

HANDBOOK

No. 10-20

JAN 10



Company Intelligence Support Team

Tactics, Techniques, and Procedures



U.S. UNCLASSIFIED
REL NATO, GCTF, ISAF, MCFI, ABCA
For Official Use Only

Handling Instructions for CALL Electronic Media and Paper Products

Center for Army Lessons Learned (CALL) authorizes official use of this CALL product for operational and institutional purposes that contribute to the overall success of U.S., coalition, and allied efforts.

The information contained in this product reflects the actions of units in the field and may not necessarily be approved U.S. Army policy or doctrine.

This product is designed for official use by U.S., coalition, and allied personnel and cannot be released to the public without the expressed written consent of CALL. This product has been furnished with the expressed understanding that it will be used for official defense-related purposes only and that it will be afforded the same degree of protection that the U.S. affords information marked "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" in accordance with U.S. Army Regulation (AR) 380-5, section 5-2.

Official military and civil service/government personnel, to include all coalition and allied partners may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official products or research. However, integration of CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" information into official products or research renders them FOUO, and they must be maintained and controlled within official channels and cannot be released to the public without the expressed written consent of CALL.

This product may be placed on protected UNCLASSIFIED intranets within military organizations or units, provided that access is restricted through user ID and password or other authentication means to ensure that only properly accredited military and government officials have access to these products.

Regulations strictly forbid posting CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents to Department of Defense (DOD) Web sites that do not restrict access to authorized personnel. AR-25-1, 15 Jul 2005, Army Knowledge Management and Information Technology, paragraph 6-4 n (2) (b) and DOD Web Site Administration Policy and Procedures (11 Jan 2002), Part II, paragraph 3.6.1 require appropriate mechanisms to protect sensitive information.

When no longer needed, all CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" paper products and electronic media will be shredded or destroyed using approved paper shredders or CDROM destroyers.

To allied and coalition personnel:

This information is furnished with the understanding that it is to be used for defense purposes only, that it is to be afforded essentially the same degree of security protection as such information is afforded by the United States, and that it is not to be revealed to another country or international organization without the written consent of CALL.



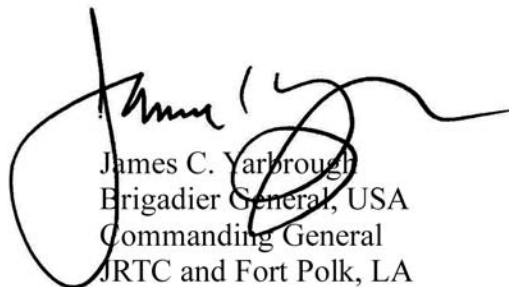
Foreword

In the current operational environment, small units are forming and resourcing company-level intelligence (S-2) sections. These sections or cells are necessary due to the decentralized nature of counterinsurgency (COIN) operations and go by a variety of names that includes the company intelligence cell, the company exploitation cell, the company S-2 section, or the company intelligence support team (COIST). For the purposes of this handbook, the term COIST will be used.

In conventional operations, intelligence is passed from higher to lower headquarters, as the higher headquarters is resourced with intelligence-gathering capabilities and sufficiently staffed with the analytical personnel necessary to collect, analyze, and disseminate pertinent information. In COIN operations, information generally flows in the opposite direction. Small units operating on the ground must gather and determine the significance of intelligence, often without the assistance, analysis, and filtering of higher-level intelligence staff support. This small-unit intelligence enables the company to maintain situational awareness and possibly even attain brief periods of situational understanding and information superiority as it conducts daily activities such as patrols, engagements, and combat logistics patrols.

Key concepts covered in this publication include:

- COIST mission and purpose
- COIST organization
- COIST systems and tools
- COIST battle rhythm
- Integration of COIST operations in platoons through brigades
- COIST targeting
- Tactical Ground Reporting System debriefing techniques



James C. Yarbrough
Brigadier General, USA
Commanding General
JRTC and Fort Polk, LA

Company Intelligence Support Team Handbook	
Table of Contents	
Chapter 1. Company Intelligence Support Team Mission and Purpose	1
Chapter 2. Company Intelligence Support Team Organization	7
Chapter 3. Company Intelligence Support Team Systems and Tools	17
Chapter 4. Company Intelligence Support Team Battle Rhythm	25
Chapter 5. Integration of Company Intelligence Support Team Operations: Platoon Through Brigade	35
Chapter 6. Company Intelligence Support Team Targeting	43
Appendix A. Ten-Step Tactical Ground Reporting System Debrief	51

Center for Army Lessons Learned	
Director	Colonel Robert W. Forrester
Chief, Analysis Division	George J. Mordica II
CALL Analyst	Brice Johnson
Production Coordinator	Kristine Bell
Editor	Jenny Solon
Graphic Artist	Dan Neal
Distribution Manager	Candice Miller

CENTER FOR ARMY LESSONS LEARNED

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications (other than CALL publications) referenced in this product, such as ARs, FMs, and TMs, must be obtained through your pinpoint distribution system.

Chapter 1

Company Intelligence Support Team Mission and Purpose

The mission of COISTs is to describe the effects of the weather, enemy, terrain, and local population on friendly operations to reduce uncertainty and aid in decision making. This is a simple and clear mission with a powerful purpose. However, the operation of the company COIST is far from simple. Company leaders must review and interpret huge volumes of data on a daily basis to determine their relevance and relationships. A few examples of this data include weapons intelligence team reports, patrol debriefs, intelligence summaries (INTSUMs), link diagrams, and be-on-the-lookout (BOLO) lists. Although the commander will determine and direct the exact requirements for the COIST, specified and implied tasks usually include targeting; intelligence, surveillance, and reconnaissance (ISR); patrol briefings and debriefings; detainee operations; and site exploitation.

