Troop Intelligence Support Team Standard Operating Procedures

JAN 2013

4th Squadron, 2nd Cavalry Regiment

SABER 6 PREFACE

1. **Intent:** The purpose of this Standard Operating Procedure (SOP) is to provide the foundation for my expectations of Troop Intelligence Support Teams (TISTs). I expect TISTs to be trained and confident in their ability to facilitate the execution of intelligence driven combat operations. Significant requirements will be placed on TISTs to develop intelligence to facilitate the Find, Fix, Finish, Exploitation, and Analysis (F3EA) targeting cycle, then disseminate intelligence to focus operations. During the intelligence cycle, TISTs will support the Squadron through the collection, analysis, processing and multi-directional dissemination of actionable intelligence.

2. **Staffing**: TIST assignments will be made thoughtfully with a minimum of one year of retainability for initial assignment. The individuals who execute TIST tasks should be critical thinkers with cognitive skills to quickly identify changes in the operational environment and act accordingly. They should have combat experience and have the cognative skills to be capable analysts. Commanders must have the upmost trust and confidence in their TIST.

3. **Training**: We will develop the most capable TISTs through realistic combat-focused training. The SQDN S2 is responsible for providing training for TISTs that ensures a baseline of proficiency. Additionally, the SQDN S2 will take TISTs into account when reserving class allocations for MI Foundry training. Commanders will ensure TIST members are afforded the time to participate in applicable training. Commanders will also ensure that TISTs are integrated into training events to the maximum extent possible. Leaders will train TIST critical tasks to include, but are not limited to pre-briefing and debriefing, Tactical Integrated Ground Reporting (TIGR), Biometric Automated Toolset (BAT)/Handheld Interagency Identity Detection Equipment (HIIDE), Combined Information Data Network Exchange (CIDNE), Intelligence Preparation of Battlefield (IPB) steps 1-4, Intelligence Surveillance and Reconnaissance (ISR) management and capabilities, basic analytics, military writing, and tactical questioning.

4. **Reporting**: The facilitation and sharing of intelligence is essential for mission success. I expect shared databases (e.g. TIGR, BATS, etc.) to be updated within two hours upon mission conclusion or Post-Troops in Contact. Additionally, all mission debriefs and subsequent data will be posted using TIGR.

5. Any questions or recommendations for this SOP should be directed to the 4rth Squadron, 2 Cavalry Regiment S2, CPT William Smith, william.b.smith314.mil@mail.mil, or 476-5346.

////Original Signed////
CHRISTOPHER L. BUDIHAS
LTC, IN
Commanding

Table of Contents

Troop Intelligence Support Team Standard Operating Procedures

1. **Expectations**:

Cohesive fully functioning tactical Troop Intelligence Support Teams (TISTs) distributed throughout the SQDN that are capable of providing enhanced battlefield situational awareness for Troop Commanders. They will do this by conducting predictive analysis of significant activities, conducting pattern analysis associated with significant activities (SIGACTs), generating lethal and non-lethal target folders, and properly briefing the commander and their subordinate units.

2. **Mission**:

The mission of the TIST is to replicate the intelligence process usually available only at higher echelons. TISTs will provide for the Troop Commander situational understanding specifically tailored to his area of operations (AO). It will describe the environmental effects on operations and possible enemy courses of action. The TISTs will accomplish these tasks by successfully applying intelligence, surveillance, and reconnaissance (ISR) assets to collect information relevant to the commander's priority information requirements (PIRs) and other information requirements, analyzing the information, disseminating intelligence products, and recommending a course of action to the Commander.

In addition to coordinating the collection effort, the TIST is the *filter and analysis* center for the raw data that comes to the cell from a variety of sources. The TIST gathers input, then filters, organizes and analyzes data in order to develop recommendations. The TIST must maintain the mentality that they are mini-Intelligence Fusion Cell and must be trained and prepared to conduct small scale intelligence spectrum operations at any given time and in any fight.

3. **Introduction**:

In the asymmetrical threat climate of the 21st century, Counter-Insurgency (COIN) Operations are often conducted from a Troop-level FOB (Forward Operating Base) or COP (Troop Outpost). These troop and platoon size units need immediate, on-scene intelligence support to deal with an enemy that can recruit, rest, and resupply amongst the population in a predominately urban environment. They must also respond to an ever-changing operational environment with ceaselessly dynamic political, social, and economic variables. This requires an intense collection and analysis effort at the lowest level.

This approach is not new. Previous combat tours have proven that a TIST can be formed, developed and successfully employed. They can gather information from missions and other local interactions to synthesize actionable intelligence for the Troop Commander and shares with the SQDN and REGT Intelligence Sections. Soldiers and Marines used a version of the TIST in small wars preceding World War II—a fact documented in the 1940 "Small Wars Manual."

Importance of the TIST

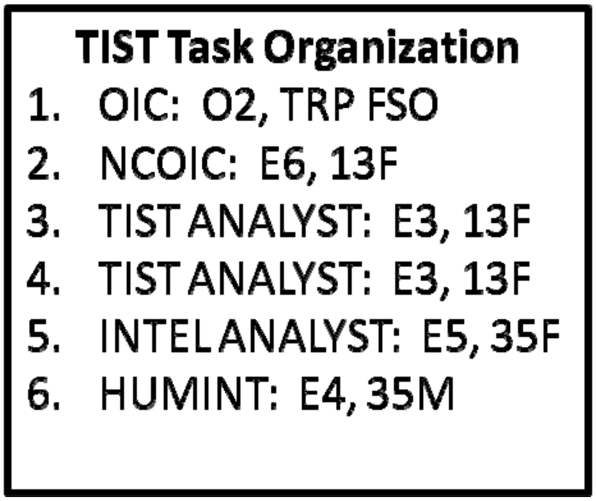
All levels of command will have a sound appreciation for intelligence support. Information flow can often inundate a Troop Command Post (CP). A TIST can reduce some of the information ambiguity and provide the necessary analysis to build situational awareness and enable mission accomplishment. For example, the TIST can reduce a tendency to get drawn into the *react* mode and allow the troop to analyze and predict, thereby retaining the initiative in all Troop operations.

Ultimately, a well-trained TIST can turn raw information into intelligence that helps achieve understanding about all aspects of the operational environment including the enemy situation. This intelligence can also often answer SQDN and REGT commander's critical information requirements (CCIRs), while giving insight into Troop-level CCIRs and PIRs.

4. **Task Organization**:

To best support 24-hour operations, the TIST should ideally consist of six (6) Soldiers, but can operate successfully with as little as four (4). The 4/2 Intelligence Support Teams will consist of 1 x OIC, 1 x NCOIC in the rank of SSG/E-6 or above, a 35F intelligence analyst in the rank of SPC/E4 (provided by SQDN S2 shop) or above, 1 x 35M Human Intelligence Soldier, and 2 x Soldiers provided by the Troop. The TIST is most effective if it works within the SQDN intelligence battle rhythm to complement the SQDN S2's mission of meeting the SQDN Commander's information requirements. The Squadron Commander may choose to task organize 35F personnel from the SQDN S2 shop to help man the TIST.

At a minimum, each Soldier in the TIST will have a secret clearance. Commanders will interview potential members of the team and determine if they are suitable to be a prime candidate to work within the TIST. Soldiers selected to work in the TIST must be submitted for a security clearance through the SQDN S2.



TIST Task Organization

1. OIC: O2, TRP FSO
2. NCOIC: E6, 13F
3. TIST ANALYST: E3, 13F
4. TIST ANALYST: E3, 13F
5. INTEL ANALYST: E5, 35F
6. HUMINT: E4, 35M

5. **TIST Operational Tasks:**

a) TIST will brief outgoing missions 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 Target List (HVTL, if applicable) with pictures if possible, Information Requirements, Possible TQ (Tactical Questioning) guidance, and Information Operations (IO) themes and analysis (WRT second and third order effects). See Annex A for a sample outline of prebrief topics.

b) TIST will debrief incoming missions to develop the Common Operating Picture for the Troop AO. Ensure the Squadron debriefing form is used to gather all pertinent information. See Annex B for a sample debriefing format. If debriefs will be entered into TIGRNET, use Annex B as a guideline for the kind of information to put into TIGRNET.

c) TIST will battle track enemy significant activities to develop enemy patterns and TTP's.

d) TIST will develop Troop-level High Value Target and associated target packets IOT effectively action targets of opportunity.

e) TIST will be prepared to brief the commander on the current situation at all times.

f) TIST will cross talk with adjacent units to develop Area of Interest awareness.

g) TIST will continuously populate all intelligence trackers and databases and maintain situational awareness within the Troop OE.

h) TIST will conduct predictive analysis and maintain a predictive analysis board identifying likely enemy activities both over the next 48 hours and over the next month.

i) TIST will analyze friendly trends from the enemy's perspective and identify unnecessary vulnerabilities and patterns the troop is setting in the course of its operations.

j) TIST will request assistance from the Squadron S2 to conduct specific, detailed analysis beyond the TIST capabilities.

k) TIST will establish clear communications with the Squadron S2 and adjacent Troops and ensure that information flows both up and down the chain of command in a timely manner; the TIST OIC must be proactive and pull information from the Squadron S2 and supporting agencies as required.

l) TIST will ensure all missions have updated intelligence information prior to departure to include updated intelligence from the Squadron S2.

m) TIST will brief attachments and units operating within the troop AO when necessary.

n) TIST will post updated intelligence information for ease of reference by mission leaders; appropriate OPSEC must be observed when choosing a location in which to post.

o) TIST will identify little-known areas within the troop AO that require informal assessments by units to identify key leaders, infrastructure, and basic population information; this information will also become Troop SIR/PIR.

p) TIST will ensure Troop-level Tactical Questioning (TQ) does not inadvertently become unlawful interrogation by adhering to the following guidance along with unit guidance involving actions on the objective and TQ.

i. Troop TQ will involve direct questions only.

ii. 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."

iii. At no time will TQ involve threats directed at the detainee or his/her family.

q) TIST will ensure that all Tactical Informants (TI) are entered into the Informant Contact Log (see Annex D) and have been entered into the Biometric Automated Toolset System (BATS); the TIST will coordinate with the SQDN S2 and HCT individual (HUMINT Collection Team) for review of these products and the assignment of informant tracking numbers.

r) TIST will assist the commander in ensuring that TI are paid CERP and accounted for in accordance with theater policy. CERP is only disbursed to those individuals that provide information that lead to the capture or killing of an HVI and or equipment. TI can receive CERP funds if they provide this information. TI's are <u>not paid for routine information</u>. Commanders are not authorized to pay a TI salary.

s) To facilitate walk-in informants, the TIST will establish an informant meeting and debriefing area and ensure that security personnel are prepared to receive local national informants:

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

ii. 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

iii. Commanders and ISTs are not authorized to task a source. They may request information from local nationals and other willing informants.

t) TQ is the only authorized method for questioning a TI. TISTs will ensure TQ of a TI concerns only routine or impending missions. For example, Troops conduct daily missions along an MSR. The troop can utilize TQ to obtain information regarding the neighborhoods along the route, sentiment towards coalition forces operating in the neighborhood, crime in the neighborhood, IED emplacers and/or emplacement, etc.

u) The following metrics should be used to assess the training level of the TIST:

