CoIST SOP

2nd Squadron, 1st Cavalry Regiment
4th BDE, 2nd Infantry Division

Version 5.0

24 FEB 12

TABLE OF CONTENTS

THIS PAGE LEFT BLANK INTENTIONALLY

PLANNING / PREPARATION

EXECUTION

POST IN CP

GRAPHICS

1. Expectation.

A cohesive fully functioning tactical CoIST that is capable of: conducting predictive analysis of significant activities, conducting pattern analysis associated with significant activities (SIGACTS) and targeting, target packet generation, and possess the ability to properly brief both the commander and maneuver units in a way that ensures enhanced battlefield situational awareness.

2. Mission.

The mission of the CoIST is to describe the effects of the weather, enemy, terrain and local population upon friendly operations in order to reduce the commander's uncertainty and aid in his decision making. This mission is accomplished by application of collection assets, analyzing intelligence from the information gathered, recommending a course of action to the commander, and disseminating any intelligence to the small unit leaders.

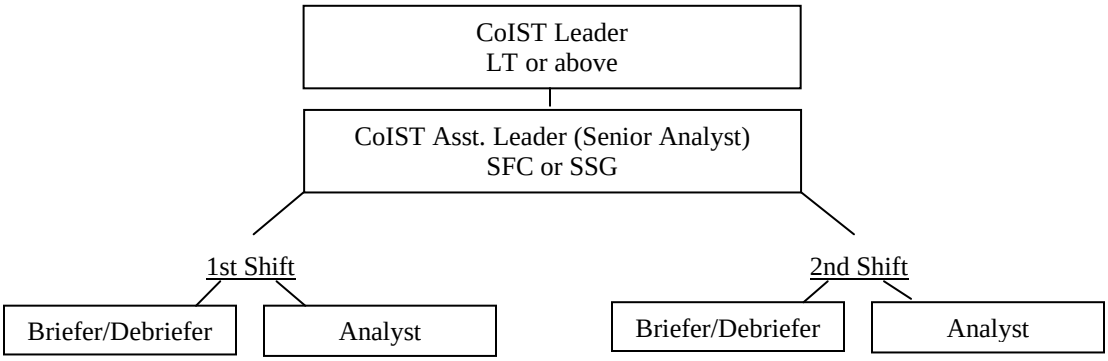
In addition to coordinating the collection effort, the CoIST is the *filter and analysis* center for the raw data that comes to the cell from a variety of sources. The CoIST, along with the Squadron S2 shop, gathers input, then filters, organizes and analyzes data in order to develop recommendations.

3. Introduction.

Importance of the CoIST

All levels of command should have a good understanding of the importance of intelligence support. Information flow can often inundate a Troop command post (CP), leaving little time to separate the important information from "noise." But, a CoIST can reduce some of the information ambiguity and provide analysis to build situational awareness to enable mission accomplishment. For example, the CoIST can reduce a tendency to get drawn into *react* mode and allow you to analyze and foresee. This is much easier said than done. It often takes patience and foresight. But the result will be that information will be turned into intelligence that helps achieve understanding about the enemy. This can also often answer Squadron and Brigade commander's critical information requirements (CCIRs) and priority intelligence requirements (PIRs), while giving insight into Troop level CCIRs and PIRs. Note that the CCIRS are broader than "just" intelligence requirements.

4. Task organization.



**Positions may be modified as necessary.*

a. Roles of the CoIST members.

(1) CoIST OIC/NCOIC: tasking, delegation, and supervision of day to day operations and advises commander on intelligence matters.

(2) CoIST Soldiers: provide intelligence support to ongoing ops, conduct mission planning for future operations (Ops), production and analysis of basic and current intelligence from databases and combat reporting.

b. Duties of the CoIST.

(1) Brief outgoing patrols, staff, attachments and units operating within the Company/Troop/Battery AO.

(2) Facilitate Patrol Debriefs.

(3) Conduct IPB – Situational Understanding of Operational Environment.

(4) Conduct collection at the Troop level.

(5) Analyze events, targets, activities, patterns, trends.

(6) Conduct Targeting (Lethal and Non-Lethal).

(7) Provide all related information to support Detention Ops.

(8) Submit reports into information and Intelligence databases.

c. Duties of the CoIST OIC/NCOIC.

(1) Ensures CoIST members are tasked appropriately and priorities of work are identified.

(2) Ensure briefs are conducted for outgoing patrols, attachments and units operating within the Troop AO.

(3) Provide intelligence briefs toTroop leadership.

(4) Supervise IPB for Troop AO and individual missions.

(5) Ensure debriefing occurs for all patrols.

(6) Manage collection effort at the Troop.

(7) Supervise and review analysis of events and combat reporting for validity to battalion intelligence effort.

(8) Attend Targeting boards/meetings to provide recommendation and supporting intelligence products to Company/Troop/Battery Commander for nomination to Battalion targeting process.

(9) Assist Troop leadership in Detention Ops by providing necessary information, intelligence and evidentiary materials to support detention.

(10) Conduct coordination with HQ to requests additional intelligence resources in accordance with Troop collection effort.

(11) Conduct coordination with adjacent and supporting units for dissemination of relevant intelligence information/products.

(12) Ensure all products are up to date pertaining to IPB, Collections, Analytical Tools, Target Packets, CoIST Journals, Squadron reports (INTSUM, TSE Supplementary reports, SITREPs, ISR Sync/Coverage Matrixes).

5. Responsibility and manning

2-1 CAV CoIST Training Strategy									
		*Class Instruction							
		Command Post Instruction	Refresher FBCB2	TIGR instruction	Critical thinking skills for junior leaders	CoIST instruction	HUMINT Control Center (HCC) instruction	BATS HIIDES	OSRVT
A TRP	CoIST OIC								
	CoIST NCOIC								
	analyst								
	analyst								
	analyst								
	analyst								
B TRP	CoIST OIC								
	CoIST NCOIC								
	analyst								
	analyst								
	analyst								
	analyst								

C TRP	CoIST OIC								
	CoIST NCOIC								
	analyst								
	analyst								
	analyst								
	analyst								

a. The CoIST is responsible for assisting the commander with intelligence analysis, reporting and dissemination, detainee operations and tactical site exploitation, and intelligence collection

b. CoIST operations are limited based on scope, training, and authority. CoISTs **ARE NOT trained or authorized to do the following:**

(1) Task Squadron and above assets directly: ISR, HCTs, STG Teams, even if operating in their AO.

(2) Run or task sources and/or informants; can conduct Tactical Questioning (TQ).

(3) Conduct Interrogations.

(4) Function as asset managers: Squadron S-2s and S-3s gather the assets for the Company/Troop/Battery.

6. CoIST operational tasks.

a. Activities.

(1) The CoIST brief outgoing patrols on the current threat assessment for the AO with regard to last 24 hour significant activities, current IED threats and locations of highly concentrated IED attacks, enemy activity expectations for the next 24 hours, Current High Value Individual List (HVIL) with pictures if possible, Information Requirements, and Possible TQ guidance.

(2) The CoIST will debrief incoming patrols in order to develop the Common Operating Picture for the Troop AO.

(3) The CoIST will battle track enemy significant activities IOT develop enemy patterns and TTP's.

(4) The CoIST will develop TROOP level High Value Individuals (HVI) and associating target packets IOT effectively action targets of opportunity.

(5) The CoIST will be prepared to brief the commander on the current situation at all times.

(6) The CoIST will cross talk with adjacent units IOT develop Area of Interest (AI) awareness.

(7) The CoIST will continuously update all intelligence trackers and databases (TIGRnet) and maintain situational awareness within the Troop Area of Operations (AO) and AI.

(8) The CoIST will conduct predictive analysis and maintain a predictive analysis board identifying likely enemy activities both over the next 48 hours and over the next few weeks.

(9) The CoIST will analyze friendly trends from the enemy's perspective and identify unnecessary vulnerabilities and patterns the Troop is setting.

(10) The CoIST will request assistance from the Squadron S-2 to conduct specific detailed analysis beyond company capabilities.

(11) The CoIST will establish clear communications with the Squadron S-2 and adjacent units and ensure that information flows both up and down the chain of command in a timely manner; the CoIST NCOIC must be proactive and pull information from the Squadron S-2 and supporting agencies as required.

(12) The CoIST will ensure that all patrols have updated intelligence information prior to departure to include updated intelligence from the Squadron S-2.

(13) The CoIST will brief attachments and units operating within the Troop AO when necessary.

(14) The CoIST will post updated intelligence information for ease of reference by patrol leaders; appropriate operations security (OPSEC) must be observed when choosing a location in which to post.

(15) The CoIST will identify little-known areas within the Troop AO that require informal assessments by patrols to identify key leaders, infrastructure, and basic population information; this information will also become Troop SIR and SOR.

(16) The CoIST will ensure that Troop-level TQ does not inadvertently become unlawful interrogation by adhering to the following guidance along with unit guidance involving actions on the objective and TQ.

(a) TQ will occur at point of capture and will cease upon arrival at COP / FOB.

(b) Troop TQ will involve direct questions only.

(c) Troop TQ will not use interrogation approaches, defined as "any means used to entice a detained person to give information he would not normally give".

(d) At no time will TQ involve threats directed at the detainee or his family.

(e) Any exploitable information will be recorded and reported to Squadron. Only Squadron CDR can authorize further TQ with regards to exploitation.

(17) The CoIST will ensure that all casual and regular informants are entered into the Informant Contact Log and have been entered into the Biometric Automated Toolset System

(BATS); the CoIST will coordinate with the Squadron S-2 and HCT (HUMINT Collection Team) for review of these products and the assignment of contact tracking numbers.

(18) The CoIST will assist the commander in ensuring that regular informants are paid and accounted for in accordance with theater policy.

(19) To facilitate walk-in informants, the CoIST will establish an informant meeting and debriefing area and ensure that security personnel are prepared to receive local national informants.

(a) The meeting room should have chairs or couches, a table, drinks available, an ashtray, large-scale unmarked maps for map-tracking purposes, and no windows.

(b) When walk-in informants are expected, ensure that security personnel are well briefed on what to expect and what to do when an informant arrives.

(c) Commanders and CoIST are not authorized to task a source. They may request information from local nationals and other willing informants.

(20) Develop and submit requirements and requests for Squadron and higher echelon collection capabilities in order to facilitate the collection of the commander's information requirements.

b. Suggested battle rhythm.

Daily.

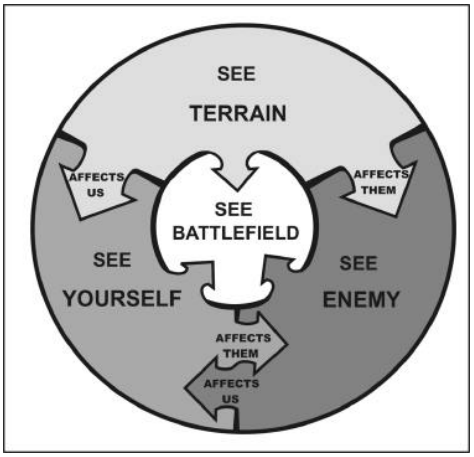
(a) Facilitate & collect patrol debriefs. (Squad Leader)
(b) Conduct mission pre-briefings and debriefings for patrols, operations. (Analysts)
(c) Review and analyze patrol debriefs. (OIC/NCOIC)
(d) Conduct data processing and update maps, templates and graphics. (Analysts)
(e) Supervise detainee packets. (OIC/NCOIC)
(f) Provide counterintelligence and deception recommendations as required. (OIC/NCOIC)
(g) Exchange data with Squadron S2 and brief commander. (OIC/NCOIC)
(h) Collect and report/disseminate, through pertinent channels, sensitive site exploitation and weapons intelligence. (CoIST)
(i) Update all trackers and graphs. (Squad Leader)
(j) Update intelligence board for outgoing patrols. (Squad Leader)
(k) Contact adjacent units for intelligence sharing. (OIC/NCOIC)
(l) Write detailed summaries of any HUMINT collected. (OIC/NCOIC)

Weekly.

(a) Analyze week's events. (OIC/NCOIC)
(b) Conduct pattern analysis for the last 30 days. (Analysts)
(c) Refine enemy situational template. (Analysts)
(d) Forecast enemy actions. (Analysts)
(e) Identify potential targets. (Analysts)

(f) Identify/update Troop named areas of interest. (Squad Leader)
(g) Update Troop priority information requirements. (OIC/NCOIC)
(h) Update sewer, water, electricity, academics, trash, medical and security (SWEAT-MS), and ASCOPE assessments. (Analysts)
(i) Brief commander. (OIC/NCOIC)

Monthly
(a) Analyze month's events. (OIC/NCOIC)
(b) Analyze patterns for the last 30 days. (OIC/NCOIC)
(c) Produce detailed monthly intelligence summary. (OIC/NCOIC)
(d) Brief TROOP leadership. (OIC/NCOIC)



7. Intelligence Preparation of the Battlefield (IPB).

a. What is IPB?

(1) IPB is a systematic, continuous process of analyzing the threat and environment in a specific geographic area. It is designed to support staff estimates and military decision making.

(2) Applying the IPB process helps the commander selectively apply and maximize his combat power at critical points in time and space on the battlefield by:

(a) Determining the threats likely Course of Action (COA).

(b) Describing the environment we're operating within and the effects of the environment on the Squadron.

(3) IPB is a continuous process which consists of four steps:

(a) Define the battlefield environment.

- Road to War.
- Area of Operation.
- Area of Influence.

- Area of Interest.
- Area of Intelligence Responsibility.

(b) Describe the battlefield's effects.

- Terrain analysis (OCOKA).
- Effects of terrain on operations.
- Civil considerations (ASCOPE).
- Weather forecast (and Lunar Data).
- Effects of weather on operations.
- Overall assessment.

(c) Evaluate the threat.

- Disposition (2 levels up minimum).
- Composition (order of battle / line & block chart).
- Strength (enemy unit strength - %).
- Enemy key systems capabilities.
- Enemy unit capabilities by Battlefield Operation Systems (BOS).
- Enemy battlefield capabilities by BOS.
- Blue systems vs. red system capabilities.
- Blue artillery vs. red artillery ranges.
- Force ratio.
- Enemy threat models.

(d) Determine threat course of action.

- Most likely enemy COA (MLECOA).
- Most dangerous enemy COA (MDECOA).
- All additional ECOA's.
- Final assessments.

b. CoIST IPB.

(1) At a minimum, units with CoIST assets will identify the following:

(a) Population (demographics).

- Tribal (leaders and locations of tribes / sub-tribes / clans / sub-clans).
- Ethnic groups.
- Local ANSF components.
- Politicians.
- Civilian press.
- Non-Government Organizations (NGOs).

(b) Terrain (including WX effects).

- Clan / sub-tribal boundaries.
- Local markets.
- Mosques or madrassases.
- Social structures (schools, hospitals, social gathering points, etc.)

- Facility structures (bridges, banks, medical clinics, police stations / check points)
. - Identify local weather for mission operations

c. OCOKA analysis of the terrain.

(1) CoIST personnel should involve other members of the Troop when conducting OCOKA terrain analysis.

(2) This will improve the knowledge base used to develop an understanding of the AO and make for better IPB products.

(3) CoIST personnel may also request the assistance of the Squadron S2.

(4) Provides the determination of how the battlefield environment affects both threat and friendly operations.

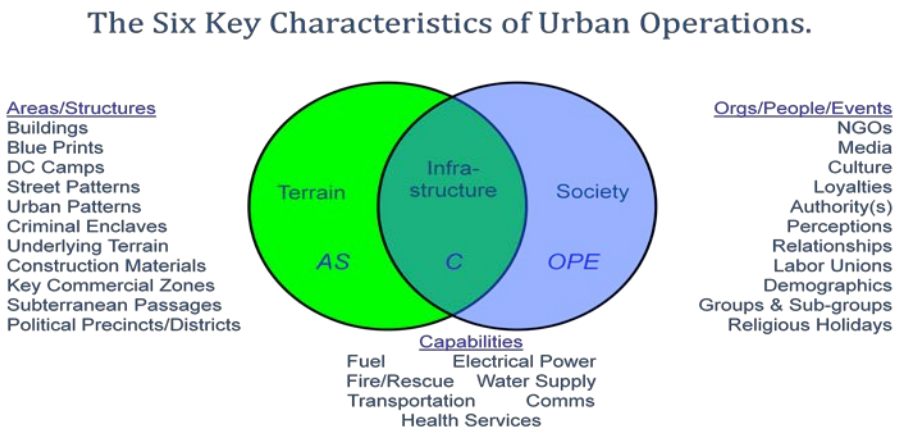
(5) Terrain analysis interprets both natural and man-made features of a geographic area to determine their affects on military operations.

(6) Will identify dismounted ground routes (camels, mules, and foot movement), mounted ground routes (HILUX capable – four-wheel drive, jingle truck – two-wheel drive capable) and air avenues of approach, draft Named Areas of Interest (NAI), identify Decision Points (DP), and potential objectives.

(a) Will determine the route trafficability with consideration of weather effects.

(7) The engineer detachment normally conducts the majority of terrain analysis, combining extensive database analysis with the results of reconnaissance.

d. The six key characteristics of urban operations – Counter Insurgency (ASCOPE).



(1) **Area**.

(a) Areas defined by political boundaries.

- City districts / neighborhoods.
- Municipalities.
- Provinces.
- Tribal / sub-tribal / clan / sub-clan boundaries.

(b) Areas of high economic value.

(c) Centers of Government and politics.

(d) Culturally important areas.

(e) Significant enclaves.

- Social.
- Ethnic.
- Tribal.
- Political.
- Religious.

(f) Trade and smuggling routes.

(g) Possible locations for temporary settlement of dislocated civilians.

(2) **Structures** including, but not limited to, government centers, military installations, courts, police stations, jails, prisons, communication centers and towns, newspaper and magazine printing plants, radio and television stations, road, bridges, tunnels, sea and air ports, power plants, dams, medical facilities, schools and universities, religious centers, public utilities, etc.

(a) Protected cultural and religious sites include churches, mosques, temples, seminaries, national libraries, hospitals, and clinics.

(b) Additional aspects to be considered:

- Location of police stations.
- Portable water wells, water distribution, and pumping stations.
- Sewage treatment plants and sewer systems.
- Refineries / fuel production facilities.
- Lines of communication – highways and arterial roads with major intersections.
- Phone service facilities.
- Airports and runway approaches.
- Universities, newspaper facilities, television stations, financial and trade districts.

(3) **Capabilities** refers to the ability of authorities to not only provide the populace with key services, but also to support the coalition military effort.

(a) General.

- Government.
- Public administration.
- Public safety.

- Emergency services.
- Food and logistics.
- Technology.

(b) Formal political systems include local and national governments, political interest groups, political parties, unions, government agencies, political elites, etc.

(c) Informal political systems include traditional authority figures, charismatic authority figures, patronage system, social elites, associated groups, religious law, conflict resolution, resistance, etc.

(4) **Organizations & People**

(a) Can be used tactically as key terrain or strategically as the center of gravity (or a mixture of the two).

(b) Understanding the demographics.

- Society.
- Social structure.
- Culture.
- Power.
- Interests.

(c) Socio-cultural factors.

- Family groups, tribal groups, racial groups, religious groups, social networks, social classes, social movements, social organizations, and individual role / status.

(d) Culture.

- Social norms, values, belief systems, cultural norms, language, customs.

(e) Interests.

- Physical security, economic resources, political participation, and grievances.

(f) Social demographic questions to ask about the insurgency.

- What is the cultural, religious, and ethnic makeup of the insurgency?
- What are the tribal / clan affiliation / allegiances with the insurgency?
- Socio-economic dynamics - is the social class the key to the insurgency?
- Is the populace sympathetic to the insurgency?
- Will the threat risk civilian casualties in an attack?
- Will the threat target population groups?
- Will symbolic targets be the threat of the attacks?

(5) **Events / Economy** are activities that significantly affect organizations, people, and military operations such as:

- Sources of local conflict such as resources, inter / intra clan / tribe warfare, property, source of revenue.

- Events such as national and religious holidays, agricultural crop, livestock, market lifecycles, elections, sporting events, civil disturbances, other celebrations, and natural or man-made disasters.

- Economic factors such as production, consumption, and distribution.

e. Identifying the threat components.

(1) Why do insurgents fight?

- Patriotism, ideology, religion, and financial gain.

(2) Study the insurgency – background information vital to the counter-insurgency fight.

- Origin and history.
- Support among the populace.
- Organization.
- Interoperative networks.
- Operational tactics.

(3) Popular support or tolerance for an insurgency.

(a) Passive support refers to the local populace “approving” of the insurgency’s motives, morals and actions. The populace does not publically acknowledge support for the insurgent group.

(b) Active popular support refers to the local populace supporting the insurgency by being embraced by the “center of gravity” of the local populace.

- There are four forms of active popular support.
    - o Active external.
    - o Passive external.
    - o Active internal.
    - o Passive external.

- Forms of active popular support include:
    - o Providing safe havens.
    - o Allowing freedom of movement.
    - o Providing logistical and financial support.
    - o Intelligence support.
    - o Supplying personnel.

(c) Both types of support require a commander to take a different type of approach. Active and passive support often requires diplomatic pressure on the government or groups supporting the insurgency.

(d) Insurgency groups are often a coalition of different forces united by their common hostility for the government.

(e) Insurgents need the active support of politically active people and the passive support of the majority.

f. Situational understanding of the operational environment (OE).

(1) The commander achieves situational understanding when he understands the relevant terrain and the relationship between friendly and enemy forces in time and space and foresees opportunities for mission accomplishment as well as potential threats. He does this by applying his experience, judgment, and intuition to his knowledge of the battlefield and the COP. Simply stated situational understanding is not only seeing the battlefield, but also understanding the actions, reactions and counteractions of the impending engagement. The commander's situational understanding of the current state allows him to visualize his desired end state (mission accomplishment) and a sequence of events that will achieve it.

(2) Graphic representation of the Operational environment.

(a) Troop CoIST will create a graphic analysis of the operating environment containing but not limited to:

Tribal overlay: Break down AO by tribal areas – sub-tribes, clans, sub-clans (tribal areas may not be 100% pure; this tracker shows the majority tribe in an area). Identify all tribal and informal leaders: Mullahs, Maliks and other influential local leaders.

Political overlay: Break down the AO by town or regional names (the names used by the local nationals).Identify local and regional dividing lines. Identify government leaders: Mayors, ANSF leaders, influential political leaders.

Key Infrastructure overlay: Include road names using Afghani naming conventions (not all roads in Afghanistan are locally named). Include significant infrastructure, to include schools, public utilities, government buildings, bridges, medical facilities, etc.

Neighborhood overlays (if required by the Squadron S-2 or CoIST Troop Commander): Only required if the AO includes towns or cities with too much detail to include on the political and key infrastructure overlays.Include neighborhood names, landmarks, and road names.

Religious overlay: Break down the AO by religious/sectarian lines to include sectarian enclaves.
Identify significant sects or sub-groups.Religious and mosque pictures can digitally hyperlink to existing digital reports and previous mosque monitoring reports using TiGRnet, or can be tracked using. an Excel spread sheet.

g. Doctrinal templates (DOCTEMPS).

(1) Doctrinal templates illustrate the deployment pattern and disposition preferred by the threat's normal tactics when not constrained by the effects of the battlefield environment.

(2) Construction of doctrinal templates.

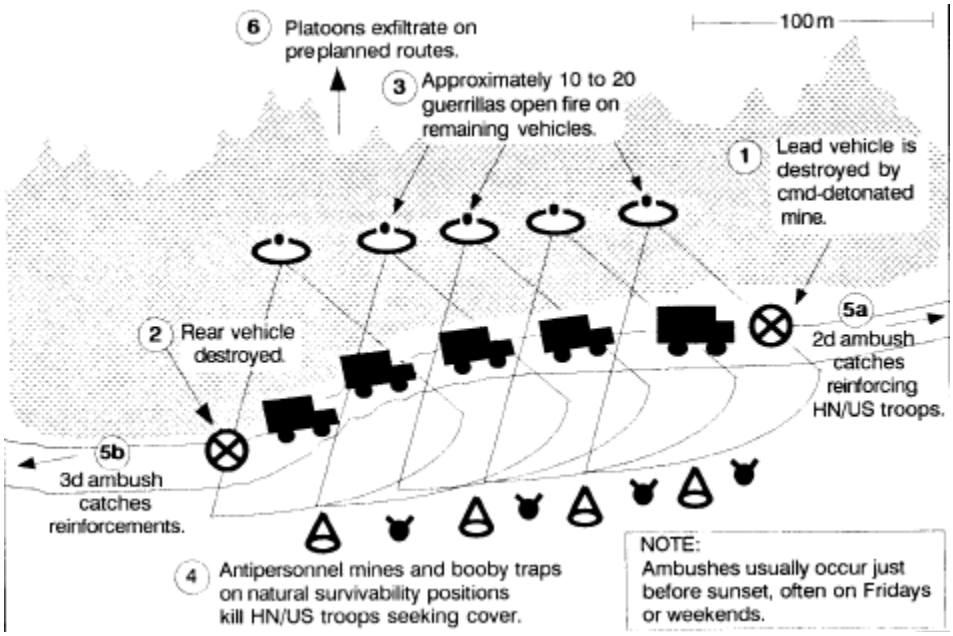
(a) Construct DOCTEMPS through analysis of the intelligence data base and an evaluation of the threat's past operations.

(b) Determine how the threat normally organizes for combat and how he employs his units and his various BOS assets.

(c) Look for patterns in task organization of forces, timing, distances, relative locations grouping, or use of the terrain or weather.

(d) Focus on the main elements and high-value targets.

(e) The figure below show an example of a DOCTEMP created using the above listed criteria.



h. Enemy Situation Template (SITTEMPS)

(1) The Squadron S2 will develop an enemy SITEMP for the ISR operation that focuses on the enemy's reconnaissance and counterreconnaissance efforts. This product will be pushed down to the CoIST team. It is designed to aid in planning friendly infiltration and survivability by identifying enemy actions that will impact on friendly reconnaissance efforts (see Figure 4-4). The enemy SITEMP should include—

(a) Locations of known and suspected enemy locations.

