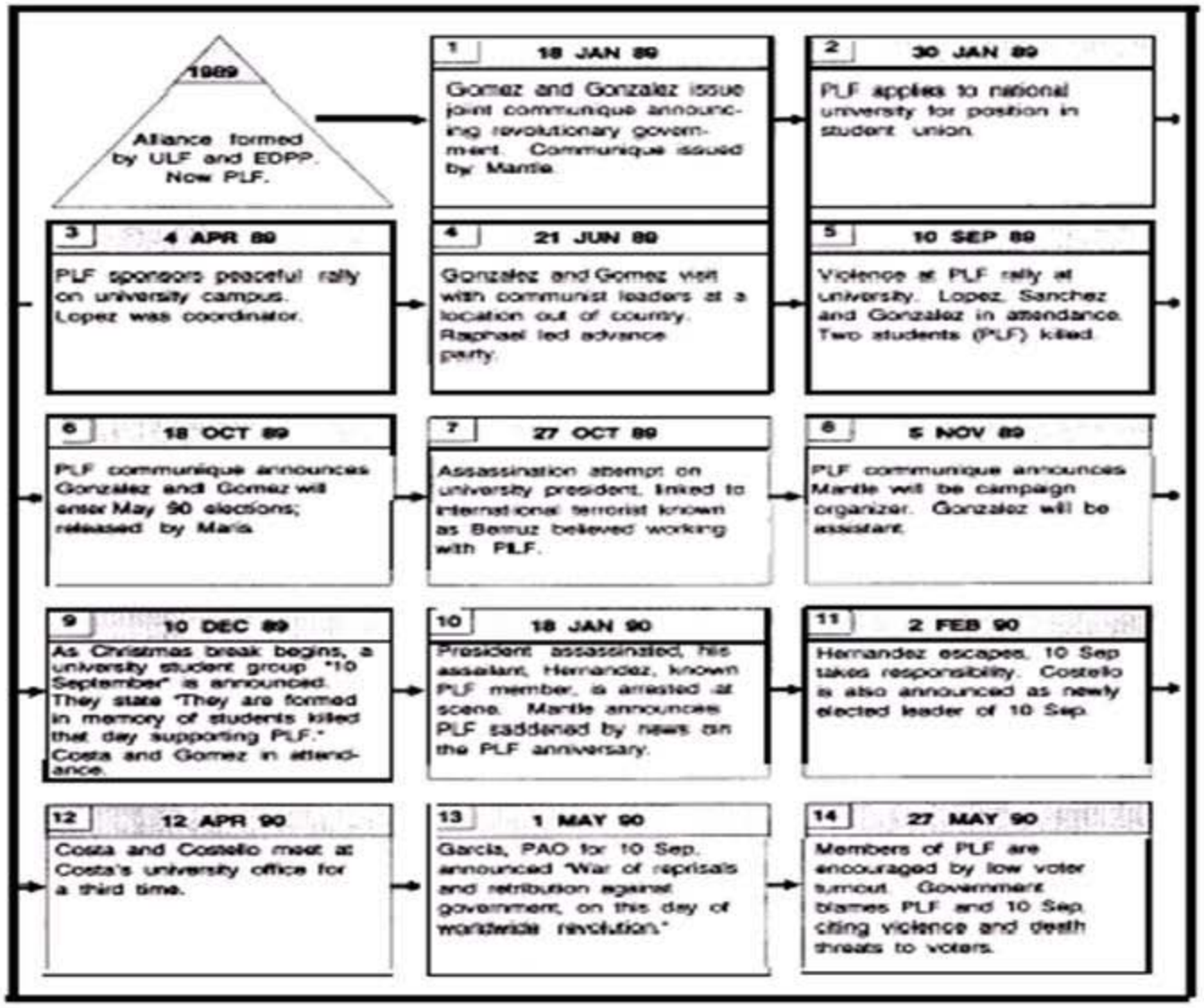
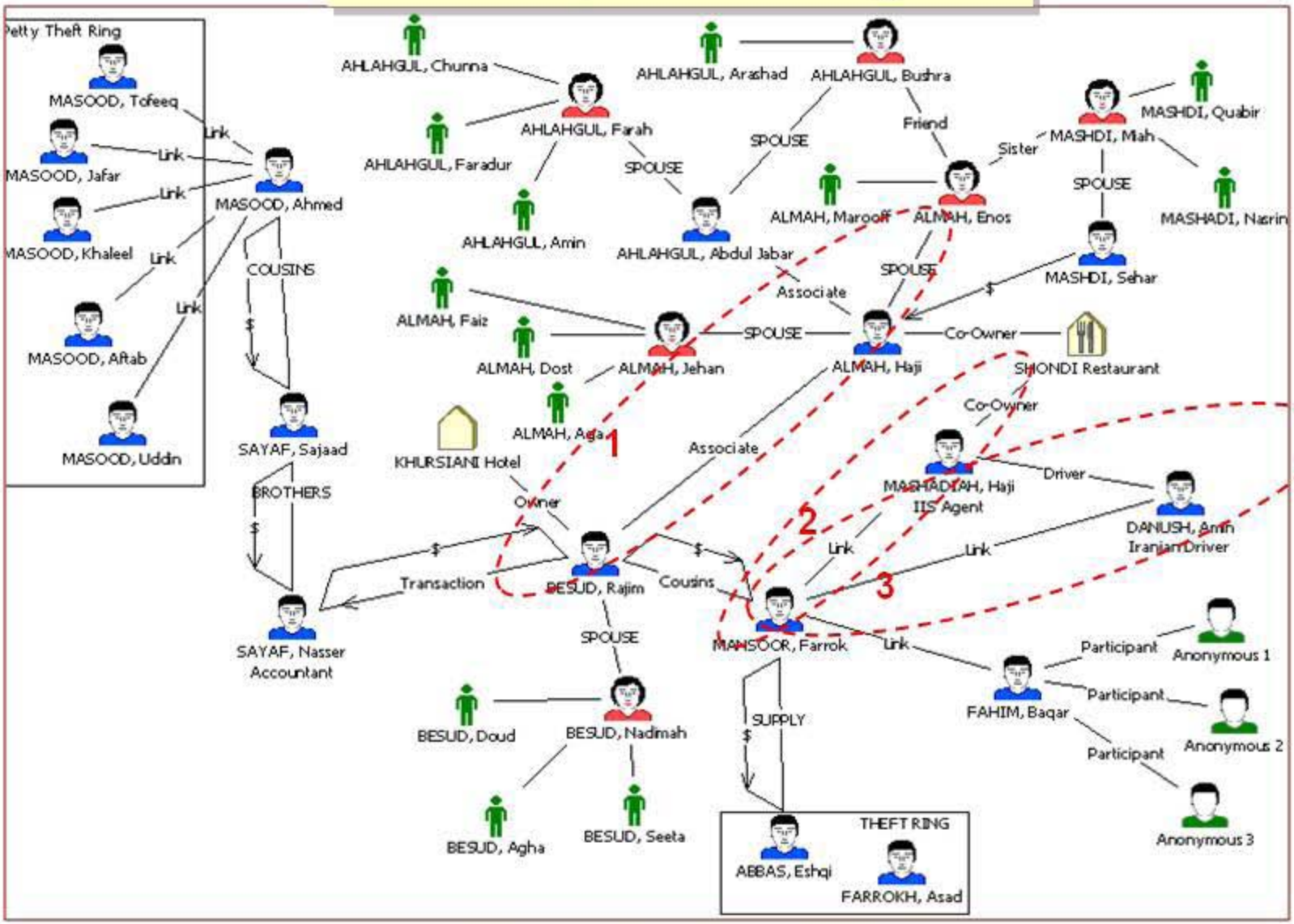


Figure 4-7. Time event chart.

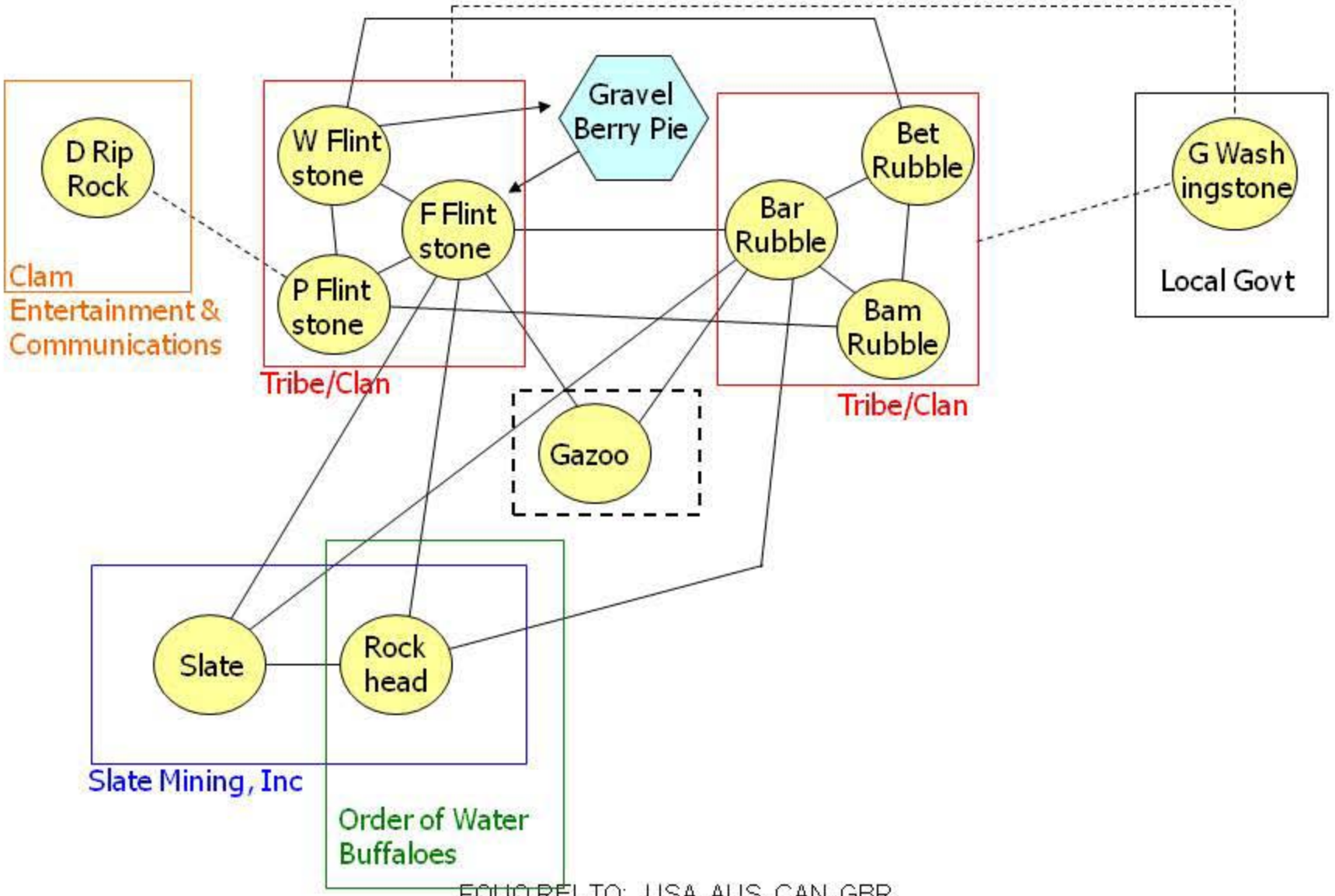
FM 34-130, 1994, p. 3-63

Social Network Analysis

An Example Link Diagram



The Link Diagram



Tying the Analysis Together

- Pattern analysis provides the where and when of the next attack and narrows the focus for the who (group-individual) by the signature of a recurring pattern. It will not reveal the network composition, just that one exists.
- SNA – Link diagram analysis provides a method for establishing and tracking associations between individuals within a group and the relationship of functions.
- Terrain analysis when combined with pattern analysis provides refinement to the where of the next event and may identify certain terrain patterns more conducive to future attack, insurgent activities and transition between events.
- Indicators provide the potential to develop start points to begin the SNA to match pattern analysis and therefore, simultaneously target all levels within the insurgent network.