Task	1	2	3	4	5
Collect	**Does not possess or collect on any PIR**	Possesses initial set of SQDN PIR and SIRs	Develop TRP-level PIR/SIR; Refine SQDN-level ISR plan into TRP-level plan; tasks patrols to collect and answer PIR and SIRs; requests higher-level ISR assets	Refine TRP SIR based on patrol debriefs and integrate higher-level assets/enablers into TRP ISR plan; give bottom-up refinement to SQDN ISR plan covering the TRP OE	Recommend TRP PIR refinements based on answered SIRs at the TRP and SQDN level; TRP ISR plan synched with maneuver plan; ISR plan results in intelligence driven operations
Disseminate	**Does not have KM plan; executes ad-hoc information sharing**	Has a copy of the REGT KM SOP and a plan for intelligence reporting	TISTs participate in intel synch meetings with SQDN S-2 daily; TISTs produce company INTSUM which goes to both SQDN and PLTs; company executing reporting according to the REGT KM SOP; TIST to TIST adjacent unit cross talk	Intelligence sharing with coalition partners; document and media exploitation (DOMEX) passed to SQDN & PLTs; collaborative intel synch meeting between all TISTs and SQDN S-2	IST conducts time sensitive reporting based on actionable intelligence; initial analysis of DOMEX
Conduct Patrol Pre-brief and De-brief	**Does not conduct pre-briefs and debriefs**	Pre-brief conducted; debrief conducted; IAW REGT standardized formats disseminated to all platoons and attachments	Pre-brief conducted using situation map, pattern analysis and previous patrol information; disseminate BOLO list; pre-briefs provide collection requirements (PIR, SIR); de-brief format addresses PIR/SIRs, SIGACTs, key leader engagements (KLE), route analysis and an overall assessment	Debriefs provide answers to collection requirements along with patrol assessment that result in operational or collection refinements; intelligence identified in debriefs communicated to SQDN with analysis	Prebriefs incorporate higher-level analysis and ISR; analysis from de-briefs are fused and incorporated into a company INTSUMs and feed the SQDN AO assessment and future patrol pre-briefs
Analyze	**Does not conduct analysis or maintain any products for use in analysis**	Has situation map to conduct SIGACT analysis; possesses SQDN S-2 products i.e. SITEMP, link analysis, pattern analysis wheel, association matrices	Conducts Trooop-level analysis i.e. IED and POO analysis, time analysis wheel, link diagrams association matrices	Incorporates reporting to include patrol debriefs and higher-level intelligence in order to conduct predictive analysis (i.e. SITEMP); analysis is nested with SQDN S2	Analysis incorporates threat analysis from all levels and "INTs" (SIGINT, HUMINT, IMINT), CF operations and non-lethal analysis (ASCOPE) into a fused product
Intelligence Support to Lethal Targeting	**Has no TRP or SQDN lethal HVTL; no target folders**	Possesses higher's threat HVTL and targeting folders	Creates TRP level HVTL using available intelligence and analysis; HVTL nested with SQDN; TIST integrates into SQDN targeting i.e. TIST recommends SQDN HVTL refinement of existing target folders; uses non-lethal means i.e. PSYOP and CA to neutralize lethal targets (HPTs, IDF POOs, IED EAs)	Develops target folders and conducts CO HVTL refinement as intelligence develops; request and plan (w/SQDN S-2) for targeting enablers such as low-level SIGINT and HCTs; developing target folders	Immediately exploits and analyzes current target leads to follow-on targeting i.e. "Domino Effect"; creates TRP-level target synch matrix includes lethal that results in successful intelligence driven operations; maintaining and sustaining unit specific target folders
Intelligence Support to non-lethal targeting	**Has no TRP or SQDN non-lethal HVTL; no target folders**	Possesses higher's HVTL and Targeting Folders (SOI and projects); COIST aware of reward money and micro-grants	Tracks key SOIs, promises made/kept, use of rewards and micro-grants; provides patrols with higher IO message/talking points and PSYOP products; refines SQDN non-lethal HVTL; establishes and disseminates consequence mngt/IO battle drill	Implements consequence management (mitigates poor actions and exploits successes); recommends projects; proactive recommendation for using reward money and micro-grants; integrates non-lethal enablers (PRT, PSYOP, HTT, HCT)	Creates TRP-level target synch matrix including non-lethal targets that result in successful intelligence driven operations
Intelligence Support to Detainee Operations	**Does not use BAT or HIIDE; has no detainee plan**	Detainees are enrolled into the HIIDE	Biometric data is synchronized with HIIDEs and BATS periodically with higher; gives tactical questioning guidance (card) as part of pre-brief; QA/QC detainee packets prior to transfer to higher; meets time standards for transfer of detainee to higher	Biometric data is synchronized with HIIDEs and BATS daily with higher; tactical question (TQ) guidance is synched with TRP PIR; TQ information included in TRP INTSUM; tracks detainee throughout entire lifecycle of detention	Conducts or expands link analysis diagram and updates target folders based on biometric data and TQ; TQ guidance synched with TRP and SQDN PIR; analysis leads to further precise, personality-based operations
Organization	**Does not field a TIST**	TIST has 2-3 Soldiers as an additional duty	TIST has 4-6 Soldiers (at least 1x NCOIC); TIST is primary duty, all Soldiers have received formal TIST MTT or TIST RSOI training; TIST is physically setup and organized IAW REGT TIST SOP or OPS Group Established Standard	TM has 4-6 Soldiers (with E6 or above as leader); TIST is primary duty; all Soldiers have received formal TIST MTT or TIST RSOI training; TIST is physically setup and organized IAW REGT TIST SOP ; all products comply with REGT TIST SOP formats	TM has 4-6 Soldiers with, 1x 35F, OIC and NCOIC; TIST is primary duty; all Soldiers have received formal TIST MTT or TIST RSOI training; TIST is physically setup and organized IAW REGT TIST SOP or OPS Group Established Standard; all products comply with REGT TIST SOP formats.

6. **Responsibilities**:

The TIST is responsible for assisting the commander with intelligence analysis, reporting and dissemination, detainee operations awareness and tactical site exploitation, and intelligence collection. TIST Leaders are overall responsible for the success of their section through ensuring the proper application and integration of the members. The initial analysis of the operational environment will be provided by the SQDN and/or REGT S2 section. The TIST will refine these products using individual Troop Commander PIR/SIRs as well as knowledge gained from assets performing missions in the troop AOR.

TIST OIC: The Troop Fires Support Officer traditionally fills this position. These Officers will be responsible for providing oversight to the TIST. They will ensure TIST members are tasked appropriately and priorities of work are established. The OIC is responsible for communicating with the SQDN S2 section to ensure all intelligence and collection assets are available to the troop and that they are tasked appropriately and synchronized. The OIC is primarily responsible for the lethal aspect of the IST. The OIC will manage all current and emerging targets and ensure target folders are created to facilitate decisive actioning of a target. The OIC will also recommend to the commander when a target is ready for actioning and the type of assets that are available to support the operation.

TIST NCOIC: Ensures all priorities of work are completed and the analysts have the time and the appropriate area to conduct their work. The NCOIC will provide guidance and support when needed. The NCOIC will recommend options for the commander on all issues related to the non-lethal fight. His duties also include:

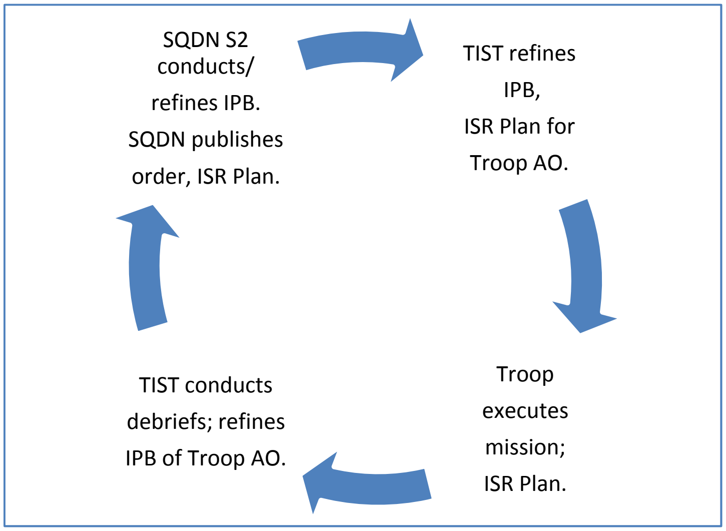
- Providing guidance to subordinate Soldiers.
- Supervising the receipt, analysis, dissemination, and storage of intelligence information.
- Supervising the IPB process.
- Ensuring quality analysis is performed by subordinates.
- Assisting in the preparation of indicators to satisfy priority intelligence requirements.
- Providing current situation briefings to subordinate maneuver elements.
- Receiving, producing and disseminating intelligence reports containing information obtained from all sources.
- Development of the Troop ISR plan
- Supervising intelligence operations within the troop.
- Acting as the primary liaison between TIST and higher echelon S2 sections.

TIST ANALYST: Responsible for reading, interpreting, researching, and analyzing all intelligence collected or generated within the troop battle space. The analyst will usually be the most knowledgeable and most informed member of the TIST because of the work they conduct and the amount of time spent on their tasks. The TIST ANALYST is charged with giving his “best assessment” of the current or upcoming situation. The TIST Analyst must be prepared to perform the following tasks:

- Preparing intelligence products to support the commander.
- Establishing and maintaining systematic, cross-referenced intelligence records and files.
- Receiving and processing incoming reports and messages.
- Assisting in determining significance and reliability of incoming information.
- Assisting in integrating incoming information with current intelligence holdings.
- Preparing and maintaining the situation map.

- Assisting in the analysis and evaluation of intelligence holdings to determine changes in enemy capabilities, vulnerabilities, and probable courses of action.
- Assisting in the preparation of Order of Battle records. Assembling and proofreading reports and assists in consolidating them into military intelligence.
- Assisting in the preparation of reports on captured enemy material.
- Drafting periodic and special intelligence reports, plans, and briefings.
- Briefing and debriefing missions.

7. **Intelligence Preparation of the Battlefield**


SQDN S2 conducts/ refines IPB. SQDN publishes order, ISR Plan.
TIST refines IPB, ISR Plan for Troop AO.
Troop executes mission; ISR Plan.
TIST conducts debriefs; refines IPB of Troop AO.

The TIST is responsible for continuing to refine the Intelligence Preparation of the Battlefield (IPB) provided by the SQDN S2. IPB is a central component of the Squadron's MDMP. The TIST must provide the CDR with his situational understanding of the operational environment. The team must explain to its CDR the effects of the environment and enemy analysis. This SOP only covers the basics of IPB. As such, FM 2-01 Intelligence and FM 2-01.3 Intelligence Preparation of the Battlefield should both be mandatory reading for all TIST members.

IPB consists of four steps: (1) define the operational environment, (2) describe the environmental effects on operations, (3) evaluate the threat, and (4) determine the threat course of actions (COAs). "Operational Environment," or OE, can be defined as the conditions, circumstances, and influences that effect the decisions of the CDR.

Step 1: Define the Operational Environment:

The TIST must identify the specific features of the environment that may influence the commander's decision. The TIST must also identify for the CDR the limits of his battlespace as well as the area of interest relevant to his operations. His battlespace limits are defined by the AO boundaries set by higher headquarters whereas the area of interest consists of both the geographical area his warfighting function can reach out and touch and adjacent/nearby regions that might affect him.

In the conventional fight, the area of interest (AI) was as easily defined as the outer range limit of the CDR's weapons systems. In a counterinsurgency (COIN) fight, the fluidity of local and international boundaries, the ease with which the enemy can blend with the local populace, and the presence of multiple enemy groups eliminate the possibility of having neatly defined boundaries for the area of interest. Because the nature of a COIN fight intrinsically means a limitless area of interest, the TIST can define the area according to a timeline set by the CDR's intended operations. In other words, the TIST can limit his definition of the area of interest only to the geographical space from which the enemy can influence friendly operations within the timeline set by the CDR for his operations. For example, if the CDR intends on executing a mission that he estimates to take two days, the TIST can define the area of interest as the space from which all threat forces/activities and other environment variables can, *within two days*, influence the mission.

Step 2: Describe the Environmental Effects on Operations:

The TIST must explain how the environment affects both friendly and enemy operations. The SQDN S2/TIST does this by conducting terrain analysis, weather analysis, and civil consideration analysis. The doctrinal method to describe the terrain is using the OAKOC mnemonic: Observation and Field of Fire, Avenues of Approach, Key and Decisive Terrain, Obstacles, Cover and Concealment. The doctrinal method to consider civilian effects is using the ASCOPE mnemonic: Area, Structure, Capabilities, Organizations, People, Events.

Step 3: Evaluate the Threat:

The TIST must determine the threat composition and disposition as well as its tactics, training, logistical operations, communications capabilities, intelligence capabilities, recruitment strength, finances, level of partnership with other organizations, local population support, and overall operational effectiveness. The TIST must understand the enemy's "doctrine" which in a conventional fight might be codified within translated enemy training manuals but in a COIN fight might be determined through trend analysis and recognized enemy TTPs. The TIST may wish to depict such TTPs within doctrinal templates, or DOCTEMPs, which are simply graphical depictions of how an enemy might fight in a given situation absent environment considerations.

STEP 4: Determine the threat Course of Action:

The final step is to determine the various threat COAs. A detailed analysis should identify all the enemy COAs that will influence the friendly mission and also identify the areas and activities, called indicators, that when collected will allow the TIST and its CDR to know which COA the enemy has chosen.

An IPB product that TISTs may product during this step is the situation template or SITEMP. This product is the graphical depiction of a possible threat COA as part of a particular threat operation in a given operational environment. While the DOCTEMP is how the enemy would fight given no external influences such as terrain or population considerations, the SITEMP is the graphical representation of doctrine applied to specific battlefield circumstances. The TIST may choose to draw multiple SITEMP overlays to cover all the different possible enemy COAs it has developed. The SITEMP should at a minimum reflect a specific enemy COA and the indicators for that COA and ideally should reflect a complete concept of operations or scheme of maneuver for the enemy operation being depicted.

Determining which COA the enemy will adopt revolves around predicting specific areas and activities that, when observed, will reveal which COA the threat has chosen. The areas should be nominated as Named Area of Interests (NAIs). NAIs then drive the initial ISR plan. Each Co has available to it a plethora of assets from which the TIST can draw data and information. See Section 8 for a sample list of the sources of intelligence available to each TIST. They can also request ISR assets from the SQDN or higher by submitting request forms to the SQDN S2. See Annex C for an example Request for Collection form.