(b) Suspected enemy boundaries.

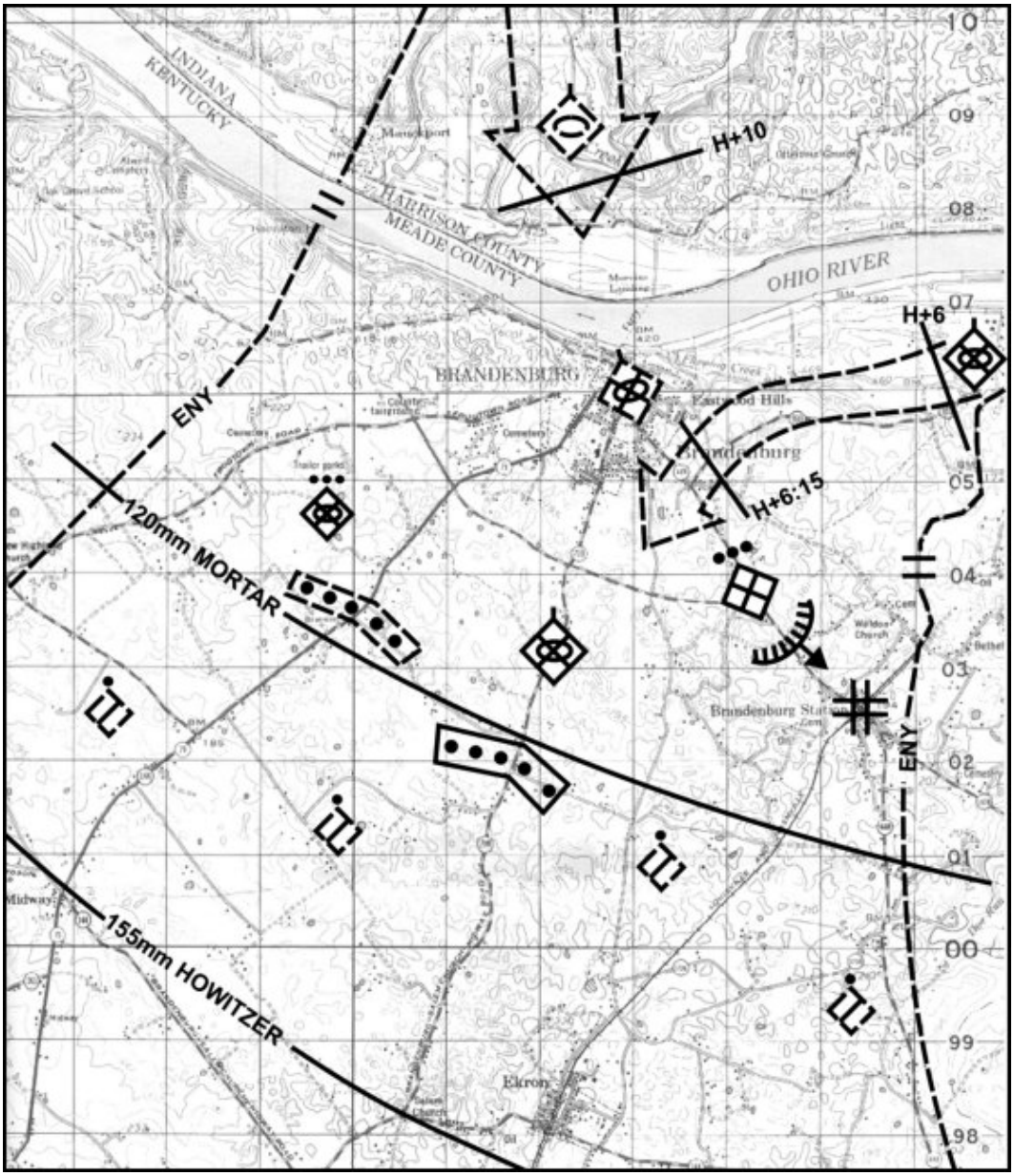
(c) Enemy avenues of approach for the main body with time phase lines (TPLs).

(d) Likely enemy reconnaissance and infiltration routes with TPLs.

(e) Likely enemy OPs and patrols.

(f) Enemy artillery range fans.

(g) Known and templated obstacles



8. CoISTsources of intelligence.

a. **Host nation army/host nation police**. Host Nation Army and Police units coupled with the Military Transition Teams (MTT) are a valuable source of intelligence because of the proximity these organizations have with the local population. The local population sees these units on a daily basis and trusts that they are helping the local population. The MTT's are American units placed with the host nation units to assist them in transitioning the responsibility of the security of the host country to host nation forces. Since the MTT's are American units the CoIST can directly ask them questions therefore allowing the CoIST team the ability to debrief both the MTT's and the host nation patrols as they return.

b. **Patrols**. These are key sources. Soldiers conducting patrols within the Troop's zone have the latest and most detailed information on what is happening on the ground. But, many patrol leaders will instinctively report patrol information that they think is important while skipping other details that may be of use to the intelligence analysts. Sometimes this is the result of the patrol leader not knowing exactly what to focus on. Therefore, the person who tasks a patrol should brief participants just what information the CoIST is looking for, where the patrol should look for it, and what the indicators will look like. When the patrol returns, the same individual that tasked the patrol should conduct a detailed debrief; and the CoIST should always be involved.

c. **Guard posts**. Soldiers on post typically observe the same areas around FOB's or key facilities over extended periods of time. These Soldiers can—and should—notice patterns and identify variations to them. In addition, those on post are often the first Soldiers approached by locals offering information or seeking assistance. This is a great source that is often only tapped into *after* a significant event takes place around the FOB. To overcome this tendency, the fusion cell should train the guard force in observation techniques—and routinely debrief them. Each guard mount should be briefed and debriefed just like a patrol.

d. **Female Engagement Teams (FETs)**. As a matter of their regular duty, FETs establish and build relationships with key female individuals within the Troop and Squadron area of responsibility. While they are identifying the needs of female LNs within the community, FETs also gain insight into the prevailing attitudes and current sympathies of the local populace. This can be valuable intelligence information.

e. **Local translators**. When used by the Troop, local translators are a valuable source of information. While Soldiers collect information as outside observers, local translators are privy to a closer, more focused cultural view of the situation within the community. These individuals will have a different viewpoint, or bias, so information drawn from these human intelligence (HUMINT) sources are important and have to be carefully screened by the fusion cell. Soldiers must also be aware of any tendency for local people to sensationalize an incident or report in order to settle 'old scores' or advance the status of their family or tribe.

f. **Convoys**. Soldiers or friendly forces conducting convoys through the TROOP's zone may observe things that organic units do not. You should do your best to debrief these personnel just like any of your own patrols.

g. **Organizations**. These include anyone stopping or passing through the area of operations. For example:

(1) Nongovernmental Organizations (NGOs). NGOs are transnational organizations of private citizens that maintain a consultative status with the Economic and Social Council of the United Nations.

(a) NGOs may be professional associations, foundations, multinational businesses, or simply groups with a common interest in humanitarian assistance activities (development and relief).

(b) NGOs work very closely with parts of the local populace.

(c) "Nongovernmental organizations" is a term normally used by non-United States organizations.

(2) Private Voluntary Organizations (PVOs).

(a) PVOs are private, nonprofit humanitarian assistance organizations involved in development and relief activities.

(b) PVOs are normally United States-based.

(c) "Private voluntary organization" is often incorrectly used synonymously with the term "NGOs."

(3) Although NGOs and PVOs may carefully guard their neutrality, they may become aware of local security information that is important both them and the FOB. Even though you cannot “debrief” them, casual conversation with them often nets key bits of important information for the CO.

h. **HUMINT Collection Teams (HCTs)**. These Soldiers are trained and skilled in drawing data and developing information from local sources. With their organic interrogation capability, they are an excellent source of detailed and actionable intelligence. Include them in the CoIST.

i. **Explosive Ordnance Disposal (EOD)**. The EOD teams are constantly seeing the latest enemy techniques used with mines, improvised explosive devices (IEDs), and booby traps. The fusion cell must seek out this information so that patrols can identify enemy emplacement and triggering techniques. This information can aid the Troop in reducing a key friendly force vulnerability.

j. **Medical units**. The medical platoon can provide insight on the effects of enemy munitions. Combined with information from the scene of an enemy activity, this information can help reconstruct enemy actions, and possibly identify new enemy TTPs.

k. **Weapons Intelligence Teams (WITs).** Special units attached to Brigades and Battalions whose mission is to exploit enemy sites such as raid houses, cache sites, IED sites, and any other place where enemy weapons are present. They have the capability to lift fingerprints, ID bomb signatures, and do extensive sensitive site exploitation.

l. **Provincial Reconstruction Teams (PRT):** PRT’s know and understand spheres of influence better than anyone on the battlefield. They have contact with the population on a daily basis, even more than HUMINT collectors. The teams work with the police, army, government,

and civilian contractors. The local population trusts the PRT's because they are giving assistance to the population they the locals in turn want to help the PRT's.

m. **Law Enforcement Professionals (LEP's):** LEP's are former local, state, and federal law enforcement personnel who are currently working with the army to help stop the extensive criminal networks in associated with insurgent financing. They bring years of real world experience to the fight and allow the brigades and battalions to pursue the enemy from an entirely different angle.

9. CoIST collection tools. There are several tools available for use by collectors to help build the intelligence picture within the Troop's zone. Some of these tools are just now becoming common at the Squadron level, while others are traditional skills.

a. **Digital Cameras**. The battalion digital cameras can be outstanding surveillance and recording tools for patrols. A patrol armed with a digital camera can bring back dozens of images to the CoIST which provide detailed data and additional information and insight. For example, as shown in the picture, operational use of digital cameras has proven valuable to identify key personnel—both friendly and enemy.

(1) This photo comes from the Patrol's Photo Log, updated after each photo when practical. Note that the DTG, unit identifier and MGRS are on the photo. The direction and photo series number are also printed on the photo. The narrative that accompanies this digital photo could read as follows: "*PSG SMITH: Picture of Alpha TROOP western ECP. The AL NAFFAR Tribe is protesting the lack of water in the town. The Police Chief and his Lieutenants are being escorted into the Troop reception area. The main instigator of the protest is circled and is believed to be ABU HANEFFA."*

(2) Digital cameras can also provide timely images of new graffiti, posters, and signs for translation/interpretation when on-scene linguists are not with the patrol. For example, this collection tool provides significant insight to a report that might have otherwise read something like, "new graffiti noted within neighborhood XX along route YY." When, upon analysis of the words and context, the graffiti may give warning of future danger or hint at a change in mood—positive or negative—of the populace.

(3) Reconnaissance and surveillance teams can show a commander actual color photographs of his objective. In addition to greatly enhancing detailed planning, an exact image can be passed along to BN for further exploitation.

(4) To support this mode of collection, the CoIST should establish a picture log. This log will have a Troop patrol identifier with date, picture number, and location using MGRS. It also indicates where the picture was taken from, general direction of the photo, and any other amplifying remarks. The picture number may have a unit coding system, so that other people who may view the photo can easily identify which unit took the photo.

(5) **Control of Photographs**. Treat photos as sensitive information with strict controls and guidance for their handling. For example, if the object of a FOB photo knows that he is being collected against, he may relocate. This may disrupt other collection methods in place such as HUMINT and SIGINT that are not under the control of the CoIST. And, there is always the possibility that our own photos could somehow be used for propaganda against us or to possibly tip off some of our TTPs.

b. **Video Cameras**. Although it is not as easy to carry as a digital camera, a video camera can record exactly what happened during significant events witnessed by Soldiers. Instead of relying solely upon a verbal debrief, a patrol can now show the fusion cell exactly what happened, and review each event in sequence. This data can also be easily passed on to HHQ in its original format, ensuring that the analysts at the Squadron, brigade, or division level can see everything just as the Soldiers on the ground saw them.

c. **Raven Unmanned Aerial Vehicle (UAV)**

(1) The UAV is small and can be transported easily in three small cases that fit into a ruck sack. The crew can bring it with them and operate wherever the patrol goes. The Raven’s three different cameras attach to the nose of the plane, an electrical optical camera that sends data either through a nose camera or a side camera, an infrared camera in the nose, and a side-mounted IR camera. The IR technology is still too big to fit into the nose section of the plane. The camera does not have a zoom and is unable to lock on a target but provides enough

resolution to show someone carrying a weapon. The Raven has about 45 to 60 minutes of flight time on a battery. The kit comes with spare batteries and a charger that plugs into a Humvee so they can land it, pop in a spare battery and get it back in the air.

(2) The Raven can be launched in just minutes, by hand, into the air like a model airplane. It lands itself by auto-piloting to a near-hover and dropping to the ground, without requiring landing gear or carefully prepared landing strips. Since it is launched and recovered in this manner, it does not require elaborate support facilities and is ideally suited to a forward-deployed unit. Its' automated features and GPS technology also make it simple to operate, requiring no specially skilled operators or in-depth flight training.

d. **Shadow UAV**

(1) The Shadow UAV is the Brigade Commander's primary Reconnaissance, Surveillance, Target Acquisition (RSTA) asset. The Shadow is equipped with an Electro-Optical and Infrared camera (EO/IR). It has a range of 50 km and can fly for up to five hours and altitudes up to 15,000 ft. One advantage of the Shadow is that it is an in house ISR asset that can provide the Squadron or BDE commander with tactical over watch whenever needed.

e. **ISR request procedures.** When the CoIST requests ISR assets they need to be aware of the following:

(1) The CoIST should request a **capability and not an asset** (i.e. "C Troop requests full motion video", not "I need a shadow/predator" etc.). The reason for this is if the CoIST requests an asset and that particular asset is not available they will not get any support. If they request a capability (such as IR or Full motion video) they will get an available platform with that capability.

(2) All ISR requests will be sent to the Squadron S2 to be requested from BDE.

(3) When requesting ISR, be sure to be as specific as possible when explaining why the CoIST needs a particular capability. The demand for ISR is extremely high and the CoIST needs to be able to convince higher that what they need is priority.

(4) CoISTs will utilize the BDE ISR request form.

10. CoIST intelligence systems.

a. **OSRVT.** One System Remote Video Terminal. The OSRVT is an innovative modular video and data system that enables war-fighters to remotely downlink live surveillance images and critical geo-spatial data directly from joint operations tactical unmanned aircraft systems. The OSRVT has the ability to capture all UAV and UAS platforms regardless of who tasked them. This means that with the OSRVT a CoIST can watch footage of any area where a platform is as long as the OSRVT and the asset are linked up.

b. **TIGRnet.** Tactical Ground Reporting System. TiGRnet is actually a software application rather than a network — allows Soldiers to download intelligence into one program. The intelligence can include photos Soldiers have taken with digital cameras, observations they have made and written in simple text or detailed maps of the areas gathered by Global Positioning System devices. Before leaving on patrol, they can study high-resolution satellite imagery of what routes they will be taking. Icons for roadside bombs, ambushes, or weapons caches populate the map so they don't have to wade through the enormous text files. They can click on a roadside bomb icon, for example, to see if there is a picture showing where it was hidden, how it was disguised, and any enemy TTP's related to the specific device.

c. **AXIS PRO** (**A**nalysis and e**X**ploration of **I**nformation **S**ources Professional). It allows analysts unprecedented freedom to find data of interest, organize and refine the results, then visualize the results and detect patterns. AXIS PRO also allows the analyst to manage data through visualization; AXIS PRO automatically loads new data as needed, freeing the analyst from the need to perform additional searches, import extra data, or laboriously build case files. AXIS PRO provides a two-way connection to multiple data sources. The analyst can build link diagrams using information from multiple data sources, then create, edit, or delete that information and commit their changers directly to the data source. AXIS PRO provides a simple yet powerful Multi-Intelligence analysis toolset that is unlike all other intelligence analysis applications. AXIS PRO extends AXIS core features to provide integrated analysis, data management, and intelligence visualization capabilities. AXIS PRO aids the analyst in the process of creating intelligence from massive amounts of information. (AXIS PRO base capabilities include link, temporal, pattern and geospatial analysis tools, net centric alarm and alerts, automated entity and relationship extraction from text documents, and an integrated web portal for information searching and sharing. Additionally, to facilitate interoperability, AXIS Pro comes standard with adaptors for plotting information to additional maps, importing and exporting to both MS Excel and other link analysis tools, and can be configured to work with SQL server. AXIS PRO can also be customized to work with other data sources for backward compatibility)

d. **GRIPP/HCT kit bag.** Global Rapid Response Information Package (GRIPP)/HCT Kit Bags: The GRIPP will allow HCTs to have a secure data and voice transmission package. The HCT Kit bags are equipped with items such as digital cameras, voice recorders, IRIDIUM phones, etc.

e. **DOMEX.** Document and Media Exploitation will support a wide range of intelligence activities, including all source analysis, open source exploitation, human intelligence, signals intelligence, geospatial intelligence, and measurement and signature intelligence. DOMEX reporting and analysis are considered intelligence products.

f. **CIDNE.** Primary means by HCT reporting is fused into the theater intelligence database (BCT S2X/MICO OMT/HCT). The underlying principle behind CIDNE is that information is only

useful when it is readily available at the right time and place to support decision-makers. Often, decisions in the battle space are made without the benefit of critical information that may exist, but is not operationalized, and therefore not available to the decision maker. CIDNE captures and correlates data and then makes that information and its relationships available to other systems, as well as to CIDNE users. The interfaces to other systems include a complete set of Web Services based upon industry standards.

g. **GMTI.** Ground Movement Target Indicator (JSTARS) Tracking can be done using GMTI (Ground Moving Target Indicator) type indicators that can observe all the objects moving in the area of interest. The GMTI measurements supplied by the sensor are assumed to belong to the road network. On the basis of this assumption, several techniques have been studied to take this information into account.

h. **BATS. Biometric Automated Toolset System (BATS).** Collects fingerprints, iris scans, facial photos and biographical information of persons of interest into a searchable data base. Used for tactical operations, detainee operations, base access, IED forensics operations, local hire screening/intelligence. See Tab C for BATS / HIIDE Smartcard.

i. **Hand-held Interagency Identity Detection Equipment (HIIDE):** Collects and matches fingerprints, iris images, facial photos and biographical contextual data of Persons of Interest against an internal database. Interoperable with BAT for biometrics data exchange back to DO biometrics Data Repository.

11. CoIST reporting instructions:

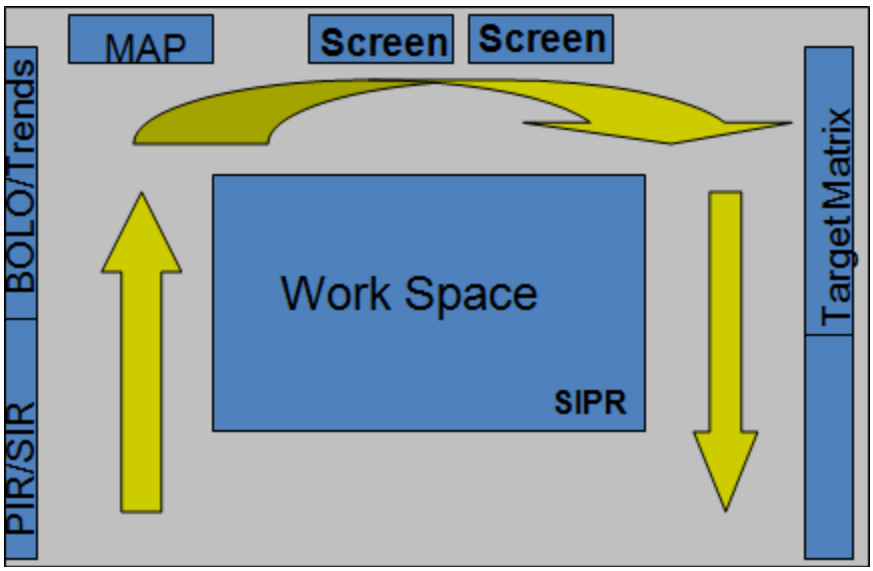
a. CoIST will report any significant activity (SIGACT) on the TIGRnet system so that adjacent and higher units can monitor the situation anywhere on the battlefield. After a SIGACT is posted on TIGRnet, the CoIST will contact Squadron through one of the chat options (mirc chat) so they will be aware of the update to the overall picture.

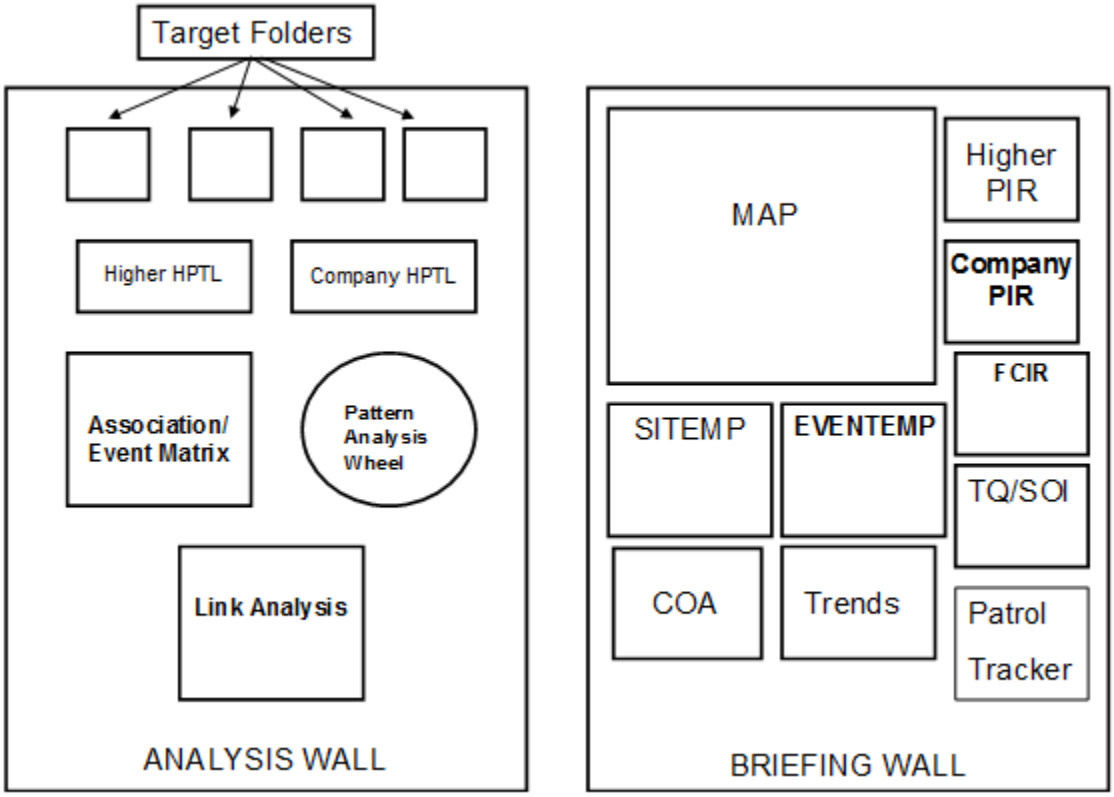
b. If the CoIST discovers a time sensitive target (TST) in an adjacent unit's AO, the CoIST will notify both Squadron as well as the CoIST where the TST is happening so they will have a chance to action the target.

c. Any information that the CoIST thinks is of intelligence value will be reported up to Squadron through email, chat, or TIGRnet. Included with the report is any associated documents and reports to help put the information in perspective for the Squadron.

12. CoIST layout.

a. CoIST should be located near the CP. Control measures need to be taken so that sensitive material is only seen by those with appropriate access. The proximity of the CoIST to the primary TOC is essential to the CoIST mission so they can have instant situational awareness and always be up to speed on current Troop activities. The CoIST needs to also have close access to the Troop Commander, 1st Sergeant, and XO.





b. The Analysis part of the CoIST is where all of the intelligence analysis tools are located so they can be used as efficiently as possible.

c. The Briefing part of the CoIST is where all of the products that you will show to the outgoing patrol leader, convoy leader, or commander will be consolidated. This technique is designed to allow the briefer to focus the person's attention to one specific part of the CoIST instead of leading them around the room trying to explain something.

d. The figure above is the standard layout for a CoIST operating in a tactical environment. This is the minimum of what the CoIST should be able to produce and disseminate. This layout seen above is a representation of what should be on the CoIST wall not how it should be arrayed. The CoIST should tailor the location of their products to best suit briefing their individual Troop and their commander. The CoIST's are encouraged to add to and improve upon the products seen here but this is what is expected as the standard.

e. CoIST's will establish a patrol tracker separate from the operations patrol tracker. This product is designed to assist the CoIST in identifying patterns and TTP's that the Troop is creating. During the patrol prebrief that briefer should recommend certain actions to the patrol leader such as leaving at a different time or taking a different route.

13. Briefing.

a. The visuals section of the CoIST should be able to "brief" itself. In other words, when the patrol leader comes in prior to leaving the FOB, all pertinent information should be displayed in a way that is easy for the leader to understand. A member of the CoIST will give the patrol pre-brief to the patrol leader until the patrol leader feels comfortable enough with the information to leave the FOB.

b. Patrol Brief highlights should include:

(1) Last 24 hour SIGACTS in the area where the patrol leader is going.

(2) Enemy trends that have been established as far as SIGACTS are concerned.

(3) What the predictive assessment is for the area (what the CoIST thinks is going to happen).

(4) Names/pictures of Troop HVI's.

(5) PIR, Specific items the patrol should be on the lookout for.

(6) Questions to ask the local populace or questions for SOI engagements.

(7) What the CoIST recommends for COA (what roads to take, what times to leave and return, where to not go or go).

(8) Current Collection and ISR Plan as it relates to the specific patrol.

(9) Information to include items specific to the patrol or area that will give the patrol leader better situational awareness.

(10) The Briefer is responsible for including all pertinent collection priorities (PIR) so that the patrol will know what they are looking for.

c. Debriefing.

(1) The CoIST is responsible for debriefing every Troop patrol as soon as they return.

(2) The patrol leader should not consider the patrol complete until the debriefing is finished.