Visualization Filtering Process

MDMP

Urban COIN Analytical Framework

1. Define the battlefield environment
2. Describe the battlefield effects
3. Evaluate the threat
4. Determine threat COA

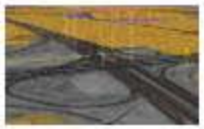
- General Description
- Weather & Terrain
- Physical Patterns & Effects
- Mobility Corridors & LOS
- Multi-Dimensional Space
- Structure Typology
- Infrastructure & Services
- Population: Cultural & Civil Factors
- Threat
- 2nd & 3rd Order Effects

Civil Considerations

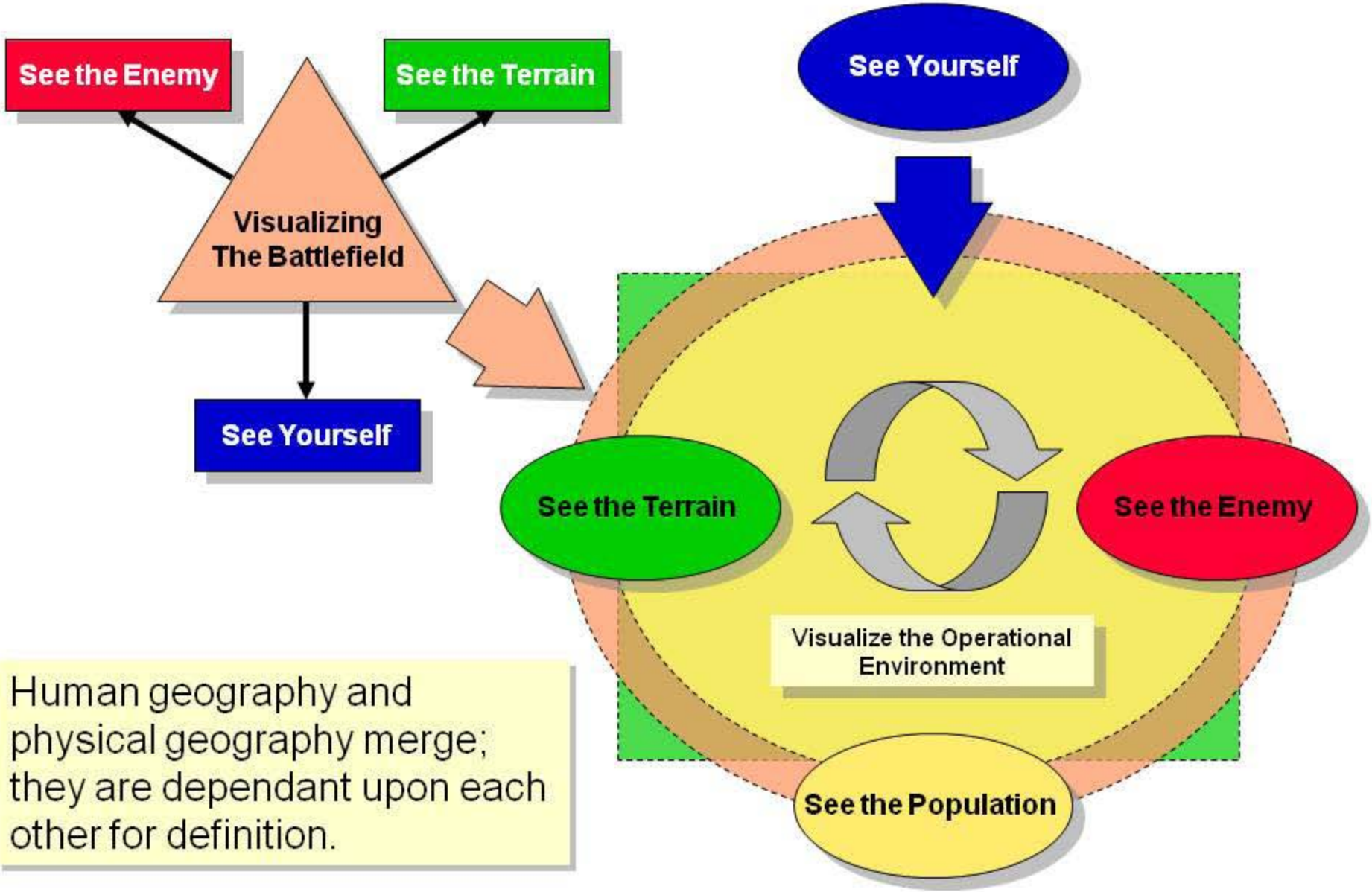
- Areas
- Events
- Organization
- Capabilities
- People
- Social Structures

Visualization

- Observation & Fields of Fire
- Avenues of Approach
- Obstacles
- Cover & Concealment
- Key Terrain

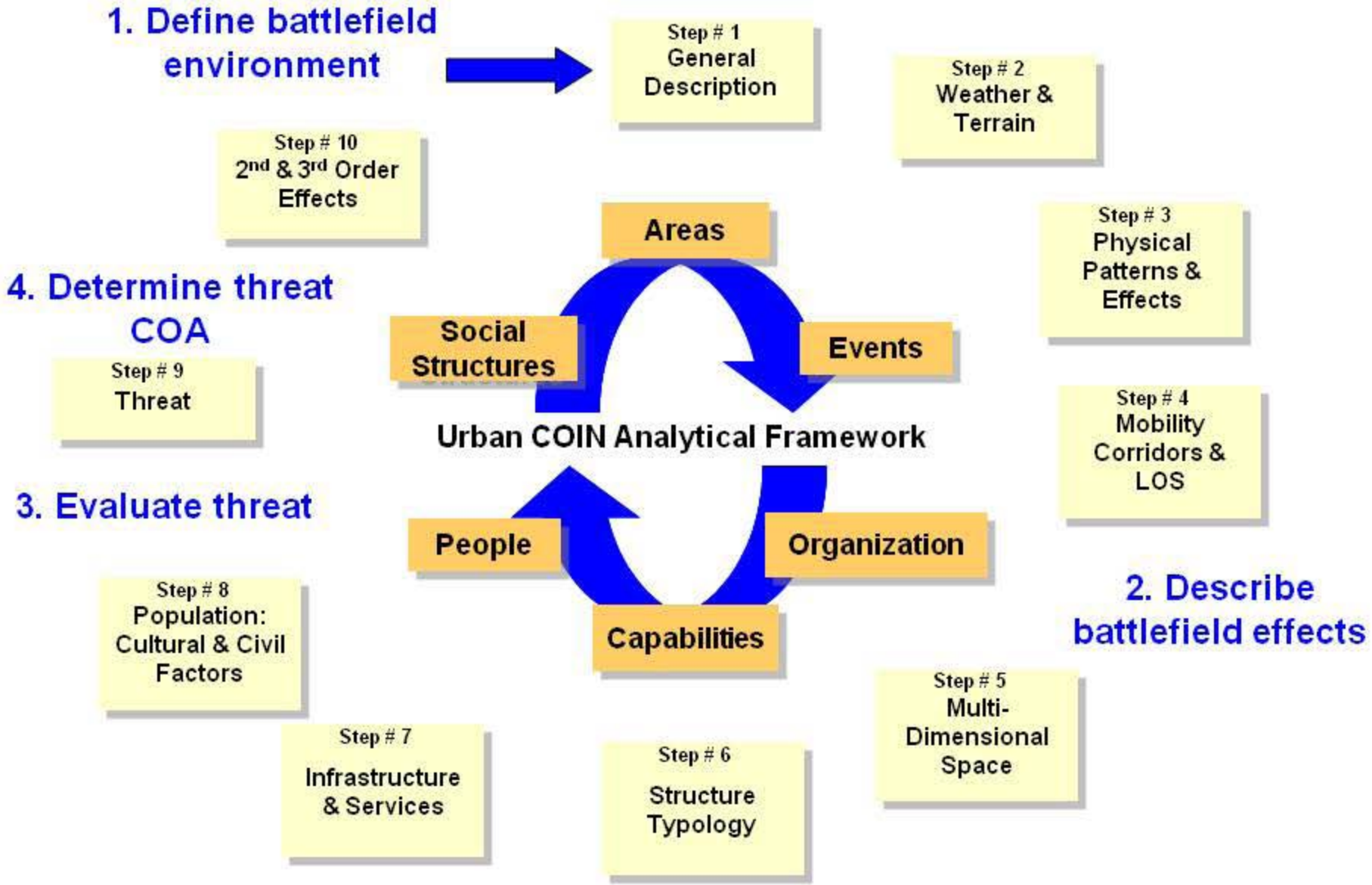


Visualization in the COIN Environment



Human geography and physical geography merge; they are dependant upon each other for definition.

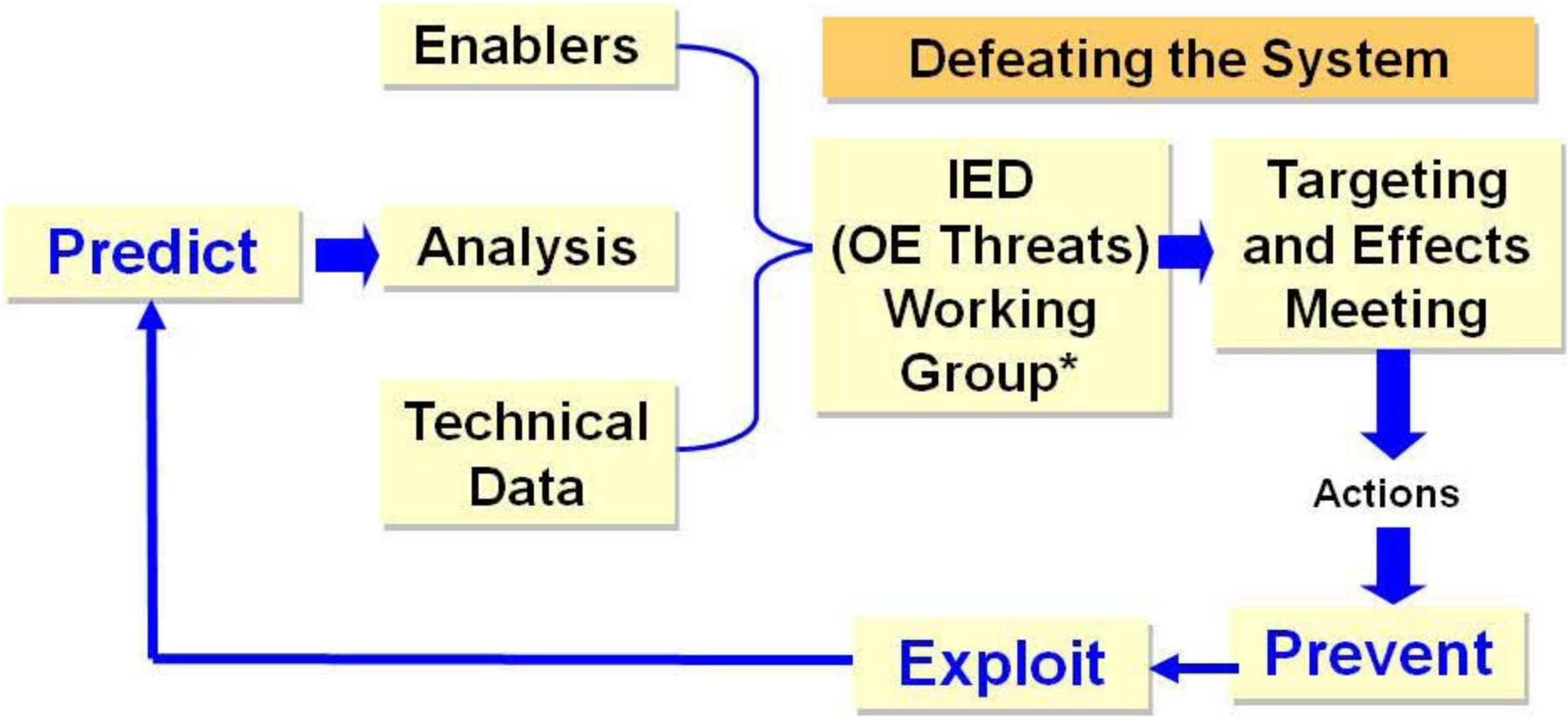
Visualization Equals IPB



Staff Process and Resources

COIN Enablers

Integration of Enablers



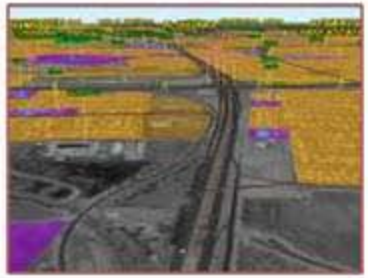
Integrating Enablers

Potential Assets : Organic and **J**oint, **I**nteragency, **I**ntergovernmental **M**ultinational (**JIIM**)

- Organic
  - Informants / unit collection of HUMINT
  - Route reconnaissance and clearance assets
  - Dog Teams, search advisors
  - BDE Terrain Team
  - Acoustical / Optical sensors
  - Sniper Employment Officer (SEO)
  - Military instruction Training Team (MiTT)