The COIST provides a 24/7 analytical, production, and dissemination capability at the company level, which gives the commander options to exploit enemy vulnerabilities. Analysis is focused on the company OE, with the ability to report and help populate the overall battalion (BN) and brigade combat team common operational picture. If managed properly, a COIST will assist the commander in managing battlefield effects and operational expectations across all full spectrum operations. COIST operations in a COIN environment are typically conducted in conjunction with the company fire support team. The company commander establishes a COIST that is a company-level intelligence section and provides an array of capabilities to the company. The COIST is part of the command post or fusion cell and has the following responsibilities:

- Provides SA and SU for the commander.
- Secures assets and intelligence information to target insurgents.
- Proposes targets to the commander for review and nomination.
- Requests classified products and sensitive information from the BN S-2 for inclusion in the target packet.
- Develops the company-level target packets, and requests assets and/or effects in support of lethal and nonlethal operations.

Key tasks for COIST operations include the following:

- Collect data and conduct pattern analysis to include the following:
 - Collect and analyze patrol debriefs.
 - Collect all electronic data such as the Biometrics Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment systems and cellular exploitation from returning patrols.
 - Track and analyze all significant activities.

CENTER FOR ARMY LESSONS LEARNED

- Generate analytical, assessment, and mission summary products for the commander.
- Conduct local intelligence analysis, forecast enemy actions, and prepare the threat situation template (SITEMP) to include threat most likely course of action/most dangerous course of action.
- Battle track enemy significant activities to develop enemy patterns and tactics, techniques, and procedures.
- Facilitate the exchange and dissemination of intelligence such as information flow between company and BN S-2 graphic intelligence summaries and intelligence sharing with adjacent units, as well as perform the following:
 - Maintain updated intelligence boards for outgoing patrols.
 - Conduct mission prebriefs and debriefs.
 - Produce, process, and analyze information/material from site exploitation.
 - Disseminate combat information and actionable intelligence.
 - Continuously update all intelligence trackers and databases (Tactical Ground Reporting [TiGR] System), and maintain SA within the company area of operation (AO) and area of interest.
 - Conduct predictive analysis, and maintain a predictive analysis board identifying likely enemy activities over the next 48 hours and over the next few weeks.
 - Establish clear communications with the BN S-2 and adjacent companies, and ensure that information flows both up and down the chain of command in a timely manner.
 - Request information from the BN S-2 as required.
- Advise the commander on intelligence-related matters to include the following:
 - Conduct intelligence preparation of the battlefield (IPB) for company operations.
 - Support situational development and maintain understanding of the OE.
 - Recommend company priority information requirements (PIRs) and specific information requirements (SIR) to the commander.
 - Provide deception recommendations to the commander.

- Conduct assessment of effects and exploitation following a mission.
- Provide predictive analysis to the commander.
- Prepare to brief the commander on the current situation at any time.
- Analyze friendly trends from the enemy's perspective, and identify unnecessary vulnerabilities and patterns the company is setting.
- Request assistance from the BN S-2 to conduct specific detailed analysis beyond company capabilities.
- Manage the company's lethal and nonlethal targeting. At the company level, targeting is the overall synthesis of all sources of available intelligence—BN and sister-company INTSUMs, link diagrams, events pattern analysis (indirect fire, sniper, improvised explosive device [IED]), terrain analysis, BOLO lists, and most importantly, patrol debriefs. This continuous data fusion helps create a running SITEMP of the unit's OE.
 - Work with the commander to further develop targets and identify gaps in the current intelligence picture.
 - Provide targeting recommendations to the commander.
 - Assist in target development (both lethal and nonlethal).
 - Develop company-level high-value individuals (HVIs) and associated target packets to effectively action targets of opportunity.
- Supervise the company's ISR program. Based on the commander's guidance regarding particular targets, the COIST develops collection SIR and an ISR collection matrix, which may require the COIST to request BN or higher-level assets, task the company's unmanned aircraft system team, or work with the commander to task organic patrols to gather required information through observation or tactical questioning (TQ).
 - Conduct planning, synchronization, and request for assets.
 - Ensure all casual and regular informants are entered into the informant contact log and have been entered into the BAT system.
 - Coordinate with the BN S-2 and human intelligence collection team for review of products and the assignment of contact tracking numbers.
 - Facilitate walk-in informants.

- Establish an informant meeting and debriefing area, and ensure that security personnel are prepared to receive local national informants:
 - * The meeting room should have chairs or couches, a table, drinks available, an ashtray, large-scale unmarked maps for map-tracking purposes, and no windows.
 - * 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.
 - * COISTs are not authorized to task a source. They may request information from local nationals and other willing informants.
- Manage the patrol prebrief and debrief processes for the company. The patrol prebrief is not to be confused with the patrol order given by the patrol leader. The prebrief is generally given by a member of the COIST to the patrol prior to departing the forward operating base, combat outpost, or joint security site. The prebrief is perhaps the most important function of the COIST. During this brief, the team shares events that occurred in the OE over the past 12–24 hours, route status, ISR collection assets in use throughout the BN's OE, SIR tasked to answer, other units operating within the OE, BOLO lists, applicable target packets, and predictive analysis based on analysis during the targeting phase. During this process, outgoing patrols are briefed on the following:
 - Current threat assessment for the AO with regard to significant activities in the last 24 hours.
 - Current IED threats and locations of concentrated IED attacks.
 - Enemy activity expectations for the next 24 hours.
 - Current HVI list with pictures if possible.
 - Information requirements.
 - Possible TQ guidance.