(3) The debriefing format is “open forum” where every member of the patrol is required to participate. The CoIST member debriefing needs to accommodate the patrol as best they can. If at all possible the CoIST member conducting the debrief needs to go to where the patrol is and coordinate with the patrol leader.

(4) The debriefing format is as follows:

(a) Use a chronological method. Have the patrol leader talk the entire patrol from start to finish, noting everything that happened. Use maps and route overlays to assist the Soldiers’ memory of where a certain event happened.

(b) Once a significant event is noted, debrief that event completely by going to each individual and have them describe what they saw.

(c) Encourage **everyone** to speak regardless of rank.

(d) Debriefer should have overlay plastic and during the debrief the patrol leader should track the patrol and compare it to the planned route. This will enable the CoIST to keep track of routes, times, and places every patrol in the Troop takes. It will help determine if the Troop is starting to inadvertently set patterns.

d. The CoIST must import all new information into all the intelligence systems (TIGRnet, AXIS PRO, BATS/HIIDE, etc) in order to populate the Squadron and BDE intelligence picture. This provides the entire BCT with one Common Operating Picture (COP).

e. All updates to the Intelligence Systems should be completed after the final patrol debrief is completed.

14. Target analysis process.

a. CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability factors).

(1) The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value. This value represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicate the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent.

(2) **Criticality** means target value. This is the primary consideration in targeting. A target is critical when its destruction or damage has a significant impact organization’s / cell’s capability to continue conducting operations at their current tempo. Targets within a system must be considered in relation to other elements of the target system. The value of a target will change as the situation develops, requiring the use of the time-sensitive methods which respond to changing situations. Criticality depends on several factors:

(a) Time: How rapidly will the impact of the target attack affect operations?

(b) Quality: What percentage of output, production, or service will be curtailed by target damage?

(c) Surrogates: What will be the effect on the output, production, and service?

(d) Relativity: How many targets are there? What are their positions? How is their relative value determined? What will be affected in the system or complex "stream"?

(e) Assigning CRITICALITY values.

CRITERIA	SCALE
Immediate halt in output, production, or service; target cannot function without it.	9-10
Halt within 1 day, or 66% curtailment in output, production, or service.	7-8
Halt within 1 week, or 33% curtailment in output, production, or service.	5-6
Halt within 10 days, or 10% curtailment in output, production, or service.	3-4
No significant effect on output, production, or service.	1-2

(3) **Accessibility** is when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. Accessibility also includes the ability to gain access to human targets (personal security, denied, areas).

(a) The four basic steps identifying accessibility are:

- Infiltration from the staging base to the target area.
- Movement from the point of entry to the target or the objective.
- Movement to the target's critical element.
- Exfiltration.

(b) Factors considered when evaluating accessibility include but are not limited to:

- Active and passive early warning systems.
- Swimmer detection devices.
- Air defense capabilities within the target area.
- Road and rail transportation systems.
- Type of terrain and its use.
- Concealment and cover.
- Population density.
- Other natural or synthetic obstacles and barriers.
- Current and climatic weather conditions.

(c) The analysis along each critical path to the target should measure the time it would take for the action element to bypass, neutralize, or penetrate barriers and obstacles along the way. Accessibility is measured in terms of relative ease or difficulty of movement for the operational element and the likelihood of detection. The use of standoff weapons should always be considered in such evaluations.

(d) Assigning ACCESSIBILITY values.

CRITERIA	SCALE
Easily accessible, standoff weapons can be employed.	9-10
Inside a perimeter fence but outdoors.	7-8
Inside a building but on ground floor.	5-6
Inside a building but on second floor or in basement; climbing or lowering required.	3-4
Not accessible or inaccessible without extreme difficulty.	1-2

(4) **Recuperability** is measured in time; that is, how long will it take to replace, repair, or bypass the destruction of or damage to the target? Human targets must consider how quickly the individual can be replaced. Is there an understudy or replacement?

(a) Factors which should be considered when assessing recuperability include, but are not limited to, the availability of:

- On hand equipment such as railroad cranes, dry docks, and cannibalization.
- Restoration and substitution through redundancies.
- On hand spares.
- Equivalent OB equipment sets that backup critical equipment or components, and the effects of economic embargoes and labor unrest.

(b) Assigning RECUPERABILITY values.

CRITERIA	SCALE
Replacement, repair, or substitution requires 1 month or more.	9-10
Replacement, repair, or substitution requires 1 week to 1 month.	7-8
Replacement, repair, or substitution requires 72 hours to 1 week.	5-6
Replacement, repair, or substitution requires 24 to 72 hours.	3-4
Same day replacement, repair, or substitution.	1-2

(5) **Vulnerability** is if the operational element has the means and expertise to successfully attack the target. When determining the vulnerability of a target, the scale of the critical component needs to be compared with the capability of the attacking element to destroy or damage it. Human targets must be exploited through vigilance and opportunity.

(a) In general, the attacking element may tend to:

- Choose special components.
- Do permanent damage.
- Maximize effects through the use of onsite materials.
- Cause the target to self-destruct.

(b) Specifically, vulnerability depends on:

- The nature and construction of the target.
- The amount of damage required.
- The assets available; for example, personnel, expertise, motivation, weapons, explosives, and equipment.

(c) Assigning VULNERABILITY values.

CRITERIA	SCALE
Vulnerable to long-range laser target designation, small arms fire, or charges of 5 pounds or less.	9-10
Vulnerable to light anti-armor weapons fire or charges of 5 to 10 pounds.	7-8
Vulnerable to medium anti-armor weapons fire, bulk charges of 10 to 30 pounds, or very careful placement of smaller charges.	5-6
Vulnerable to heavy anti-armor fire, bulk charges of 30 to 50 pounds, or requires special weapons.	3-4
Invulnerable to all but the most extreme targeting measures.	1-2

(6) **Effect** is a measure of possible insurgent, military, political, economic, psychological, and sociological impacts at the target and beyond. This is closely related to the measure of target criticality. The type and magnitude of given effects desired will help planners select targets and target components for attack. Effect in this context addresses all significant effects, whether desired or not, that may result once the selected target component is attacked. Human targets can affect the population’s opinion just as significantly, if not more than inorganic targets.

(a) Possible effects can be speculative and should be labeled as such. Effects of the same attack may be quite different at the tactical, operational, and strategic levels. For example, the destruction of a substation may not affect local power supply but cuts off all power to an adjacent region.

(b) Assigning EFFECTS values.

CRITERIA	SCALE
Overwhelmingly positive effects; no significant negative effects.	9-10
Moderately positive effects; few significant negative effects.	7-8

No significant effects; neutral.	5-6
Moderately negative effects; few significant positive effects.	3-4
Overwhelmingly negative effects; no significant positive effects.	1-2

(7) **Recognizability** is the degree to which a target can be recognized by an operational element and/or intelligence collection and reconnaissance assets under varying conditions. Weather has an obvious and significant impact on visibility. Rain, snow, and ground fog may obscure observation. Human targets require wide dissemination of photos and biographical data. An effective biometrics program must be utilized IOT assist the difficult task of identifying an individual.

(a) Other factors which influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the attackers.

(b) Assigning RECOGNIZABILITY values.

CRITERIA	SCALE
The target is clearly recognizable under all conditions and from a distance; it requires little or no training for recognition.	9-10
The target is easily recognizable at small-arms range and requires a small amount of training for recognition.	7-8
The target is difficult to recognize at night or in bad weather, or might be confused with other targets or target components; it requires some training for recognition.	5-6
The target is difficult to recognize at night or in bad weather, even within small-arms range; it is easily confused with other targets or components, it requires extensive training for recognition.	3-4
The target cannot be recognized under any conditions, except by experts.	1 -2

(8) CARVER Matrix.

(a) The CARVER factors and their assigned values are used to construct a CARVER matrix. This is a tool for rating the desirability of potential targets and wisely allocating attack resources.

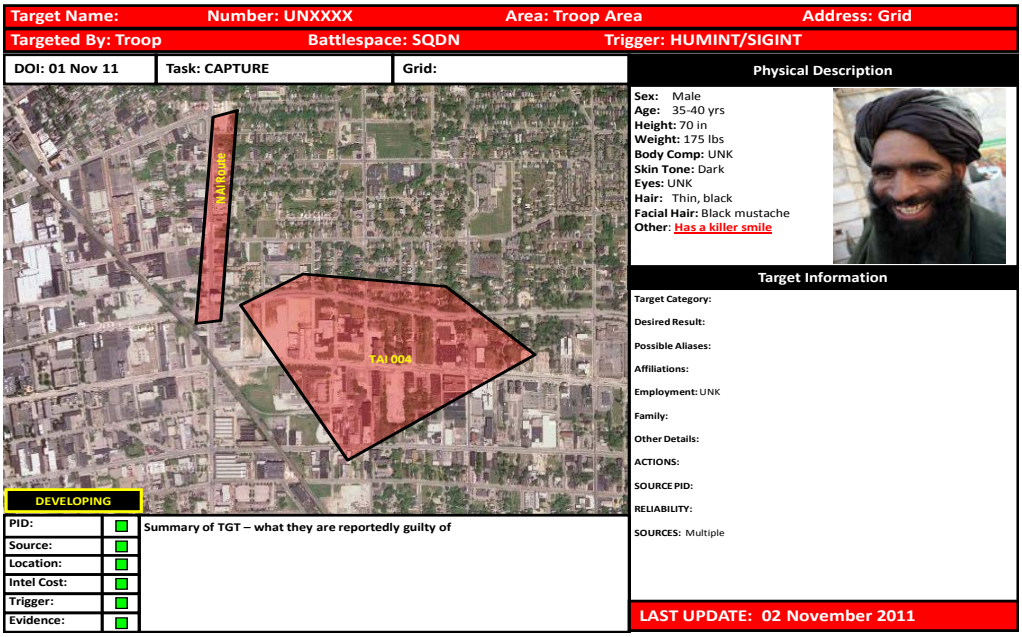
(b) To construct the matrix, list the potential targets in the left column. For tactical level analysis, list the complexes or components of the subsystems or complexes selected for attack by your higher headquarters. See the example diagram below.

IED MANUFACTURING FACILITIES							
POTETIAL TARGETS	**C**	**A**	**R**	**V**	**E**	**R**	**TOTAL**
GARAGE - DC 3848 4838	5	7	2	3	3	1	21
WAREHOUSE - DC 3822 4983	7	3	3	5	3	8	29
HOUSE - DC 3876 5037	9	2	5	8	6	4	34
HOUSE - DC 4076 5137	4	2	7	5	9	6	33

(c) As each potential target is evaluated for each CARVER factor, enter the appropriate value into the matrix. Once all the potential targets have been evaluated, add the values for each potential target. The sums represent the relative desirability of each potential target; this constitutes a prioritized list of targets. Attack those targets with the highest totals first.

(d) If additional men and/or munitions are available, allocate these resources to the remaining potential targets in descending numerical order. This allocation scheme will maximize the use of limited resources. The SIO can use the CARVER matrix to present operation planners with a variety of attack options. With the matrix he can discuss the strengths and weaknesses of each COA against the target. Having arrived at conclusions through the rigorous evaluation process, the Commander can comfortably defend his choices.

b. Target packets.

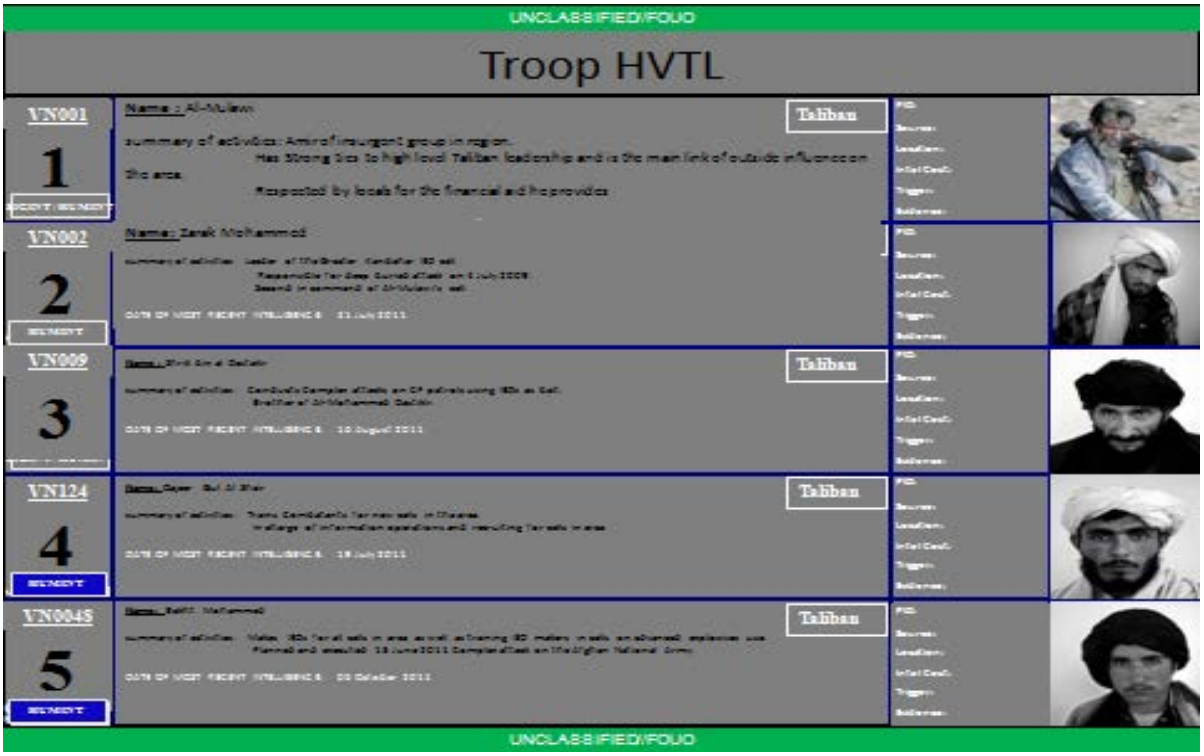


a. Above is an example of the target folder format that will be presented to the commander for approval. This is just a method and should be tailored to fit the personality of the commander.

b. Characteristics that could be integrated into a target folder are: picture ID, sources, corroborating evidence, location to include grid coordinates and multiple pictures, Description of target, patterns of the target, significance of the target to the enemy, name of the target and

aliases. Each CoIST is encouraged to add as much evidence to a target folder so that the actioning unit will have all the information they need to prosecute the target and also for the court system to successfully convict the target.

15. HVTL Format.



a. This is an example of a HVTL target list layout. The HVTLs are put in order of priority and are given target numbers that associate them with other information about them. The target information consists of the most pertinent information about the individual such as religious affiliation, threat group association, rank within the threat group, job/responsibility within the group, past accusations/convictions.

b. It is the responsibility of the CoIST and their commanders to establish what are the prerequisites for each of the categories.

c. The rating system used for PID is as follows:

(a) PID: Positive Identification: Indicators are Green/Yellow/Red.

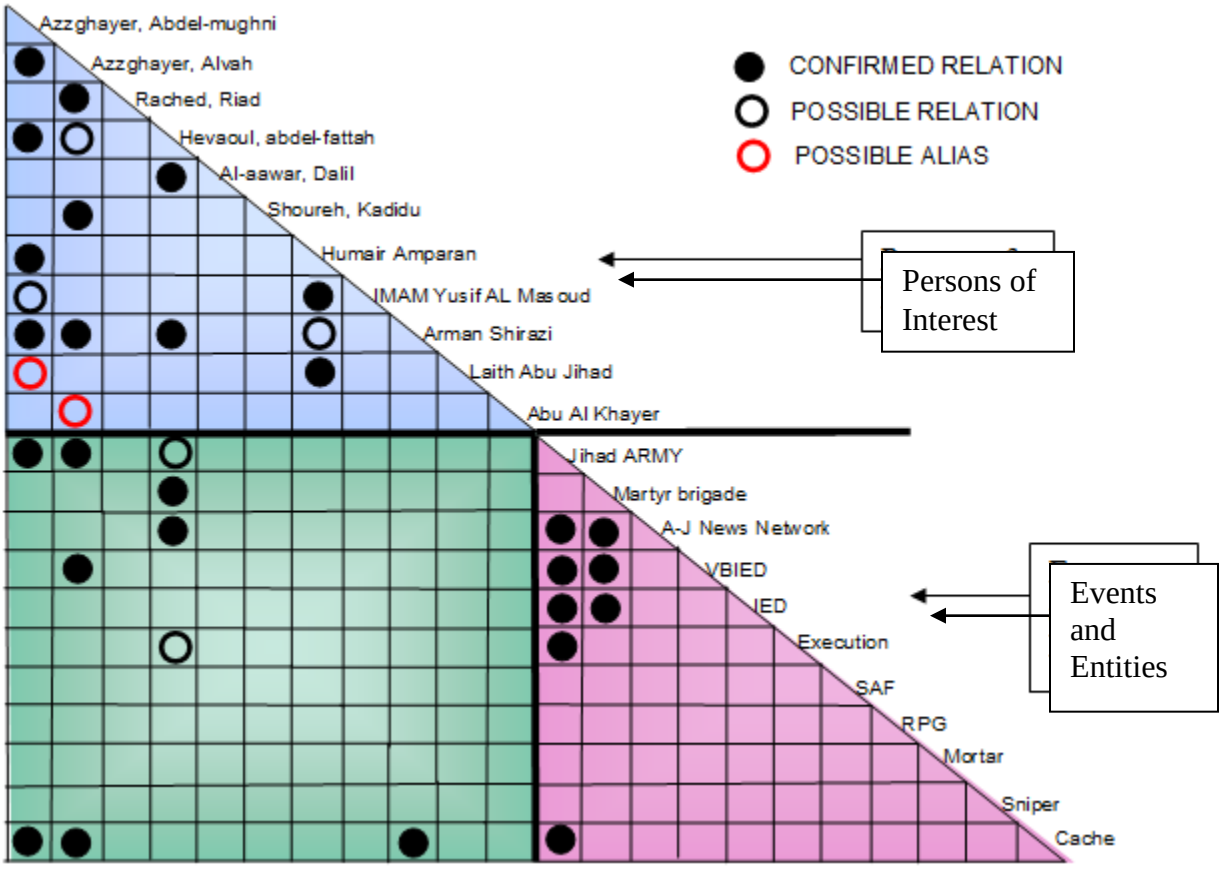
(b) Green is 100% positive identification (Quality Picture, Picture and identifying source).

(c) Yellow is 50% positive identification (Report of physical description but no secondary source or very poor picture).

(d) Red is 0% meaning the CoIST has no idea what the individual looks like only that they exist.

d. The information on the right of the list is the indicators of how “close” the CoIST is to totally identifying all actionable intelligence on the HVI.

16. Association/event matrix.



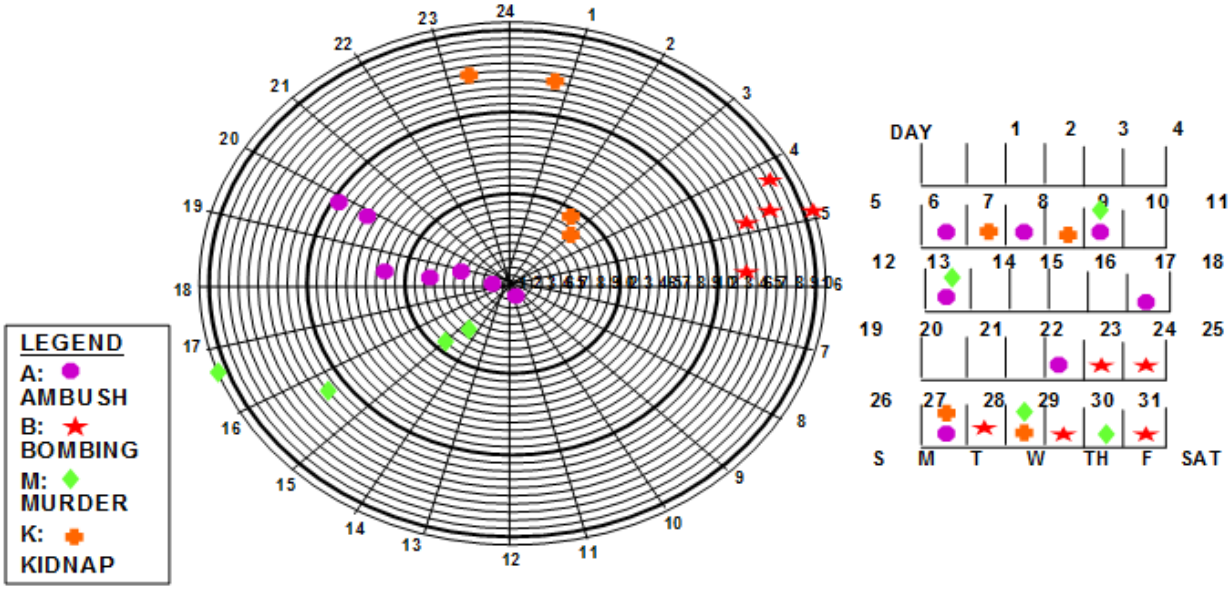
a. The association/event matrix shows known and suspected associations. Analysts determine a known association by "direct contact" between individuals. Direct contact is defined as face-to-face meetings or confirmed telephonic conversation between known parties and all members of a particular organization. This is depicted as a filled circle and placed in the square where the two names meet within the matrix. An unfilled circle indicates suspected or weak associations. When an individual dies, a diamond is added at the end of his or her name.

b. The association/event matrix also determines connectivity between individuals and anything other than persons (interest/entity). Analysts develop a tab to the matrix listing the short titles of each interest/entity. Each short title explains its significance as an interest or entity.

c. The association/event matrix also reveals an organization's membership, organizational structure, cell structure and size, communications network, support structure, linkages with other organizations and entities, group activities and operations, and national or international ties. The activities matrix format uses a rectangle base. Rows are determined by the names from the association matrix, and columns are determined by the interest or entity short titles.

d. The association/event matrix also shows known and suspected connections. Analysts develop the criteria for known connectivity. Criteria may be determined and are defined by CCIR, commander's intent or directive, insurgent doctrine, or the staff judge advocate. Known connectivity is depicted as a filled circle and placed in the square where the individual and interest or entities meet within the matrix. An unfilled circle indicates suspected or weak associations.

17. Pattern analysis wheel and chart.



22

a. The pattern analysis wheel and chart is a tool to assist the CoIST with pattern analysis. Each concentric circle represents 1 day and each wedge in the circle is 1 hour in the day. Most pattern analysis wheels will replicate 1 month or 1 week. Every time an event happens the time and type of event is plotted on the chart and wheel.

b. Pattern analysis.

(1) Pattern analysis of attack times and locations will be conducted at the Troop level.

(2) Mission and commander’s preference will dictate how pattern analysis is conducted at the Troop level; this SOP is meant to guide rather than specify exactly what tools are used.

(3) Predictive analysis is the end state for effective pattern analysis; specific analysis beyond what is presented in this SOP should be conducted whenever the Troop Intel Cell believes that another external factor may be driving enemy patterns (i.e. nightly illumination may influence IED emplacement at a certain location, joint U.S./ANSF patrols may draw more small arms fire than pure U.S. patrols, etc).

(4) Pattern analysis can be conducted with separate time analysis wheels and location analysis maps, or the two can be combined into one product covering one specific form of enemy attack; this type of pattern analysis is represented below.

c. Indirect fire (IDF): Tracks acquired points of origin (POO) and points of impact (POI); un-acquired POOs will be estimated when possible and represented in dashed lines.

(1) Improvised Explosive Device (IED). Tracks IED's found and IEDs detonated; IED symbols should be hyperlinked to associated IED reports.

(2) Small Arms Fire (SAF). Tracks SAF engagements, snipers, drive-by shootings, and short-range rocket fire; SAF symbols should be hyperlinked to associated SAF reports.

(3) Insurgent-on-Civilian. Tracks known and suspected insurgent activities against civilians; symbols should be hyperlinked to associated reports.

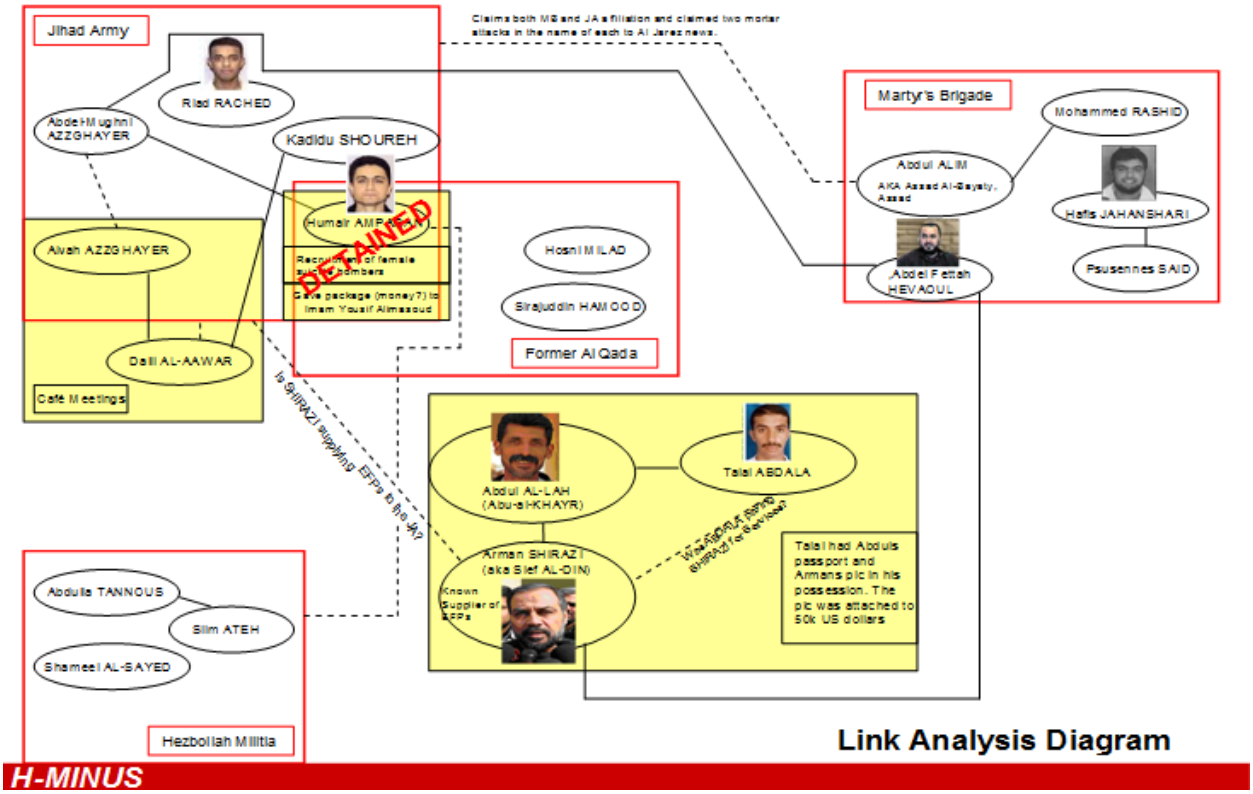
d. The BDE standard for Axis Pro properties include the following, at a minimum:

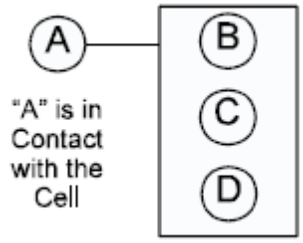
(1) Appearance.
(2) Education History.
(3) Entity Language.
(4) Military History.
(5) Nicknames.
(6) Symbol Information.
(7) Vital Information.