8. **Sources of Intelligence:**

The TIST may draw information from any number of available sources. Listed below are some common sources of information from which to draw data for analysis.

a) **Host Nation Security Forces (HNSF).** HNSF coupled with the Stability Transition Teams (STTs) 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 STTs are American units placed with the HNSF to assist them in transitioning the responsibility of the security to host nation forces.

b) **Mission Debriefs.** Sabers conducting missions within the Troop's AO have the latest and most detailed information on what is happening on the ground. However, many leaders will instinctively report 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 mission leader not knowing exactly what to focus on. Therefore, the TIST should brief participants on what information the TIST requires.

c) **Tactical Site Exploitation**. Units will conduct a systematic search of a secure location which permits the collection of information leading to the development of tactical intelligence. This search provides evidence that can be used in the prosecution and conviction of detainees. The TIST will ensure the information collected from these searches are processed, analyzed, and pushed up to SQDN (See SQDN TSE SOP, TBP).

d) **Guard Posts**. Sabers on post typically observe the same areas around FOBs or key facilities over extended periods of time. These Sabers can—and should—notice patterns and identify variations to them. In addition, those on post are often the first Sabers 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 TIST should train the guard force in observation techniques—and routinely debrief them.

e) **Civil Affairs Teams (CATs)**. As a matter of their regular duty, CATs establish and build relationships with key individuals within the troop and Squadron area of responsibility. While they are identifying the infrastructure or government needs of the local community, CATs also gain insight into the prevailing attitudes and current sympathies of the local populace.

f) **Local Translators**. While Sabers collect information as outside observers, local translators are privy to closer, more focused cultural views of the situation within the community. These individuals will have a different viewpoint, or bias, so information drawn from these human intelligence (HUMINT) sources is important and has to be carefully screened by the TIST.

g) **Convoys**. Sabers or friendly forces conducting convoys through the troop's zone may observe things that organic units do not. These convoys should be debriefed just like any of your own units.

h) **Organizations**. These include anyone stopping or passing through the area of operations. Although these organizations may carefully guard their neutrality, they may become aware of local security information that is important both for them and the FOB. Even though you cannot "debrief" them, casual conversation with them often nets key bits of important information for the Co. For example:

i. **Nongovernmental Organizations (NGOs)**. NGOs are private non-profit organizations with no official ties or relationships to any government. The types of NGOs a TIST will encounter within its OE will often have a humanitarian aid or development and relief focus.

- NGOs work very closely with parts of the local populace.
- NGOs can vary in size from global operations such as Medecins San Frontieres (Doctors without Borders), Human Rights Watch, or Amnesty International or can be as small as many religiously-based NGOs found throughout the United States but have limited aid relief operations around the world.
- NGOs can be global or local. Not all NGOs are based exclusively in the United States.

ii. **Intergovernmental Organizations (IOs).** IOs are international inter-government organizations that are often founded by an international treaty or charter. These organizations may be global or regional in scope.

i) **HUMINT Collection Teams (HCTs)**. These Sabers are trained and skilled in drawing data and developing information from local human sources. With their organic interrogation capability, HCTs are an excellent source of detailed and actionable intelligence. HCTs attached to any Squadron-level unit should regularly de-brief Troop ISTs in whose sector they operate.

j) **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 TIST must seek out this information so that missions can identify enemy emplacement and triggering techniques. This information can aid the Troop in reducing a key friendly force vulnerability by taking the latest intelligence from EOD and disseminating it among its troop maneuver elements.

k) **Medical Units**. The medical platoon can provide insight on the effects of enemy munitions. Combined with information from the scene of any enemy activity, this information can help reconstruct enemy actions, and possibly identify new enemy TTPs or capabilities.

l) **Weapons Intelligence Teams (WIT):** WITs are special units attached to Brigades and Squadrons. The WIT mission is to exploit enemy sites such as raid objectives, cache sites, IED sites, and any other place where enemy weapons are present. They have the capability to lift fingerprints, ID bomb signatures, and conduct extensive sensitive site exploitation.

m) **Provincial Reconstruction Teams (PRT):** PRTs know and understand spheres of influence (SOI) better than anyone on the battlefield. They have contact with the population on a daily basis, often more than HUMINT collectors. The teams work with the police, army, government, and civilian contractors.

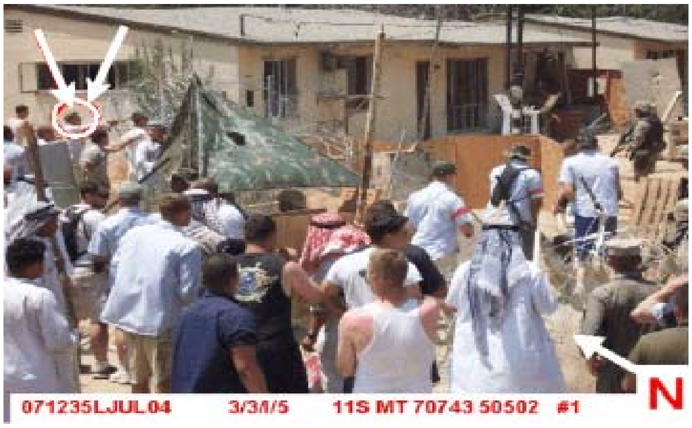
n) **Law Enforcement Professionals (LEPs):** LEPs are former local, state, and federal law enforcement personnel who are currently working with the Army to help stop the extensive criminal networks in Afghanistan. They bring years of real-world experience to the fight and allow the Regiment and Squadron to pursue the enemy from an entirely different angle.

9. **<u>TIST Collection Tools</u>**:

There are several tools available for use by collectors to help build the intelligence picture within the troop's OE. Again, this is not an exhaustive list. The TIST is responsible for devising as many possible ways of collecting information as possible, to include working through the SQDN S2s to coordinate request for collection assets from higher echelons. See Annex C for an example form for Collection Requests.

a) **Digital Cameras**. Digital cameras can be an outstanding surveillance and recording tool for missions. A unit armed with a digital camera can bring back dozens of images to the TIST, providing 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.

This photo comes from the 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 SFC Doe: Picture of Outlaw Troop eastern ECP. The AL JABBURI 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 DHABI.

i. Digital cameras can also provide timely images of new graffiti, posters, and signs for translation/interpretation when on-scene linguists are not with the unit. 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.

ii. 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 SQDN for further exploitation.

iii. To support this mode of collection, the TIST should establish a picture log. This log will have a troop/mission identifier with date, picture number, and location using the military grid reference system (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. Treat photos as sensitive information with strict controls and guidance for their handling.

b) **Video Cameras**. Although it is not often as easy to carry as a digital camera, a video camera can record exactly what happened during significant events witnessed by Sabers. Instead of relying solely upon a verbal debrief, a unit now shows the TIST exactly what happened, and review each event in sequence.

c) **Voice Recorders**. These devices allow troops to record details without having to write legible notes for later reports. It gives them the ability to keep their eyes on the situation at hand. The troopers can also use the recorder to determine if the translators are properly translating.

d) **RAVEN UAS:**

The Raven 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 unit goes, contingent on ROZ and A2C2 approval. The Raven has three different cameras that 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 (infrared) 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 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, exchange a spare battery, and get it back in the air.

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. Its automated features and GPS technology also make it simple to operate, requiring no specialty skilled operators or in-depth flight training.

e) **SHADOW UAV:**

The Shadow UAV is the Brigade Commander's primary Reconnaissance, Surveillance, and 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.

The Shadow is rail-launched via a catapult system, has an automated takeoff/landing system, and has electro-optical (EO), infra-red (IR), and laser range finder (LRF) capabilities.

f) **MQ-8B FIRE SCOUT:**

The Fire Scout is a Vertical Take-Off and Landing Tactical Unmanned Aerial Vehicle (VTUAV) system and is comprised of up to three MQ-8B Fire Scout air vehicles, ground control stations, and associated control handling and support equipment. The VTUAV system will provide a significant improvement to organic surveillance capability. With vehicle endurance greater than eight hours, a VTUAV system will be capable of twelve continuous hours of operations providing coverage 203 kilometers from the launch site. The air vehicle is capable of providing UHF/VHF voice communications relay and has a baseline payload that includes electro-optical/infrared sensors and a laser designator that enables the system to find tactical targets, track and designate targets, accurately provide targeting data to strike platforms and perform battle damage assessment. The Fire Scout has a max alititude of 20,000 ft.

ISR Request Procedures: When the TISTs are requesting ISR assets they need to be aware of the following:

a) The TIST should request a capability and not an asset (i.e. "N/4/2 CR requests full motion video", not "I need a shadow/predator" etc.). The reason for this is if the TIST requests an asset and that particular asset is not available, the requests will likely go unsupported. If they request a capability (such as IR or Full motion video) they have a higher chance of receiving support from other assets that can offer the requested capability.

b) All ISR requests will be sent to the SQDN S2 and then requested from appropriate higher HQ.

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

d) TISTs will utilize the SQDN ISR request form (Annex C).

10. **TIST Intelligence Systems**: These are some of the automated tools that may be available to TISTs.

a) **One System Remote Viewing Terminal (OSRVT):** 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 manned or unmanned aircraft systems. The OSRVT has the ability to capture all manned UAS platforms with FMV regardless of who tasked them. This means that with the OSRVT a TIST can watch footage of any area where a platform is as long as the OSRVT and the asset share a digital link. The range for OSRVT is 10km from UAS with extended range of 50 km with MDAS antennae.

b) **Tactical Ground Reporting System (TIGRNET):** TIGRNET is actually a software application rather than a network — allows soldiers to download information into one program. The information 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 mission, 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.

The TISTs will use TIGRNET as a tool to data mine any information that they need for the entire AO. TISTs will populate their specific information on TIGRNET so that adjacent units in the AO can have visibility of information not dealing with their AO. TISTs should populate TIGRNET immediately, but no later than 2 hours after the SIGACT takes place in order to allow adjacent units and higher units to have timely situational awareness in the AO. **TIGRNET reporting will be conducted IAW SQDN specific reporting instructions. TIGR naming conventions will be standardized and disseminated IAW Annex F. Naming is subject to change based off the REGT SOP to ensure consistency.**

c) **Distributed Common Ground System–Army (DCGS-A):** Allows analysts unprecedented freedom to find data of interest, organize and refine the results, then visualize the results and detect patterns. DCGS-A also allows the analyst to manage data through visualization; DCGS-A automatically loads new data as needed, freeing the analyst from the need to perform additional searches, import extra data, or laboriously build case files. DCGS-A 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 changes directly to the data source. DCGS-A provides a simple yet powerful Multi-Intelligence analysis toolset that is unlike all other intelligence analysis applications. DCGS-A extends core features to provide integrated analysis, data management, and intelligence visualization capabilities.

d) **Document and Media Exploitation (DOMEX):** DOMEX supports 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.

e) **Combined Information Data Network Exchange (CIDNE):** Primary means by which HCT reporting is fused into the theater intelligence database (SQDN 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.

f) **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.

g) **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 BATS for biometrics data exchange back to do biometrics data repository.

h) **Multi-user Internet Relay Chat (MIRC):** MIRC is a system that allows the TISTs to both monitor multiple situations at once and communicate instantly across the battlefield with anyone who is connected. This will be the SQDN primary Observation and Intelligence (O/I) network. The TIST can monitor a number of "chat rooms" depending on their preference. The TIST needs someone to monitor MIRC at all times because of the time sensitive information that moves across it.

11. **TIST Reporting Instructions**:

a) TISTs will populate any significant activity (SIGACT) on the TIGRNET system so that adjacent and higher units can monitor the situation anywhere on the battlefield. See Annex B for a sample debriefing format for an example of the types of information necessary within a TIGRNET mission report.

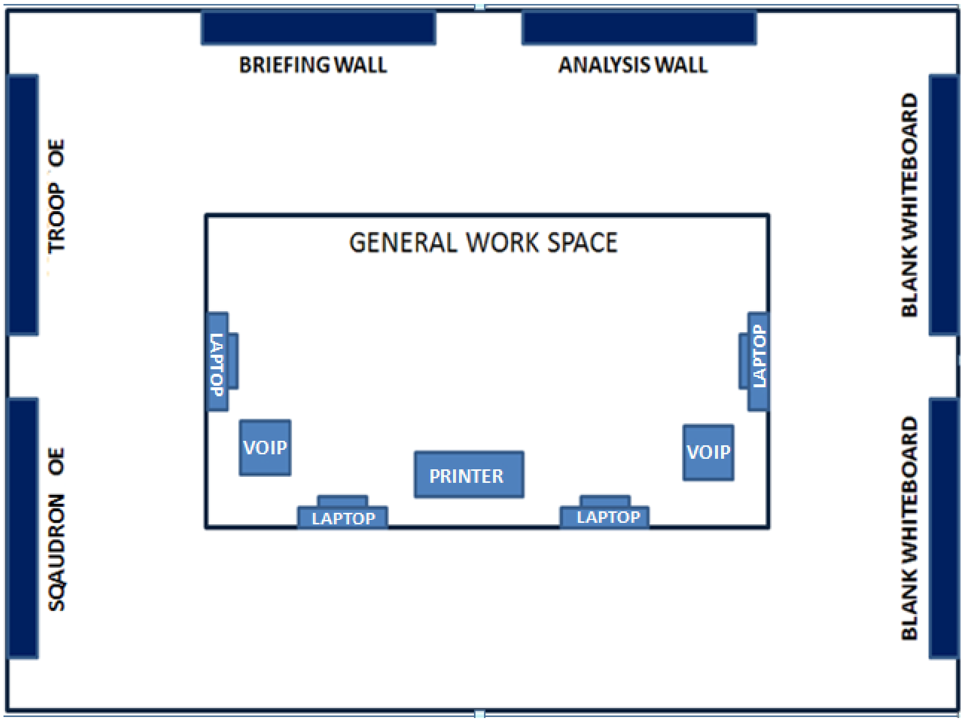
b) If the TIST discovers a time sensitive target (TST) in an adjacent unit's AO, the TIST will notify both SQDN as well as the TIST where the TST is located so they will have a chance to action the target and begin the process of acquiring the appropriate assets.

c) Any information that the TIST believes is of intelligence value will be reported up to SQDN through email, MIRC, or SVOIP. Included with the report are any associated documents and reports to provide the necessary context for the HHQ.