- **J**oint
  - Joint IED Defeat Organization (JIEDDO)
  - Weapons Intelligence Teams (WIT)
  - Tactical HUMINT Teams (THT)
  - EW Coordination Cell (EWCC)
  - UAS & Aviation assets
  - Special Operations Forces (SOF)

- **I**nteragency
  - Combined Explosive Exploitation Cell (CEXC)
  - Exploitation of evidence collected (searches, cordons, TCPs, etc.)
  - National Ground Intelligence Center (NGIC)
  - National Geospatial Intelligence Agency (NGA)



- **I**ntergovernmental
  - Ministry of Oil
  - Ministry of Interior

- **M**ultinational
  - Joint patrols

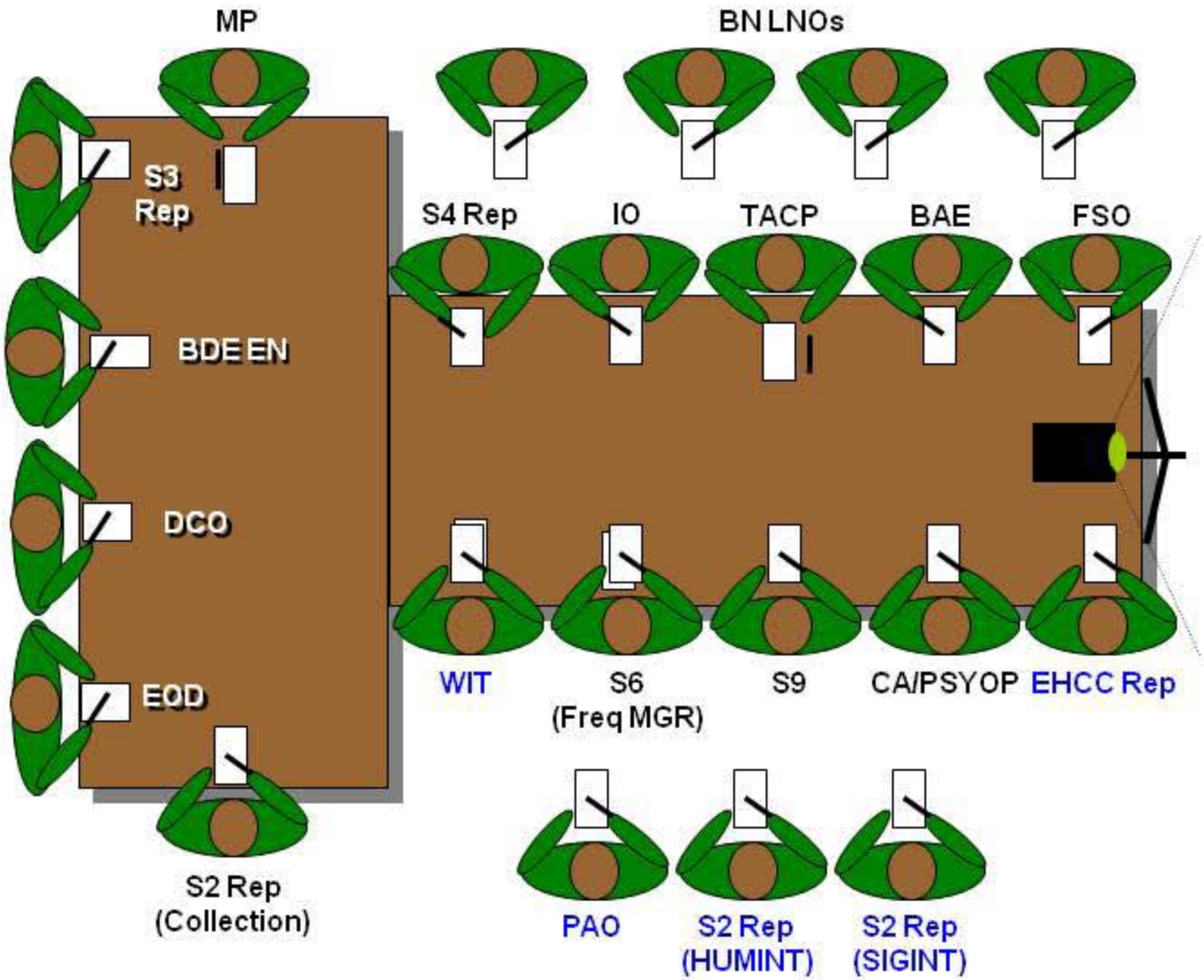
Additional Agencies

- Special Operations Forces
- Explosive Ordnance Disposal (EOD)
- Counter Explosive Hazards Center
- CALL
- OPTAG (British Operations Training Assistance Group)
- National Geospatial Intelligence Agency (NGA)
- Asymmetric Warfare Group (AWG)

Coordinating Offensive Operations

Targeting

The IED Working Group: Brigade



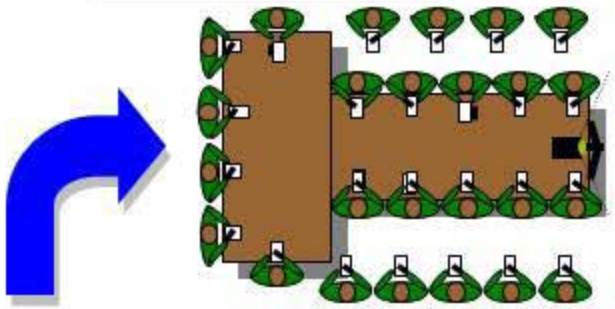
Agenda

- Old Business
- Trends & New TTPs
- New Equipment / Resources
- IED (OE Threats) Countermeasures
- Targeting

Linkage

Output focus is mitigation & interdiction

IED Working Group



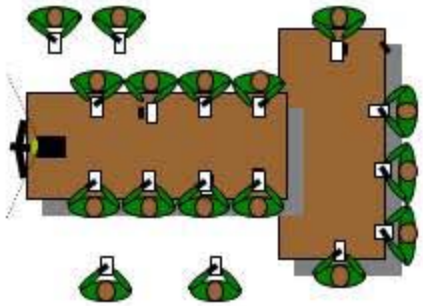
- EW Plan / CREW Plan
- Route clearance plan / schedule
- Recommended fielding plan
- Technical forensics trends
- RT clearance analysis
- Equipment fielding
- Analysis / Determination of Tier I sites

Analysis & Recommendations for CDR

Technical data and focus input:

- Trend analysis
- Frequency Management
- CREW
- Technical forensics trends
- RT clearance analysis
- Equipment fielding

Feeds



Targeting Meeting

- Lethal & non-lethal
- Collection Plan
- Allocation of resources
- Recommendation to act on Intelligence (or not)
- Actions / projects nested to Campaign Plan to achieve effects
- Ultimate result: actions to identify, capture or kill a specific individual

Example IED Working Group Agenda

- Introduction
  - Review of working group purpose and products
- Current IED / EH trends in theater
- Current TTPs
- New equipment and resources
- IED countermeasures
- Identification of Lessons Learned for feedback
- Analysis and recommendations
  - Outputs / products for targeting
- Questions

Example IED Working Group Agenda

- Introduction
  - Review of working group purpose and products
- Current IED / EH trends in theater
- Current TTPs
- New equipment and resources (frequencies)
- IED countermeasures
- A
- Q

Review IED SIG events & enemy TTPs
Review CEXC investigations & enemy TTPs
Review EOD technical IED reports & enemy TTPs
Review mine incidents & enemy TTPs
Review EW Jammer frequencies
Review geo-spatial products

Example IED Working Group Agenda

- Introduction
  - Re
- Curre
- Curre
- New e
- IED c
- Analysis and recommendations
  - Outputs / products for targeting
- Questions

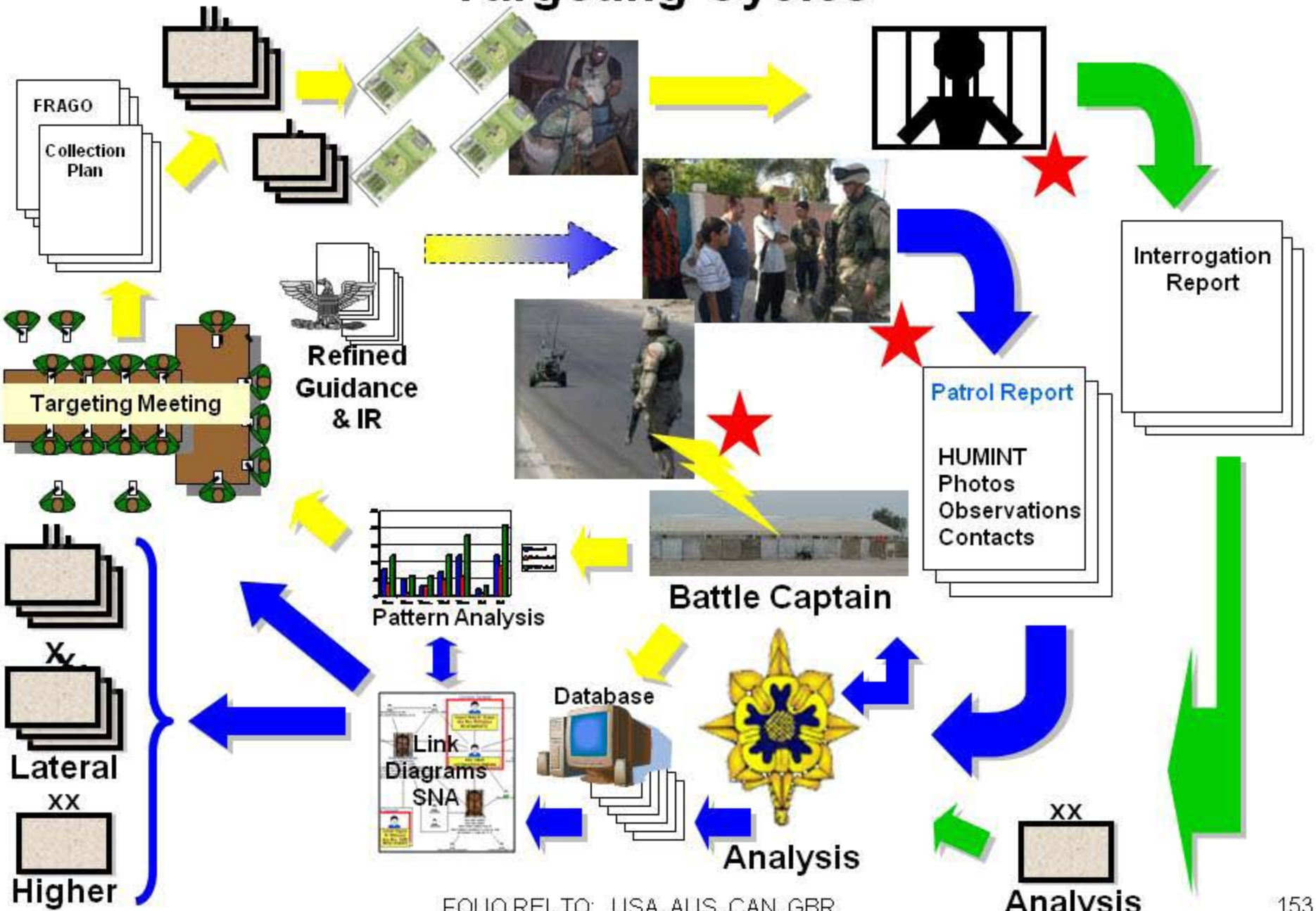
Determine Tier 1 Hot Spots on geo-spatial product
Recommend AF EW targets (& frequencies)
Recommend actions for defeating IED cell
Recommend target areas for defeating IED emplacement cell

Example IED Working Group Agenda

- Introduction
  - Revie
- Current I
- Current T
- New equ
- IED coun
- Analysis and recommendations
  - Outputs / products for targeting
- Questions

Division
JIEDDO web page
Daily sync brief / BUB
Weekly CEXC update
Sensitive site exploitation (EOD, WIT, CEXC, JIEDDO)