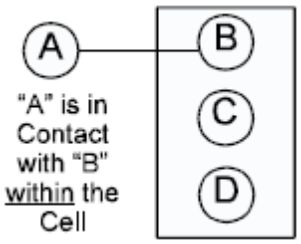
18. Link Analysis:

a. Link Analysis Chart is an analytical tool to connect persons of interest with events, dates, transactions, etc. It is best used in conjunction with the association and event matrix. The chart allows the user to see persons in relation to groups and who else is associated with those groups so that the targeting process becomes more detailed.

b. All Link Diagram generation will be created through the AXIS PRO program.







c. **Constructing Link Diagrams.** The following steps will assist the CoIST's in creating link diagrams.

(1) Collate and organize all raw data related to a situation.

(a) Put in a narrative or report format.

(b) This step is important because the basic data may come from many different sources, ranging from news clippings, to interviews, or reports from surveillance units, photo analysis teams, undercover operatives, or informants.

(2) Identify relevant data points.

(a) In this case the data points are names of the suspects, the people they know, or reports from surveillance units, photo analysis teams, undercover operatives, or informants.

(b) Underline these references in the reports, and make lists.

(3) Construct matrices from the lists. Organize the data points (the names of suspects and organizations or activities) into rows and columns.

(4) Put contact or association points (e.g., A knows B) in the matrix where the corresponding rows and columns intersect.

(a) When working with both confirmed and unconfirmed contacts among suspects, use different symbols to represent the strength of evidence. For example:

(b) Use a "1" for a confirmed contact between two data points.

(c) Use a "2" or any other symbol for unconfirmed contacts.

(d) Use zeros at matrix intersections where no known contact between suspects exists.

(5) Analyze the matrix to determine the number of links associated with each suspect or activity.

(a)Count through each row to find out how many entries appear in it.

(b) Do the same for the columns.

(6) Draw a draft link diagram, grouping suspects together into rectangles representing cells, actions, or organizations.

(a) Start with the individual with the largest number of contacts and work outward.

(b) Use circles to represent individuals and rectangles for organizations or cells.

(7) Draw additional drafts of the link diagram to clarify the relationships, avoiding crossed lines.

(8) Complete the final draft.

(a) Examine the relationships that appear.

(b) Study the diagram carefully and make assessments about patterns in contacts and cell memberships.

(c) Is there a uniform size to the cells, or does size vary?

(d) Do suspects belong to more than one cell?

(e) Are the cells linked tightly together, sharing a number of suspects, or are they spread out, with few connections?

(9) Make recommendations about the group's structure. Identify areas for further analysis.

(a) Are there suspected connections that need verification?

(b) Are there people who appear central to the organization, without whom the structure would collapse?

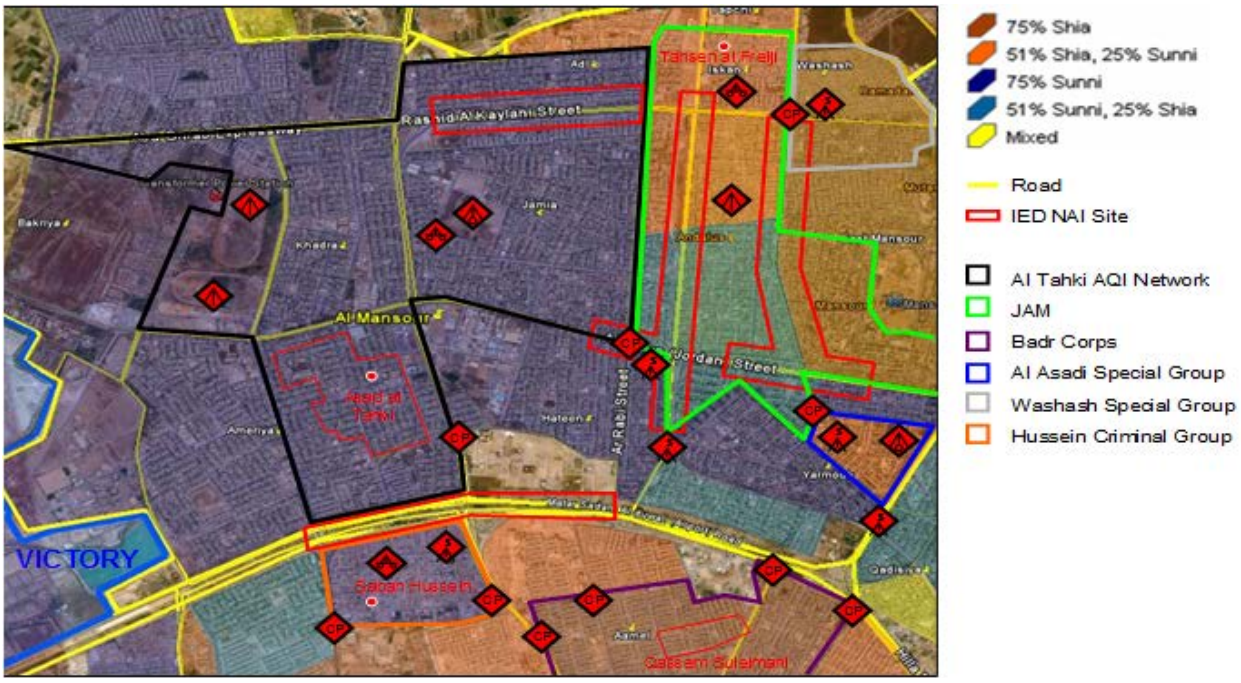
(c) Are there a few individuals with contacts to many others who would be the best targets for surveillance?

(d) Be prepared to substantiate logically the conclusions and assessments drawn from the link analysis.

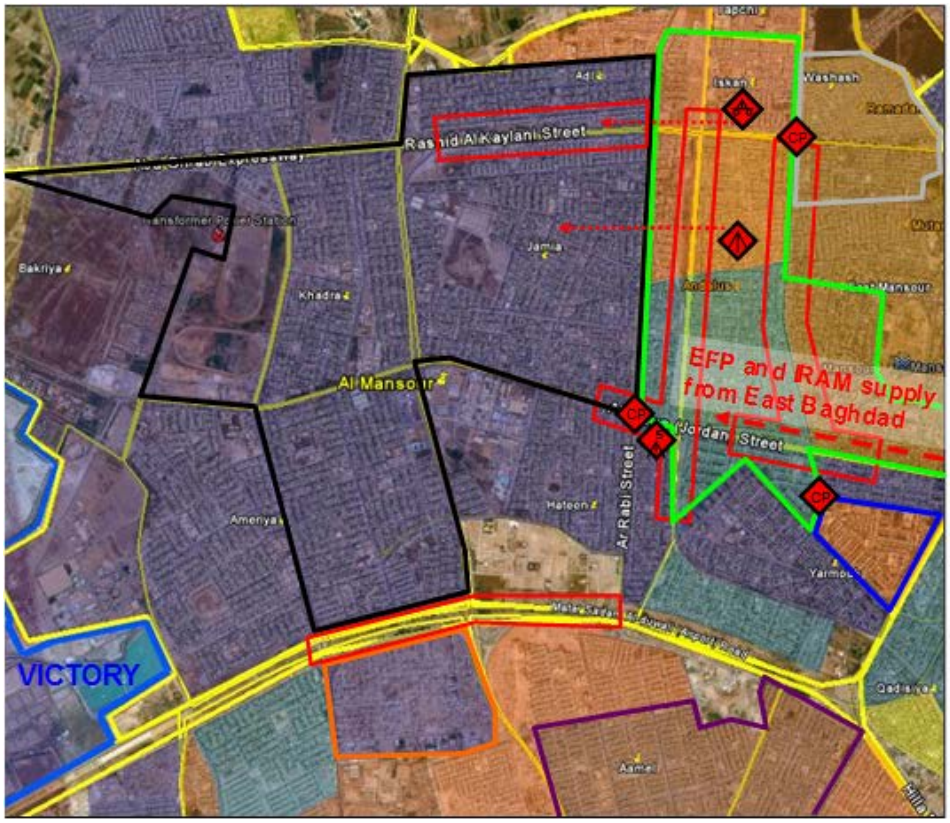
19. SITEMP, EVENTEMP, TRENDS.

a. SITEMPS are a visual representation of how the CoIST sees the enemy on the battlefield at the time. These products are an easy way for the CoIST's to represent to BN what the enemy situation is currently on their AO.

b. This is a reproduction of what a TIGRnet SITEMP may look like.



c. An EVENTEMP Is a visual representation of what the CoIST thinks the enemy is going to do over a certain period of time in the future, usually 24-48 hours or a week.



JAM

MLCOA: Continued IED focus on Sunni in Andulus and Mansour IOT cleanse Sunni from neighborhood.

IEDs and DF attacks will continue against Sons of Iraq CP on Jordan Street in Jamia.

VBIED Construction from Iskan focused on Sunni markets on Rashid Street.

CPs emplaced on borders with Special Groups will continue to serve as flashpoints of DF

MDCOA: Chance of increased DF attacks, murder and intimidation against mixed neighborhoods in Andalus as JAM attempts to limit Sunni ability to vote in upcoming election.

Possible IRAM usage against Sunni population center.

d. These are products and tools to help the CoIST represent to higher and adjacent units what the current and future enemy situation is in the AO.

20. Trends.

a. Within the CoIST should be posted a list of things that the enemy has currently been doing, such as using a different IED TTP, or attacking the FOB at a certain time everyday.

b. This is valuable take away information for both outgoing patrol leaders but also the commander. The information that is posted could save a Soldier's life by telling them that something has been happening and it probably will happen again. The trends list is a simple form of predictive analysis but the only difference is it is just a list of things that have happened and the patterns they have created.

21. CoIST information requirements / PIR. PIR is a way for CoIST to task patrols with finding out information that they need to know. This is an information requirement that cannot be satisfied by RFI, higher guidance or ISR tasking. These are specific questions about the AO that will allow CoIST to have a better understanding of the situation on the ground.

22. Local National Questioning (LNQ). LNQ is a technique to allow the CoIST to suggest possible questions to ask while out on patrol. These questions are usually directed at the general public but can be tailored to a specific individual.

23. Recommended courses of action.

a. CoISTs will recommend courses of action to the commander for his review. These COA's are developed after careful analysis of the situation and creation of the best possible way to handle it.

b. For example, recommending to the commander that he visit a certain key leader because the CoIST is tracking that individual having influence in the area of operations.

c. The format for a recommended COA is as follows:

(1) Situation: A brief rundown of what is going on. The situation needs to be limited to a small number of events, preferably one so that the course of actions is easy to develop at the TROOP level.

(2) Recommendation: Courses of action that will either eliminate the situation or turn the situation in favor of Coalition Forces.

(3) As soon as a course of action is completed it needs to be recommended to the commander so that an opportunity is not missed.

d. Recommended course of action example.

Recommended Course of Action

Situation: A recent spike in high visibility suicide bombings in AO Arrow have made these attacks a serious threat to the stability of the Blackhawk AO. Attacks bear the hallmarks of Jihad Army methods and source reports indicate that Humair AMPARAN may be involved. Historical reporting shows his use of female suicide bombers to revenge the death of males killed by CF forces. Attacks seem to take place in public places alternating between Sunni and Shiite neighborhoods.

Recommendation:

- Emplace TCPs at grid locations (38S MB 4225 9065, 38S MB 4266 9085, 38S MB 4314 9101 and 38S MB 4365 9125) to deter insurgent traffic from entering the AO from the south.
- Increase local security in market places, sporting events and other high visibility gathering places in the sector.
- TQ of Humair AMPARAN has indicated that he owns an electronics storefront in A Troop. AO. Targeting and SSE of the storefront is highly recommended. This is a time sensitive action.

24. Troop informant operations.

a. **Troop Informant Operations are not Source Operations!**

(1) CoIST's need to inform their commander's that they are not authorized to task an informant.

(2) An informant is defined as an individual who comes to you to willingly give information.

b. Informant operations are a valuable source of intelligence if exploited correctly. The Troop will most likely experience both walk in and repeat informants and it is up to the CoIST to both track them and exploit them.

c. The CoISTs will follow these suggested techniques to be able to successfully safeguard and exploit the informant.

(1) Safeguard informant's real names; use aliases on the tracker and disclose real names only to leaders who you trust to be careful with the information.

(2) Pictures can digitally hyperlink to more detailed information.

(3) Ensure that all informant meetings are recorded on the Informant Contact Log and have updated Informant Personal Information Sheets.

(4) The informant overlay must be tightly controlled as public knowledge would likely cause the death of Troop informants; hard copies of the overlay should be shredded when obsolete and should not go forward on patrols nor be posted anywhere that ANSF or interpreters can view.

//ORIGINAL SIGNED//
CHARLES T. LOMBARDO
LTC, AR
Commanding

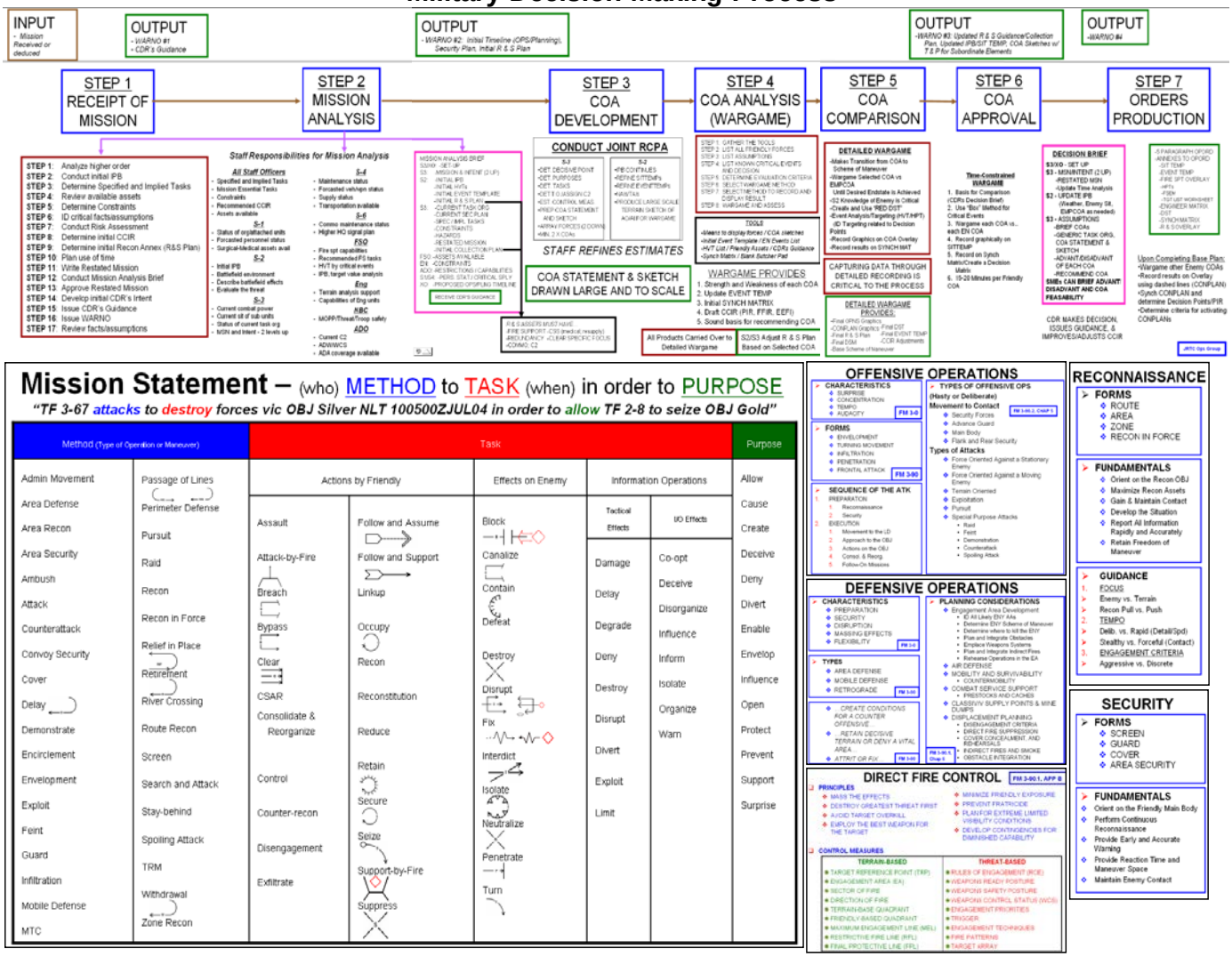
PLANNING / PREPARATION

EXECUTION

POST IN CP

GRAPHICS

TAB A: MDMP

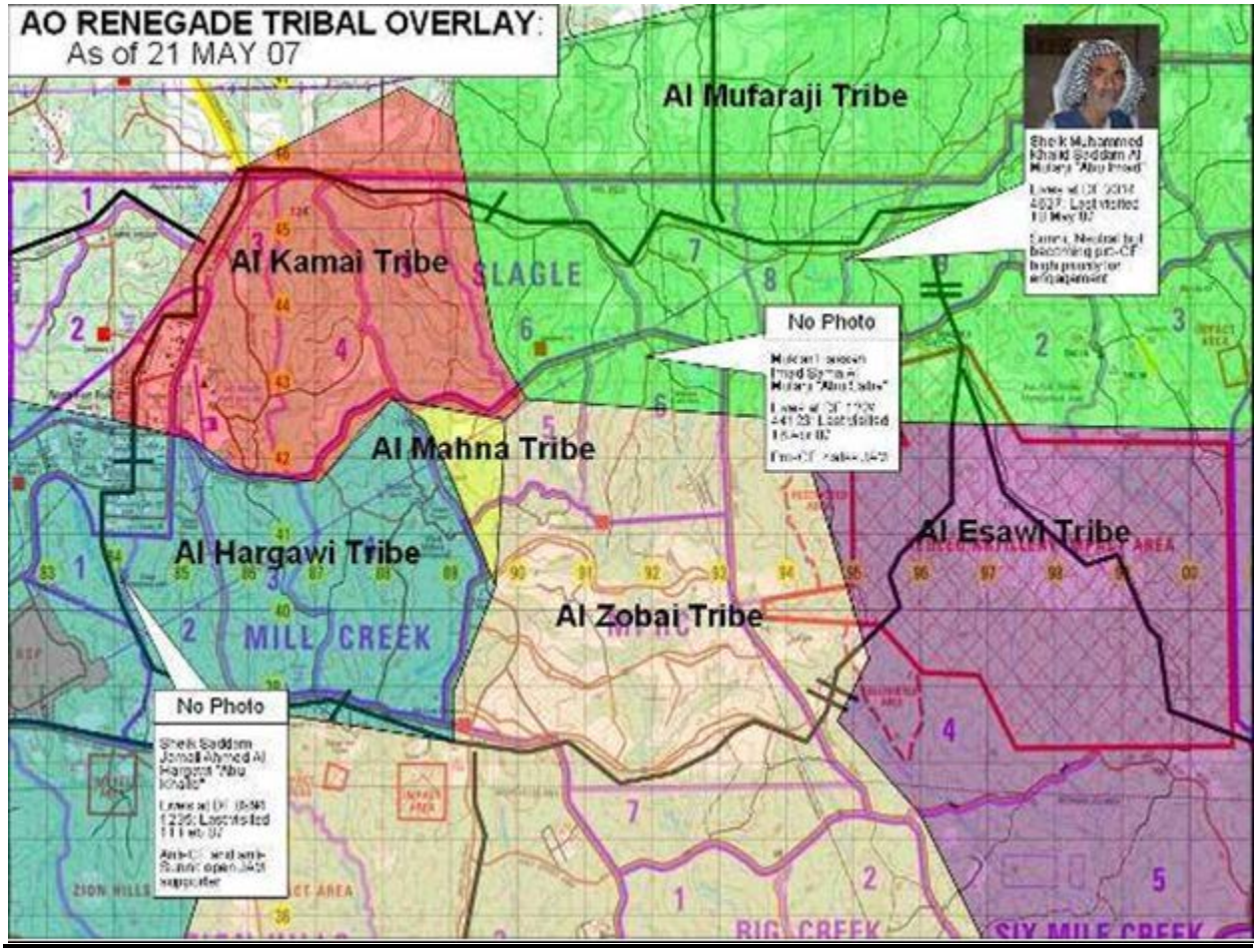

Military Decision Making Process
INPUT
OUTPUT
OUTPUT
OUTPUT
OUTPUT
STEP 1 RECEIPT OF MISSION
STEP 2 MISSION ANALYSIS
STEP 3 COA DEVELOPMENT
STEP 4 COA ANALYSIS (WARGAME)
STEP 5 COA COMPARISON
STEP 6 COA APPROVAL
STEP 7 ORDERS PRODUCTION
CONDUCT JOINT RCPA
STAFF REFINES ESTIMATES
COA STATEMENT & SKETCH DRAWN LARGE AND TO SCALE
WARGAME PROVIDES
Mission Statement – (who) METHOD to TASK (when) in order to PURPOSE
"TF 3-67 attacks to destroy forces vic OBJ Silver NLT 100500ZJUL04 in order to allow TF 2-8 to seize OBJ Gold"
Method (Type of Operation or Maneuver)
Task
Purpose
Admin Movement
Area Defense
Area Recon
Area Security
Ambush
Attack
Counterattack
Convoy Security
Cover
Delay
Demonstrate
Encirclement
Envelopment
Exploit
Feint
Guard
Infiltration
Mobile Defense
MTC
Passage of Lines
Perimeter Defense
Pursuit
Raid
Recon
Recon in Force
Relief in Place
Retirement
River Crossing
Route Recon
Screen
Search and Attack
Stay-behind
Spoiling Attack
TRM
Withdrawal
Zone Recon
Actions by Friendly
Assault
Attack-by-Fire
Breach
Bypass
Clear
CSAR
Consolidate & Reorganize
Control
Counter-recon
Disengagement
Exfiltrate
Follow and Assume
Follow and Support
Linkup
Occupy
Recon
Reconstitution
Reduce
Retain
Secure
Seize
Support-by-Fire
Suppress
Effects on Enemy
Block
Canalize
Contain
Defeat
Destroy
Disrupt
Fix
Interdict
Isolate
Neutralize
Penetrate
Turn
Information Operations
Tactical Effects
IO Effects
Damage
Delay
Degrade
Deny
Destroy
Disrupt
Divert
Exploit
Limit
Co-opt
Deceive
Disorganize
Influence
Inform
Isolate
Organize
Warn
Allow
Cause
Create
Deceive
Deny
Divert
Enable
Envelop
Influence
Open
Protect
Prevent
Support
Surprise
OFFENSIVE OPERATIONS
DEFENSIVE OPERATIONS
DIRECT FIRE CONTROL
RECONNAISSANCE
SECURITY

TAB B: Situational Understanding of the Operational Environment

1. Tribal overlay.

a. Break down AO by tribal areas (most tribal areas are not 100% pure; this tracker shows the majority tribe in an area).

b. Leader pictures and tribe names can digitally hyperlink to existing digital reports.