The debrief, when based on a solid prebrief, feeds the COIST with data to continue its IPB and ultimately help begin the next targeting cycle for the company. The debrief should provide feedback on all areas covered in the prebrief as well as provide updated pictures and may also include data from detainee operations and site exploitation. Other important points regarding debriefs include the following:

- Debrief incoming patrols to develop the common operational picture for the company AO.
- Ensure a standard and approved debriefing form is used to record all pertinent information.

- Post updated intelligence information for ease of reference by patrol leaders, and consider operational security when choosing a location in which to post the information.
- Identify little-known areas within the company AO that require informal assessments by patrols to identify the following:
 - * Areas
 - * Structures
 - * Capabilities
 - * Organizations
 - * People
 - * Events
- All debriefs should be entered as quickly as possible as a text report in TiGR so information can be entered into the database and shared throughout the unit's OE.

Detainee Operations

Detainee operations for the COIST are twofold:

- Ensure departing patrol units are armed with complete detainee packets and the knowledge to properly complete the forms and use the equipment.
- Maintain detainee packet data, copies of complete packets, and track the current location and status of the company's detainees.

Site Exploitation

This function is similar to detainee operations in that the COIST must ensure units depart on patrols trained and equipped with the proper site exploitation paperwork and equipment. Upon completion of the patrol and following debriefs, the COIST sorts through photos collected, downloads biometric data, and manages databases. It is here that the COIST once again begins its data synthesis to update its targeting, thus beginning the cycle again. The COIST submits document and media exploitation material to higher headquarters in a timely manner.

COISTS must ensure company-level TQ does not inadvertently become unlawful interrogation by adhering to the following guidance:

- TQ will involve direct questions only.
- TQ will not use interrogation approaches, defined as “any means used to entice a detained person to give information he would not normally give.” At no time will TQ involve threats directed at the detainee or his family.

Conclusion

The COIST is not manned, equipped, or authorized by a modified table of organization and equipment but is commonplace in deployed companies due to terrain, distances, and the decentralized nature of operations being conducted in theater. COIST functions are performed through an ad hoc arrangement of personnel, equipment, communications, and procedures employed by a company commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the company's assigned mission. Companies do not possess specialized staff personnel to perform this mission and must constitute COISTs out of hand. Regardless of how large or how well manned, the COIST must facilitate the collection, analysis, and dissemination of information both up and down the chain of command. Providing accurate, timely information assists, informs, and enables the commander to make key decisions and effectively manage unit resources. The Army has formally recognized the need for a COIST, and a pending force design update, when implemented, will address this requirement.

Chapter 2

Company Intelligence Support Team Organization

Companies, regardless of function, are currently neither authorized nor staffed for company intelligence support team (COIST) operations. As mentioned in chapter one, a force design update will address this shortcoming. In the meantime, tough decisions regarding manpower and personnel are necessary. Every Soldier or leader involved in COIST operations is one less Soldier or leader who can be sent on patrol, provide security, or man a quick reaction force.

That being said, most commanders with combat experience in theater believe the contributions of the COIST are well worth the costs associated with resourcing it. There are multiple ways to man the COIST. However, a good rule to follow is, "If it doesn't hurt, it's probably not the right personnel." The payoff for manning the COIST appropriately is large dividends in the volume, timeliness, and value of information passed to the commander, his subordinates, and leaders to drive operations.

The overall goal of the COIST is twofold:

- Aids the company commander in his decision making by bringing a fused intelligence picture down to the company.
- Assists the battalion (BN) by providing a flow of bottom-up intelligence to higher units.

While the COIST is a company asset, its effectiveness is contingent on its ability to fuse diverse forms of information from both inside and outside the company sector into a picture that will aid the company commander in his decision making. The quality and format of the information one COIST provides have a direct impact on the success of its adjacent units and thus these things must be managed from the higher (BN) level. Consequently, the BN intelligence officer (S-2)/COIST relationship is critical to the success of the BN. BN S-2 shops typically have very limited manpower and therefore must set themselves up for success by putting significant effort into the COIST processes.

Battalion Intelligence Section

The creation of systems whereby the BN receives analyzed intelligence products rather than raw information will reduce the overall workload on the BN analysts and lead to the creation of better intelligence products at all levels. To achieve this effect, the S-2 needs to provide five things to the COIST:

- Training
- Standing operating procedures (SOPs)
- Guidance
- Feedback
- Advocacy

Training

A typical maneuver BN only has school-trained Military Occupational Specialty 35F Intelligence Analysts within the BN S-2 shop. While mobile training teams provide a baseline of training to most COISTs, many Soldiers never attend due to moves within the company, so the S-2 shop must step up to ensure these individuals receive basic analytical training.

In addition to basic analyst tasks, S-2 shops owe their COISTs training on aspects of the intelligence fight specific to their particular area of operations (AO). Examples of training would be the following:

- Instruction in the BN standard 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 COIST improves, more complicated tasks such as intelligence preparation of the battlefield (IPB), development of enemy courses of action, and writing of company intelligence requirements (IRs) should also be taught. If the BN S-2 takes a hands-off approach to the training of the COISTs, their effectiveness will be greatly diminished upon arrival in the combat zone.