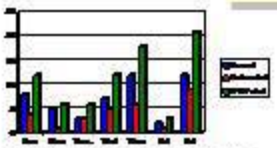
Targeting Cycles



A System of Interconnected Action Loops

Operations Loop

Response Loop



Mitigate

Neutralize

Intelligence Loop

Detection Loop

Visualization Tools

Detect

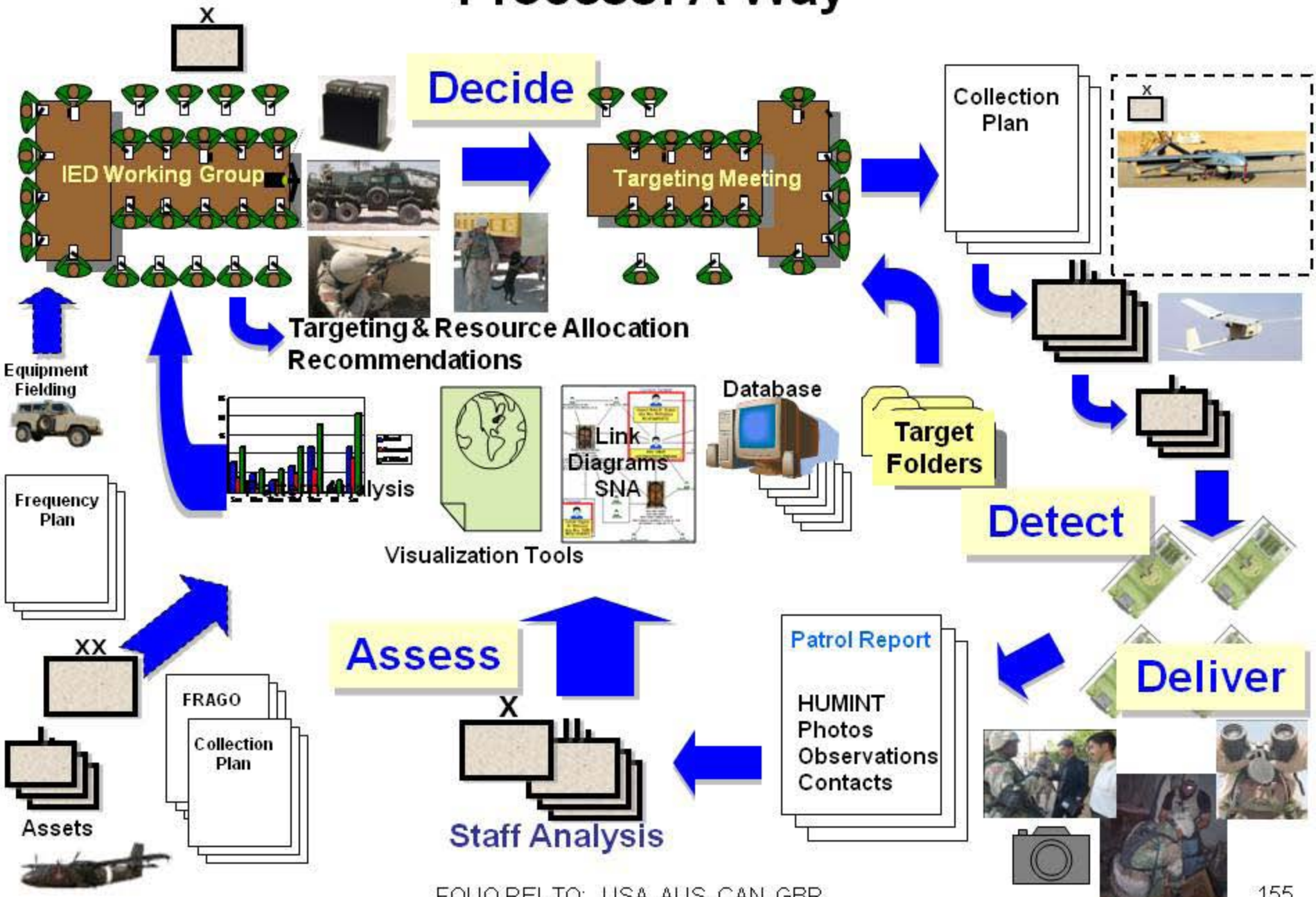
Predict

Prevent

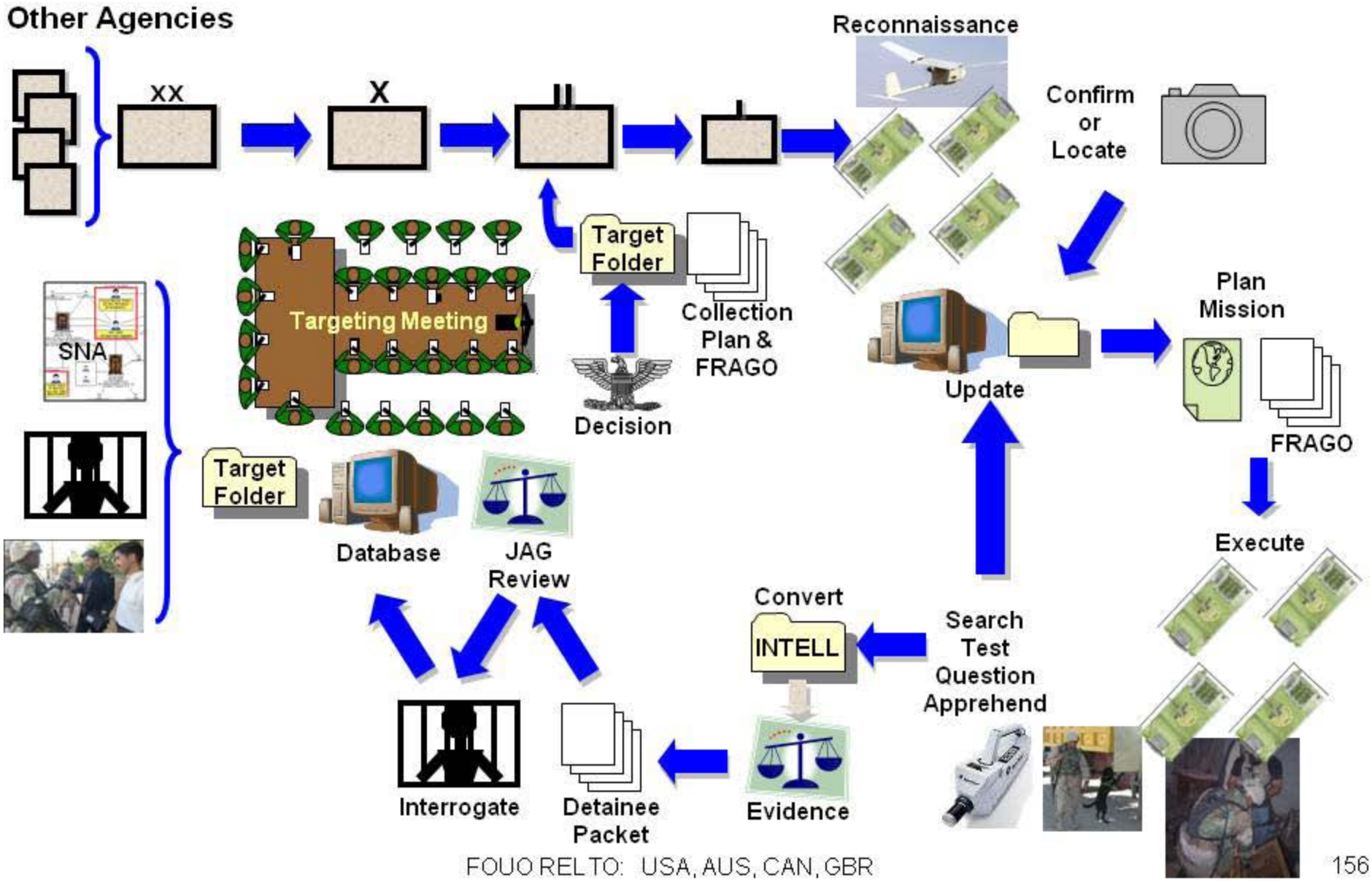
External Input Loop

Network Defeat Loop

Process: A Way

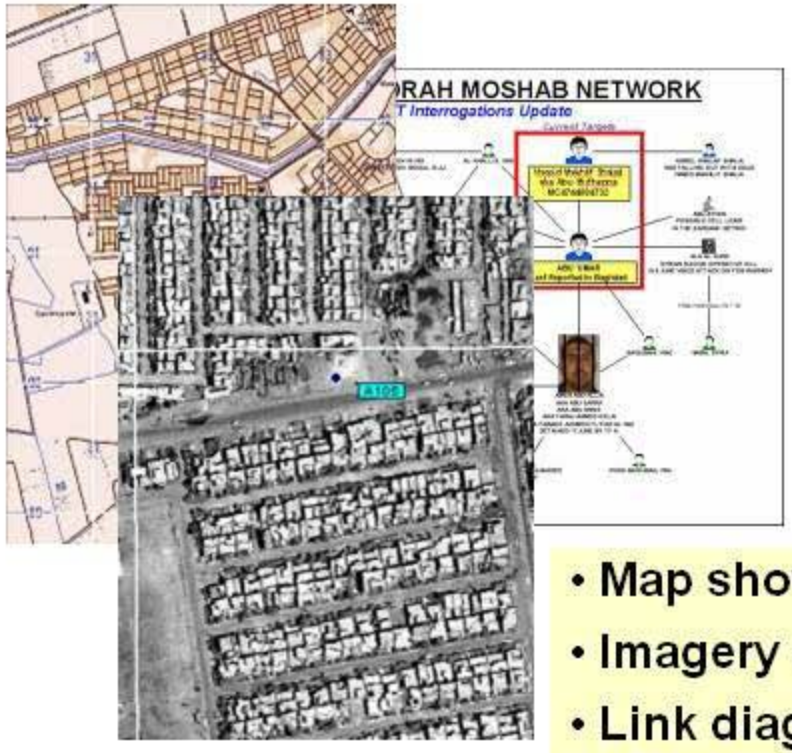


Target Folder Life Cycle



Target Folder Composition

(May vary by Unit)



- **Map showing address**
- **Imagery of address**
- **Link diagram**

- Name
- Associates and family
- Vehicle
- Address (636, 54, 29)
- Job or trade
- Patterns / mosque
- What he's done
- Intelligence reports, HUMINT collected
- Copies of witness statements or interrogation reports

Obtain photo of individual and vehicle if available; also a photo of the gate at the residence is considered to be a critical reconnaissance product.

Intelligence data provides the basis for a detainee packet

Staff Process and Resources

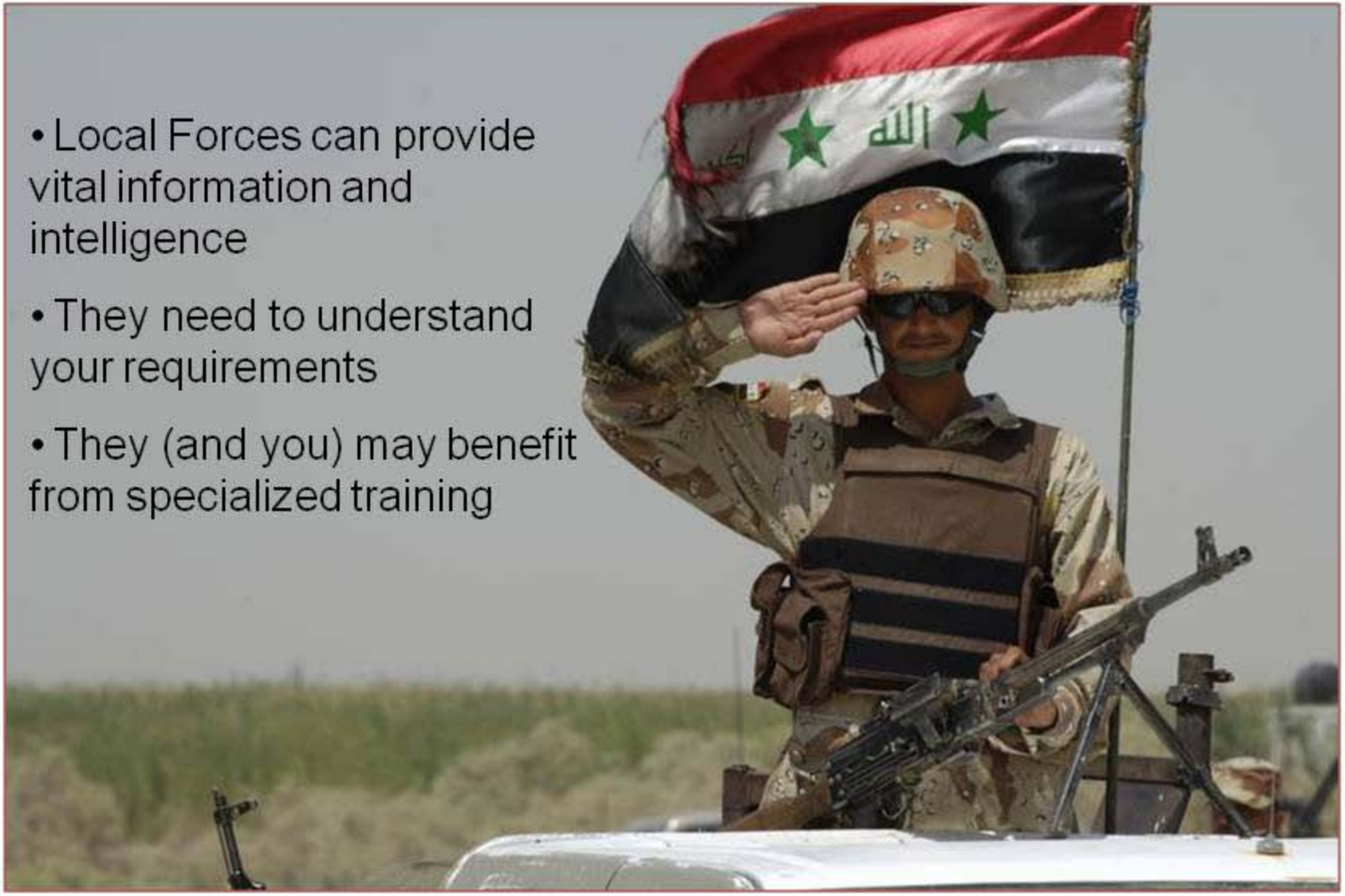
Gathering Data and Intelligence

The Ultimate Weapon

- Patrols must be given reconnaissance objectives
- FSO / IO targeting must focus patrols with objectives
- Every patrol is a combat patrol
- Every patrol must be debriefed