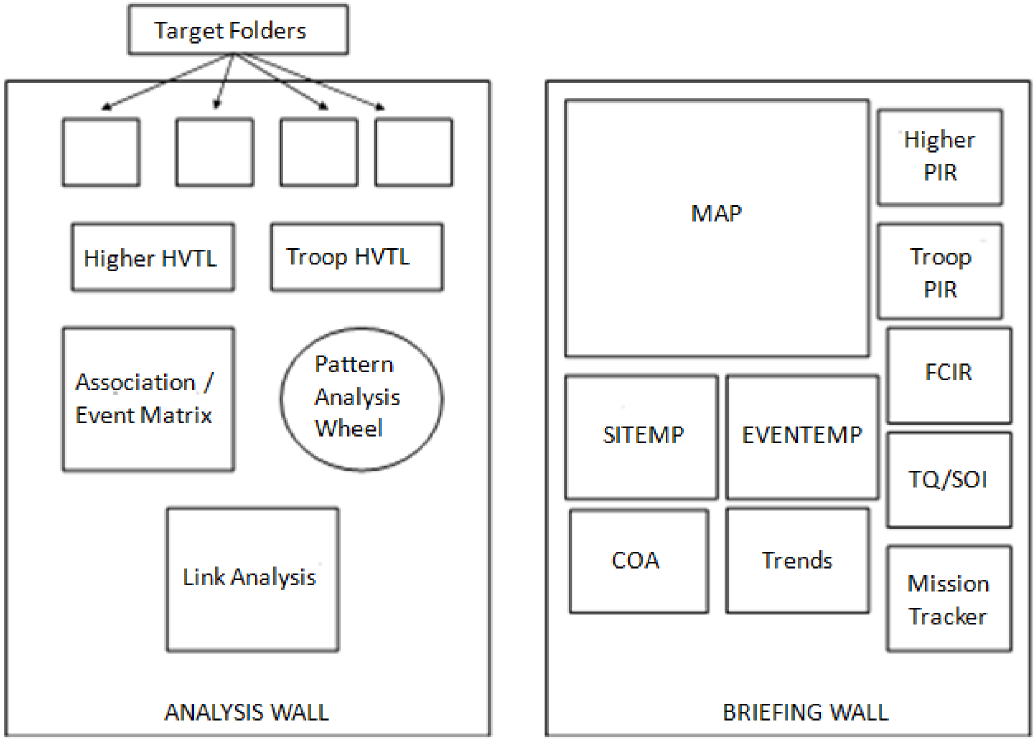
d) TISTs must adhere to their REGT, SQDN, and Troop standard reporting instructions. These are baseline formats. SQDN S2s may adjust these formats to fit the needs of the SQDN CDRs.

e) Sample Reporting Instructions is found in Annex H.

12. **Example TIST Layout**:



a) The TIST 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 TIST to the primary TOC is essential to ensure the TIST has instant situational awareness and can maintain current situational awareness (SA) on troop activities. The TIST needs to also have rapid access to the Troop Commander, 1st Sergeant, and XO.

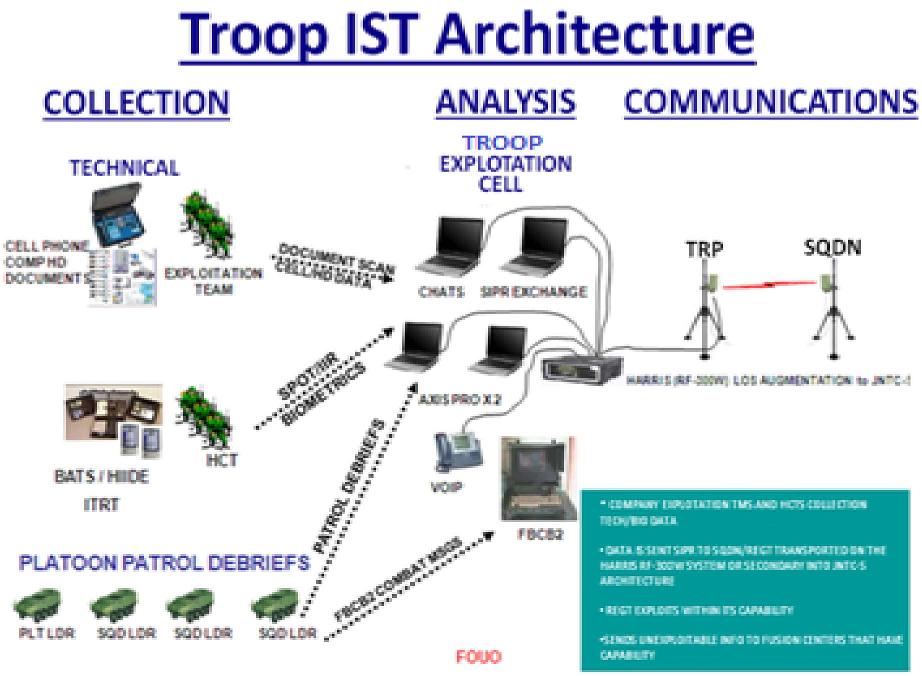


b) The Analysis area of the TIST is where all of the intelligence analysis tools are located so they can be used as efficiently as possible.

c) The Briefing area of the TIST is where all of the products displayed to the outgoing mission leader, convoy leader, or commander is consolidated. This technique is designed to allow the briefer to focus attention to one specific part of the TIST while still allowing the TIST to operate efficiently.

d) This is the standard layout for a TIST operating in a tactical environment. This layout represents a minimum of what the TIST should be able to produce and disseminate. The layout above is suggestive and not proscriptive. The TIST should tailor the location of their products to best suit briefing their commander. The TISTs are encouraged to improve upon their TIST products and to share those improvements with their sister TISTs and HHQ.

e) TISTs will establish a mission tracker separate from the operations mission tracker. This product is designed to assist the TIST in identifying patterns and TTPs the troop is creating. During the mission prebrief, the briefer should recommend certain actions to the mission leader such as leaving at a different time or taking a different route.



f) Sample TIST Architecture is depicted here. Sample equipment listing required to set up a TIST is listed in Annex G.

<u>13. TIST Briefing TTPs</u>:

a) **TIST Graphical Products.** The graphic depictions of the TIST should be able to “brief” themselves. In other words, when the mission 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.

b) **Mission Pre-Briefs.** A member of the TIST will give the mission pre-brief to the mission leader until the leader feels comfortable enough with the information to leave the FOB.

Mission Pre-Brief highlights should include:

- Last 24 hour SIGACTS in the area where the mission leader is going.
- Enemy trends that have been established as far as SIGACTS are concerned.
- What the predictive assessment is for the area; what the TIST thinks is going to happen.
- Names/Pictures of Troop HVTs/HPTs.
- IR [Intelligence Requirements], specific items the mission will focus on.
- Questions to ask the local populace or questions for SOI (Spheres of Influence) engagements.
- Concerns TIST personnel have for the planned operation from a threat or force protection perspective (based on planned routes, duration, departure and return times)
- Current Collection and ISR Plan, as it relates to the specific mission.
- BOLO lists.

Information to include items specific to the mission or area that will give the mission leader better situational awareness. The briefer is responsible for including all pertinent collection priorities so that the unit will know what they are looking for. See Annex A for further examples of the types of information necessary to discuss during a prebrief.

c) **Debriefs.** The TIST is responsible for debriefing every troop mission as soon as they return. The mission leader should not consider the mission complete until the debriefing is finished. **The debriefing format is dependent on each individual Squadron SOP**. The TIST member debriefing needs to accommodate the unit as best they can. If at all possible the TIST member conducting the debrief needs to go to where the unit is and coordinate with the mission leader to facilitate the debriefing process.

A recommended debriefing technique follows:

- Use a chronological method: Have the mission leader review the entire mission from start to finish, noting everything that happened. Use maps and route overlays to assist the Soldiers' memory of where a certain event happened.

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

- Encourage everyone to speak regardless of rank.

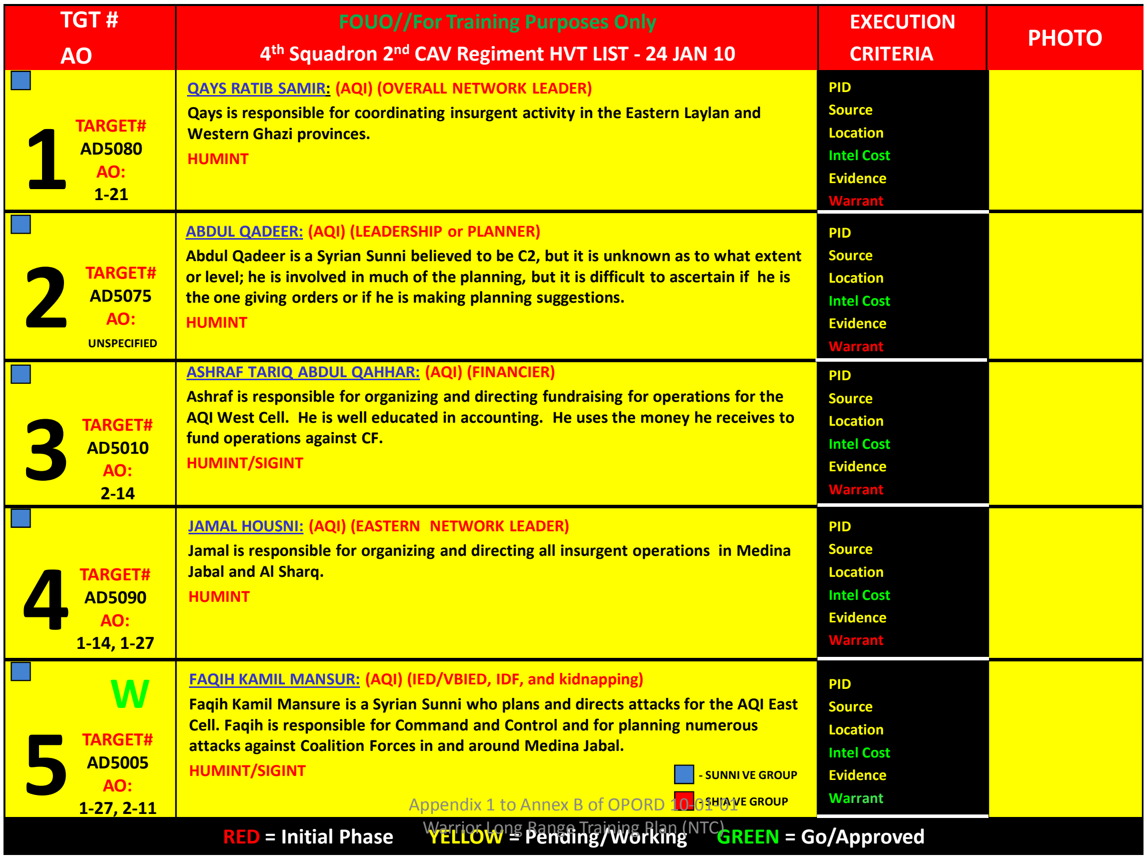
- During the debrief, the mission leader should review the route taken and compare it to the planned route. This will enable the TIST to keep track of routes, times, and places every mission the troop takes. It will help determine if the troop is starting to inadvertently set patterns.

The TIST must import all new information into all the intelligence systems (TIGR, BATS/HIIDE, etc) in order to populate the SQDN and REGT intelligence picture. This provides the entire SQDN with a Common Operating Picture (COP). All updates to the Intelligence Systems should be completed within **2 hours** after the final mission debrief. Mission Leaders should carry the debriefing form with them during the mission to record pertinent information.

Annex B is the 4/2 SQDN baseline format for all mission debriefs. SQDN S2s are authorized to adjust that format and to create a standardized form for their S2 section and all TISTs in their SQDN provided the new form still recognizably answers the information requirements outlined within the REGT standard.