SOPs

The BN S-2 owes the COIST detailed SOPs on all aspects of COIST operations. Again, the format and quality of information posted by one COIST have a direct impact on the success of adjacent COISTs and thus must be managed from the higher level. The SOPs required generally fall into four broad categories:

- Primary, alternate, contingency, and emergency communications
- Reporting requirements
- Intelligence synchronization products
- Databasing and knowledge management guidelines

Some common examples of procedures the BN S-2 owes the COIST are the following:

- Battalion debrief SOP.
- Targeting products SOP.

- Daily intelligence summary/graphic intelligence summary SOP (or whatever format is used to pass information between company and BN level).
- Data entry SOPs for the various Tactical Ground Reporting (TiGR) System functions (significant activities, human intelligence reports, signals intelligence reports, personality entry, place entry, and area cataloging).
- SOP for the format of products produced by company-level ISR systems (unattended ground sensors, Raven, integrated communications (ICOM) scanners, Rapid Aerostat Initial Deployment towers/Cerberus towers, and biometric data systems).
- SOP for the immediate exploitation and then passage of information gleaned from site exploitation.
- SOP for the exploitation and transportation of detainees.
- Other SOPs a BN S-2 might determine apply to a specific AO.

The BN S-2 must use his understanding of the overall intelligence fight as well as his knowledge of the specific capabilities of various ISR and analytical platforms when developing these SOPs. The basic guideline is the SOPs must be understandable to Soldiers at even the most junior level. They should be written in a way that maximizes the use of digital systems to make the company's information searchable to adjacent units. Commanders need to recognize the creation of these SOPs is an extensive amount of work for the BN S-2 shop but is necessary to ensure a smooth flow of information throughout the BN sector.

Guidance

While the COIST works for the company commander, the company is in fact the best intelligence asset in the BN's possession. As a result, the company will be often tasked to answer BN-level IRs. The information a BN commander needs to be successful can at times be broad and extremely complicated. The S-2 must work to redefine this broad swath of necessary information into clear and specific information requirements (SIR) and then work with the S-3 (operations and training officer) to task these requirements to the appropriate units. Ideally, they will be pushed to the company as part of the BN daily fragmentary order in the form of specific orders and requests (SOR) or intelligence taskings. The S-2's work does not end here, however, as he must ensure the company tasked with the IRs has a clear understanding of the meaning and importance of the request and then develop an adequate method of tracking the results. His interaction with the COIST will be crucial to ensuring these BN-level IRs are answered in a timely and effective manner.

Feedback

The BN S-2 owes the COIST clear and useful feedback on all products it produces. COISTs that believe they are operating in a vacuum and no one is looking at the work they present will invariably produce substandard products. Feedback on whether products such as debriefs and area assessments are meeting the intent for

the BN can easily be entered through the comment feature on TiGR but is best offered in a discussion between the S-2 and the COISTs. This discussion usually takes the form of a meeting (either face-to-face or over a digital communications system) between the S-2 shop and COISTs to discuss the information that has flowed into each company sector during the week and also the status of any IRs that have been answered or remain unanswered. The more feedback the COISTs receive on their piece of the intelligence effort, the better the results will be for both the company and the BN.

Advocacy

The understanding of COIST operations is still at a low level within the Army. Often the positive effects of a successful COIST may be invisible to a company for many months, and the commander and first sergeant may wonder why they have sacrificed four to six Soldiers toward this effort. The S-2, however, should always be looking at the big picture of the BN's intelligence fight and therefore should always understand the effect of the COIST. The BN S-2 is often the individual who must fight for the most capable Soldiers to be assigned COIST duties. The S-2 must also fight to limit the number of side or distracter taskings that COIST members encounter. Finally, the S-2 will know the origin of effective intelligence and must ensure that company and BN commanders are aware of what successes have resulted from the hard work of the COIST. Only by sharing the successes of effective COISTs can the BN bring about a general understanding of the importance of their efforts.

Overall, the successful implementation of COISTs involves extensive effort on the part of the BN S-2. If the S-2 fails to do the required preparatory work, his own effort to effectively utilize the COIST will likely fail. S-2s must put in the required planning to ensure the fused intelligence picture is pushed to the company level. COISTs must understand that no matter what their geographic disposition, their efforts are not isolated, and a failure to implement the guidance and SOPs of the BN S-2 could lead to their own failure as well as a weakening of their adjacent units' COIST efforts. Commanders at all levels must understand the S-2/COIST relationship to ensure effective flow of intelligence from the lowest levels up, which will ultimately ensure the success of the unit in intelligence-based operations.

The company commander is a key player in all aspects of company-level operations. This is especially true when it comes to the structure, manning, and integration of the COIST. The commander and his subordinate leaders can greatly increase the effectiveness of the COIST by selecting the best qualified individuals for this duty. The personnel selected should:

- Possess or be able to be granted a secret security clearance.
- Possess strong analytical aptitude.
- Have an ability to think, speak, and write clearly.
- Possess strong computer skills and normal color vision.
- Understand battle tracking, and have an ability to organize information.

- Understand how to work with intelligence system hardware and software (see Chapter 3).
- Possess operational experience to understand what information is important and how to present it.

It is also important the COIST has a sufficient number of personnel to conduct continuous 24-hour operations.