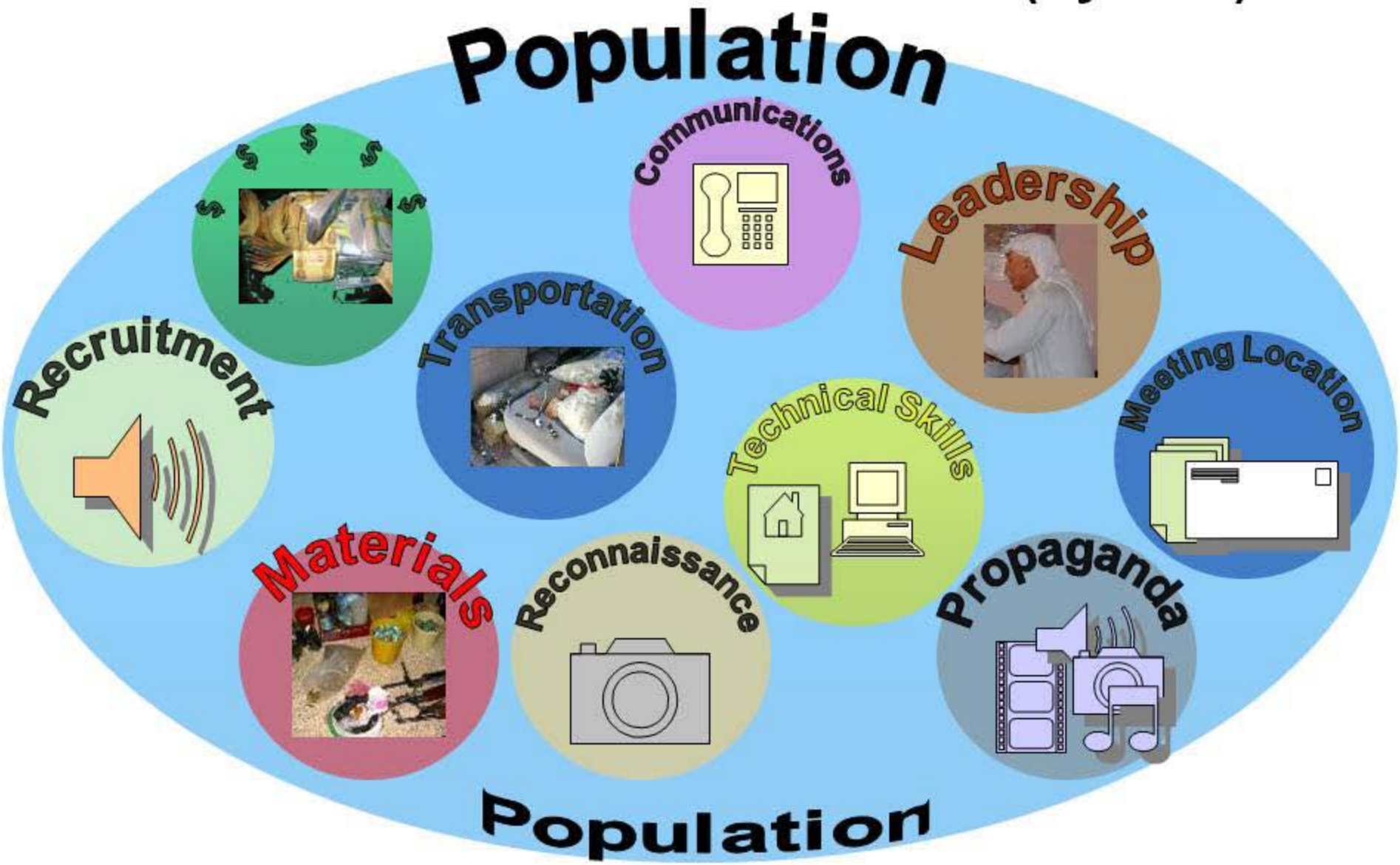
- The best source of reliable intelligence is a soldier on the ground, on patrol
- Every soldier is a sensor
- HUMINT provides the critical ingredient needed to paint the intelligence picture

Don't Forget Our Allies



07/13/06 - An Iraq army soldier from 4th Battalion, 1st Brigade, 4th Infantry Division salutes

Indicators to Reveal the Network (System)



Imperatives for Locating the Indicators

- Patrols must engage the population, even if it requires creating situations to force the interaction.
- Patrols must dismount vehicles and seek out information (interact).
- Soldiers must be empowered as part of the collection process.
- Soldiers must know and understand what information they are looking for and why it is important.

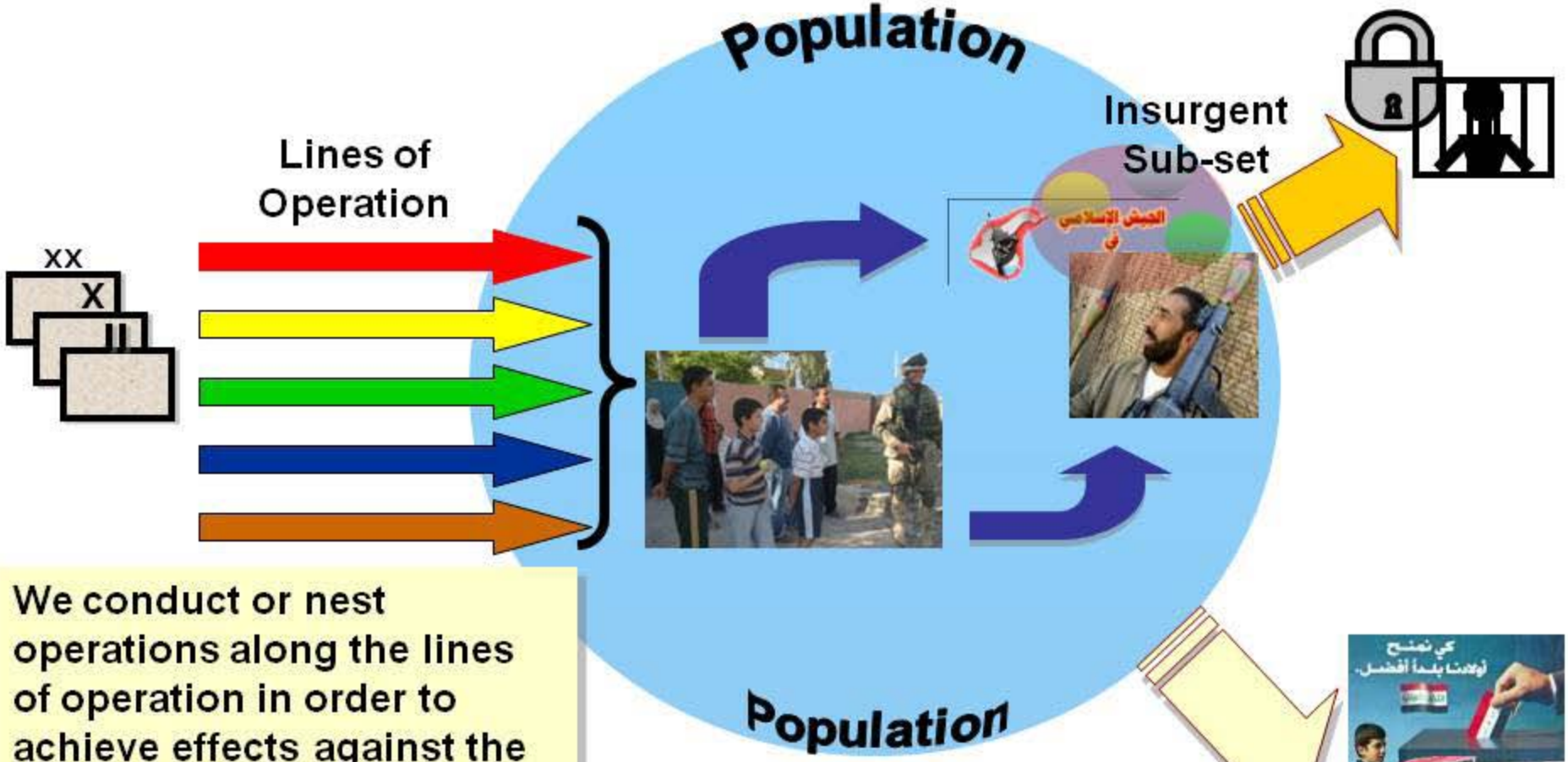
HUMINT

Collection via Surrogate (sources and organizations)

Resources: CA Team and Money

Operations such as 'Cordon and Knock' to deliver information may provide actionable INTEL leading to the capture of insurgents hidden in the community.

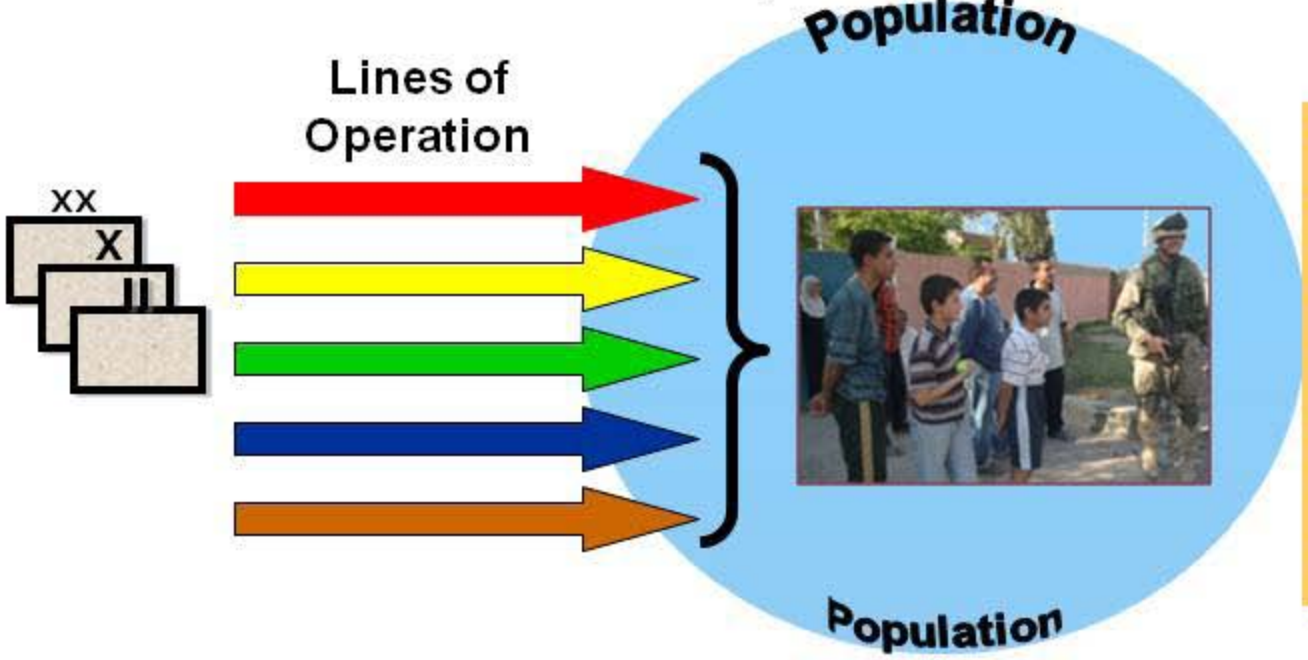
Capitalize on Activities Across LOO



We conduct or nest operations along the lines of operation in order to achieve effects against the center of gravity towards a desired end-state.