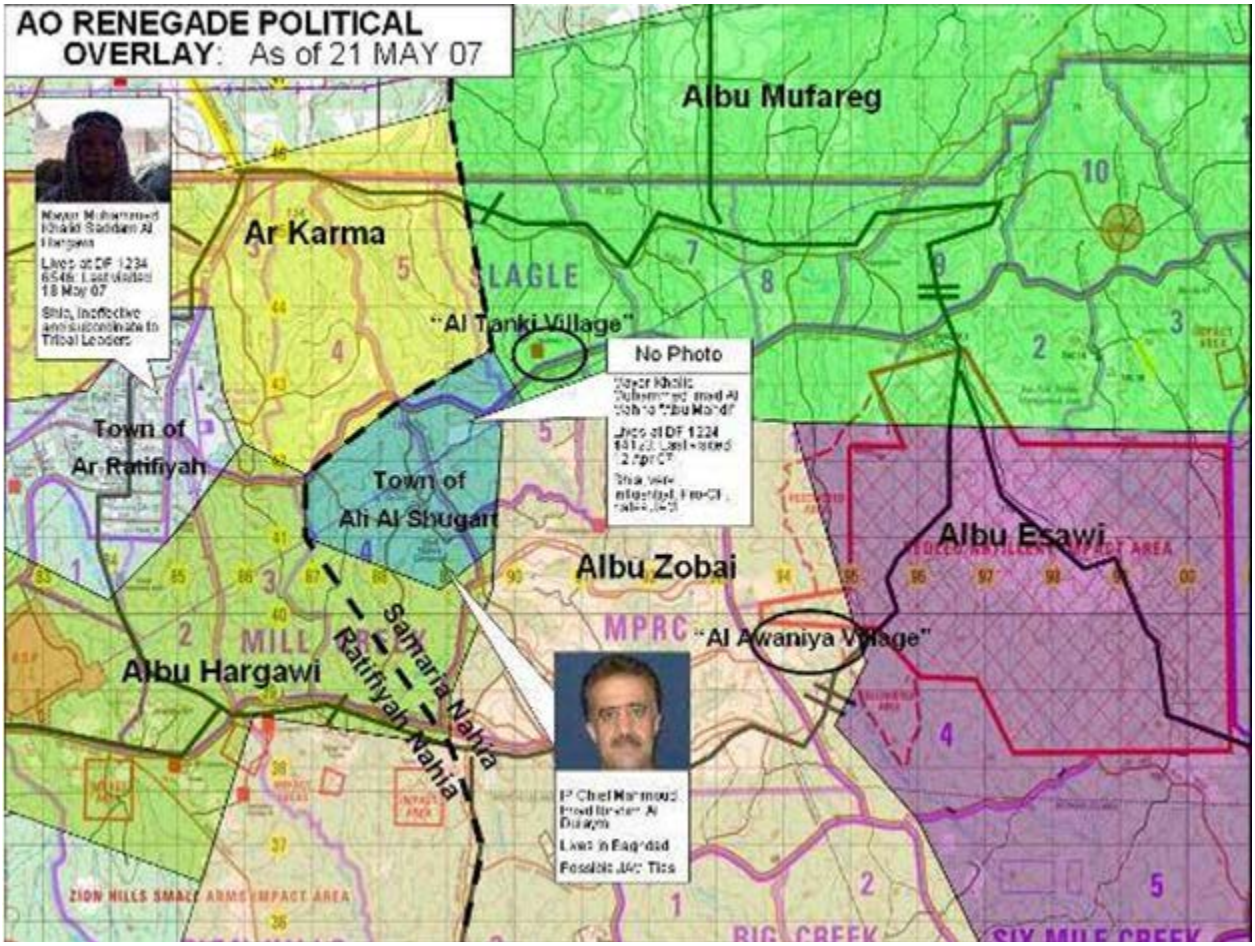


2. Political overlay.

a. Break down the AO by town or regional names (the names used by the local nationals).

b. Identify tribal and regional dividing lines.

c. Identify government leaders such as mayors, ANSF leaders, influential political leaders.

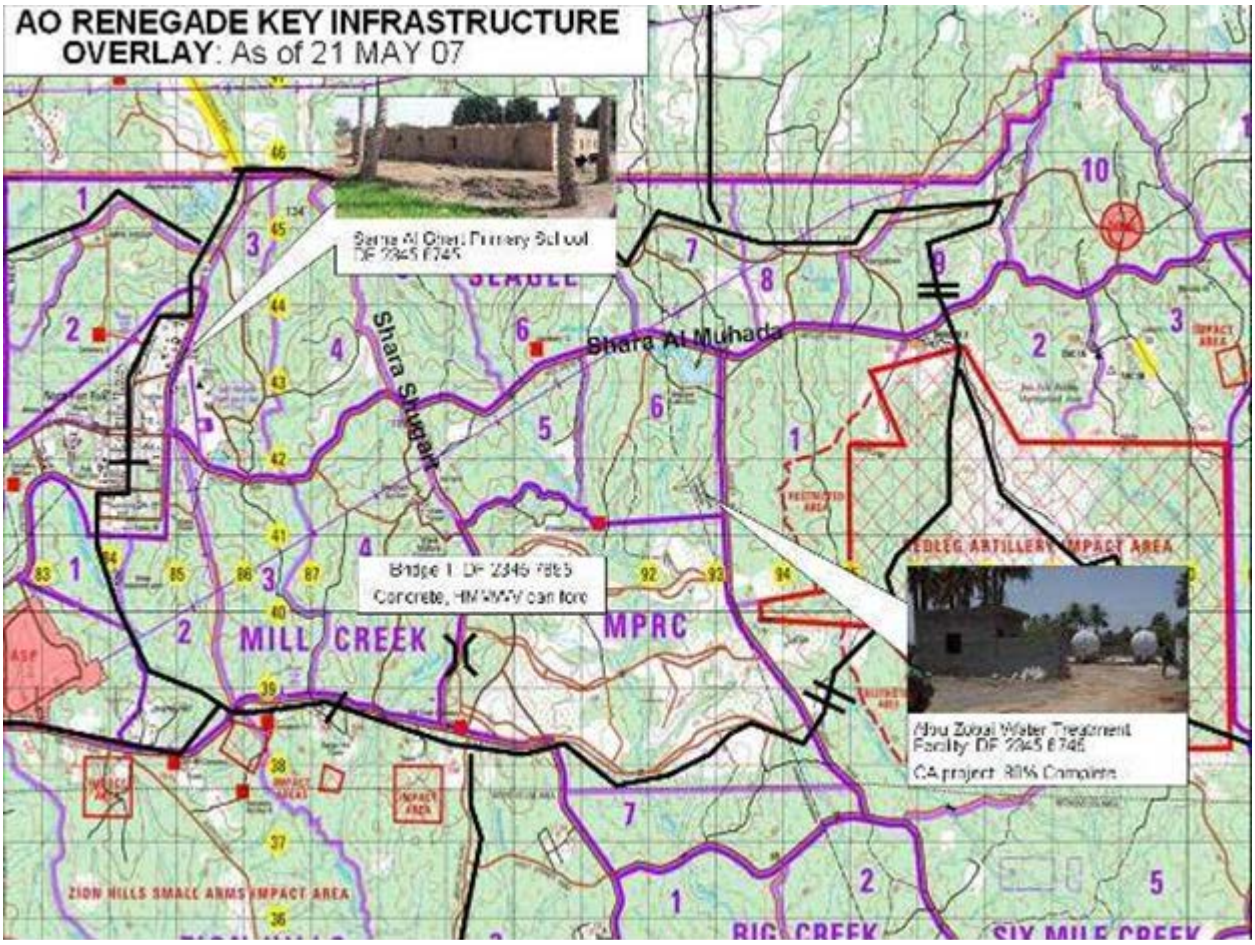


3. Key infrastructure overlay.

a. Include road names using Afghani naming conventions (not all roads in Afghanistan are locally named).

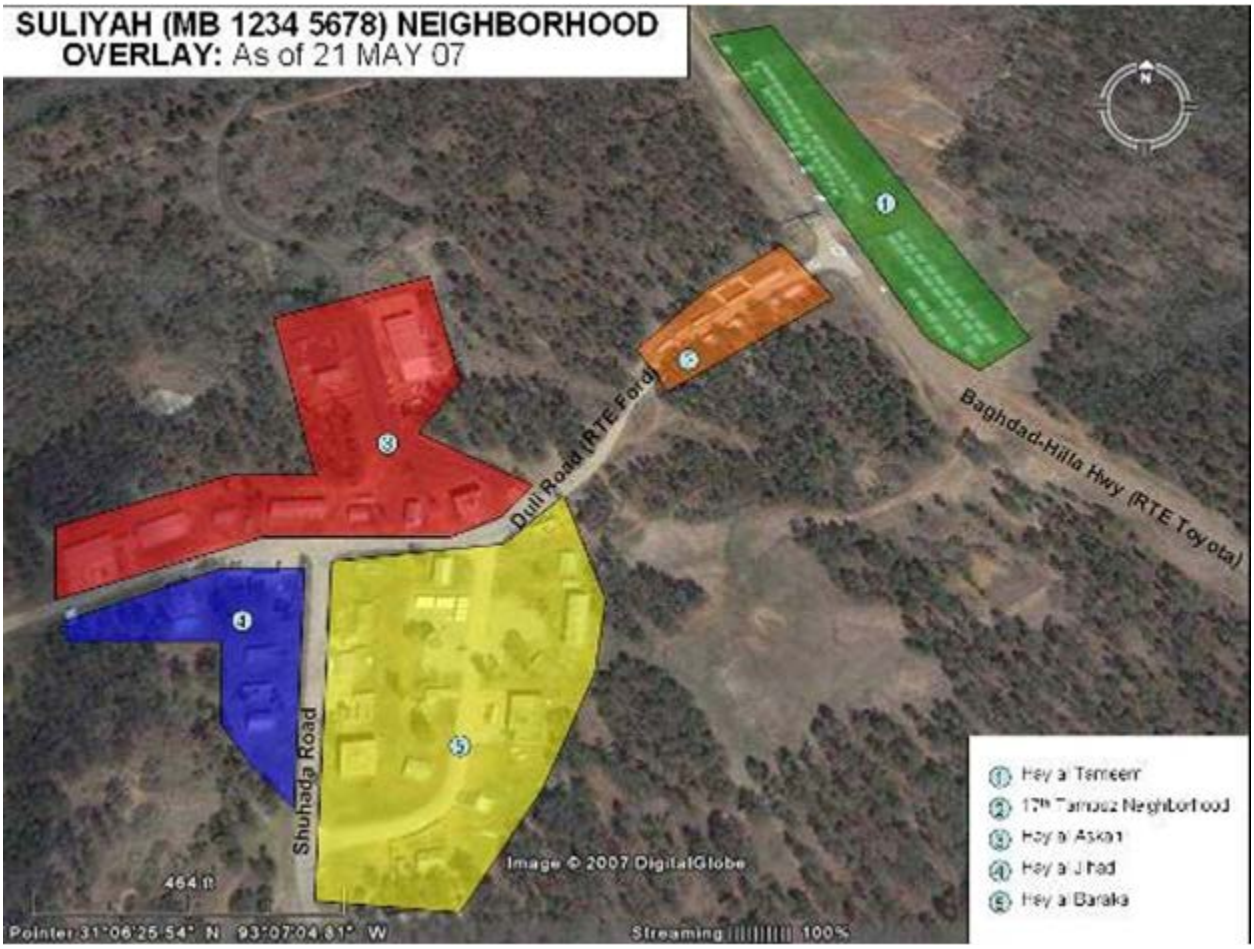
b. Include significant infrastructure such as schools, public utilities, government buildings, bridges, medical facilities, ongoing CA projects .

c. Infrastructure pictures can digitally hyperlink to more detailed information in TIGRnet, or can be tracked Via an excel Data base.



4. Neighborhood overlays (if required by the Troop).

a. Only required if the AO includes towns or cities with too much detail to include on the political and key infrastructure overlays. This overlay will include neighborhood names, landmarks, and road names.

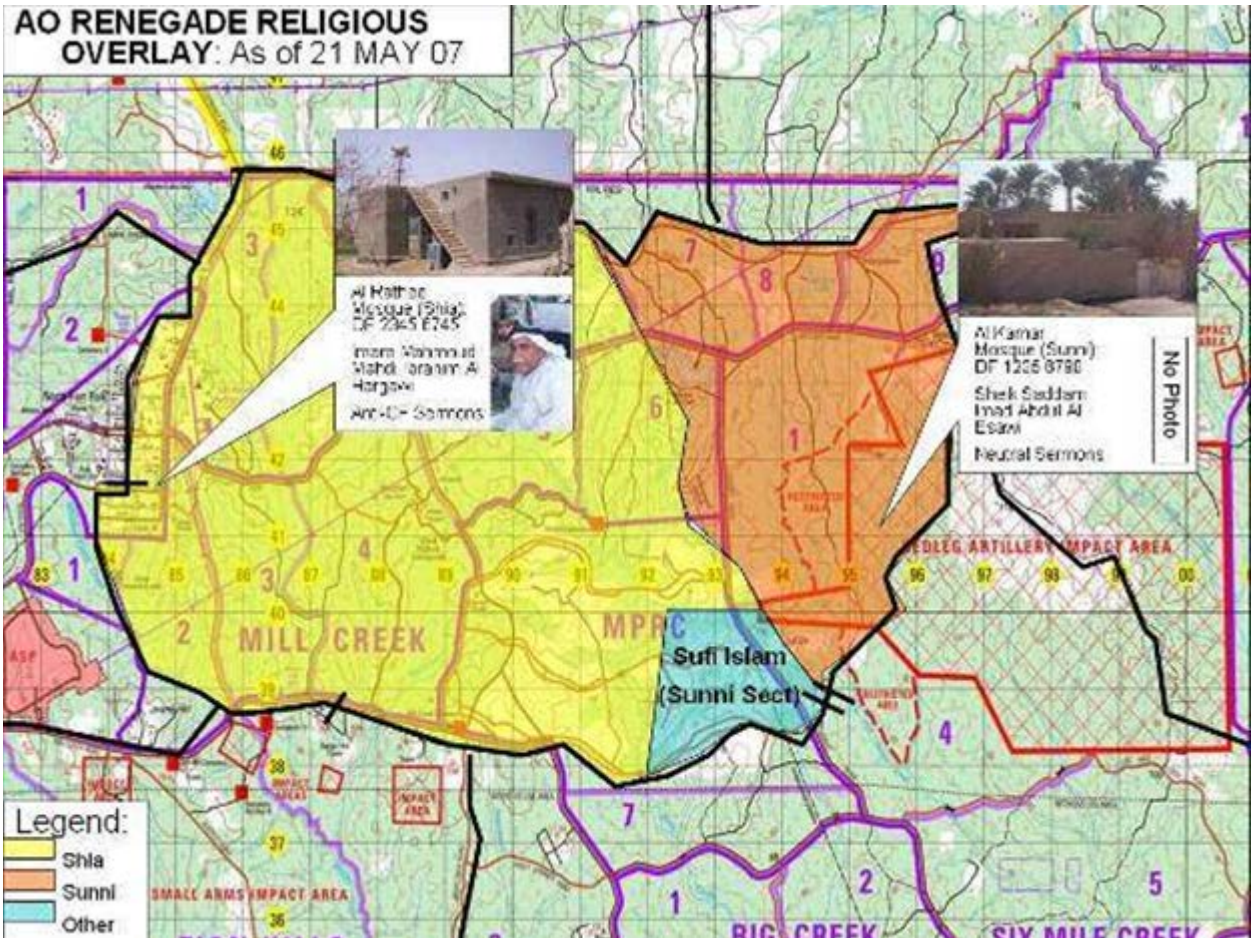


5. Religious overlay.

a. Break down the AO by religious/sectarian lines to include sectarian enclaves.

b. Identify significant sects or sub-groups.

c. Religious leaders and mosque pictures can digitally hyperlink to existing digital reports and previous mosque monitoring reports using TIGRnet, or can be tracked using an Excel spread sheet.



6. Enemy situational template (SITTEMP).

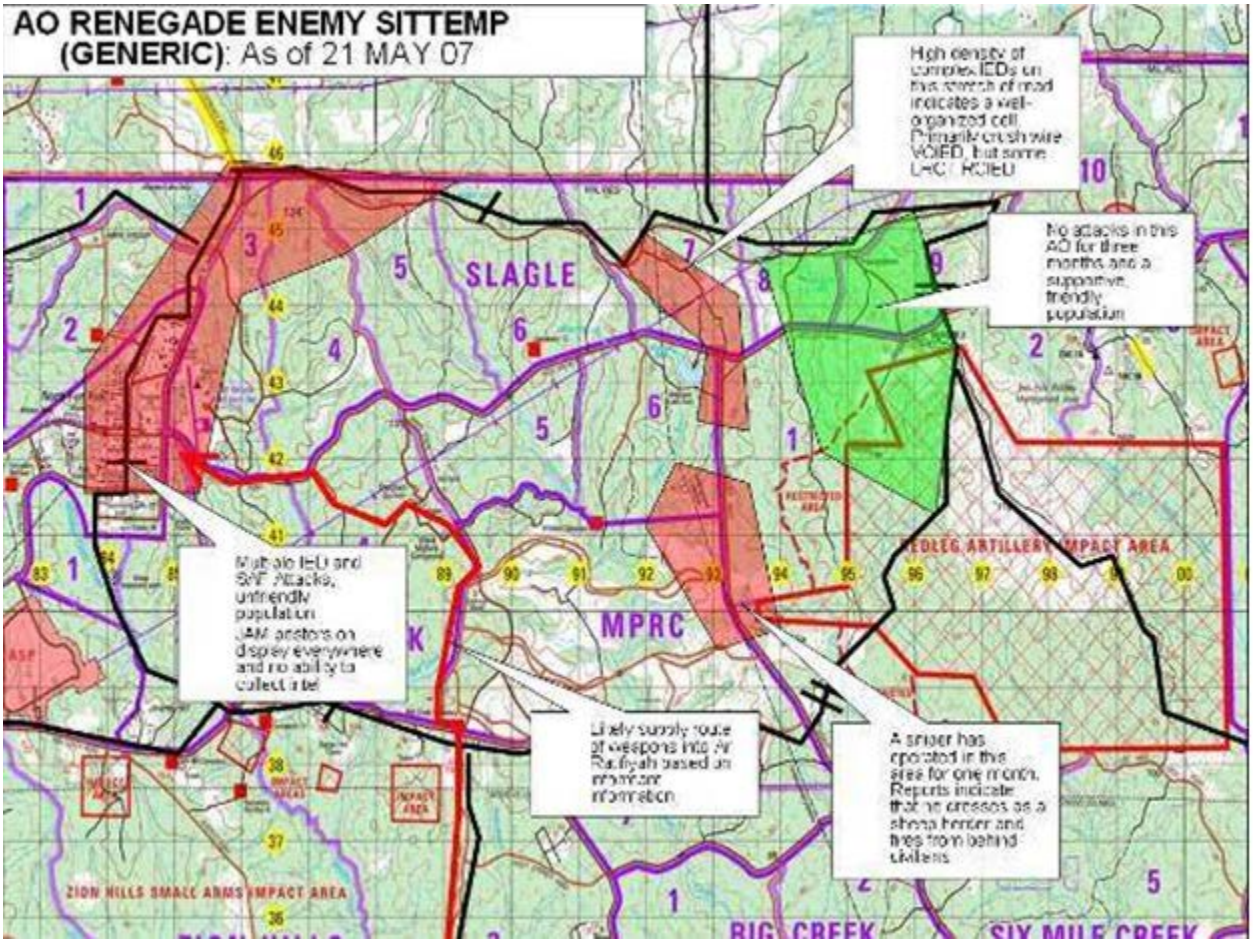
a. Basic SITTEMP should include generic information about the enemy situation in the AO.

b. Detailed SITTEMPs cover one group or threat in much more detail.

c. Ensure local nationals who should be detained on sight are identified on the SITTEMP.

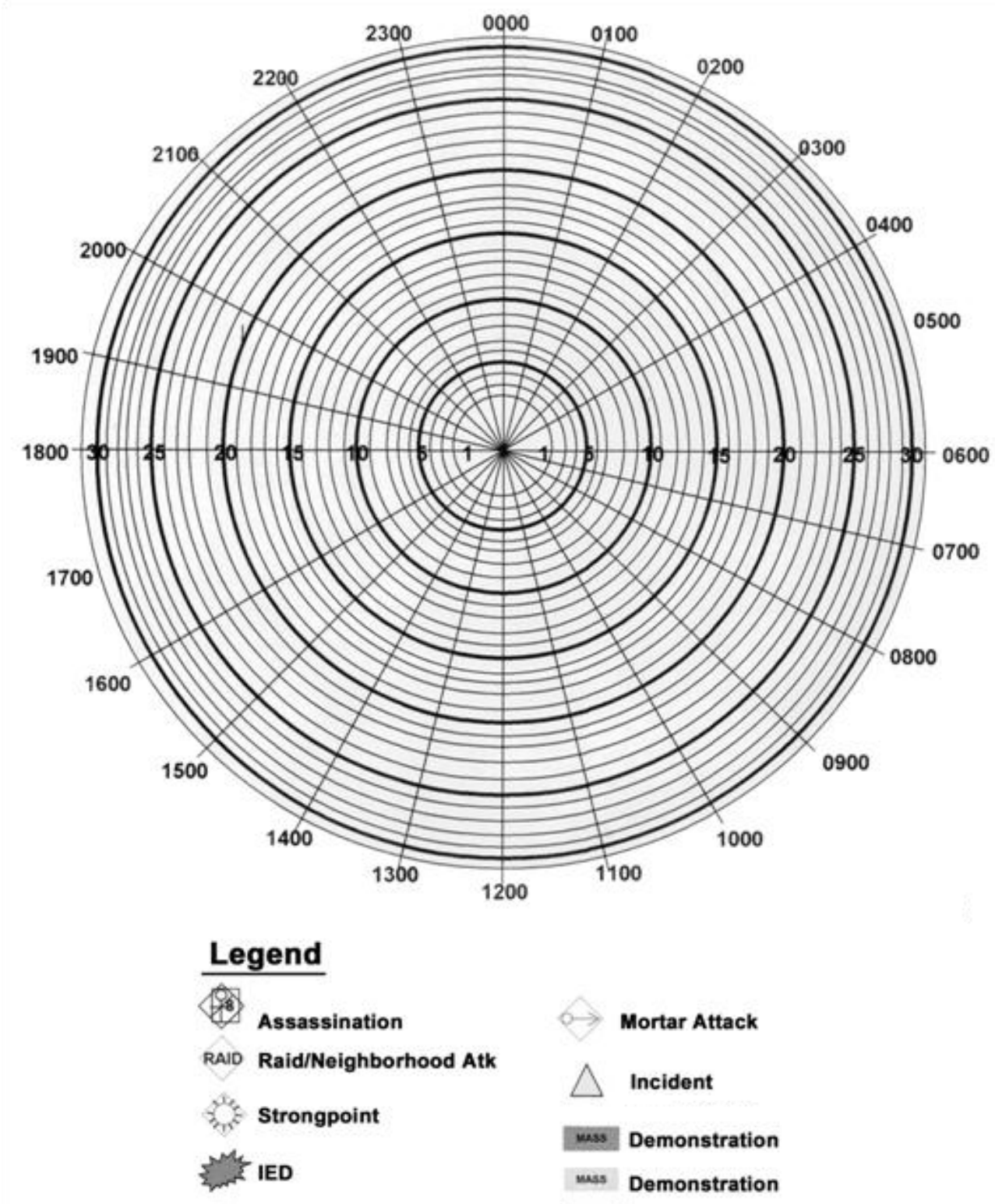
d. Pictures can digitally hyperlink to more detailed information.

e. Association analysis tools and link diagrams can be used as required to further analyze enemy information as presented on specific SITTEMPs.