Leaders in the COIST must be vigilant in the following areas to derive the most benefit from the organization:

- Enforce the debrief standards.
- Enforce priority intelligence requirements (PIRs), SIR, and SOR (commanders cannot allow their IRs to stagnate).
- Follow SOPs.
- Maintain regularly scheduled communication with higher headquarters' staff.
- Maintain and retain COIST personnel once they have been trained.
- Minimize distracter tasks for the COIST.

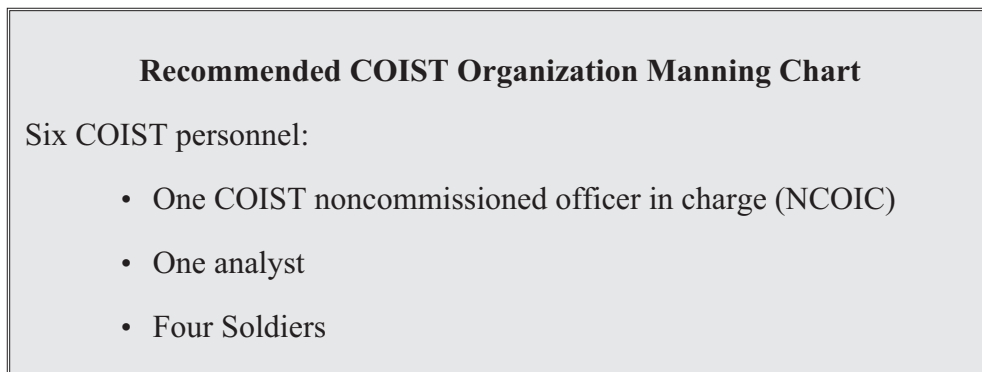


Figure 2-1

Company Intelligence Support Team Leader/Soldier Responsibilities

Company commander responsibilities include the following:

- Creates, equips, selects, and trains personnel.
- Integrates COIST into all aspects of company-level operations:
 - Military decision-making process

CENTER FOR ARMY LESSONS LEARNED

- Targeting
- Patrol briefing and debriefing
- Listens and acts on the analyses and recommendations of the COIST.
- Allocates space for execution of COIST responsibilities and functions.
- Provides guidance and direction on information presentation, and approves PIRs.

The COIST NCOIC has the following responsibilities:

- Supervises intelligence operations within the company.
- Responsible for all COIST actions and operations.
- Gives updated enemy threat briefs to patrols prior to start point time.
- Ensures COIST members are tasked appropriately and identifies priorities of work.
- Ensures priorities are completed and analysts have time and appropriate area to work.
- Acts as liaison between the COIST and higher echelon S-2 sections.
- Requests BN intelligence and collection assets for company and platoon operations, and synchronizes collection efforts and priorities with the BN S-2.
- Assists in the preparation of indicators to satisfy PIRs.
- Manages all current and emerging targets, and ensures target packets are created to facilitate servicing of targets.
- Recommends to the commander when a target is actionable and what assets are available.
- Responsible for and recommends options to the commander on nonlethal fight operations.

The COIST analyst is responsible for reading, interpreting, researching, and analyzing intelligence and information pertaining to the company's operational environment. Additional traits and responsibilities include the following:

- Most knowledgeable and informed member of the COIST (debriefs and prebriefs, communicating with the BN S-2 analyst).
- Makes recommendations and gives the commander his "best guess" based on information he obtains.
- Updates PIRs, SIR, and SOR from the commander.

The COIST Soldiers' responsibilities include the following:

- Prepare intelligence products to support the commander/company.
- Assist in establishing and maintaining systematic, cross-referenced intelligence records and files.
- Receive and process incoming reports and messages.
- Assist in determining significance and reliability of incoming information.
- Assist in integrating incoming information with current intelligence holdings.
- Prepare and maintain the situation map.
- Assist in the analysis and evaluation of intelligence holdings to determine changes in enemy capabilities, vulnerabilities, and probable courses of action.
- Assist in the preparation of order of battle records using information from all sources and the preparation of estimates of enemy unit and organization strengths and capabilities.
- Assemble and proofread reports and assist in consolidating them into military intelligence.
- Prepare IPB products.
- Assist in the preparation of reports on captured enemy material.
- Draft periodic and special intelligence reports, plans, and briefings.
- Brief and debrief patrols.

Materiel

To effectively perform its functions, the COIST should be equipped with dedicated computers and access to communications equipment. The COIST 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 via TiGR, if available.

Currently the Army resources mapping through Falcon View, the Distributed Common Ground System–Army, or Aeronautical Reconnaissance Coverage Geographic Information System mapping applications; personality linkage through Analyst Notebook, an analyst development tool; and event linkage through Crystal software application. However, units are currently fielding newer, updated software such as Analysis and eXploration of Information Sources Professional (AXIS Pro) (see Chapter 3).