14. **<u>HVTL Format</u>**

The TIST is responsible for creating and maintaining the enemy's High Value Target List (HVTL). This list is a summation of the key targets the enemy commander(s) must enable or disable in order to accomplish his mission. This list, produced as part of the Intelligence Preparation of the Battlefield (IPB) process, feeds into the targeting cycle and helps the Commander generate his HVTL/HPTL. It lists the targets the troop commander needs to enable or disable in order to accomplish *his mission.* Those targets then become target folders, a subject explained in the next section.

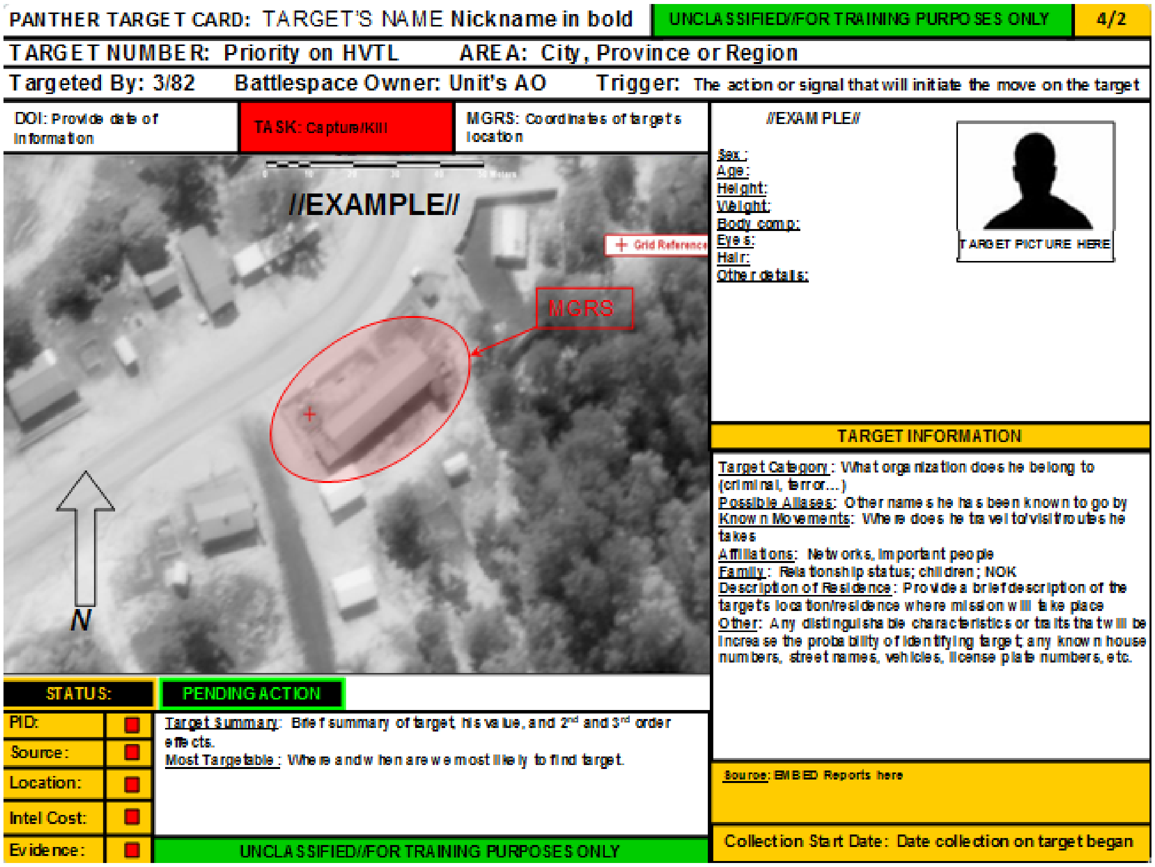


TGT # AO	FOUO//For Training Purposes Only 4th Squadron 2nd CAV Regiment HVT LIST - 24 JAN 10	EXECUTION CRITERIA	PHOTO
🟦 1 TARGET# AD5080 AO: 1-21	QAYS RATIB SAMIR: (AQI) (OVERALL NETWORK LEADER) Qays is responsible for coordinating insurgent activity in the Eastern Laylan and Western Ghazi provinces. HUMINT	PID Source Location Intel Cost Evidence Warrant	
🟦 2 TARGET# AD5075 AO: UNSPECIFIED	ABDUL QADEER: (AQI) (LEADERSHIP or PLANNER) Abdul Qadeer is a Syrian Sunni believed to be C2, but it is unknown as to what extent or level; he is involved in much of the planning, but it is difficult to ascertain if he is the one giving orders or if he is making planning suggestions. HUMINT	PID Source Location Intel Cost Evidence Warrant	
🟦 3 TARGET# AD5010 AO: 2-14	ASHRAF TARIQ ABDUL QAHHAR: (AQI) (FINANCIER) Ashraf is responsible for organizing and directing fundraising for operations for the AQI West Cell. He is well educated in accounting. He uses the money he receives to fund operations against CF. HUMINT/SIGINT	PID Source Location Intel Cost Evidence Warrant	
🟦 4 TARGET# AD5090 AO: 1-14, 1-27	JAMAL HOUSNI: (AQI) (EASTERN NETWORK LEADER) Jamal is responsible for organizing and directing all insurgent operations in Medina Jabal and Al Sharq. HUMINT	PID Source Location Intel Cost Evidence Warrant	
🟦 W 5 TARGET# AD5005 AO: 1-27, 2-11	FAQIH KAMIL MANSUR: (AQI) (IED/VBIED, IDF, and kidnapping) Faqih Kamil Mansure is a Syrian Sunni who plans and directs attacks for the AQI East Cell. Faqih is responsible for Command and Control and for planning numerous attacks against Coalition Forces in and around Medina Jabal. HUMINT/SIGINT 🟦 - SUNNI VE GROUP 🟥 - SHIA VE GROUP	PID Source Location Intel Cost Evidence Warrant	

RED = Initial Phase YELLOW = Pending/Working GREEN = Go/Approved

15. **TIST Target Folders**:

The TIST is responsible for creating, maintaining, and tracking target folders for its commander. These target folders are the extension of the HVTL within the troop level targeting process. See Annex G for an example Target Folder. These folders should be tailored to each specific commander's requirements. Possible elements of a target folder are picture ID, relevant message data/corroborating evidence, target location to include grid coordinates and/or photographs, descriptions of the target, patterns of life, associates, significance of target to the enemy, and known aliases. Each TIST is encouraged to add as much relevant evidence as possible to a target folder to that the auctioning unit will have all the information they need to prosecute the target and also for the host nation judicial system to successfully try and convict the target.


//EXAMPLE//
Grid Reference
MGRS
N
TARGET PICTURE HERE

PANTHER TARGET CARD: TARGET'S NAME **Nickname in bold** | UNCLASSIFIED//FOR TRAINING PURPOSES ONLY | 4/2

TARGET NUMBER: Priority on HVTL AREA: City, Province or Region

Targeted By: 3/82 Battlespace Owner: Unit's AO Trigger: The action or signal that will initiate the move on the target

DOI: Provide date of information

TASK: Capture/Kill

MGRS: Coordinates of target's location

//EXAMPLE//

Sex:
Age:
Height:
Weight:
Body comp:
Eyes:
Hair:
Other details:

TARGET INFORMATION

Target Category: What organization does he belong to (criminal, terror…)
Possible Aliases: Other names he has been known to go by
Known Movements: Where does he travel to/visit/routes he takes
Affiliations: Networks, Important people
Family: Relationship status; children; NOK
Description of Residence: Provide a brief description of the targets location/residence where mission will take place
Other: Any distinguishable characteristics or traits that will be Increase the probability of identifying target; any known house numbers, street names, vehicles, license plate numbers, etc.

STATUS: PENDING ACTION

PID:	🟥
Source:	🟥
Location:	🟥
Intel Cost:	🟥
Evidence:	🟥

Target Summary: Brief summary of target, his value, and 2nd and 3rd order effects.
Most Targetable: Where and when are we most likely to find target.

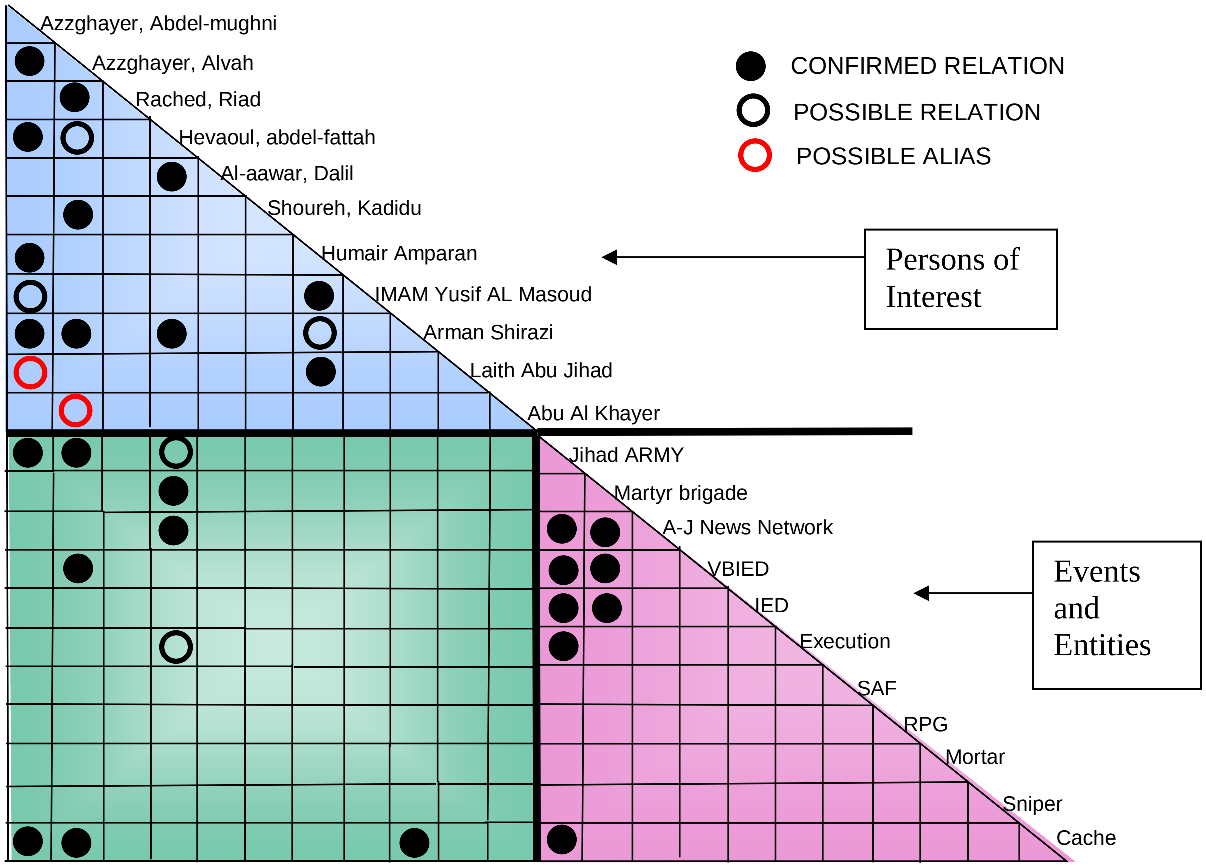
UNCLASSIFIED//FOR TRAINING PURPOSES ONLY

Source: EMBED Reports here

Collection Start Date: Date collection on target began

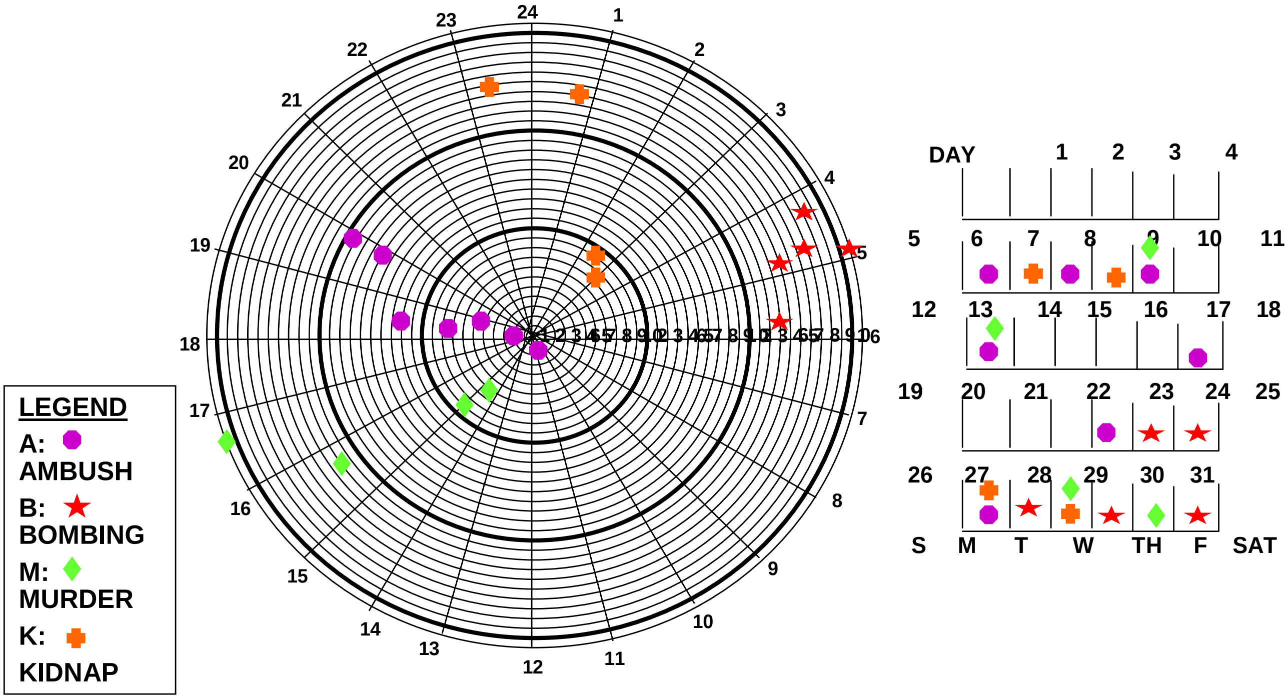
16. Analytical Tools.

a) **Association/Event Matrix.** The association/event matrix shows known and suspected associations. 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. 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. Analysts determine a known association by "direct contact" between individuals. Direct contact is defined as face-to-face meetings or confirmed conversations 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 or is detained, a diamond is added at the end of his or her name. 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.



b) **Pattern Analysis Wheel and Chart.** The pattern analysis wheel and chart is a tool to assist the TIST 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.