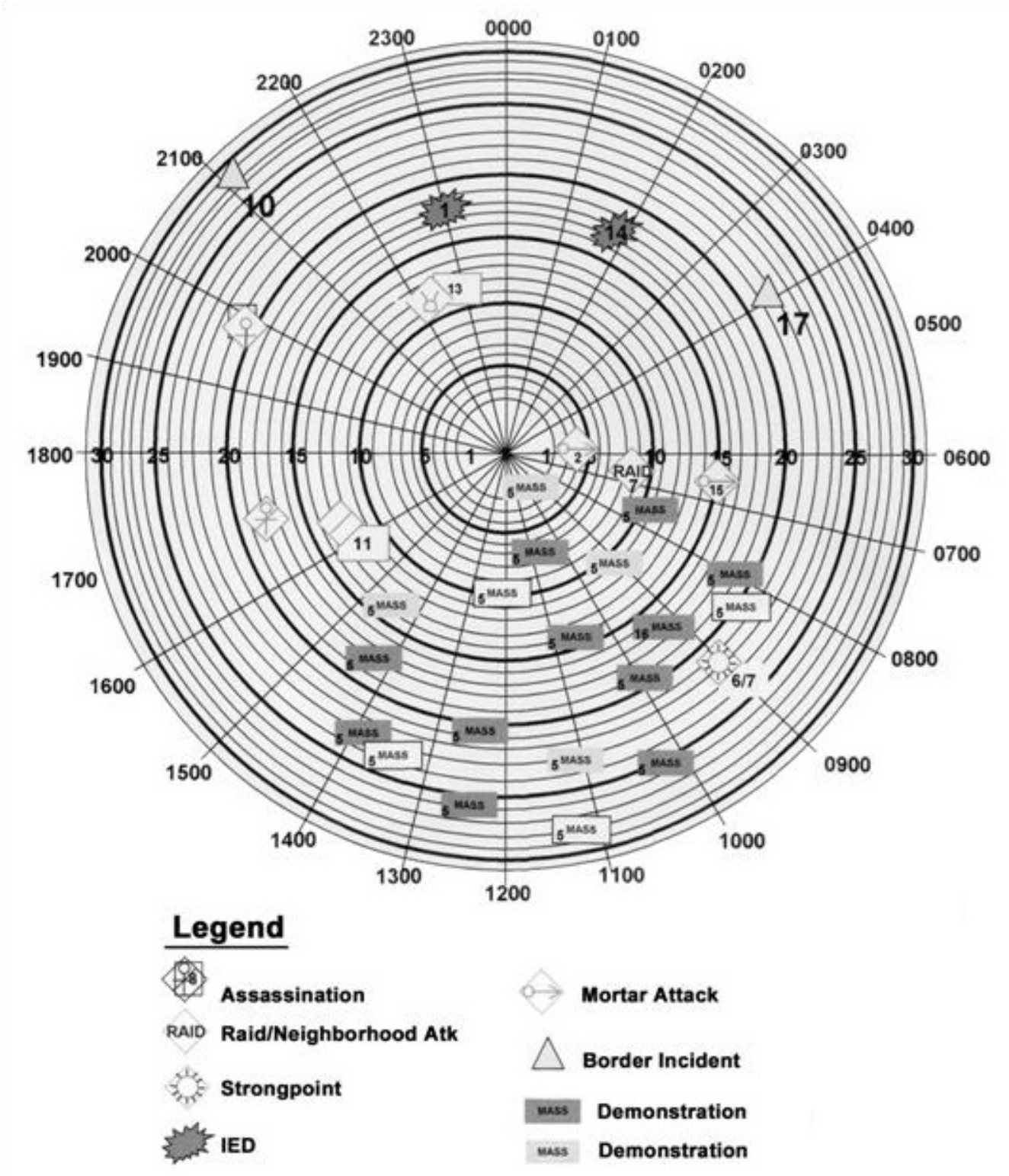


TAB C: PATTERN ANALYSIS WHEEL

1. Blank Pattern Analysis Wheel.



2. Example of completed Pattern Analysis Wheel.

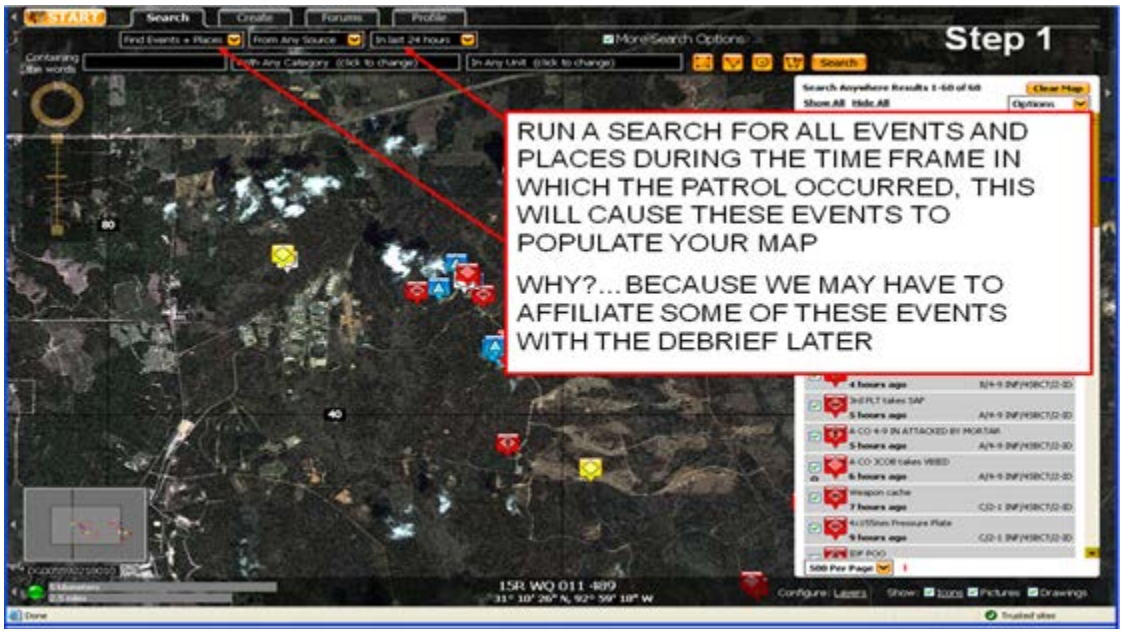


TAB D: TIGR (STEP-BY-STEP WALKTHROUGH)

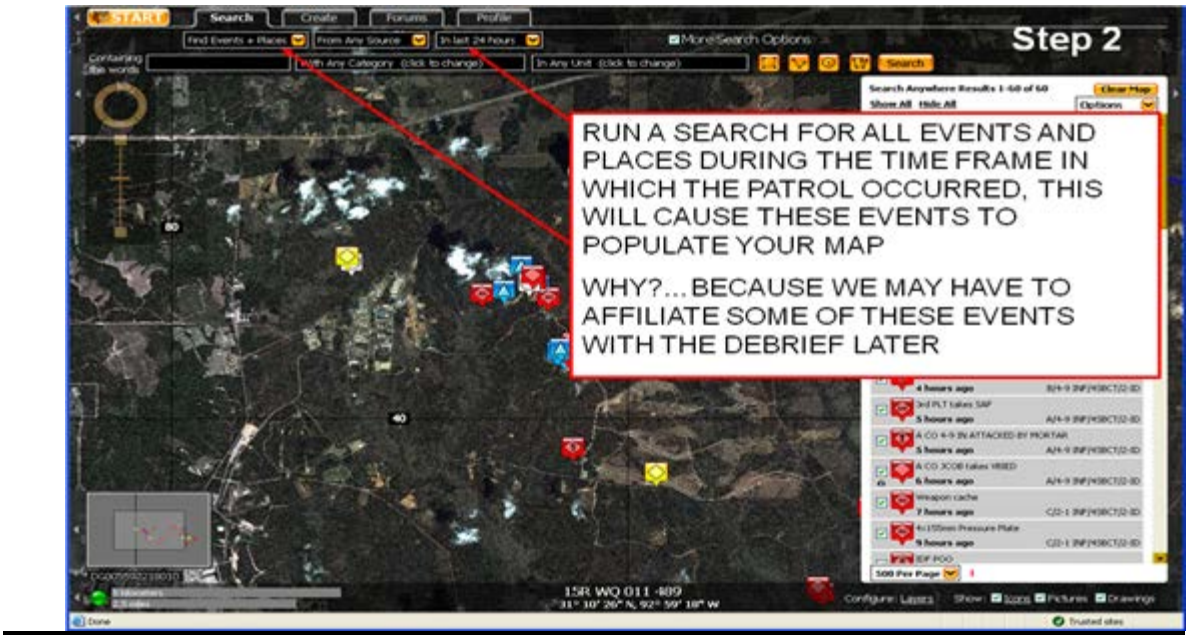
1. Purpose. This appendix will display the standards for creation of a TIGR brief by identifying the ten steps for “Bottom-Up Intelligence Flow”.

2. Ten Steps for “Bottom-Up Intelligence Flow”.

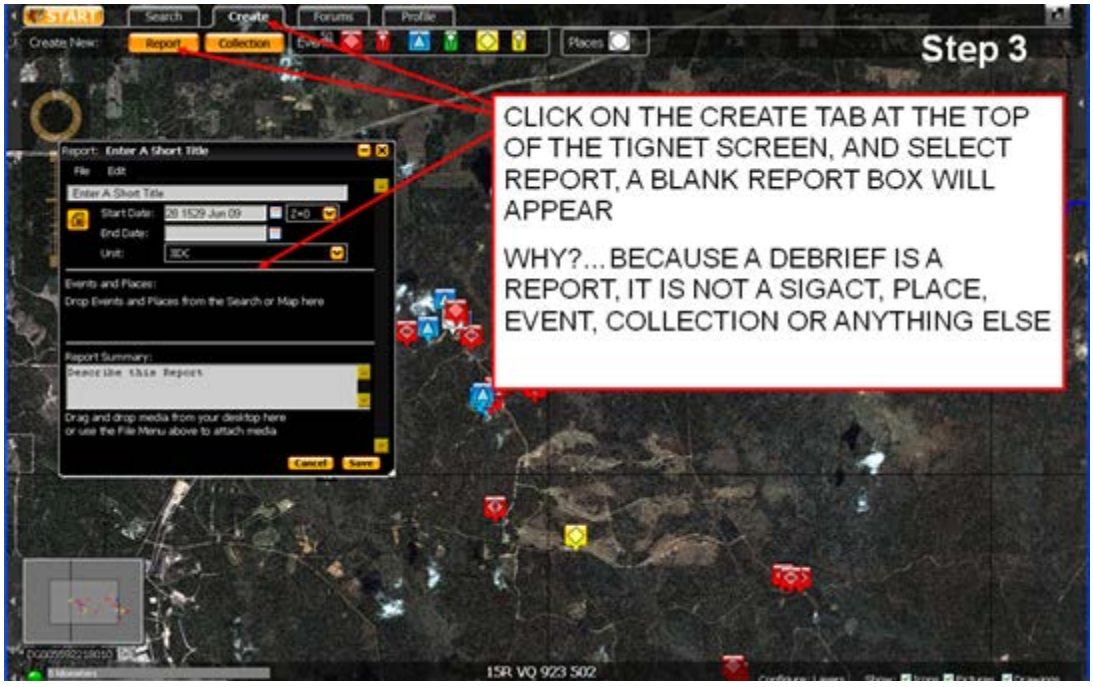
a. Step 1 – Log onto TIGRnet and start with a blank map background on your AO.



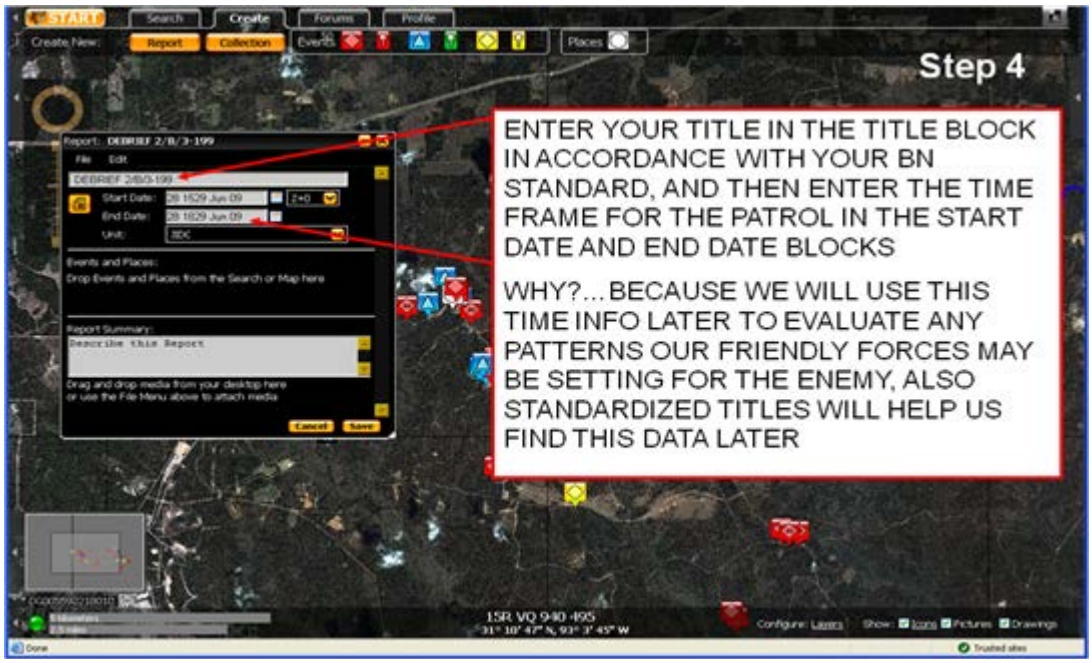
b. Step 2 – Run a search for all events and places during the time frame in which the patrol occurred. This will cause the events to populate on your map. The events may have to be affiliated with the debriefer at a later time.



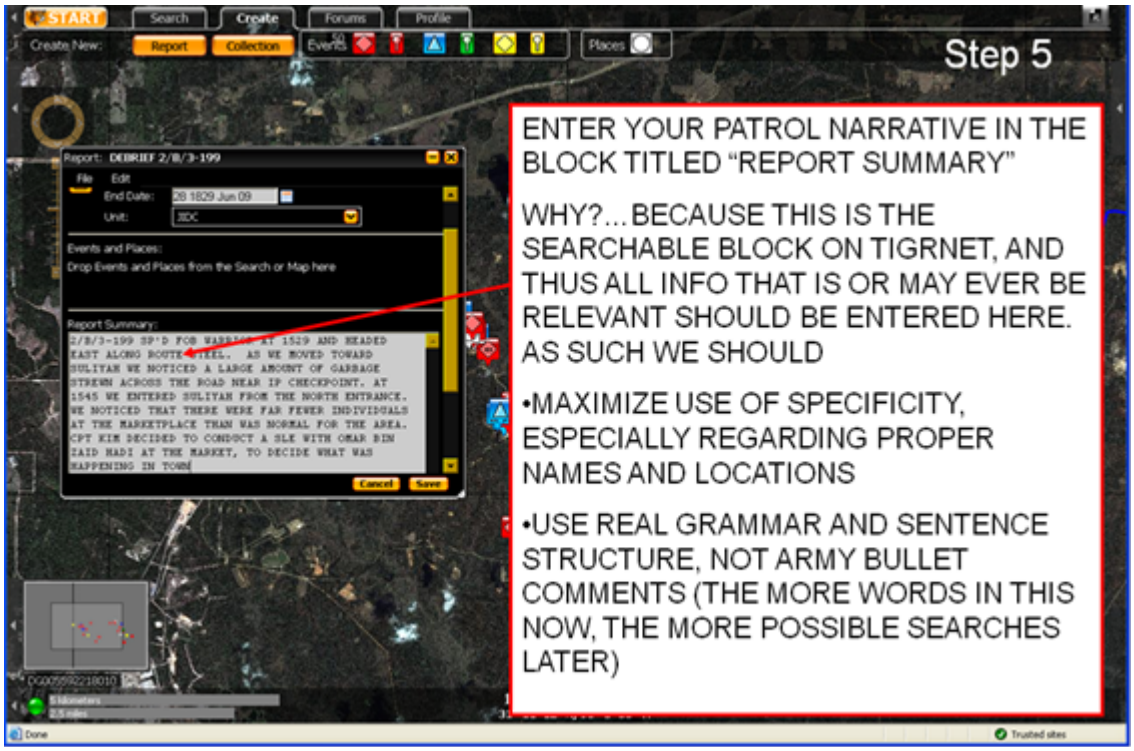
c. Step 3 – Click on the create tab at the top of the TIGRnet screen and select report. A blank report box will appear. A debrief is a report, not a SIG ACT, Place, event, collection or anything else.



d. Step 4 – Enter your title in the title block IAW your Squadron standard. Then enter the time frame for the patrol in the start and end date blocks. This will allow the use of time to evaluate any patterns our friendly forces may be setting for the enemy. In addition, standardized titles will help us find this data later.

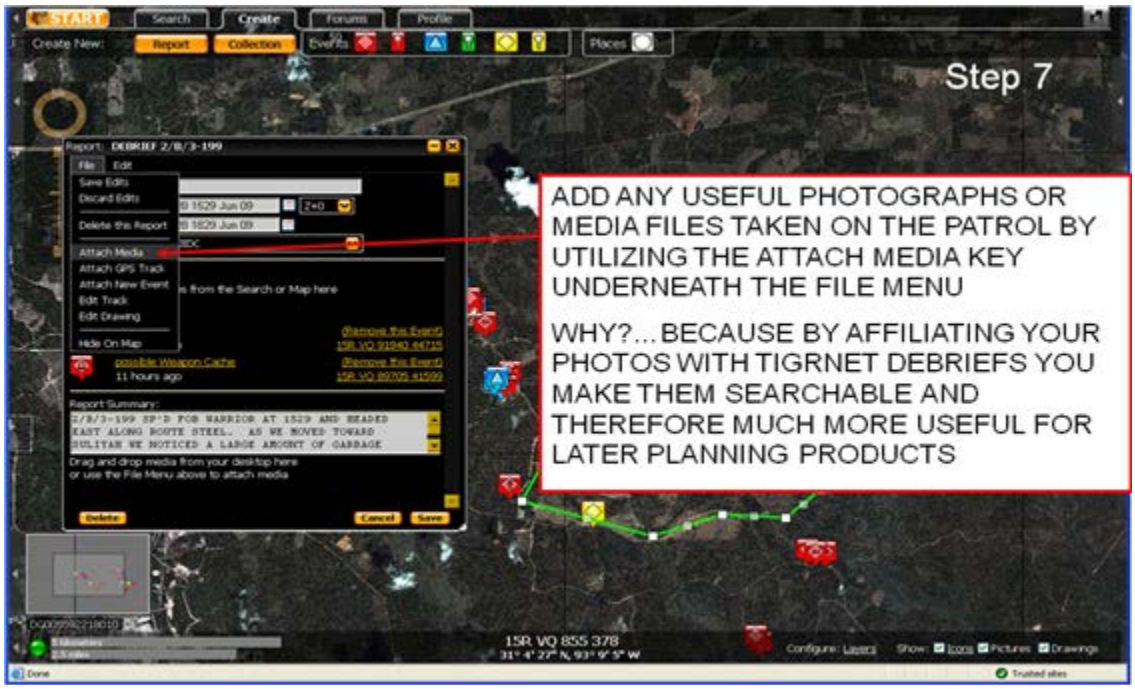


e. Step 5 – Enter your patrol narrative in the block title “Report Summary”. This is the searchable block on TIGRnet and any info that may ever be relevant should be entered here. Maximize use of specificity (especially when using proper names and locations). Use correct grammar and sentence structure (not bullet comments).



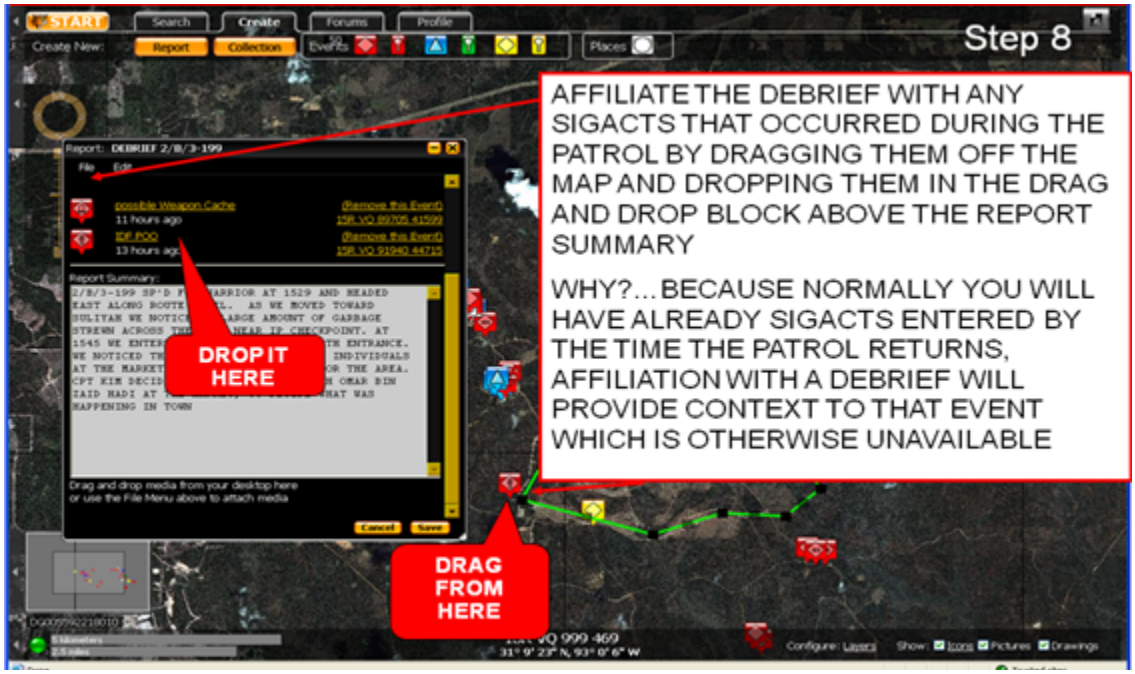
f. Step 6 – Add an “Honesty Trace” – This is a line following the route of your patrol by selecting the “Draw Track” feature underneath the file menu. This will allow the debrief to be directly associated with a specific geographic area (searchable).

g. Step 7 – Add any useful photographs or media files taken on the patrol by utilizing the attach media key in the file menu. This will affiliate your photo with TIGRnet debriefs (searchable) and much more useful for later planning products.



h. Step 8 – Affiliate the debrief with any SIGACTSs that occurred during the patrol by dragging them off the map and dropping them in the drag and drop block above the report

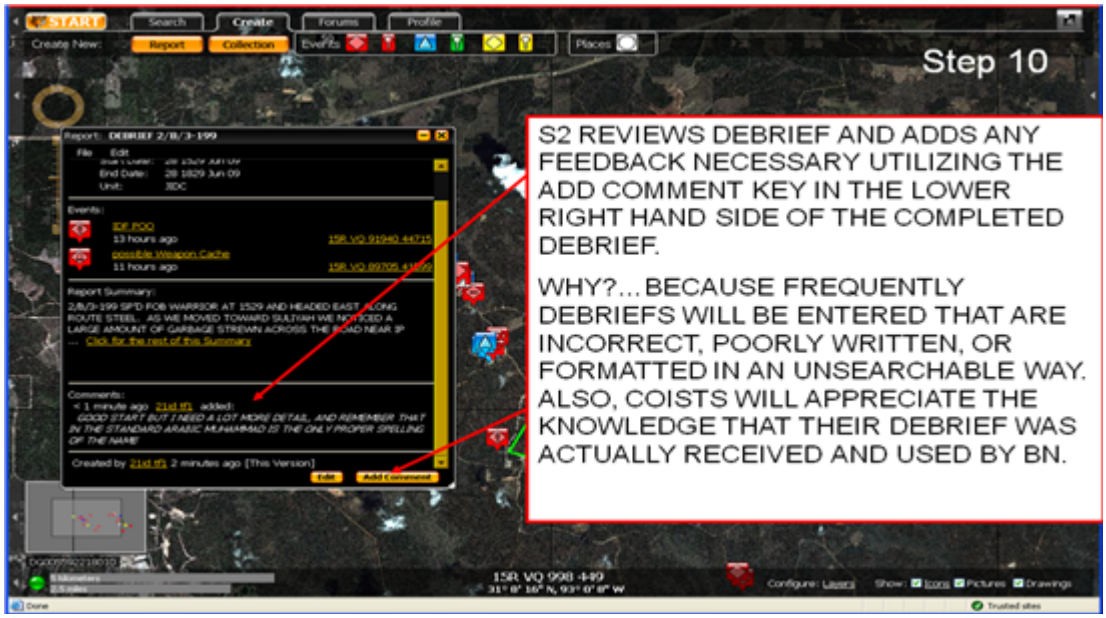
summary. Normally the SIGACT will already be entered before the patrol returns. Affiliating a debrief will provide context to that event which is otherwise unavailable.



i. Step 9 – Save your debrief by hitting the "Save" key in the lower right hand side of the report box. Failing to save the debrief will result in having to complete the process from the beginning.

j. Step 10 – S2 reviews the debrief and adds any feedback necessary by utilizing the "Add Comment" key in the lower-right side of the completed debrief. Frequently debriefs will be entered that are incorrect, poorly written, or formatted in an unsearchable way. In addition,

CoIST will appreciate the knowledge that the debrief was actually received and used by the Squadron.



k. If all steps were completed properly you will have a debrief that is:

(1) Searchable by words and entities through the narrative in the report block.

(2) Searchable through geography by the attached honesty trace.

(3) Useful for the S3 or commander because he can visualize where his patrols are conducting operations.

(4) Useful for planners as they can catalog photos and media files for later use.

(5) Useful for the S2 allowing visibility regarding how friendly forces might be affecting the enemy and impacting pattern analysis.

(6) A product that allows the best possible way to push the information from the Troop level up for facilitating later analysis.

Handheld Interagency Identity Detection Equipment (HIIDE)

Enroll/Collecting

Login: hiide

Password: hiide

Use the Stylus pen to touch the white box for the keypad

Choose COLLECT

Choose dropdown option

Hold HIIDE about 14-16 inches from eye.

Touch Main Bar, Aim crosshairs, slowly moving the HIIDE in and out, to raise focus bars. Press, holding for a few seconds, one of the HIIDE shoulder triggers. Unsuccessful capture allows another attempt.

Successful capture moves to next capture screen.

Place appropriate fingertip on fingerprint sensor.

Touch Main Bar, Wait for focus bars to fill.

Press HIIDE shoulder button, or Accept button, to complete the capture.

Unsuccessful capture will allow another attempt.

Successful capture moves to next capture screen.

Hold HIIDE about an arms length from the subjects face.

Aim crosshairs at face and wait for focus bars to fill.

Press HIIDE shoulder trigger, to complete the capture.

Unsuccessful capture will allow another attempt.

Successful capture moves to the Enroll Profile screen.

Touching the text fields open the keyboard touch screen.

The appropriate data is entered with the keyboard.

The Done button returns to the Enroll Profile screen and populates the text field with the typed in data.

Note: height and weight must be 3 digits example 5'6" tall =506

14 mandatory fields must be filled out.

When done hit "Save"

Identify

Choose COLLECT

Choose dropdown option

Start enrollment

During enrollment HIIDE identifies while Collecting/enrolling.

If no match is found

If match is found, dossier will show. If shows red person is on alert. Read alert text.

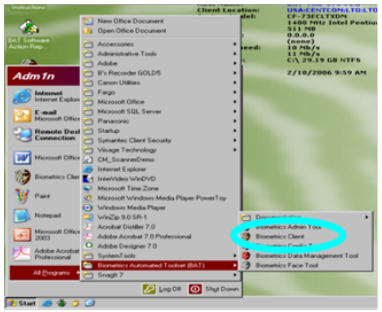
Responsibilities of HIIDE User

HIIDE user must enroll to the best of his ability.

HIIDE user must charge HIIDE when not using.

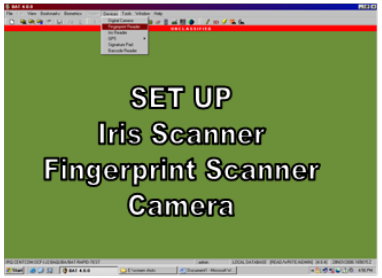
HIIDE user must bring HIIDE to BAT system daily.

Biometric Automated Toolset (BAT) Version SP-6

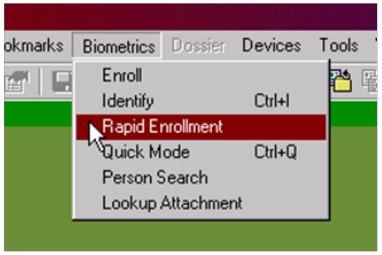


Login: Biouser
Password: pa$$word123456

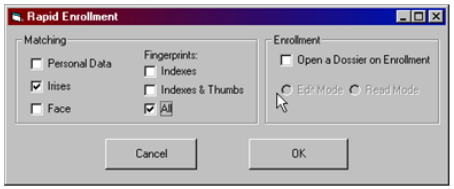
Click Biometrics client
Then choose appropriate sever or "local server" if not hooked up to network.
(No Password Required)



Click Device and install the specific Model of equipment from the menu's.
Note: The Camera Must be on and set to: **Auto-Green -on top**
Play-Blue -on back



Choose rapid Enrollment
or **Identify** if applicable pending mission
Note: Rapid Enrollment allows the user to continue enrolling before the comparisons are Complete SP-5 feature not available for earlier versions

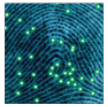


Choose comparison methods against other dossiers already loaded in the system

Click Appropriate boxes to input data
Iris
Fingerprints
Photo
Name and other Data

For Iris hold the F-2 button on the Iris Scanner until two Bars light up then release and hold for three seconds
Note: No glasses may be worn.