CENTER FOR ARMY LESSONS LEARNED

A suggested equipment and materiel list includes:

- Equipment:
 - 3x workstations (2x SECRET Internet Protocol Router [SIPR]/1x Non-Secure Internet Protocol Router [NIPR])
 - Laptop computer
 - AXIS Pro/Analyst Notebook (AXIS Pro is replacing Analyst Notebook)
 - TiGR
 - Falcon View
 - Microsoft Internet Relay Chat (mIRC) or other chat capability software
 - Microsoft Office Suite
- Systems:
 - Biometric Automated Toolset and Handheld Interagency Identity Detection Equipment
 - One System Remote Video Terminal
 - Cellular exploitation/CelleBrite handheld, portable forensic device for cellular phones
- Materiel:
 - Color printer, scanner, and copier (1x SIPR/1x NIPR)
 - Safe
 - Secure Voice Over Internet Protocol phone
 - Digital camera
 - In-focus projector
 - Shredder
 - Maps
 - Tent, tables, chairs, dry-erase board, power source, lights, and environmental controls (air/heat)

Location

The COIST must stay current on all operations and should be collocated with the company command post, which allows it to communicate directly with the BN S-2 as well as units on patrol. Further, its proximity to radios increases situational awareness. Again, to maintain continued intelligence collection and analysis, the COIST serves as a function of the command post. Do not use the COIST to run the company-level command post. Control measures must be established so sensitive material is only seen by those with appropriate access. The proximity of the COIST to the primary company command post is essential to enable the COIST to have timely situational awareness and always be up to speed on current company activities. The COIST also requires close access to the company decision maker (commander, first sergeant, or executive officer).

Figures 2-2 and 2-3 depict a way to lay out a COIST for operations in a tactical environment. The graphics depict what a COIST should be able to produce and disseminate and represent what should be included and displayed on a COIST wall, not how it should be arrayed. The COIST should tailor the location of its products to best suit briefing the individual company and its commander.

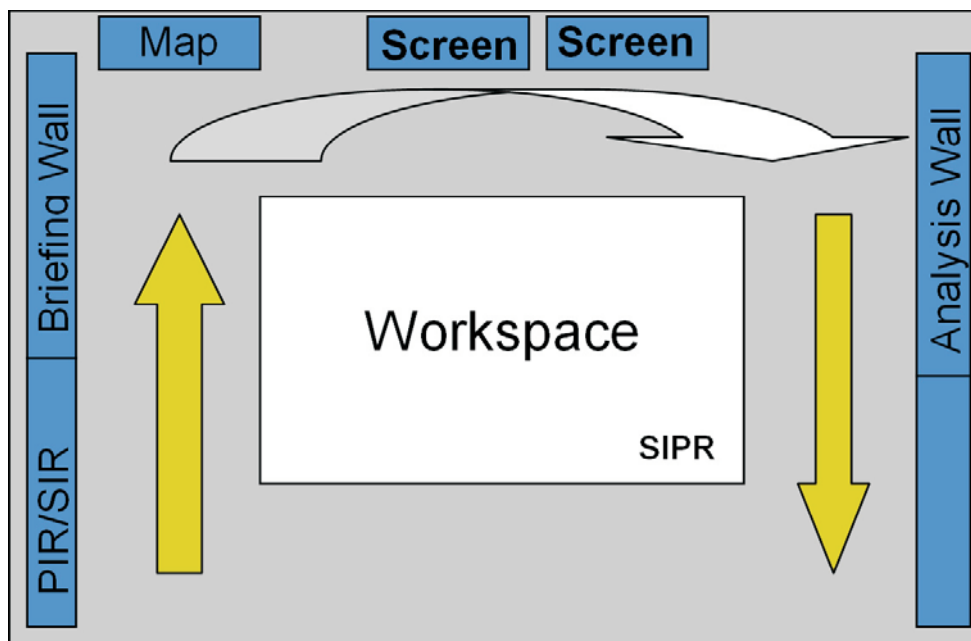


Figure 2-2. COIST physical layout

The analysis area of the COIST is where all the intelligence analysis tools are located so they can be used as efficiently as possible. The briefing area of the COIST is where all the products for the outgoing patrol leader, convoy leader, or commander are consolidated. The area facilitates a focused one-stop location where all available information is displayed and disseminated.