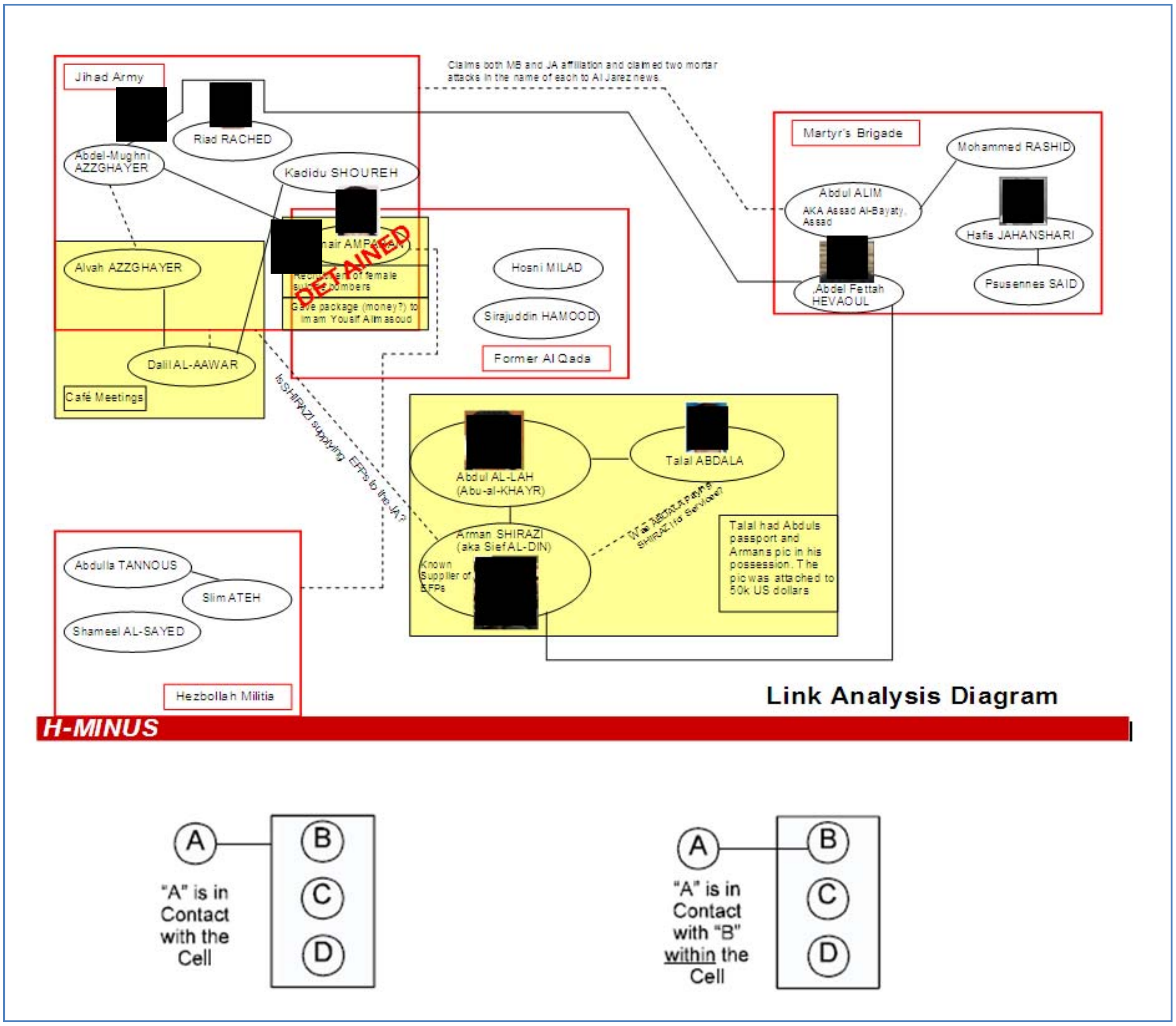
Pattern analysis of attack times and locations will be conducted at the troop level. Mission and commander's preference will dictate how pattern analysis is conducted at the troop level. Pattern analysis can be conducted with separate time analysis wheels and location analysis maps, or the two can be combined into one product covering one specific form of enemy attack; this type of pattern analysis is represented below:



[22]

c) **Link Analysis.** A Link Analysis Chart is an analytical tool that connects 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.

Link charts can be designed on PowerPoint at the TIST level and then submitted to the SQDN S2 for refinement on Analyst Notebook/DCGS-A Program.


Jihad Army
[redacted]
[redacted]
Abdel-Mughni AZZGHAYER
Riad RACHED
Kadidu SHOUREH
[redacted]
[redacted]
hair AMPA
DETAINED
Recruitment of female suicide bombers
Gave package (money?) to imam Yousif Almasoud
Alvah AZZGHAYER
Dalil AL-AAWAR
Café Meetings
Claims both MB and JA affiliation and claimed two mortar attacks in the name of each to Al Jarez news.
Hosni MILAD
Sirajuddin HAMOOD
Former Al Qada
Martyr's Brigade
Mohammed RASHID
Abdul ALIM
AKA Assad Al-Bayaty, Assad
[redacted]
Hafis JAHANSHARI
[redacted]
Abdel Fettah HEVAOUL
Psusennes SAID
Is SHIRAZI supplying EFPs to the JA?
[redacted]
Abdul AL-LAH (Abu-al-KHAYR)
[redacted]
Talal ABDALA
Was ABDALA paying SHIRAZI for Services?
Talal had Abduls passport and Armans pic in his possession. The pic was attached to 50k US dollars
Arman SHIRAZI (aka Sief AL-DIN)
Known Supplier of EFPs
[redacted]
Abdulla TANNOUS
Slim ATEH
Shameel AL-SAYED
Hezbollah Militia
Link Analysis Diagram
H-MINUS
A
B
C
D
"A" is in Contact with the Cell
A
B
C
D
"A" is in Contact with "B" within the Cell

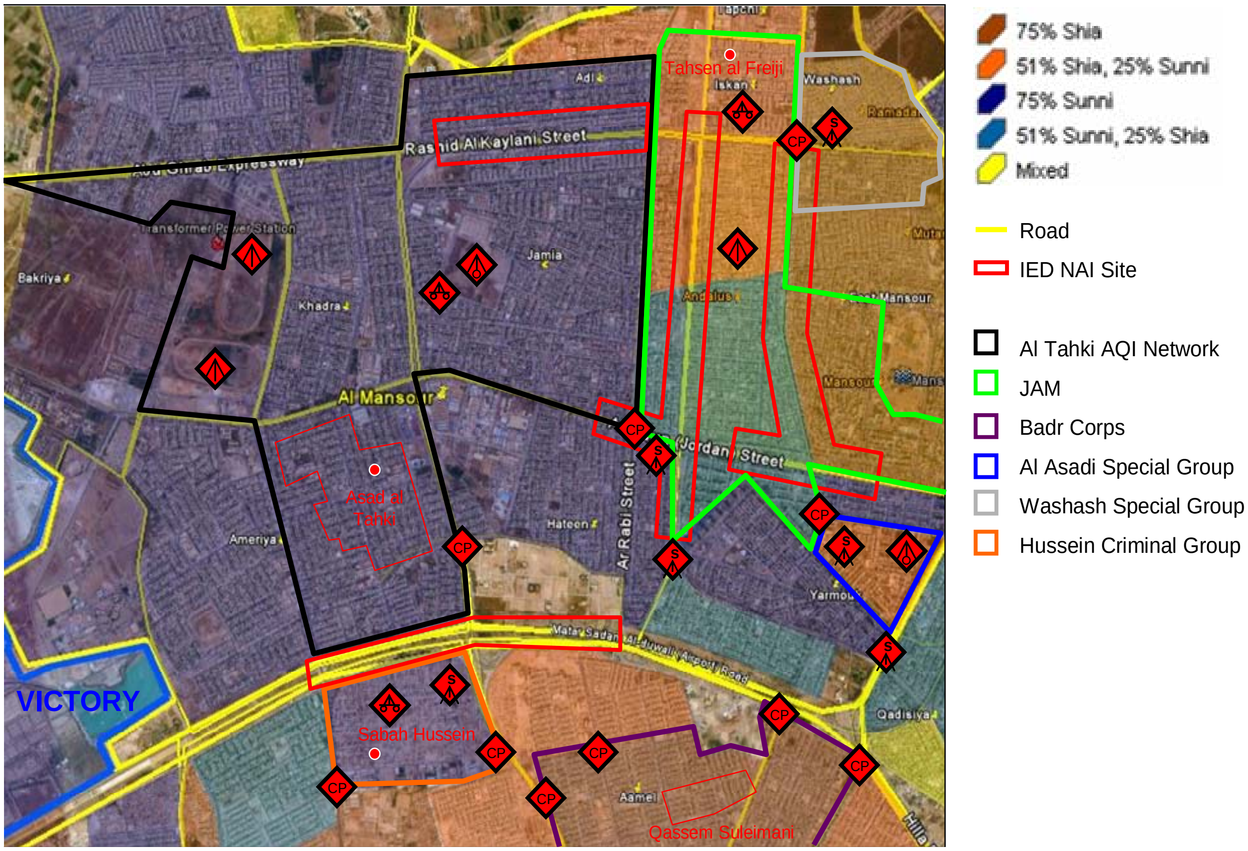
Constructing Link Diagrams: The following steps will assist the TIST in creating link diagrams.

- Collate and organize all raw data related to a situation.
  - Put in a narrative or report format.
  - 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.
- Identify relevant data points.
  - 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.
  - Underline these references in the reports, and make lists.
- Construct matrices from the lists.

- Organize the data points (the names of suspects and organizations or activities) into rows and columns.
- Put contact or association points (e.g., A knows B) in the matrix where the corresponding rows and columns intersect.
- When working with both confirmed and unconfirmed contacts among suspects, use different symbols to represent the strength of evidence. For example:
  - Use a "1" for a confirmed contact between two data points.
  - Use a "2" or any other symbol for unconfirmed contacts.
  - Use zeros at matrix intersections where no known contact between suspects exists.
- Analyze the matrix to determine the number of links associated with each suspect or activity.
  - Count through each row to find out how many entries appear in it.
  - Do the same for the columns.
- Draw a draft link diagram, grouping suspects together into rectangles representing cells, actions, or organizations.
  - Start with the individual with the largest number of contacts and work outward.
  - Use circles to represent individuals and rectangles for organizations or cells.
- Draw additional drafts of the link diagram to clarify the relationships, avoiding crossed lines.
- Complete the final draft.
  - Examine the relationships that appear.
  - Study the diagram carefully and make assessments about patterns in contacts and cell memberships.
  - Is there a uniform size to the cells, or do sizes vary?
  - Do suspects belong to more than one cell?
  - Are the cells linked tightly together, sharing a number of suspects, or are they spread out, with few connections?
- Make recommendations about the group's structure. Identify areas for further analysis.
  - Are there suspected connections that need verification?
  - Are there people who appear central to the organization, without whom the structure would collapse?
  - Are there a few individuals with contacts to many others who would be the best targets for surveillance?
  - Be prepared to substantiate logically the conclusions and assessments drawn from the link analysis.