For Photo, ensure you have full face shot and snap must be done with the computer not the camera



Take appropriate fingerprints as necessary

Once done hit "Submit ID"
If found a match it will display possible matches
If no match found it will ask for more Data entries where the yellow fields are required to complete enrollment

Example of the status Bar, you can continue to enroll other individuals while comparing previous enrollments to database
To Complete, click the Dossier, and click Enroll

For researching or querying dossiers look in the "File" menu and choose the Open Find option then select search criteria- i.e.. Last name, entity etc…

BATS has An excellent help guide with step by step instructions In the help TAB. When In doubt use it.

HIIDE UPLOADING AND DOWNLOADING INSTRUCTIONS WHEN CONNECTED TO BAT

*** An IP is preset into the HIIDE, no changing is to be done to the network settings in the HIIDE**
*** From BAT you download from HIIDE's and from BAT you upload to HIIDE's.**
*** HIIDE user's should bring HIIDE's to BAT to download and upload daily.**
- **The HIIDE operator's job is to bring the HIIDE to the BAT, and the BAT operator's job is to download and upload to the HIIDE.**
- **CHARGE HIIDE DAILY IF NOT USING WITH AC/DC BATTERY CHARGER.**

Downloading from HIIDE to BAT:
- Connect HIIDE to crossover LAN cable from back of BAT laptop.
- Log on to the WINDOWS XP login :biouser / pa$$word12345678 (pa$$word1234- CF-73) .
- Double click on the Biometrics client icon and log in: biouser / pa$$word123456 (pa$$word1234-CF-73)
- Turn on HIIDE device, wait for it to come up and look like the picture below - **DO NOT LOG-IN**
- In the BATS client application Select File, Synchronize device, HIIDE, Download
- If asked, Select Securimetrics Hiide 4.0 from drop down menu and hit OK
- If not there type in user name: hiide & password is : hiide & IP is : 10.0.0.11
- Hit Connect Button
- Device Status should turn green and inform you that HIIDE is active, hit OK
- Select download
- Hit YES if you want to automatically enroll (suggested), NO to manually enroll
- ID Queue will appear, when done click exit
- If you choose NO, click OPEN if you want to enroll each dossier

Uploading from BATS TO HIIDES:
- Connect HIIDE to crossover LAN cable from back of laptop
- Log on to the BATS System
- Bring up the Biometrics client application and log in
- Turn on HIIDE device, wait for it to come up, same as picture above - **DO NOT LOG-IN** .In the BATS client application Select File, Synchronize device, HIIDE, Upload
- If asked, Select Securimetrics Hiide 4.0 from drop down menu and hit OK
- User name: hiide & password is: hiide & IP: 10.0.0.11
- Hit Connect Button
- Device Status should turn green and inform you that HIIDE is active, hit OK
- Select next, next, next.
- Click the Add From Server button
- Select per-last name from drop down - type in an * in the enter search criteria and hit Filter
- Select individual records using the (>) to upload or hit double arrows (>>) to move all records to box on right of screen
- Hit Upload
- Hit OK when it pops up to inform you it's done
- Hit Exit

TAB F: STANDARD DEBRIEFING FORM

1. Standard Debriefing Form (w/o walkthrough).

Unit (Sqd/Plt/Co):	Patrol Leader:
Date of Mission:	Debrief Number (S2 Only):
Depart Time:	Return Time:
Mission:	
☐ Dismounted Patrol in TOWN OF:	GRID:
☐ Mounted Patrol in TOWNS OF:	
GRIDS:	
☐ Fixed guard/checkpoint at:	
☐ Respond to:	
☐ Other:	
☐ Attitude of General Population Towards CF/ISF (Select One): **Favorable / Neutral / Unfavorable**	

Describe key locations visited during patrol (town, ethnic minority neighborhood, school, market, religious bldgs., etc.)

LOCATION	GRID	OBSERVATIONS, TRENDS (e.g. BETTER OR WORSE?)	DIGITAL PHOTO #

PERSONNEL ENCOUNTERED

List important/interesting persons encountered. Describe what they said/did that was significant in the **PATROL NARRATIVE.**

NAME (LAST/First)	SEX	ETHNICITY	HOMETOWN	TAG # (if detained)	DESCRIPTION (or digital photo #)

VEHICLE ENCOUNTERED

List passengers in **PERSONNEL ENCOUNTERED** (above). Discuss significant vehicles in the **PATROL NARRATIVE.**

SSENGERS (LAST/First)	COLOR	MAKE	MODEL	LIC NO.	LOCATION	DIGITAL PHOT

CAPTURED EQUIPMENT

Explain circumstances leading to capture of equipment in the **PATROL NARRATIVE.**

QUANTITY	ITEM DESCRIPTION	TAG NUMBER	SERIAL NUMBER	DIGITAL PHOTO #

Page 1

PIRs/IRs ANSWERED
Provide information pertaining to Priority Information Requirements (PIRs) or Information Requirements (IRs). List PIR or IR #.
PIR/IR # ANSWERED

PATROL NARRATIVE	
Describe the important events of patrol. Include 5 W's (**who**, **what**, **when**, **where**, and **why**). Provide **Digital Photo** #.	
	What to report when you don't know what to report:
	● Local population's reactions/ attitudes
	● Upcoming events
	● Conditions of schools/clinics
	● Status of electric power
	● Condition of crops/harvest
	● Map corrections
	● New construction/material
	● New military weapons/ vehicles/tactics/capabilities
	minefields/IEDs
	● Billboards/poster/leaflets
	● New damage or vandalism
	● What's new and on sale in shops
	● Black market activity
	● Upcoming market days
	● Number of houses in town
	● Stretches of bad road
	● Buses and who is in them
	● New antennas or wires
	● NGO presence/stickers
	● Possible gang/criminal activity
	● Local address system (street names and numbers)

ATTACHMENTS
List attachments or enclosures to this debrief. Example: sketch, disk with digital photos, captured documents, political rally poster, confiscated weapon, etc. Ensure that any attached item is described in the **PATROL NARRATIVE** above.

2. Standard Debriefing Form (w/ walkthrough).

Page 1

PIRs/IRs ANSWERED

Provide information pertaining to Priority Information Requirements (PIRs) or Information Requirements (IRs). List PIR or IR #.

PIR/IR # ANSWERED

PATROL NARRATIVE

Describe the important events of patrol. Include 5 W's (**who**, **what**, **when**, **where**, and **why**). Provide **Digital Photo #**.

	What to report when you don't know what to report:
	● Local population's reactions/ attitudes
	● Upcoming events
	● Conditions of schools/clinics
	● Status of electric power
	● Condition of crops/harvest
	● Map corrections
	● New construction/material
	● New military weapons/ vehicles/tactics/capabilities
	minefields/IEDs
	● Billboards/poster/leaflets
	● New damage or vandalism
	● What's new and on sale in shops
	● Black market activity
	● Upcoming market days
	● Number of houses in town
	● Stretches of bad road
	● Buses and who is in them
	● New antennas or wires
	● NGO presence/stickers
	● Possible gang/criminal activity
	● Local address system (street names and numbers)

ATTACHMENTS

List attachments or enclosures to this debrief. Example: sketch, disk with digital photos, captured documents, political rally poster, confiscated weapon, etc. Ensure that any attached item is described in the **PATROL NARRATIVE** above.

LIST ALL ATTACHMENTS IN THIS BLOCK. ENSURE THEY ARE ALL ATTACHED BEFORE TURNING THEM IN TO THE COMPANY.

Page 2

TAB G: CoIST INTELLIGENCE SUMMARY

<table>
<tr><th colspan="2">X CO FUSION UPDATE</th></tr>
<tr><td rowspan="2">CO SIGACTS AND PATROL REPORTING
ANSWERING SIR
(EXTRACTS FROM TIGR FORUM)</td><td>CO HPTL</td></tr>
<tr><td rowspan="2">CURRENT CO SITTEMP</td></tr>
<tr><td>PIR/SIR TASKED (RED)
AND ANSWERED (GREEN)</td><td>CO BOLO LIST (HIGHLIGHT CHANGES)</td></tr>
</table>

TAB H: SBCT INFORMANT PERSONAL INFORMATION SHEET FORMAT

**** "INFORMANT" DOES NOT MEAN "SOURCE". CoIST'S ARE PROHIBITED FROM CONDUCTING SOURCE OPERATIONS. CoIST'S WILL ASSIST IN ENSURING THAT TROOPs DO NOT CONDUCT UNAUTHORIZED SOURCE OPERATIONS.**

Type of Contact: _____ (walk-in, patrol, casual, community, liaison)

Contact Log Identifier: _____

This sheet is used to record the biographic and other details of individuals met during passive HUMINT collection operations. These include walk-ins, patrol collection, casual, community & liaison contacts. Not source operations.

Biographic Details

A. What is the contacts' full name?
   First Name:
   Middle Name:
   Last Name:
   Tribal/clan Name:
   Nickname:

B. What is the contacts' date of birth? (YYYYMMDD)

C. What is the contacts' place of birth? (neighborhood, city)

D. Where does the contact live now? (address, neighborhood, city)

Placement/Access

E. Where did the contact obtain the information he/she provided?

F. When did you obtain this information?

Motivation

G. Why did the contact come forward to give information?

H. Has the contact provided information to Coalition Forces in the past? (other than this unit) Yes/No (If yes, to whom and what was the information.)

I. Is the contact currently providing information to other members of Coalition Forces? (other than this unit) *(IF YES, STOP AND CONTACT THT FOR FURTHER GUIDANCE):*

J. Is the contact willing to pass information to others within the coalition?

K. What are the contact's feelings about the Coalition Forces operating within his nation?

Security

L. Who else knows the information being reported?

M. Who else knows the contact is talking with us?

Contact Details
N. Is the contact able to contact/meet with us again? (where/when)

Meeting History (refers to previous screening sheets & contact logs)
O. When has the contact been met? (from first meeting onwards: include Date, Time, Location, Collector Details – including linguist):

Information Provided (refer to previous screening sheets & contact logs)
P. What information has the contact provided? (include date, general details and SPOT or other report numbers if written):

Inspection by Brigade S2/Review by THT
Q. When was this sheet inspected by the Brigade S2X staff or reviewed by a HCT member? (include Date, HCT member details, action taken):

Sheet Compiled/Information Updated
R. Who compiled this sheet and updated the details? (include Date, member details):

Physical Description
S. What is the contact's physical description? ("A to I" acronym)

- A: Age/Sex (estimate within 5 years, eg 25-30 years old male)
- B: Build (include estimate of weight within 10 pounds, eg 150-160lbs)
- C: Complexion (Ethnic Group/Skin Complexion)
- D: Dress (from head to feet: headwear, shirt, pants, shoes, plus accessories)
- E: Elevation (Height) (estimate within 2 inches)
- F: Face (include eye color, facial hair)
- G: Gait
- H: Hair (color, length, style)
- I: Interesting (Distinguishing) Features (jewelry, language, scars, marks, tattoos)

Attach photo (if available)

Handover/Termination
T. When was the contact handed over to a HCT, or terminated as a source of information?

**** NOTE: Forward completed document to Squadron S2.**

TAB I:SBCT INFORMANT CONTACT LOG FORMAT

Sheet #:_____

Date	Time	Type	Location	Contact's Name	Residence	Unit Member Met	Notes

Type of contact: W = walk-in; P = patrol; CS = casual (irregular); CO = community (regular); L = liaison (official)

TAB J: INTELLIGENCE BATTLE RHYTHM (Tentative)

1. The intelligence battle rhythm is designed around the Raider BDE's battle rhythm. The INTEL battle rhythm will be adjusted as required. Below is a template of the INTEL battle rhythm.

Troop/Squadron

0800 – Shift change slides information cutoff (S2)
0830 – Shift change slides due to BN Battle CPT
0830 – CoIST/S2 Net Call via Breeze
0900 – Squadron Shift Change
1000 – squadron BUA/Staff Sync Meeting (S2)
1300 – Squadron ISR Sync Meeting (S2, CoIST)
1700 – Squadron Collection Planning session (S2, CoIST)
1800 – Troop Collection plan due to BN (CoIST)
1900 – CoIST INTSUM information cutoff (CoIST)
2000 – CoIST INTSUM due to BN
2000 – Shift change slides information cutoff (S2)
2030 – Shift change slides due to BN Battle CPT
2030 – Squadron INTSUM posted
2100 – Squadron Shift Change

BDE/SCIF

0800 – Squadron shift change slides information cutoff
0800 – SCIF shift change slides information cutoff (SCIF NCIOC, Ops, Fusion, S2X, CM&D, SIGINT)
0900 – Squadron shift change slides due to BDE
0930 – BDE shift change
0930 – BDE shift change slides due to SCIF
1000 – SCIF shift change
1030 – S2 Conference Call via Breeze
1100 – BCT BUA/Staff SYNC Meeting (S2)
1400 – BDE ISR Sync Meeting (S2, ISR, TGT, MICO)
1530 – BCT Daily Targeting Meeting (S2, ISR, TGT)
1830 – Squadron Collection Plan/ Asset Status update to BCT (ISR)
1830 – SCIF Huddle (SCIF NCIOC, Fusion, S2X, CM&D, SIGINT)
1900 – BN INTSUM information cutoff
2000 – BN shift change slides information cutoff
2000 – SCIF shift change slides information cutoff (SCIF NCIOC, Ops, Fusion, S2X, CM&D, SIGINT)
2030 – Squadron INTSUM due to BDE (S2)
2100 – Squadron shift change slides due to BDE
2130 – BDE shift change
2130 – BDE INTSUM posted
2130 – BDE shift change slides due to SCIF
2200 – SCIF shift change

TAB K: ISR REQUEST FORM

Request for Collection

POC Contact Info	Organization		
	Name		
	Secure Phone		
	SIPR Email		
Imagery Sensor requested (EO/IR/RADAR/MSI, FMV)			
Date of Request			
Collection start/stop date			
NIIRS Required			
Target Information	MGRS Coords	BE Number (if available)	Tgt Name/Description
Justification (Who, What, When, Where, Why)			
Essential Elements of Information (EEI)			
Intel Report that cued collection (if available)			
Reporting instructions (IPIR, etc.)			
Notes or Comments			

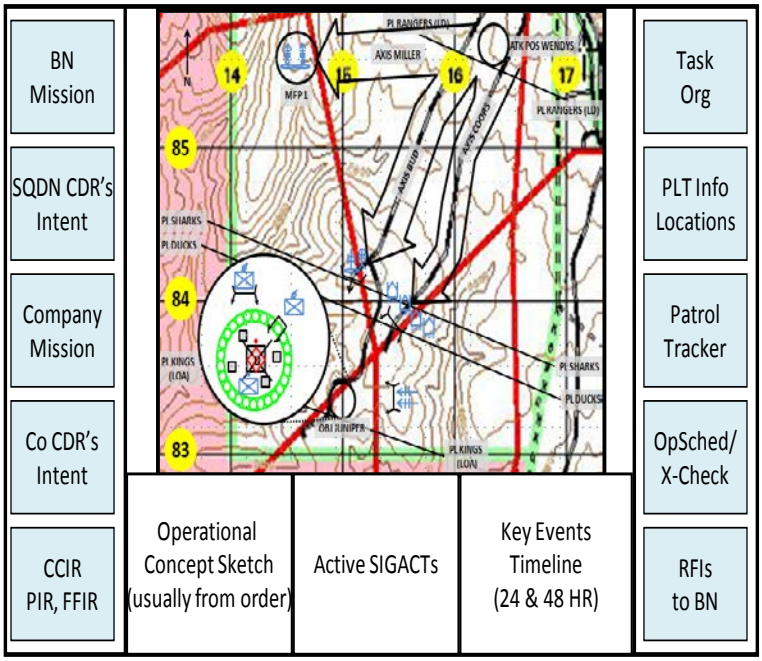
Troop CP SOP

Chapter 1	**CP Functions**
	General
	CP Functions and Battle Rhythm
	Daily CP Checklist
Chapter 2	**Duties and Responsibilities of CP/COIST Personnel**
	Company Executive Officer
	Fire Support Officer
	Company Intelligence Officer or NCO
	Company Operations Sergeant
	RTO (Day)
	RTO (Night)
	Supply Sergeant
	CBRN NCO
Chapter 3	**CP Information Flow**
Chapter 4	**CUB Agenda**
Chapter 5	**CP Setup and Layout**
Chapter 6	**CP Displacement**
Chapter 7	**Planning or TLP SOP**
Chapter 8	**Digital SOP (include COP Icon)**
Chapter 9	**Company CP Battle Drills**
Chapter 10	**Shift Change**
	Annexes
Annex A	**SIR**
Annex B	**Targeting Format**
Annex C	**DA 1594**
Annex D	**9-Line MEDEVAC Request**
Annex E	**Counter-fire Checklist**
Annex F	**SPOT Report**
Annex G	**CP Rules**

3

A Way to Display your Map

Time Zone



TTPs:
- **Wing board**
- **Cork Board**
- **TSC green fold out**
- **Plexiglas**
- **On a Table**

Overlays (analog or digital):

• **Operations and Fire Support** (include units that are close or you may contact). Map must big enough to show all of your units and areas you will or may be directed to go ***with enough space to post icons!***

• **Route Status**.

• **Enemy Situation Template**. "drill down" to known and proposed squad-sized enemy forces and crew served weapons. (You may include enemy contacts)

• **Obstacles**. Natural and man-made

Tracking Charts/Leader Board Reference

Squadron Mission

Blackhawk 6's Intent

PIR

As of_____

1. Where will the eny reserve attack?
Decision: Commit reserve to…

FFIR

1. Loss of two Strykers in a PLT
Decision: Adjust task org by…

Locations

CMD POST	LOCATION	JUMP	TRIGGER
BN TOC			
CO CP			
CTCP			
UMCP			

CDR		XO	
XO			
ISG			

1st PLT	LOCATION	NET	2nd PLT	LOCATION	NET
3rd PLT	LOCATION	NET	4th PLT	LOCATION	NET
SIGN:			COUNTER:		

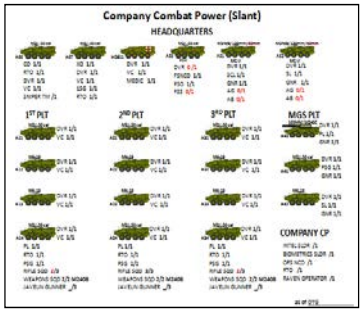
TRP Mission Statement

TRP Commander's Intent

EEFI

As of_____

1. Communication Cards with FREQ…
Decision: Change freq, load, etc.



ROE/Tactical Guidance

PERSTAT

As of_____

Troop Commander Update to Commander

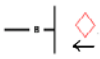
- **Blackhawk Big 8**
- **PERSTAT with key or significant changes**
- **Combat Power Slant (#FMC/#On Hand)…talk new NMCs or NMCs with issues**
- **Significant activities (last 24 hours)**
- **Squadron CCIR answered (last 24 hours)**
- **Total of enemy contact and BDA with engagement summary**
- **Enemy situation assessment and projected enemy action in CO AO**
- **Changes to Task Organization (task and purpose)**
- Raven missions, Fires updates, etc. (if used)
- **Upcoming (48 hours) missions plan with troop to task**
- Status on Current or Proposed CMO projects and cost in AO
- **Logistical status (if not green across CL I, III, V)**
- Changes to Communication Plan or Critical shortfalls
- Changes to CASEVAC
- **Issues or Concerns**

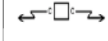
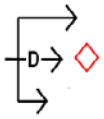
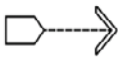
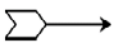
BLACKHAWK BIG 8 SCORING STANDARDS					
	BLACK(1)	RED (2)	AMBER (3)	GREEN (4+5)	
1. OPORD	No orders issued	Failure to issue or develop any paragraph or failure to restate essential tasks or task and purpose	Maximizes available time through the use of WARNOs and FRAGOs; a five paragraph Order that has been developed through analysis of the higher order; clearly restates the essential tasks (task and purpose); addresses accomplishment of each specified task from the higher HQ order; assigns a task and purpose to each subordinate element, and is based on IPB	Analyses of implied tasks and addresses further development of branches and sequels to the base plan.
A. DIRECT FIRE PLAN	No plan	Did not attain one or more areas under criterion for (AMBER)	Leaders apply factors of METT-T. IPB/OCOKA, and the Fire Control Process to determine direct fire control and execution to support task/purpose; ID scheme of maneuver and adequate control measures to focus, shift, mass, and distribute the combined effects of weapon systems	Leaders specific methods to control fires; fire control plan is rehearsed; integration of indirect fires into fire control plan; plans for limited visibility and degraded capabilities.
B. INDIRECT FIRE PLAN	No Plan	Plan not in accordance with commander's guidance; supporting targeting documents missing.	Plan follows commander's guidance; Adequate plan in place; Fire support overlay present, but targets sheets not attached.	Soldiers and leaders know fire support frequencies, are certified in CFF procedures, & know names & grids for all targets; Max range of indirect support plotted on map; FSO has approved and is tracking all all preplots; All overlays and targets sheets in place.
D. ADJACENT UNIT COORDINATION	No Coordination Done.	Adjacent unit notified of patrol's presence.	Adjacent units are notified of patrol's route, composition, and time expected to be conducted.	Coordination verified by patrol leader; All leaders and vehicles have callsigns and freqs for adjacent units and their QRFs; Drivers know fastest route to all adjacent medical centers.
E. MEDEVAC PLAN	No plan	Medevac plan in place, but not briefed to subordinates.	Patrol briefed on medevac freqs; Also notified of location of closest LVL II medical centers.	All Soldiers and leaders know fastest route to LVL II care facility as well as air medevac freqs; Patrol route has been screened and possible medevac LZs identified and preplotted; All Soldiers are carrying 9-line Medevac cards; All patrol medical equipment has been inspected prior to SP; CLS-qualified personnel and equipment evenly distributed.
F. INFIL PLAN	No plan	Plan in place, but not briefed to subordinates.	Route briefed, but not screened; Time/distance calculations estimated by patrol leader.	Primary, secondary and alternate routes understood by all drivers and leaders. All routes screened for SIGACTs & possible vehicle hazard areas (bridges/canals). Times & distances between all CPs understood by drivers &leaders. VCs understand navigation highlights of all routes.
G. EXFIL PLAN	No plan	Plan in place, but not briefed to subordinates.	Route briefed, but not screened; Time/distance calculations estimated by patrol leader.	Primary, secondary and alternate routes (all different from infil routes) understood by all drivers and leaders. All routes screened for SIGACTs & possible vehicle hazard areas (bridges/canals). Times & distances between all CPs understood by drivers & leaders. VCs understand navigation highlights of all routes.
2. GRAPHICS	Not done	No refinement of graphics; no dissemination or briefing of SITEMP; and/or graphics not issued to all subordinate elements or attached/OPCON elements.	Support task and purpose, scheme of fires, scheme of maneuver, throughout the AO's depth; disseminated to all vehicle commanders; infantry squad leaders, and attached/OPCON elements.	Graphics support branch plans and sequels; issues refined SITEMP; issues a refined DST, disseminates a copy of consolidated graphics; issues CSS graphics.
3. PCC/PCI	Not conducted	Did not attain one or more areas under the criterion for(RED); did not attempt to correct deficient areas	Conduct prep-to-fire checks; weapons test fires; load plans inspected and made safe; camouflage applied; perform before-ops PMCS; complies with UNIT commanders prescribed det from WO/OPORD/SOP; CONDUCTS A COMMD CHECK ON Command, subordinate, fire support, and CSS nets; uniform and MOPP are IAW OPORD; graphics checked and subordinate unit briefbacks conducted.	Progress of preparations tracked and reported to higher HQ; Commander inspects or has designated inspection team SMEs check prescribed areas; deficiencies re-inspected
A. BORESIGHT	Not done	All combat systems boresighted to a known distance at day and night; verified and reported to higher HQ	Conducted at multiple ranges by weapon type against moving targets	
B. 5988E	Not done or turned in	PMCS, faults verified by mechanics; Not done by all or not conducted to same standard	Administrative and equipment data correct; PMCS conducted, all faults verified by mechanics; all faults annotated all faults have part numbers or job orders. Signed or initialed by operator and mechanic NCO.	All corrected faults annotated, all parts on order have valid status.
C. RESUPPLY	Not identified.	Unit has not met one of the above criteria for a (AMBER); insufficient material to accomplish the mission; unaware of CL III/V/VII status	Unit crosses LD or defends with "Green" UBL status on CLIII/V/VII; completes and verifies at least 90% of combat systems 5988s, and maintains a status of NMC vehicles	Available assets to conduct resupply of III/IV/VII enroute or at consolidation; issues infantry demolitions (breach kits) and hand grenades; and planned for normal and NBC casualty evacuation; CSS plan and maneuver plan integrated and briefed, rehearsed, and on graphics
4. REHEARSALS	Not conducted	Did not meet one or more of the criteria for a (AMBER)	Reinforces higher and lower's task and purpose, scheme of maneuver, fires, and support; integrates actions of subordinate elements throughout operation; identified MPCOA, MDCOA, composition, deposition, and strength; depicts graphics, terrain, enemy, and friendly forces during rehearsal; uses appropriate type and technique given available time and resources	Discusses higher intent, scheme of maneuver, fires and CSS; branch plans and contingencies without wargaming; addresses the 7 forms of contact; incorporates attached/OPCON units into rehearsal; subordinate elements conduct generic, mission oriented battle drill rehearsals prior to; conducts separate CSS and/or fire support rehearsals; crews conduct rollover and water drills.
5. SECURITY	No plan	Security drops below required levels, unaware of compromise	Designates a security plan; maintains security throughout planning and preparation phases; has passive NBC defense established (M22 detectors/M9 paper); conducts active/passive security patrols; and enforces REDCON levels	Designates air guards; conducts adjacent unit coordination for security plans and patrols routes; designates a QRF in case of imminent attack, and/or executes a jump plan to a new location if compromised by enemy ground or air reconnaissance.
6. R&S	No R&S conducted	No specified R&S tasks and/or coverage of the higher HQ specified NAIs	Commander has assigned NAIs to answer PIRs; the specified NAIs from the higher HQ R&S plan have been assigned and are covered	Uses NAIs for DST and Direct Fire Planning; tasks the NAIs in the AO/AI; and continues to refine SITEMP; has made requests for UAS, AH-64, or satellite imagery for most recent views of all NAIs.
7. TIME MANAGEMENT	Subordinates given less than ½ of available time from the end of the OPORD and backbriefs No Warning Order issued.	Subordinates given less than 2/3 of available time from end of OPORD and back-briefs. Warning Order issued but not complete or timely	Subordinates given 2/3 of available time from end of OPORD and backbriefs. WARNO issued in a timely manner. Companies and platoons conduct generic rehearsals. PCC/PCI, and logistic resupply based on WARNO.	Subordinates given 4/5 of available time from end of OPORD and back-briefs. Warning Order issued that allows detailed parallel planning in subordinate units. The commander/staff assessing useful time such as amount of daylight and for 5; sequencing tasks arrayed against the available time to maximize the preparation
8. RISK MANAGEMENT	No risk assessment conducted	Risk identified but no reduction by control measures	Uses an effective SOP or conducts formal risk assessment to ID & assess hazards, develop control measures, deconflicts control measures, implement control measures, and supervise	Continues to refine or regularly update risk level by FM or voice; tracks risk level in company CP; ID types of risk – Tactical and Accidental; and conducts and internal evaluation risk review after mission execution