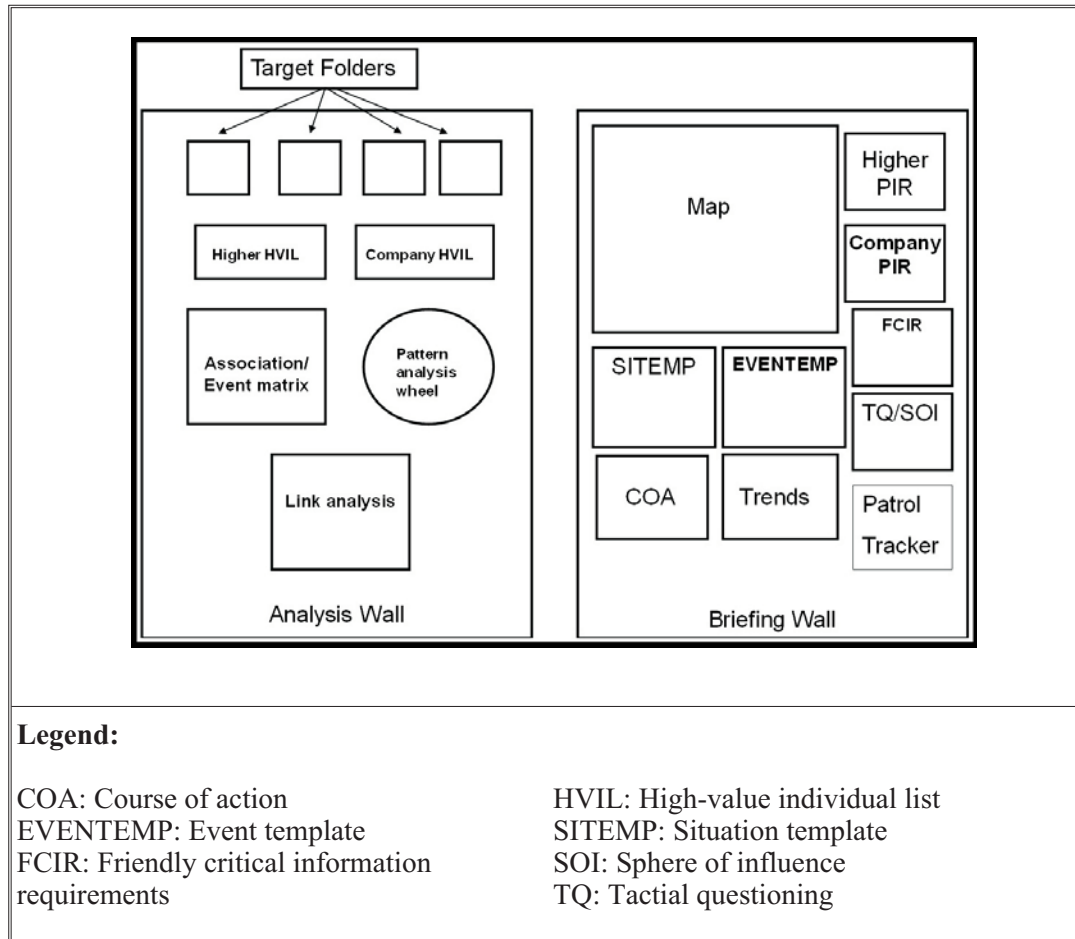


Figure 2-3. COIST product display

The COIST should establish a patrol tracker separate from the operations patrol tracker. The patrol tracker is designed to assist the COIST in identifying patterns and TTP the company is creating. During the patrol prebrief, the briefer should recommend certain actions to the patrol leader, such as leaving at a different time or taking a different route.

Conclusion

Intelligence-driven operations have become a cornerstone of the contemporary counterinsurgency fight. Senior tactical commanders are requiring more of their subordinates. Accordingly, companies are establishing COISTs. The COIST mission, function, and resource requirements are known or can be determined; however, its success in combat will be limited if the requirements are not adequately addressed. The secret to its success is commander involvement, leadership, and participation. The commander’s mission and intent are critical to the COIST as they provide PIRs, SIR, SOR, and indicators. Additionally, the commander must establish clear priorities to assist the COIST in the execution of his intent. The commander will set the tone by selecting, training, and assigning the correct personnel for the job and by integrating the COIST, its capabilities, analyses, and recommendations into operations and planning.

Chapter 3

Company Intelligence Support Team Systems and Tools

To accurately conduct predictive analysis on enemy activity, the company intelligence support team (COIST) must accurately track and analyze enemy activity. In addition to tracking events, the COIST must be able to display and brief the information to the commander and the unit. There are many methods for collecting and tracking data on the enemy and events. The data must be tracked daily; however, whatever the method chosen to conduct analysis, the COIST must conduct weekly and monthly event analyses to determine patterns of enemy events (i.e., time, place, and type of activity).

The COIST is responsible for collecting and archiving data at the company level for use at all echelons. It also maintains a local database for use in company operations and planning. Additionally, given the capability, the COIST can search existing databases and update the company database or gather information to fill intelligence gaps. To manage company information, the COIST must establish a filing system for information gained by the unit.

The COIST will have access to several systems and tools to aid in the collection, analysis, reporting, and dissemination of information. These systems and tools can help build an accurate intelligence picture within the company area of operations (AO). Some of these tools are just now becoming common at the company level, while others are traditional skills and systems that have been available for some time.

Systems and Tools

Digital cameras and photographs

The digital camera can be an outstanding surveillance and recording tool for patrols. A patrol armed with a digital camera can bring back dozens of images to the COIST that provide detailed data and additional information and insight. For example, operational use of digital cameras has proven valuable to identify both friendly and enemy key personnel.

Figure 3-1 is an example photo that would come from the patrol's photograph log. The photograph and marginal information should be updated as soon as possible after each patrol when practical. Note that in the example, the date-time group, unit identifier, and Military Grid Reference System (MGRS) are on the photograph. The direction and photograph series number are also printed on the photograph. The narrative that accompanies this digital photograph could read as follows:

Platoon Sergeant Smith: Picture of Alpha Company western ECP (entry control point). The al-Nafar tribe is protesting the lack of water in the town. The police chief and his lieutenants are being escorted into the company reception area. The main instigator of the protest is circled and is believed to be Abu Haneffa.



Figure 3-1. Example digital photo

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

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 the battalion (BN) for further exploitation. To support this mode of collection, the COIST should establish a picture log. This log will have a company/patrol identifier with date, picture number, and location using the MGRS. It also indicates where the photograph was taken, general direction of the photograph, and any other amplifying remarks. The picture number may have a unit coding system so other people can easily identify which unit took the photograph.

Photographs must be secured and carefully controlled. COISTs must treat photographs as sensitive information with strict controls and guidance for their handling. For example, if the object of a photograph knows that he is being collected against, he may relocate. This may disrupt other collection methods in place such as human intelligence (HUMINT) and signals intelligence (SIGINT) that are not under the control of the COIST. Additionally, there is always the possibility that our own photographs could somehow be used for propaganda against us or to possibly reveal some of our tactics, techniques, and procedures (TTP).