17. **<u>TIST IPB Products</u>**:

a) Enemy situation graphics are a visual representation of how the TIST sees the enemy on the battlefield at the time. These products are an easy way for the TIST to convey to its HHQ the current enemy situation in their AO. See below for a reproduction of what a TIGR SITEMP may look like. 4/2 SQDN TIST products that outline demographic data will always, if at all possible, depict ethnic, sectarian, and tribal breakdowns in addition to any other data the TIST wishes to incorporate.



b) A Doctrinal Template (**DOCTEMP**) illustrates the preferred deployment pattern and disposition of the threat's normal tactics when not constrained by the effects of the battlefield environment. A DOCTEMP is usually a scaled graphic depiction of threat dispositions for a particular type of standard operations, such as a Squadron movement to contact, an insurgent daisy-chained IED attack, or a terrorist kidnapping.

Within the TIST should be posted a list of current enemy trends or specific TTP the enemy is using, such as using a different IED TTP, or attacking the FOB at a certain time everyday.

This is valuable information for outgoing mission leaders and the commander. The information that is posted could save a Soldiers life by helping them predict enemy actions. 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.

c. A Situational Template (**SITEMP**) is the graphic depiction of expected threat dispositions should the threat adopt a particular Course of Action (COA). The template usually depicts the most critical point in the operation as agreed upon by the S2 and the S3 (or in the case of the troop, the TIST and the Commander). The TIST may wish to draw several SITEMPs representing different snapshots in time starting with the threat's initial array of forces. At a minimum, there the TIST must graphically depict an enemy Most Likely COA (MLCOA) and a Most Dangerous COA (MDCOA).

d. An Event Template **(EVENTEMP)** is a guide for ISR collection and planning. It depicts where to collect the information that will indicate which COA the threat has adopted. The TIST combined all the various SITEMPs depicting alternate COAs onto one operational environment overlay and then uses the combined COAs to identify Named Areas of Interest (NAIs) and indicators to assist with the ISR collection plan.

18. **TIST Information Requirements (TIST-IR):** TIST-IR is a way for TISTs to task units with finding out information that they need to know. This is an information requirement that cannot be satisfied by RFIs, higher guidance or ISR tasking. These are specific questions about the AO that will allow the TIST to have a better understanding of the situation on the ground.

19. **Recommended Courses of Action**: TISTs will recommend courses of action to the commander for his review. These COAs are developed after careful analysis of the situation and creation of the best possible way to handle it. For example, recommending to the commander that he visit a certain key leader because the TIST is tracking that individual having influence in the area of operations.

a) The format for a recommended COA is as follows:

i. 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 action is easy to develop at the troop level.

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

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

Example Recommended Course of Action:

Situation: A recent spike in high visibility suicide bombings in the Nemesis TRP AO have made these attacks a serious threat to the stability of this sector. Attacks bear the hallmarks of Jihad Army methods and source reports indicate that an HVT named Humair AMPARAN, who has recently been detained, may be involved in the use of female suicide bombers seeking revenge for the death of males killed by CF and ISF forces. Attacks seem to take place in public places alternating between Sunni and Shiite neighborhoods.

Recommendation:

- 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 CO AO. Targeting and SSE of the storefront is highly recommended. This is a time sensitive action.

21. **Troop Tactical Informant Operations:**

Troop Tactical Informant Operations are not Source Operations. TISTs might often have to remind their commanders that they are not authorized to task an informant. An informant is defined as an individual who comes to you to willingly give information. 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 TIST to both track them and incorporate HCT expertise to exploit these informants.

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

a) 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.

b) Pictures can digitally hyperlink to more detailed information.

c) Ensure that all informant meetings are recorded in the Tactical Informant Contact Log (Annex D) and have updated Informant Personal Information Sheets (see Annex E).

d) 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 missions nor be posted anywhere that ISF or interpreters can view them.

NOTE: Tactical Informants are completely within the bounds of a Troop's ability to use and exploit. The issue is when the informant becomes a source, and it is at that time that the informant must be handed over to an HCT so that they can be incorporated legally into the unit's collection plan.

Right Way to Use an Informant: A local national comes to the FOB and informs you that he has information that would be of value to the coalition forces. The local national is then brought into the FOB and is questioned on what he knows. After he tells you what he knows he can also be questioned about whatever else you would like to know about emerging or upcoming operations.

Wrong Way to Use an Informant: A local national comes to the FOB and informs you that he has information that would be of value to the coalition forces. The local national is then brought into the FOB and is questioned on what he knows. The person questioning then asks the local national to go back out and bring back information on different subjects and places. (This is called "**TASKING"** and it is **UNAUTHORIZED**). Only certified personnel within HCTs are authorized to TASK an informat.

HUMINT is a very effective form of intelligence if the information is utilized properly. It can be a commander's greatest and most lethal weapon if they embrace the concept of tactical informants and adhere to the proper rules and regulations. Any information that is taken in from a local national should be questioned and vetted to ensure the information is actually of value.

22. **Training**: A typical maneuver SQDN only has school-trained Military Occupational Specialty 35F Intelligence Analysts within the SQDN S-2 shop. While mobile training teams provide a baseline of training to most TISTs, many Soldiers never attend due to moves within the troop, so the S-2 shop must ensure these individuals receive basic analytical training.

In addition to basic analyst tasks, S-2 shops owe their TISTs training on aspects of the intelligence fight specific to their particular area of operations (AO). Training includes, but is not limited to, the following:

- Instruction in the SQDN standard prebriefing and debriefing process.
- Classes in the threat groups and enemy tactics, techniques, and procedures (TTP) of a particular AO.
- Classes in database search techniques that would be effective in a particular AO (i.e., entity-based searches versus geography-based searches).
- Classes in the intelligence, surveillance, and reconnaissance (ISR) assets that operate within the AO.

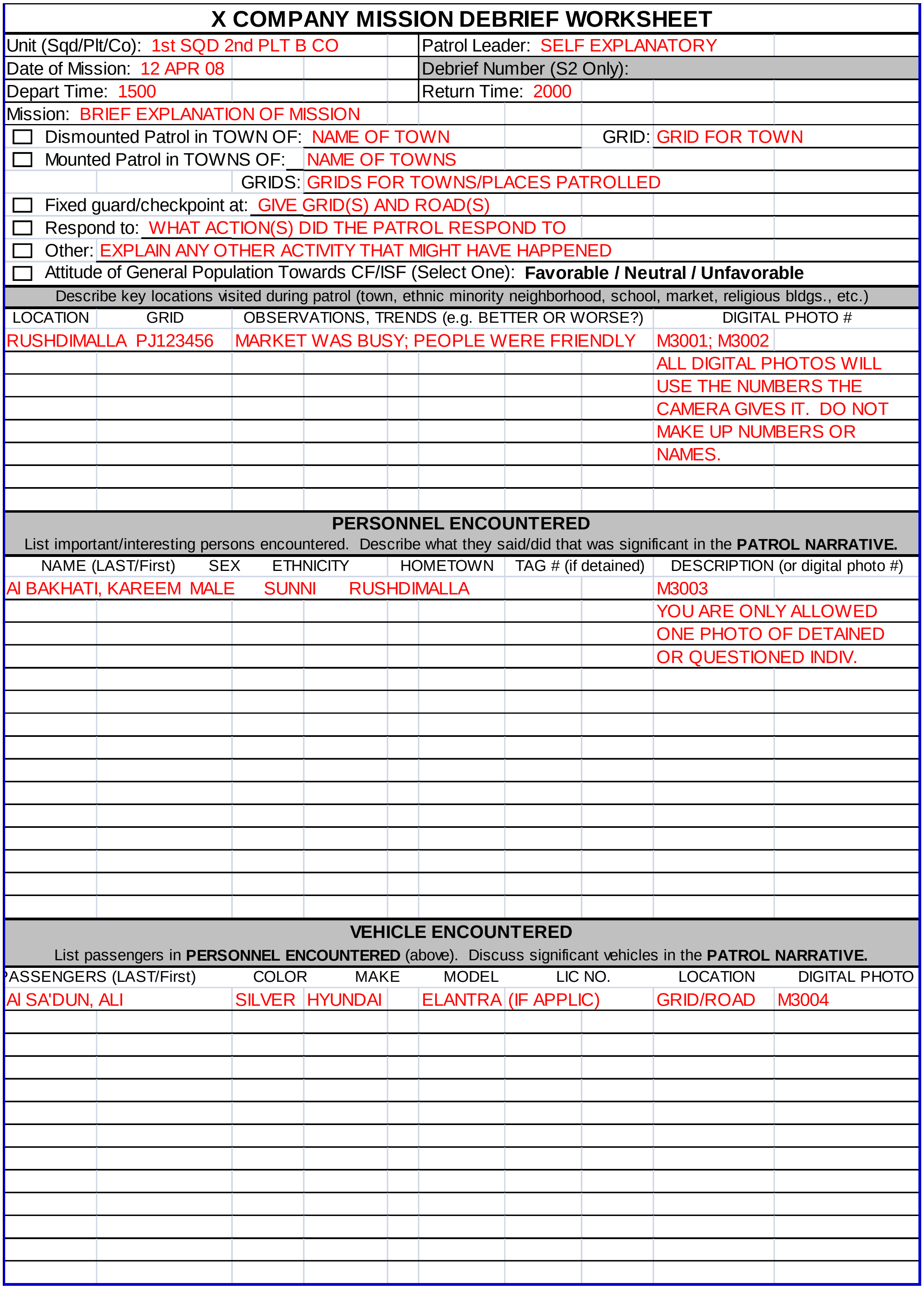
As the analytical skill of the TIST improves, more complicated tasks such as intelligence preparation of the battlefield (IPB), development of enemy courses of action, and writing of troop intelligence requirements (IRs) should also be taught. If the SQDN S-2 takes a hands-off approach to the training of the TISTs, their effectiveness will be greatly diminished upon arrival in the combat zone.

ENCL:
Annex A – Prebrief Checklist
Annex B – Debrief Format
Annex C – Request for Collection Asset Form
Annex D – Tactical Informant Contact Log
Annex E – Informant Personal Information Sheet
Annex F – Standardized Naming Conventions for TIGR Input
Annex G – Sample Equipment Listing
Annex H - Sample TIST Reporting Instructions

Annex A – Prebrief Checklist (To be used by TIST personnel when conducting prebrief)

Weather:	High Temp	Low Temp	% Precip
	Wind Speed	Wind Direction	
Light Data:	Sunrise	Sunset	% Illum
	Moonrise	Moonset	
Enemy Update (from S2/TIST)			
24/48hr SIGACTs			
CURRENT TRENDS/TTPs			
Key Personalities Updates			
IED/Ambush hotspots along route			
SIGNIFICANT EVENTS (culture and political)			
PIR/SIR			
BOLO			
SQDN PIR			
SQDN FFIR			

Annex B – Debrief Format



X COMPANY MISSION DEBRIEF WORKSHEET

Unit (Sqd/Plt/Co): 1st SQD 2nd PLT B CO | Patrol Leader: SELF EXPLANATORY

Date of Mission: 12 APR 08 | Debrief Number (S2 Only):

Depart Time: 1500 | Return Time: 2000

Mission: BRIEF EXPLANATION OF MISSION

□ Dismounted Patrol in TOWN OF: NAME OF TOWN GRID: GRID FOR TOWN

□ Mounted Patrol in TOWNS OF: NAME OF TOWNS

GRIDS: GRIDS FOR TOWNS/PLACES PATROLLED

□ Fixed guard/checkpoint at: GIVE GRID(S) AND ROAD(S)

□ Respond to: WHAT ACTION(S) DID THE PATROL RESPOND TO

□ Other: EXPLAIN ANY OTHER ACTIVITY THAT MIGHT HAVE HAPPENED

□ 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 #
RUSHDIMALLA	PJ123456	MARKET WAS BUSY; PEOPLE WERE FRIENDLY	M3001; M3002
			ALL DIGITAL PHOTOS WILL
			USE THE NUMBERS THE
			CAMERA GIVES IT. DO NOT
			MAKE UP NUMBERS OR
			NAMES.

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 #)
Al BAKHATI, KAREEM	MALE	SUNNI	RUSHDIMALLA		M3003
					YOU ARE ONLY ALLOWED
					ONE PHOTO OF DETAINED
					OR QUESTIONED INDIV.

VEHICLE ENCOUNTERED

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

PASSENGERS (LAST/First)	COLOR	MAKE	MODEL	LIC NO.	LOCATION	DIGITAL PHOTO
Al SA'DUN, ALI	SILVER	HYUNDAI	ELANTRA	(IF APPLIC)	GRID/ROAD	M3004

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

QUANTITY	ITEM DESCRIPTION	TAG NUMBER	SERIAL NUMBER	DIGITAL PHOTO #
1	AK-47 ASSAULT RIFLE	APPROPRIATE TAG #	IF IT HAS ONE	M3005

PIRs/IRs ANSWERED

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

PIR/IR # ANSWERED

LIST THE PIR/IR # ANSWERED AND ANY INFORMATION APPLICABLE

MISSION NARRATIVE

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

THIS IS A BRIEF OVERVIEW OF THE PATROL. INCLUDE THE 5 W'S. USE THE LIST TO THE RIGHT IF YOU START TO DRAW A BLANK. INCLUDE THE THE DIGITAL PHOTO # OF ANYTHING MENTIONED THAT HAD A PHOTO TAKEN OF IT DURING THE PATROL.