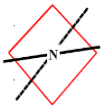
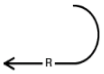
BOLO List						
Type of Vehicle (Sedan, Truck, 4-door, etc.)	**Color**	**Make and Model**	**License Number**	**Driver and Passengers in Vehicle**	**Date and Grid/Route vehicle was last seen**	**Activity; Reason vehicle is wanted**

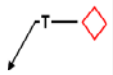
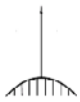
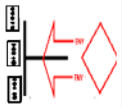
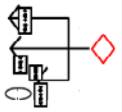
GRAPHICS

Tactical Misison Tasks

Tactical Task	Military Symbol	Definition
ATTACK BY FIRE		A tactical mission task in which a commander uses direct fire, supported by indirect fires, to engage an enemy without closing with him in order to destroy, suppress, fix or deceive him. See also combat attack; support by fire. (FM 3-90, p. B-3; FM 1-02, p. 1-16) (Graphic: FM 1-02, p. 7-32)
BLOCK (ENEMY FORCE)		A tactical mission task that denies the enemy access to an area or prevents his advance in a direction or along an avenue of approach. (FM 3-90, p. D-13; FM 1-02, p. 1-23) (Graphic: FM 1-02, p. 7-49, p. A-2)
BREACH		(Army): A tactical mission task in which the unit employs all available means to breakthrough or secure a passage through an enemy defense, obstacle, minefield, or fortification. (FM 3-90) (Marine Corps) The employment of any means available to breat through or secure a passage through an obstacle. (FM 1-02, p. 1-24) (Graphic: FM 1-02, p. A-...
BYPASS		A tactical mission task in which the commander directs his unit to maneuver around an obstacle, avoiding combat with an enemy force. (FM 1-02, p. 1-26; FM 3-90). (Graphic: FM 1-02, p. A-2)
CANALIZE		(DOD) To restrict operations to a narrow zone by use of existing or reinforcing obstacles or by fire or bombing. (Army) A tactical mission task in which the commander restricts enemy movement to a narrow zone by exploiting terrain coupled with the use of obstacles, fires, or friendly maneuver. See also obstacle. (FM 1-02, p. 1-27; FM 3-90) (Graphic: FM 1-02, p. A-2)
CLEAR		(Army) 1. A tactical mission task that requires the commander to remove all enemy forces and eliminate organized resistance in an assigned area. (FM 3-90) 2. To eliminate transmissions on a tactical radio net in order to allow a higher-precedence transmission to occur. (FM 11-32) 3. The total elimination or neutralization of an obstacle that is usually performed by follow-on engineers and is not done under fire. (FM 3-34.2) See also reduce. (FM 1-02, p. 1-32) (Graphic: FM 1-02, p. A-2)
CONTAIN		(JP 1-02) A tactical mission task that requires the commander to stop, hold, or surround enemy forces or to cause them to center their activity on a given front and prevent them from withdrawing any part of their forces for use elsewhere. (FM 3-90, p. Glossary-8) (Graphic: FM 1-02, p. A-2)
CONTROL	No Symbol Available	A tactical mission task that requires the commander to maintain physical influence over a specified area to prevent its use by an enemy (FM 3-90, FM 1-02, p. 1-44)
COUNTERATTACK		(JP 1-02) Attack by all or part of a defending force against an enemy attacking force for such specific purposes as regaining lost ground, or cutting off or destroying enemy advance units, and with the general objective of denying to the enemy the attainment of his purpose in attacking. In sustained defensive operations, it is undertaken to restore the battle position and is directed at limited objectives. (FM1-02, p. 1-46) (Army) – A form of attack by part or all of a defending force against an enemy attacking force, with the general objective of denying the enemy his goal in attacking. (FM 3-90, p. Glossary-8; FM 3-0) (Graphic: FM 1-02, p. A-3)

COVER		(JP 1-02) –(DOD, NATO) 1. The action by land, air, or sea forces to protect by offense, defense, or threat of either or both. [Joint definitions 2-5 non applicable] (Army) 1. Protection from the effects of fires. (FM 6-0) 2. A form of security operation whose primary task is to protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of, and direct fire against, the main body. Unlike a screening or guard force, the covering force is a self-contained force capable of operating independently of the main body. See also covering force. (FM 1-02, p. 1-49; FM 3-90) (Graphic: FM 1-02, p. A-6)
DEFEAT	No Symbol Available	A tactical mission task that occurs when an enemy force has temporarily or permanently lost the physical means or the will to fight. The defeated force's commander is unwilling or unable to pursue his adopted course of action, thereby yielding to the friendly commander's will, and can no longer interfere to a significant degree with the actions of friendly forces. Defeat can result from the use of force or the threat of its use. See also decisive point. (FM 1-02, p. 1-54; FM 3-90)
DELAY		A form of retrograde in which a force under pressure trades space for time by slowing the enemy's momentum and inflicting maximum damage on the enemy without, in principle, becoming decisively engaged. (FM 3-90) (See page A-3 for symbol.)
DESTROY		1. A tactical mission task that physically renders an enemy force combat ineffective until it is reconstituted. 2. To damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt. (FM 1-02, p. 1-59; FM 3-90) (Graphic: FM 1-02, p. A-3)
DISRUPT (ENEMY FORCE)		1. A tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt his timetable, or cause his forces to commit prematurely or attack in piecemeal fashion. (FM 3-90) 2. In information operations, breaking and interrupting the flow of information between selected command and control nodes. (FM 3-13) (FM 1-02, p. 1-63) (Graphic: FM 1-02, p. A-3)
FIX (ENEMY FORCE)		A tactical mission task where a commander prevents the enemy from moving any part of his force from a specific location for a specific period of time. (FM 3-90) (FM 1-02, p. 1-81) (Graphic: FM 1-02, p. A-3)
FOLLOW AND ASSUME		A tactical mission task in which a second committed force follows a force conducting an offensive operation and is prepared to continue the mission if the lead force is fixed, attrited, or unable to continue. See also attack; offensive operations. (FM 3-90; FM 1-02, p. 1-82) (Graphic: FM 1-02, p. A-4)
FOLLOW AND SUPPORT		A tactical mission task in which a committed force follows and supports a lead force conducting an offensive operation. See also direct pressure force; encircling force; exploitation; pursuit. (FM 1-02, p. 1-82) (FM 3-90) (Graphic: FM 1-02, p. A-4)

GUARD		(DOD, NATO) 1. A form of security operation [Note: the NATO definition replaces "security operation" with "security element"] whose primary task is to protect the main force by fighting to gain time while also observing and reporting information [Note: the
INTERDICT		A tactical mission task where the commander prevents, disrupts, or delays the enemy's use of an area or route. (FM 3-90; FM 1-02, p. 1-103) (Graphic: FM 1-02, p. A-4)
ISOLATE		A tactical mission task that requires a unit to seal off—both physically and psychologically—an enemy from his sources of support, deny an enemy freedom of movement, and prevent an enemy unit from having contact with other enemy forces. See also encirclem
NEUTRALIZE		(DOD) 1. As applies to military operations, to render ineffective or unusable. 2. To render enemy personnel or material incapable of interfering with a particular operation. See FM 3-90. 3. To render safe mines, bombs, missiles, and booby traps. See FM 5-25
OCCUPY		A tactical mission task that involves a force moving into an area so that it can control the entire area. Both the force's movement to and occupation of the area occur without enemy opposition. (FM 3-90; FM 1-02, p. 1-136) (Graphic: FM 1-02, p. A-4)
PASSAGE OF LINES (FORWARD)		(Army) A tactical enabling operation in which one unit moves through another unit's positions with the intent of moving into enemy contact. (FM 3-90; FM 1-02, p. 1-142) (Graphic: FM 1-02, p. A-4)
PASSAGE OF LINES (REARWARD)		(Army) A tactical enabling operation in which one unit moves through another unit's positions with the intent of moving out of enemy contact. (FM 3-90; FM 1-02, p. 1-142) (Graphic: FM 1-02, p. A-4)
PENETRATE		(DOD, NATO) In land operations, a form of offensive which seeks to break through the enemy's defense and disrupt the defensive system. (Army) A form of maneuver in which an attacking force seeks to rupture enemy defenses on a narrow front to disrupt the d
REDUCE	No Symbol Available	A tactical mission task that involves the destruction of an encircled or bypassed enemy force. (FM 3-90, FM 1-02, p. 1-159)
RELIEF IN PLACE		(DOD, NATO) An operation in which, by direction of higher authority, all or part of a unit is replaced in an area by the incoming unit. The responsibilities of the replaced elements for the mission and the assigned zone of operations are transferred to the incoming unit. The incoming unit continues the operation as ordered. Also called RIP. (FM 3-90, FM 1-02, p. 1-160) (Graphic: FM 1-02, p. A-5)
RETAIN		(DOD) 1. When used in the context of deliberate planning, the directed command will keep the referenced operation plan, operation plan in concept format, and any associated joint operation planning system of Joint Operation Planning and Execution System automated data processing files in an inactive library status. The plan and its associated files will not be maintained unless directed by follow-on guidance. 2. A tactical task to occupy and hold a terrain feature to ensure that it is free of enemy occupation or use. (Army) A tactical mission task in which the commander ensures that a terrain feature already controlled by a friendly force remains free of enemy occupation or use. (FM 3-90, FM 1-02, p. 1-163) (Graphic: FM 1-02, p. A-5)
RETIREMENT		(DOD, NATO) An operation in which a force out of contact moves away from the enemy. [Note: the Army classifies retirement as "a form of retrograde."] (FM 3-0, FM 1-02, p. 1-163). (Graphic: FM 1-02, p. A-5)
SCREEN		(DOD, NATO) 4. A security element whose primary task is to observe, identify, and report information, and which only fights in self-protection. See FM 3-90. 5. (DOD only) A task to maintain surveillance; provide early warning to the main body, or impede, destroy, and harass enemy reconnaissance within its capability without becoming decisively engaged (Army) A form of security operation that primarily provides early warning to the protected force. (FM 3-90) See also concealment; flank guard; guard; security operations. (FM1-02, p. 1-167) (Graphic: FM 1-02, p. A-5)
SECURE		(DOD, NATO) In an operational context, to gain possession of a position or terrain feature with or without force, and to make such disposition as will prevent, as far as possible, its destruction or loss by enemy action. See FM 3-90. (Army) 1. A tactical mission task that involves preventing a unit, facility, or geographical location from being damaged or destroyed as a result of enemy action. (FM 3-90) 2. One of the five breaching fundamentals. Those actions which eliminate the enemy's ability to interfere with the reduction and passage of combat power through a lane. Secure may be accomplished by maneuver or by fires. (FM 3-34.2) See also assault; breach; denial measure; reduce; suppress. (FM 1-02, p. 1-167) (Graphic: FM 1-02, p. A-5)
SEIZE		(DOD) To employ combat forces to occupy physically and control a designated area. (Army) A tactical mission task that involves taking possession of a designated area using overwhelming force. (FM 3-90) (Marine Corps) To clear a designated area and obtain control of it. See also contain. (FM1-02, p. 1-168) (Graphic: FM 1-02, p. A-6)
SUPPORT BY FIRE		A tactical mission task in which a maneuver force moves to a position where it can engage the enemy by direct fire in support of another maneuvering force. See also attack by fire; overwatch. (FM 3-90, FM 1-02, p. 1-179) (Graphic: FM 1-02, p. 7-32)

SUPPRESS		1. A tactical mission task that results in the temporary degradation of the performance of a force or weapon system below the level needed to accomplish the mission (FM 3-90, FM 1-02, p. 1-179). 2. One of the five breaching fundamentals. The focus of all fires on enemy personnel, weapons, equipment to prevent effective fires on friendly forces. The purpose of suppression is to protect forces reducing and maneuvering through the obstacle and to soften the initial foothold. (FM 3-34.2) (Graphic: FM 1-02, p. A-6)
TURN (ENEMY FORCE)		A tactical mission task that involves forcing an enemy force from one avenue of approach or movement corridor to another. (FM 3-90, FM 1-02, p. 1-192) (Graphic: 1-02 p. 7-49 and p. A-6)
WITHDRAW		Listed for both types of withdraw: (JP 1-02) – A planned operation in which a force in contact disengages from an enemy force. [The Army considers it a form of retrograde.] (Army) – A type of retrograde where a force in contact plans to disengage from the enemy and move in a direction away from the enemy. (FM 3-90, p. G-27, FM 1-02, p. 1-199) (Graphic: FM 1-02, p. A-6)
WITHDRAW UNDER PRESSURE		A type of retrograde where a force in contact plans to disengage from the enemy and move in a direction away from the enemy while under pressure from the enemy. (FM 3-90, p. 11-16) (Graphic: FM 1-02, p. A-6)
AMBUSH		(Army) A form of attack by fire or other destructive means from concealed positions on a moving or temporarily halted enemy. (Marine Corps) A surprise attack by fire from concealed positions on a moving or temporarily halted enemy. (FM 1-02, FM 3-0) (Graphic: FM 1-02, p. 7-33)
BLOCK (OBSTACLE EFFECT)		An obstacle effect that integrates fire planning and obstacle effort to stop an attacker along a specific avenue of approach or to prevent him from passing through an engagement area. (FM 3-90, p. D-13; FM 1-02, p. 1-23) (Graphic: FM 1-02, p. 7-49, p. A-2)
DISRUPT (OBSTACLE EFFECT)		An engineer obstacle effect that focuses fire planning and obstacle effort to cause the enemy to break up his formation and tempo, interrupt his timetable, commit breaching assets prematurely, and attack in a piecemeal effort. (FM 90-7) (FM 1-02, p. 1-63) (Graphic: FM 1-02, p. A-3)
FIX (OBSTACLE EFFECT)		An engineer obstacle effect that focuses fire planning and obstacle effort to slow an attacker's movement within a specified area, normally an engagement area. (FM 3-90) (FM 1-02, p. 1-81) (Graphic: FM 1-02, p. A-3)
TURN (OBSTACLE EFFECT)		A tactical obstacle effect that integrates fire planning and obstacle effort to drive an enemy formation from one avenue of approach to an adjacent avenue of approach or into an engagement area. (FM 3-90) (Graphic: 1-02 p. 7-49 and p. A-6)

Stryker Mission

"Close with the enemy by means of fire and maneuver to defeat or capture him or to repel his assault by fire, close combat, and counterattack."

7-Step EA Development

1. Identify likely enemy avenues of approach
2. Identify the enemy scheme of maneuver
3. Determine where to kill the enemy
4. Emplace weapon systems
5. Plan and integrate obstacles
6. Plan and integrate indirect fires
7. Conduct an EA rehearsal

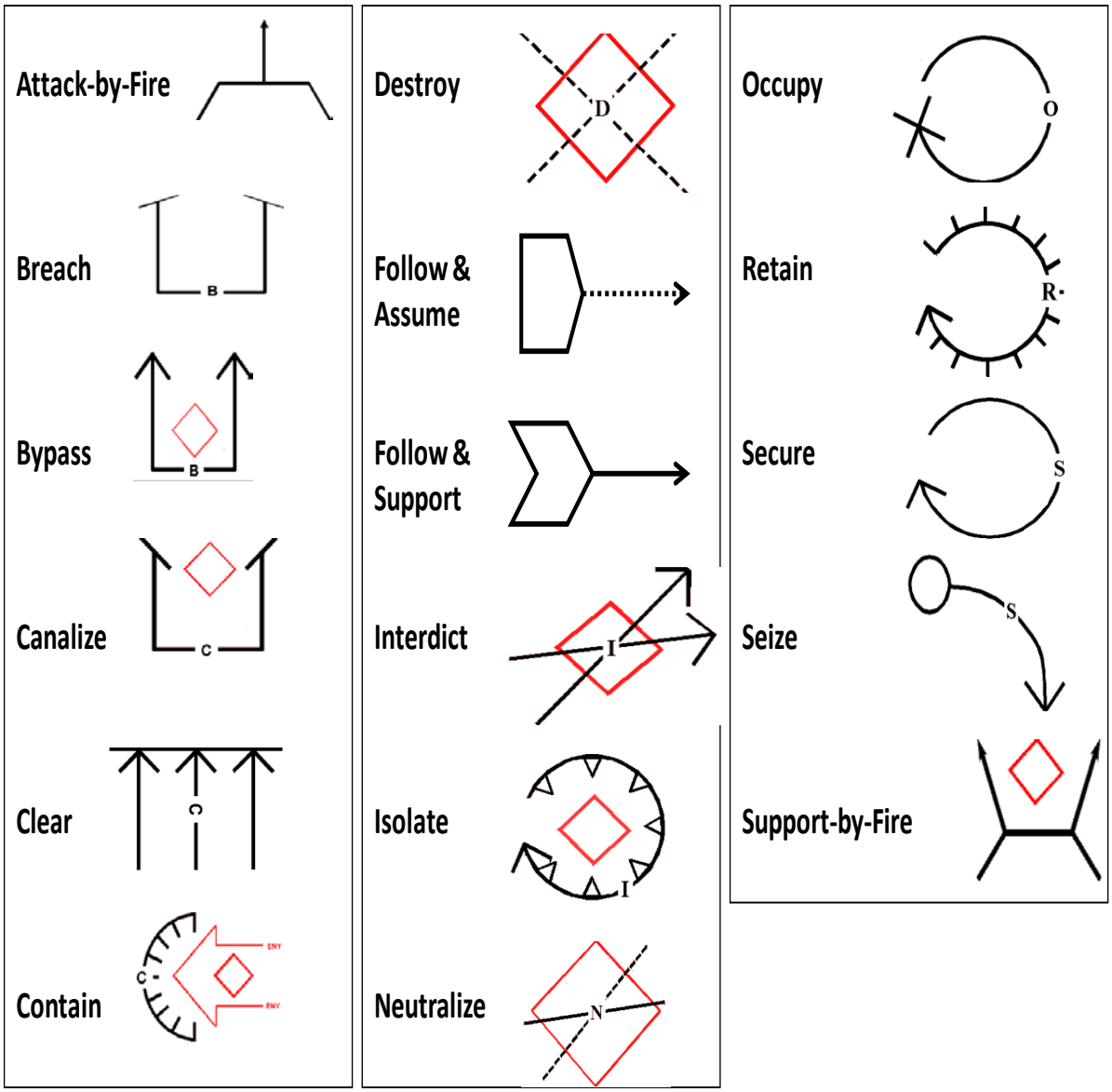
Troop Leading Procedures

1. Receive the Mission
2. Issue the WARNO
3. Make a Tentative Plan
4. Start Necessary Movement
5. Reconnoiter
6. Complete the Plan
7. Issue the Complete Order
8. Supervise

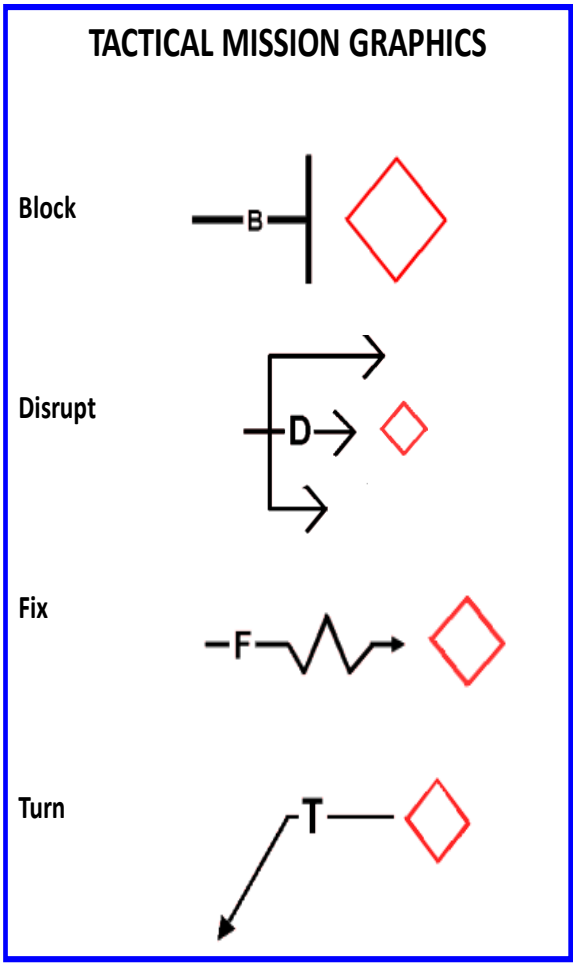
"Big 10" PCI Checks

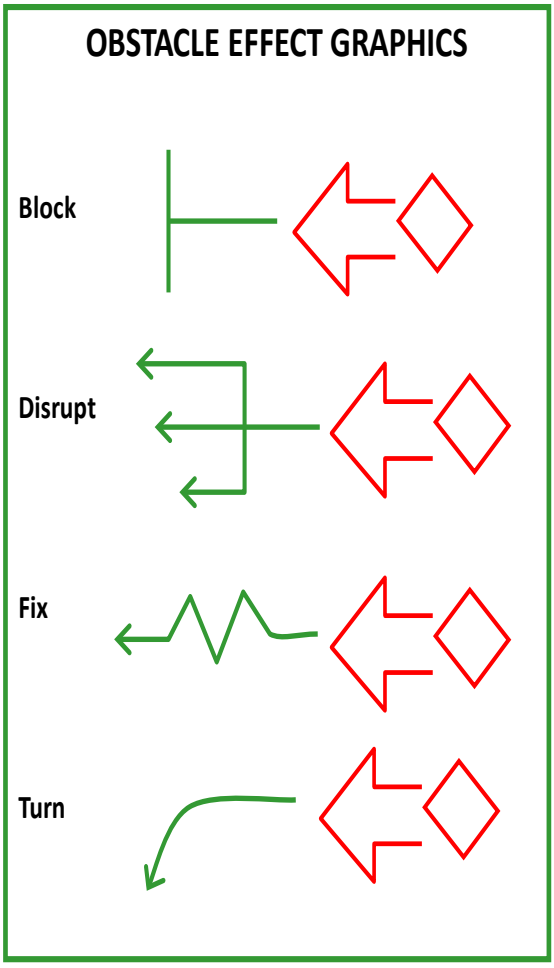
1. Weapons zero
2. PCC/PCI with leader focus area
3. CL III, V, Maintenance, Medics
4. Rehearsals & MSN specific Battle Drills
5. 5 Para OPORD (1/3, 2/3 daylight rule)
6. Timeline (time management)
7. Graphics completed (FM 1-02)
8. Composite Risk Management
9. CP comms check
10. ROE and EOF review

Tactical Mission Graphics



Tactical Mission Graphics





MISSION STATEMENT

WHO

WHAT-Essential Task

WHEN

WHERE

(IOT)

WHY

O/O

ACTIONS BY FRIENDLY FORCE		EFFECTS ON ENEMY FORCE
Assault*	Follow and Assume	Block
Attack-by-Fire	Follow and Support	Canalize
Breach	Linkup*	Contain
Bypass	Occupy	Defeat
Clear	Reconstitutioin**	Destroy
Combat Search and Rescue	Reduce	Disrupt
Consolidation & Reorganization*	Retain	Fix
Control	Secure	Interdict
Counterreconnaissaince	Seize	Isolate
Disengagement	Support-by-Fire	Neutralize
Exfiltrate	Suppress	Penetrate
		Turn

TYPES AND FORMS OF OPERATIONS	
MOVEMENT TO CONTACT*	RETROGRADE OPERATIONS*
Search and Attack*	Delay*
ATTACK*	Withdrawal*
Ambush*	Retirement
Demonstration*	RECONNAISSANCE OPERATIONS**
Feint*	SECURITY OPERATIONS*
Raid*	INFORMATION OPERATIONS**
Spoiling Attack*	COMBINED ARMS BREACH OPERATIONS**
EXPLOITATION*	PASSAGE OF LINES*
PURSUIT*	RELIEF IN PLACE*
FORMS OF OFFENSIVE MANEUVER*	RIVER CROSSING OPERATIONS**
Envelopment*	TROOP MOVEMENT*
Frontal Attack*	Administrative Movement*
Infiltration*	Approach March*
Penetration*	Road March*
Turning Movement*	
AREA DEFENSE*	*Defined elsewhere in this manual
MOBILE DEFENSE**	**Defined in other manuals

Figure B-1. Tactical Mission Tasks

MARVIN GIPSON
CPT, MI
Squadron S-2

CHARLES T. LOMBARDO
LTC, AR
Commanding