We must capitalize on the synergy of efforts along the lines of operation to gain intelligence.

Information Operations as a Catalyst

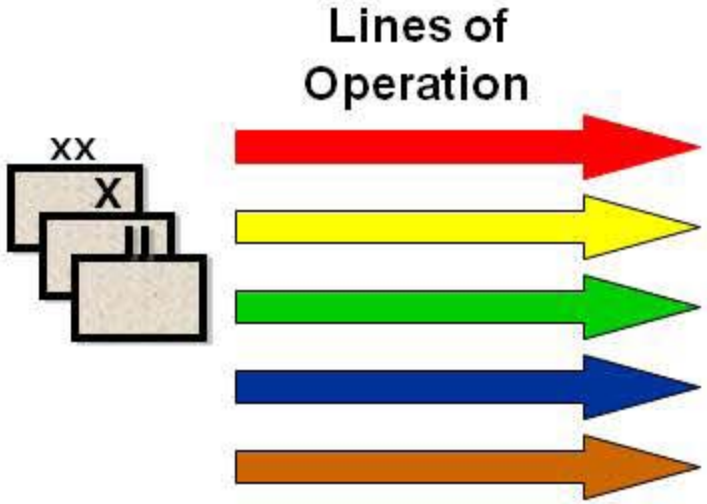


- "Tips" hotlines
- Consequence management battle drills
- Talking points and themes
- Broadcasts
- Handbills

- Sets conditions to gather information of intelligence value
- Creates conditions for people to provide us information
- Counters the insurgents' ability to mold public opinion
- Affects recruiting, undetected movement
- Utilizes consequence management after every detonation to gain information and neutralize insurgents' ability to capitalize on the success of the event

Accomplishing Tasks by Surrogate

Consider synergy across multiple LOO by using surrogates to accomplish tasks requiring non-military expertise that would otherwise consume your organic manpower. Data collection (particularly relating to MOE) is an example.



Use of Surrogates

"In Iraq, there is an old saying that you cannot buy a tribe, but you can certainly hire one"

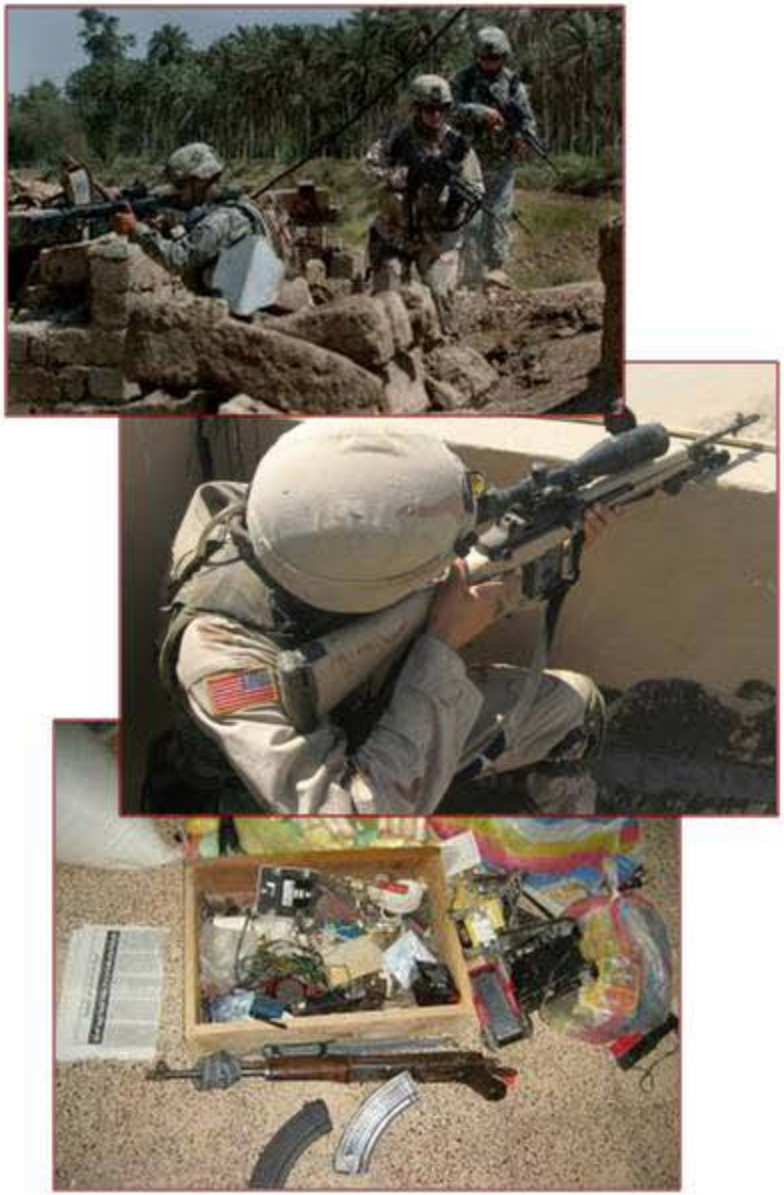
Amatizia Baram,
"Victory in Iraq, One Tribe at a Time,"
New York Times, 28 Oct 03

IED detection is problematic in conditions similar to those shown on the left. Consider the hiring of local population to clean roads and shoulders particularly in high threat or heavy use areas.

Review

- **Defining the Problem**
  - COIN Warfare & Characteristics
  - The Enemy
  - The IED
  - The Insurgent Sniper
- **The Operational Situation and Battle Staff Framework**
- **Role of the Battle Staff in COIN Operations**
  - Observations on Battle Staffs
  - Battle Staffs Organization
- **IED Defeat Tenets Related to Battle Staffs**
- **Analyzing the IED Threat**
  - Models and Applied Analysis
  - Principles & Tools
- **Staff Process and Resources**
  - COIN Enablers
- **Coordinating Offensive Operations**
  - Targeting the insurgent System
- **Gathering Intelligence and Data**

Summary



Staffs must:

- Remain adaptive and proactive in order to effectively predict, engage the Operational Environment (OE) threat, and protect friendly forces
- Take aggressive measures to detect devices before detonation and interdict the device before emplacement
- Focus the actions of the staff and the resources of the Brigade to predict events and subsequently defeat the enemies' systems / networks

Conclusion

"There is no technological silver-bullet for defeating the enemy's use of IEDs. Technological solutions are a key part of the solution but a renewed and focused emphasis on training also is required to defeat the enemy's use of IEDs in the USCENTCOM AOR."

CENTCOM *Commander's Guidance* 17 Sep 05

Battle Staff Practical Exercise (PE 1)

Practical Exercise Procedures

- Part I
  - Break the class into groups of 3-5.
  - Plot incidents 31-40 on the map. Incidents 1 – 30 are already plotted on the map.
  - Complete Pattern Analysis Plot Sheets 1 and 2, and Narrative Notes page for **all** incidents.
  - Answer questions about the incidents after analyzing all data.
- Part II
  - Split the class into 2 groups.
  - Group 1 will discuss limitations and constraints of the IED Working Group.
  - Group 2 will discuss benefits and considerations of the IED Working Group.
  - The class will regroup and discuss the findings.

End –

Primary Lesson Presentation

Continue –

to review optional materiel (not required for the Practical Exercise)

Optional Sections

Optional Section #1
Is your Command Post "reactive" or "proactive"?

Staff Organizational Challenges

- Internal versus external focus
- Offensive versus defensive focus
- Integration versus compartmentalization

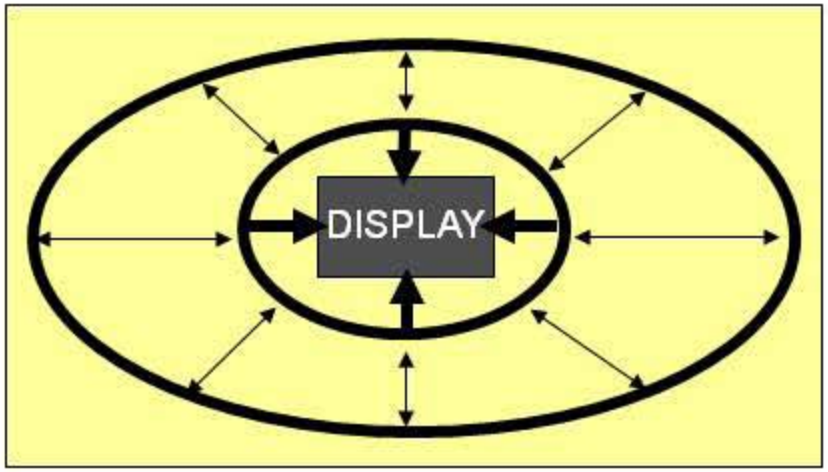
What Should You Look For?

- Can leaders make decisions under pressure?
- Can leaders and staffs translate decisions into communication to subordinates quickly?
- Are subordinates technically, tactically, physically, and mentally capable of carrying out their orders?

Optional Section #2
The Command Post –
How do you organize it logically?

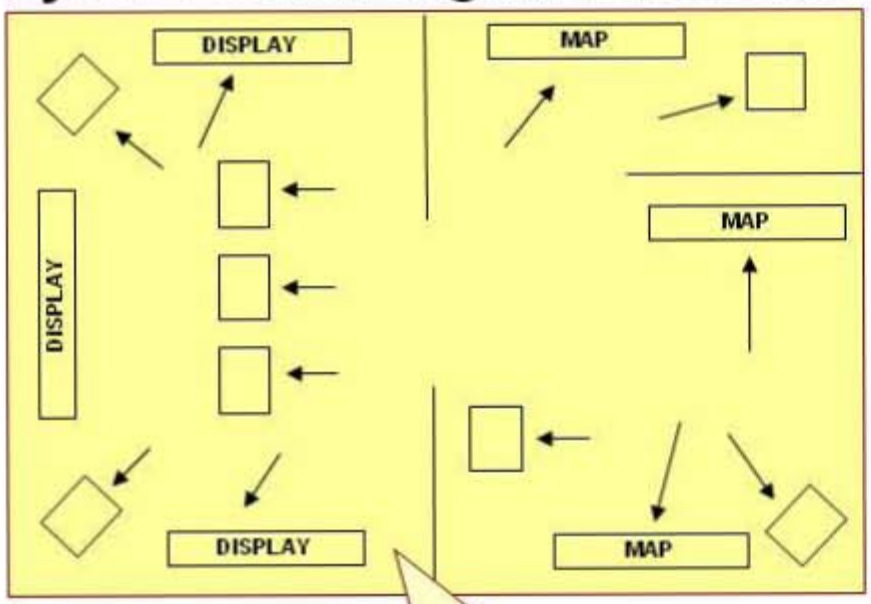
Garrison HQ versus Command Post

CONF ROOM	XO	S1	S4
CDR	CSM	S3	S2



TOC / CP Organization

Is your TOC/CP organized like this?



"Attention in the CP!"

Human to Machine Interaction
Computers Substitute for Situational Awareness

Cells Develop Own Prioritization of Info Requirements

Reactive & Procedural Focus

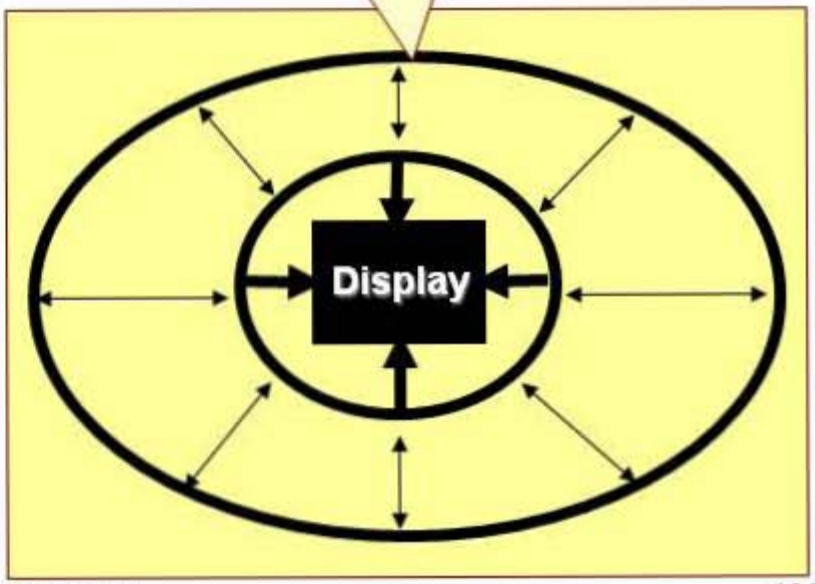
or like this?