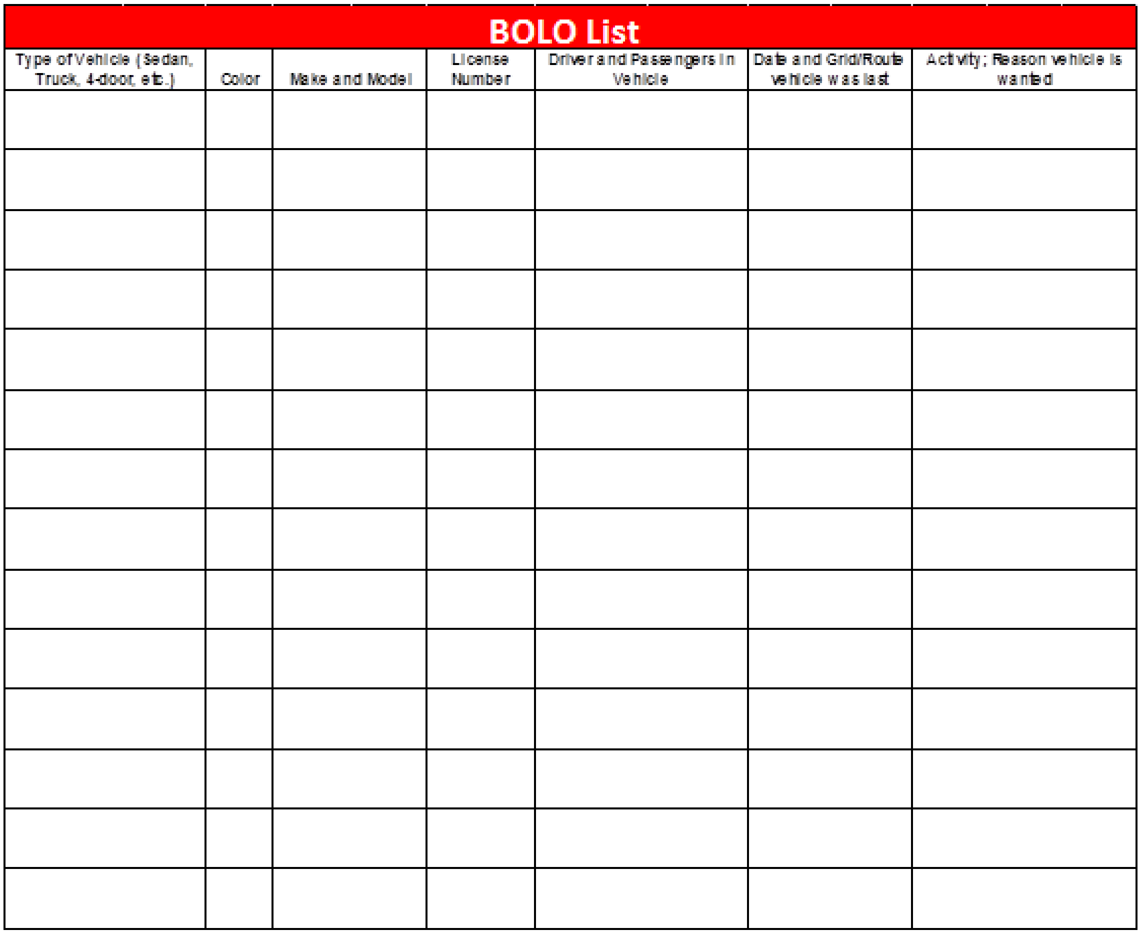
What to report when you don't know what to report:

- 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)

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

People Tracker

Known variations of target's name	Number of reports	Reason target is wanted	References where target's name	Additional information



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	Activity; Reason vehicle is wanted

ANNEX C: Request for Collection Assets

POC Contact Info	Organization		
	Name		
	Secure Phone		
	SIPR Email		
Type of information requested (imagery, FMV, MASINT, etc)			
Date of Request			
Collection start/stop dates/times			
LTIOV			
Intended Dissemination/Classification requirements			
NAIs			
Target Information	MGRS Coords	TGT Name (if available)	Tgt Name/Description
Essential Elements of Information – What are you trying to find out?			
Justification - What are you trying to answer? Relevant PIR/SIRs, etc			
Intel Report that cued collection (if available)			
Notes or Comments			

Annex D – Tactical Informant Contact Log

Unit:

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)

Annex E – Informant Personal Information Sheet

UNIT:
TI #: __________________ (assigned by SQDN S2)
Type of TI: _______________ (walk-in, mission, casual, community, liaison)

This sheet is used to record the biographic and other details of individuals met during passive HUMINT collection operations. These include walk-ins, mission collection, casual, community & liaison contacts.

Biographic Details

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

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

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

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

E. What is the TI's mobile phone #(s)?

Placement/Access

F. Where did the TI obtain the information he/she provided?

G. When did you obtain this information?

Motivation

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

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

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

K. Is the TI willing to pass information to others within the Coalition?

L. What are the TI's feelings about the Coalition Forces operating within Iraq?

Security

M. Who else knows the information being reported?

N. Who else knows the TI is talking with us?

Contact/Recontact Details

O. Is the TI able to contact/meet with us again? (Where/when)

Meeting History (refer to previous screening sheets & contact logs)
P. When has the TI been met? (from first meeting onwards: include date, time, location, collector details – including linguist):

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

Inspection by Brigade S2X/Review by HCT
R. 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
S. Who compiled this sheet and updated the details? (include date, member details):

Physical Description

T. What is the TI’s physical description? (“A to I” acronym)

- A: Age/Sex (estimate within 5 years, e.g. 25-30 years old male)
- B: Build (include estimate of weight within 10 pounds, e.g. 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

U. When was the TI handed over to a HCT, or terminated as a source of information?

Annex F – Standardized Naming Conventions for TIGR Input

Each entry into the TIGR share folder must be specifically named IOT enable all TIST entities to query the folder and find groups of events. During a relief in place, the following naming convention is subject to change pending outgoing unit SOPs. Follow the guidelines set below.

1. The naming convention will be as follows: Reporting unit (to PLT level) followed by an underscore, type of incident followed by an underscore, a general place name followed by an underscore, and finally the date time group. (Make sure to use ALL CAPS for the incident, location and month abbreviation) i.e. If 1/B hit an IED on ASR Ia Drang at 1500 Zulu on September the fifth, the incident would be named as follows:
1-B-1-4/2CAV_IED_IADRANG_051500Z SEP11

2. The following are types of incidents and the required text entry:

a. If a bomber dies in the blast classify it as a suicide. There are two types:
SVBIED- ***(Suicide Vehicle Borne Improvised Explosive Device)*** Only use this if a vehicle was used in the blast.
SBOMB- ***(Suicide Bomb)*** Use this when no vehicle was used. [i.e. Suicide vest, backpack, grenade, etc.]

b. If an RKG is thrown classify it as an RKG attack (also known as a Direct Fire Weapon System). There are two types; if you use the second, place an underscore between the base attack abbreviation and the more specific abbreviation.
RKG- Only in instances where no other arms are used.
RKG_CMPLX- If other arms are used in the attack. [i.e. RKG-3 thrown at vehicle then followed by small arms fire, mortars, RPG attack, or sniper]

c. If an IED detonates classify it as an IED attack. If you know what kind of IED was used place an underscore after the base attack abbreviation and then add more specific abbreviation.
IED- If an IED detonates and the type is unknown.
IED_MTR-If an IED detonates and the type of ammunition used was a mortar round. [IED_MTR155 or IED_MTR82]
IED_EFP- If an IED detonates and it was an explosively formed penetrator.
IED_HME- If an IED detonates and it was made from household explosive products/homemade explosive.
IED_RC- If an IED detonates and it was detonated by a remote controlled trigger.
IED_CD- If an IED detonates and it was detonated by a command detonation trigger.
IED_VO- If an IED detonates and it was detonated by a victim operated trigger (i.e. crush wire, pressure plate, infrared beam, etc).
IED_FOU- If an IED is found by CF or ANSF and is either destroyed in place, or is rendered inert by any means.

****If you know what type of explosives were used and the type of detonator which was used place the abbreviation of the type of explosive followed by an underscore followed by the type of detonator abbreviation.-→ IED_EFP_VO ****

d. If a small arms attack (.50CAL and below) is conducted against CF, ANSF, or civilians classify it as a small arms fire attack.
SAF- Only if an element less than a squad size conducts the attack.
SAF_CMPLX- If an element, larger than a squad size, conducts the attack using other weapon systems in conjunction with small arms weapons. (Element must be military/insurgents/organized)
SAF_RIOT- If a non-military element (mob) conducts a small arms fire attack.
PSAF- If precision small arms fire is taken by either CF or ANSF forces.
SAF_ASSN- If SAF is deemed a political or religious assignation.
SAF_CRIME- If criminal elements conduct the small arms fire attack. [i.e. robbery, gang related violence, murder, etc.]

e. If enemy indirect fire is detected, either point of origin or point of impact, classify it as in direct fires.
IDF_POO- If the point of origin of indirect fires is known.
IDF_POI- If the point of impact of indirect fires is known.

f. If any enemy ground elements fires upon aerial vehicles of any kind classify it as surface to air fire.
SAFIRE- Any fires taken by CF or ANSF forces air assets from ground enemy troops.
If you are unsure of the type of attack label it UNK and continue to finish the naming convention. Put as much detail into the TIGR report as possible.

4. For the date time group (DTG) use the standard military format of DDTTTTZMMMYY (Day Time {ZULU} Month Year). Ensure that the time is as near the time which the event occurred as possible. [i.e. 191547LSEP09]

Annex G – Sample Equipment List

To effectively perform its functions, the TIST should be equipped with dedicated computers and access to communications equipment. The TIST can function on two computers but ideally should be resourced with three: one for biometrics (if allocated); one for mapping, personality and event linkage, and event-trend analysis; and one for prebriefs and debriefs.

Equipment and materiel list includes:

Equipment:

- 3x workstations (2x SECRET Internet Protocol Router [SIPR]/1x Non-Secure Internet Protocol Router [NIPR])
- 2 or more Laptop computers (1x SIPR/1x NIPR)
- DCGS-A
- TiGR
- Falcon View/Google Earth
- Microsoft Internet Relay Chat (mIRC) or other chat capability software
- Microsoft Office Suite

Systems:

- Biometric Automated Toolset and Handheld Interagency Identity Detection Equipment (BAT for FOB and HIIDEs for Missions)
- One System Remote Video Terminal (OSRVT)
- Cellular exploitation/CelleBrite handheld, portable forensic device for cellular phones (CELLEX)
- DCGS-A system (if available)

Materiel:

- 2X Color printers, scanner, and copier (1x SIPR/1x NIPR)
- Field Safe
- Secure Voice Over Internet Protocol phone (SVOIP)
- Digital camera
- Projector
- Shredder
- Maps
- Tent, tables, chairs, dry-erase board, power source, lights, and environmental controls (air/heat)

Annex H – Sample TIST Reporting Instructions

- The Troop's primary communications to SQDN when reporting is FM. Once a SIGACT occurs, the troop CP will send a salute report via FM to SQDN NLT X= (SIGACT) + 10 minutes. After the FM call, the Troop will send the same salute report to SQDN via Blue Force Tracker (BFT).

- After every update of a report the TIST will call via FM to inform the SQDN of the update. The TIST will inform the FM monitor at SQDN the report naming convention and confirm that SQDN received the update. Updates will also be entered into TIGRNET (as seen below).

- At X + 20 minutes, the TIST will post an initial report into TIGRNET. The initial report will include a SALUTE report and any information regarding the SIGACT.

- At X + 60 minutes, the TIST will use the initial TIGRNET report and add the new information required.
  - The second report will include a commanders initial assessment, the TIST's preliminary analysis, and any battle damage assessment (BDA) or post blast analysis (PBA)

- At X + 2 hours, the TIST will input any new information that is received into the report in addition to the new requirements.
  - The third report will include a final commanders assessment, TIST analysis and threat assessment, and a confirmed BDA

- After the TIST inputs the 2 hour TIGRNET report, the TIST is still responsible for any new information or reports regarding the incident. The TIST is responsible for embedding any reports into the TIGRNET report so that the information is available to any unit.

- In the event the TIST discovers a time sensitive target (TST) in an adjacent unit's AO, the TIST will notify both SQDN as well as the TIST where the TST is located so they will have a chance to action the target and begin the process of acquiring the appropriate assets.

- Along with the SIGACT reports on TIGRNET, the TIST is also responsible for reporting intelligence information to the SQDN S2. The reports will consist of but are not limited to; area assessments, graphic intelligence summaries (GRINTSUM) of the AO, and lethal target folders.