Continuous Targeting & Situational Awareness

Human to Human Interaction
Computers Provide Info Support

Prioritization of Info Requirements

Proactive & Anticipation Focus



A Typical BDE CP in Iraq

How should you assess the unit you are replacing?

Does their CP help or hurt the efforts of subordinates?

Should you accept their way without question?

Optional Section #3
Prediction - Caches

Caches

- Since the enemy is a creature of habit, we analyze what he has done in the past to predict what he will do in the future.
- We look for previous caches in the Area of Operation (AO).
- We study imagery to determine:
  - Distance from the IED to the cache
  - The characteristics of a potential IED site
    - Size
    - Distance from road, mosque, gas station, canal, etc.
    - Type of terrain preferred
    - Ploughed field, abandoned house, palm grove, obstacles & egress routes
- We then use the information available to evaluate Tier 1 sites to determine if cache locations are near.

Optional Section #4
Pattern Analysis

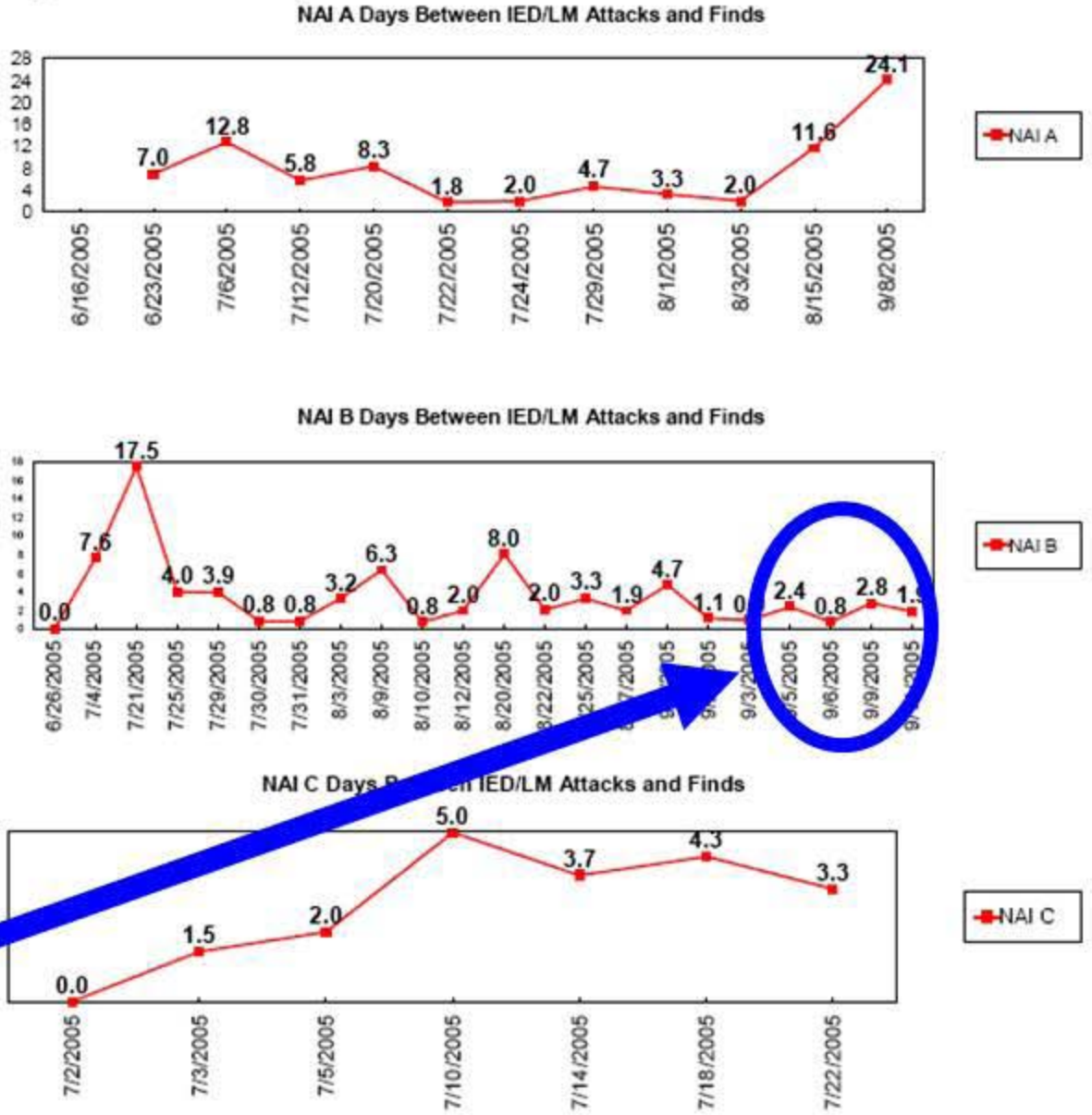
Crystal Reports

Process

- CIDNE query to Excel
- Plot: Excel to FalconView
- Designate NAIs
- Input NAI grids
- Evaluate each NAI chart

Cue offensive ops

- NAI A: Recent attack site (08 Sep) but seldom used (24 days between attacks)
- NAI C: Frequent use pattern (3.3 days) but not recently used (22 Jul)
- NAI B: *Best target*. Frequently used (1.9 day pattern) and recently used (11 Sep).



Crystal Reports

IED attacks and finds by NAI & time of day

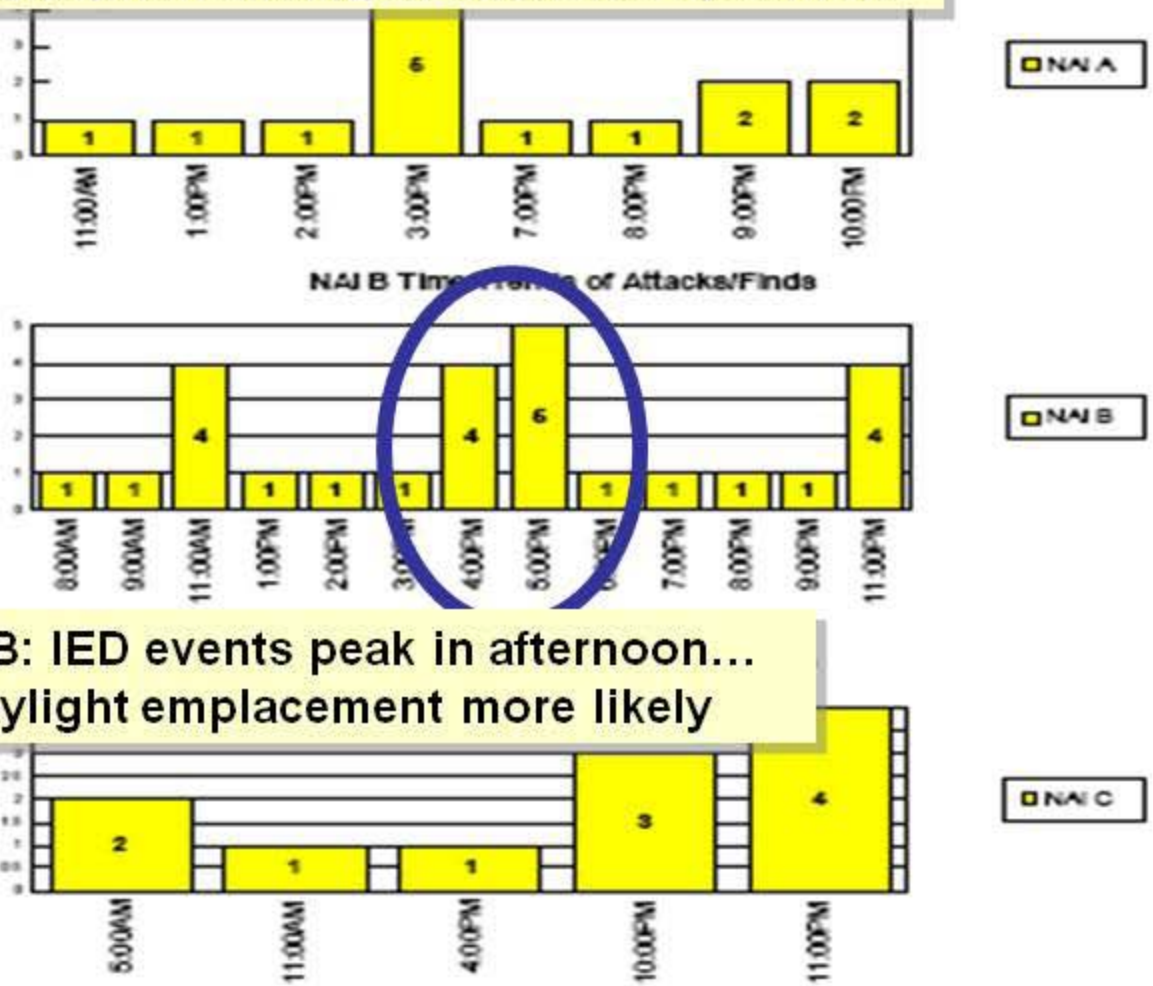
Suggests appropriate timing of offensive operation

Benefits

- Increases awareness of enemy patterns
- Saves time

Results

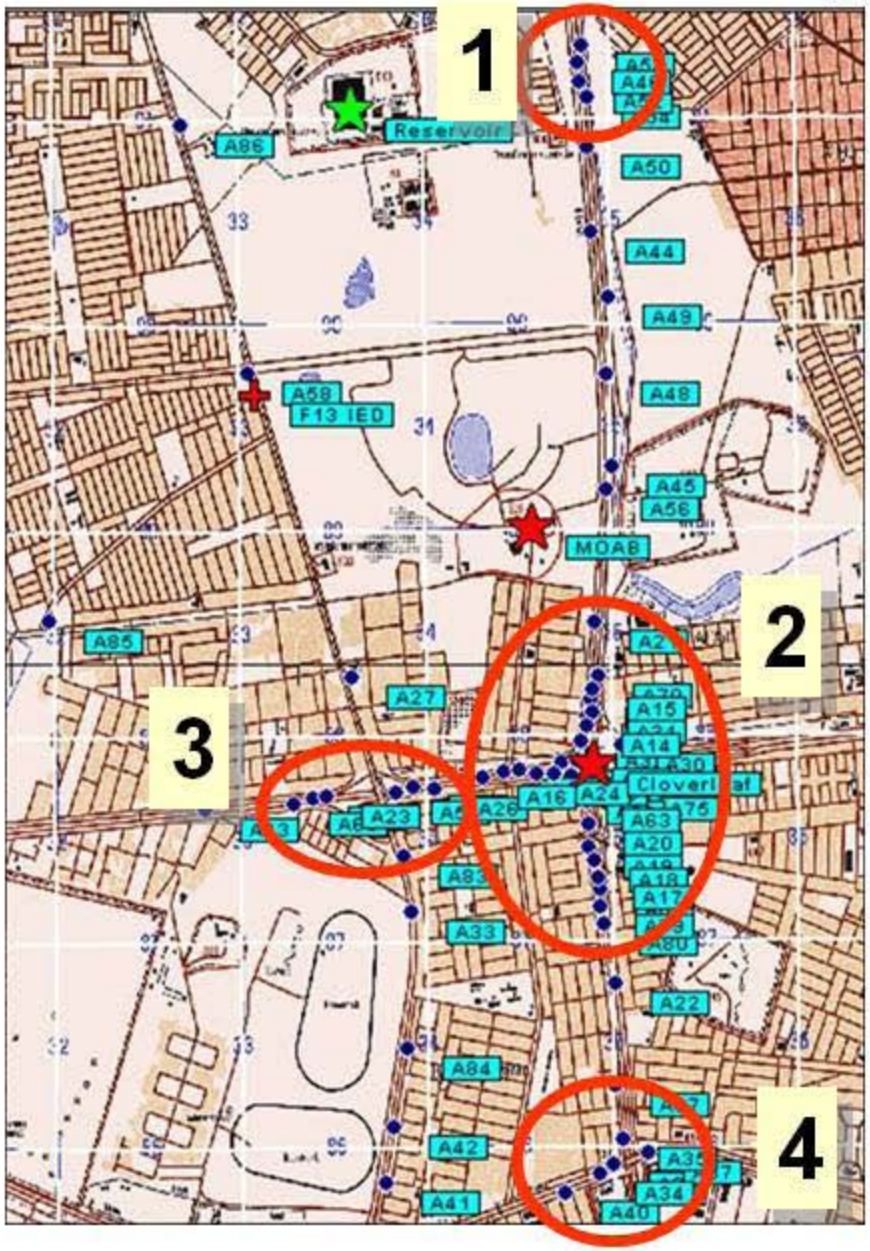
- CF used product to identify ambush and clearance locations with highest probability of success
- Killed AIF emplacement team assessed location after first use
- Significant increase in IEDs found during clearance ops



NAI B: IED events peak in afternoon…

…Daylight emplacement more likely

Tier 1 Analysis

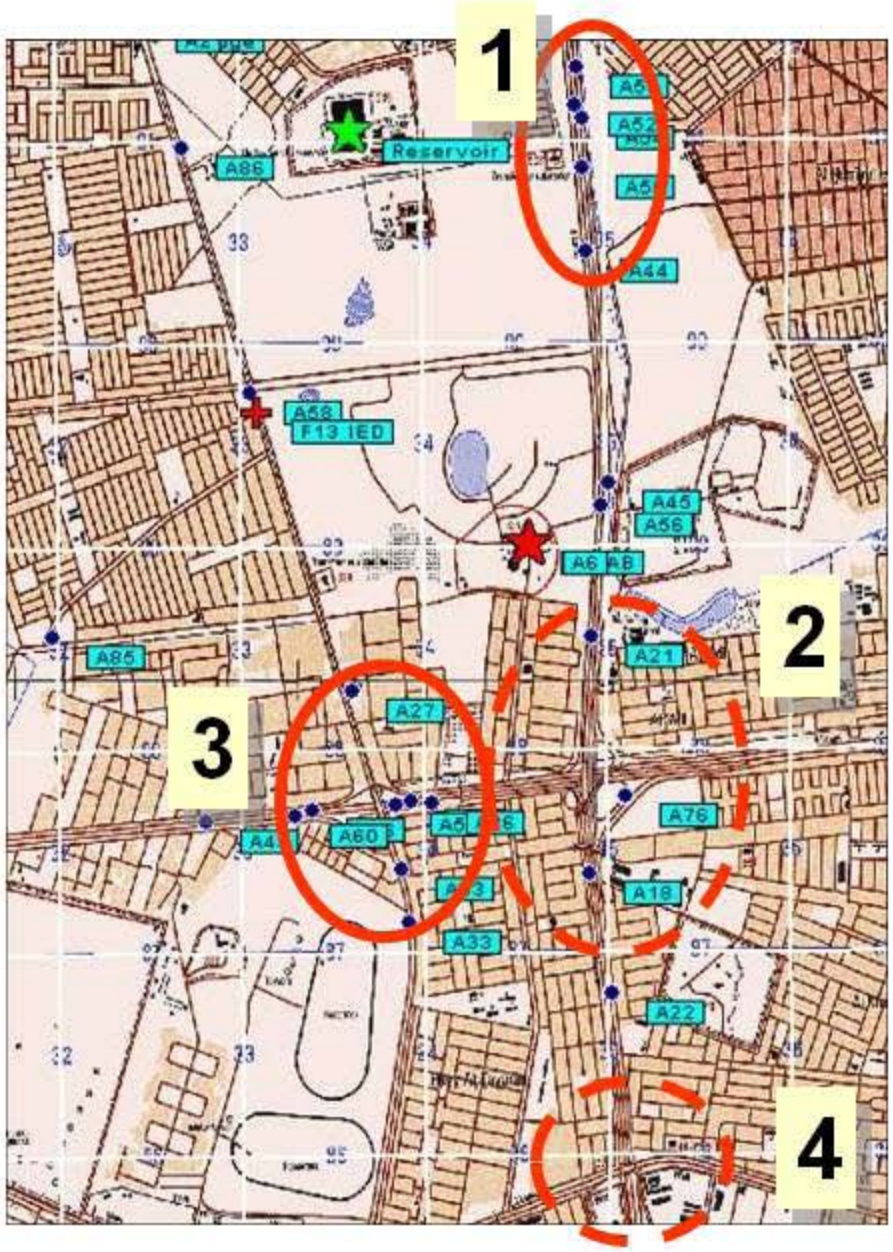


Plotting all IEDs identifies four distinct Tier 1 Hot Spots

Group 2 clearly has the highest density, but is it the biggest problem?

Groups 1,3 & 4 all appear to be about the same

Effectiveness Analysis



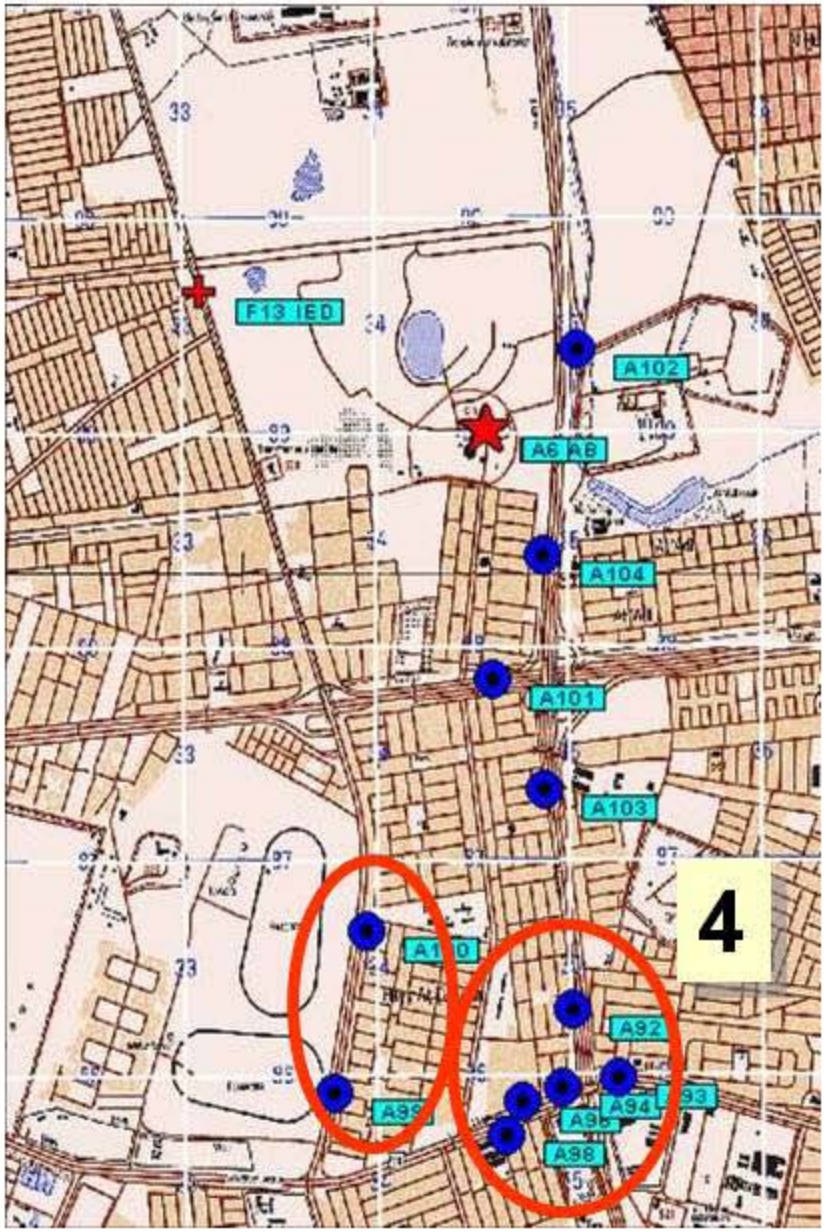
Plotting only IEDs causing significant damage shows a different picture

Group 2 becomes less of a concern; IEDs much less effective despite overall density

Groups 1 & 3 show pattern of occurrence and effectiveness

Group 4 disappears

Effectiveness Analysis



Plotting only IEDs reported by local citizens shows a different picture

Almost all of the IEDs in Group 4 reported by locals

What are we doing "right" in this area?

What conditions cause this in Group 4

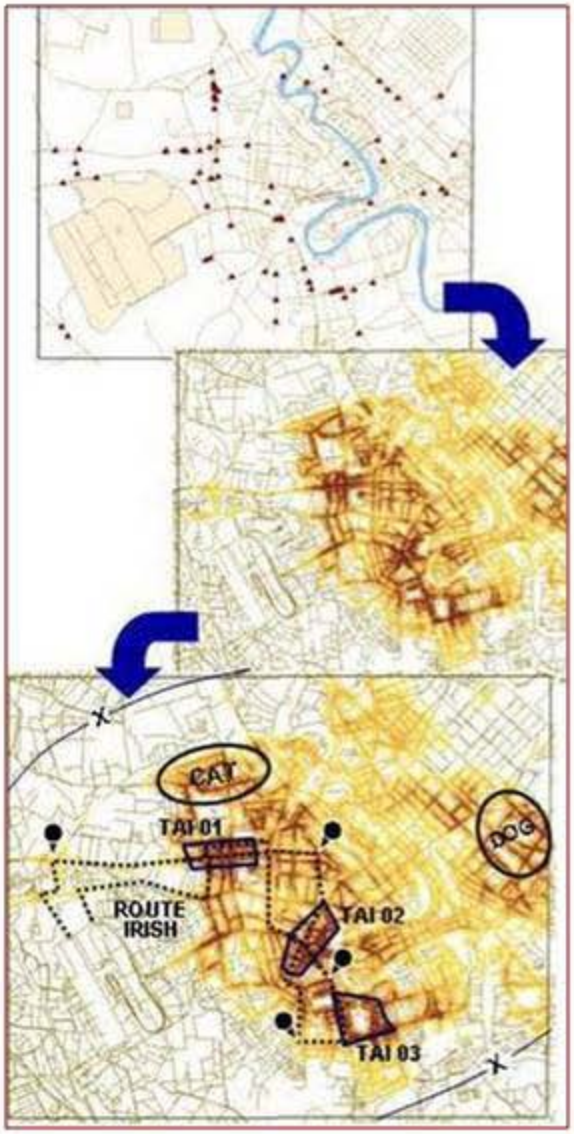
What can we exploit in this vicinity?

Threat Mapper: Operational Concept

Although applicable at many levels, Threat Mapper's primary focus is the Brigade.

- Brigade operating areas provide an area of analytic interest up to ~ 50 x 50 kilometers.
- Threat Mapper can help forecast many tactical problems (e.g., safe houses, caches, IEDs).
- Brigade analysts have the most tactically relevant incident and feature data.
- The Brigade can assemble a robust analytic team: geospatial, intelligence, operations research, and functional expert.
- Threat maps contribute to the intelligence estimate and are used to help plan ISR and tactical operations.

Threat Mapper provides predictive analysis support to the war fighter.



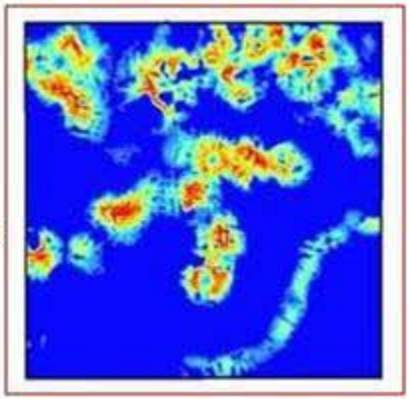
The Analyst's Role

- *Be careful!* Powerful empirical methods can fascinate, and at times even charm or hypnotize, both the analyst and decision maker.
- The empirical spatial model is just that – a model. The model is not analysis.
- It is the analyst's responsibility to analyze.
- It is the analyst's responsibility to understand the nature of the model and its associated strengths and weaknesses.
- It is the analyst's responsibility to present the results of the analysis to the decision maker in a manner that both resonates and is operationally useful.

What Threat Mapper Does

Threat Mapper measures

"spatial similarity"

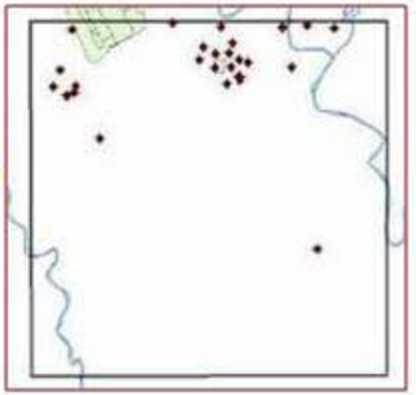


between

your area of interest

and

a collection of incidents.



Threat Mapper: Strengths and Weaknesses

- Threat Mapper will measure the spatial similarity between given terrain and a collection of incident points.
- Threat Mapper is a new tool that provides a cutting-edge capability. However, it is rough around the edges - it has not yet been completely developed.
- Runtimes will vary by machine, by resolution, map area, number of features, and number of incidents.
- Threat Mapper does not fully explain threat maps.
- Threat Mapper has an upper limit of about 40 features for record runs (runs that produce a threat map and accuracy score).