Video cameras

Although it is not as easy to carry as a digital camera, a video camera can record exactly what happened during significant events witnessed by Soldiers during the conduct of routine operations and patrols. Instead of relying solely upon a verbal debrief, a patrol can show the COIST exactly what happened and review each event in sequence. This data can also be easily passed on to the higher headquarters in its original format, ensuring the analysts at the BN, brigade combat team (BCT), or division level can see everything just as Soldiers on the ground saw it.

Unmanned aircraft systems (UAS)



Figure 3-2. Raven

The Raven is small and can be transported easily in three small cases that fit into a ruck sack. The crew can bring it with them and operate wherever the patrol goes. The Raven has three different cameras that attach to the platform: an electrical optical camera that sends data either through a nose camera or a side camera, an infrared (IR) camera, and a side-mounted IR camera. The IR technology is still too big to fit into the nose section of the platform. The camera does not have a zoom feature and is unable to lock on a target but provides enough resolution to show someone carrying a weapon. The Raven has about 45 to 60 minutes of flight time on one battery. The kit comes with spare batteries and a charger that plugs into a high-mobility multipurpose wheeled vehicle, so the operator can land it, pop in 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 needing landing gear or carefully prepared landing strips. Since it is launched and recovered in this manner, it does not require elaborate support facilities and is ideally suited to a forward-deployed unit. Its automated features and Global Positioning System (GPS) technology also make it simple to operate, and it requires no specially skilled operators or in-depth flight training.



Figure 3-3. Shadow

The Shadow UAS is the brigade commander's primary reconnaissance, surveillance, and target acquisition asset. The Shadow is equipped with an electro-optical/IR camera. It has a range of approximately 100 kilometers, can fly for up to 4 hours, and operates at altitudes between 6,000 and 10,000 feet. One advantage of the Shadow is that it is an in-house intelligence, surveillance, and reconnaissance (ISR) asset that can provide a BN or BCT commander with tactical overwatch whenever needed. The COIST can request use of or information from this BCT-level asset through the BN S-2 as part of the company ISR plan.

Additional COIST intelligence systems

- One System Remote Video Terminal (OSRVT): The OSRVT is an innovative modular video and data system that enables warfighters to remotely downlink live surveillance images and critical geospatial data directly from a joint operations tactical UAS. The OSRVT has the ability to capture all UAS platforms regardless of who tasked them, which means that with the OSRVT a COIST can watch footage of any area that a platform is observing as long as the OSRVT and the asset are linked up digitally. The OSRVT is also small enough to be vehicle-mounted, enabling the commander on the objective to receive real-time information.
- Tactical Ground Reporting (TiGR) System: TiGR is a Web-based application that allows Soldiers to download information into one program. TiGR is the main reporting and database tool for the COIST. It allows for flattening networks and provides situational awareness across the BN and BCT operational environment. The intelligence can include photographs Soldiers have taken with digital cameras, observations Soldiers have made and written in simple text, or detailed maps of the areas gathered by GPS devices. Before leaving on patrol, Soldiers 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 Soldiers do not have to wade through enormous text files. They can click on a roadside bomb icon, for example, to see if there is a picture showing where the bomb was hidden, how it was disguised, and any TTP related to the specific device.

- Analysis and eXploration of Information Sources Professional (AXIS Pro): This is the system that is replacing Analyst Notebook and is installed on Distributed Common Ground System–Army (DCGS–A) systems. It performs many of the same functions as Analyst Notebook (e.g., link diagrams) but is more user friendly because it reduces the amount of time analysts spend on data input. AXIS Pro is a visualization tool. It allows analysts to find data of interest, organize and refine the results, and then visualize the results and detect patterns. AXIS Pro also allows the analyst to manage data through visualization; AXIS Pro automatically loads new data as needed, freeing the analyst from the need to perform additional searches, import extra data, or build case files. AXIS Pro provides a two-way connection to multiple data sources. The analyst can build link diagrams using information from multiple data sources and then create, edit, or delete that information and add changes directly to the data source. AXIS Pro provides a simple multi-intelligence analysis toolset. AXIS Pro extends AXIS core features to provide integrated analysis, data management, and intelligence visualization capabilities. AXIS Pro aids the analyst in the process of creating intelligence from large amounts of information. AXIS Pro base capabilities include link, temporal, pattern, and geospatial analysis tools; net centric alarm and alerts; automated entity and relationship extraction from text documents; and an integrated Web portal for information searching and sharing. Additionally, to facilitate interoperability, AXIS Pro comes standard with adaptors for plotting information to additional maps, importing and exporting to both Microsoft Excel and other link analysis tools, and can be configured to work with structured query language servers. AXIS Pro can also be customized to work with other data sources.
- Document and media exploitation (DOMEX) and cellular exploitation (CELLEX): DOMEX capabilities at COIST level are extremely limited. Beyond limited on-scene analysis for rapid decisions or targeting, the COIST must forward DOMEX data and material to a higher-level headquarters where DOMEX can be conducted. The COIST should know how to request and access analyzed DOMEX data. COISTs will have CELLEX kits and possess the capability to conduct limited CELLEX. DOMEX will support a wide range of intelligence activities to include all-source analysis, open-source exploitation, HUMINT, SIGINT, geospatial intelligence, and measurement and signature intelligence. DOMEX reporting and analysis are considered intelligence products.
- Combined Information Data Network Exchange (CIDNE): CIDNE is a secure Internet host site that contains an engagement tool for tracking three types of entities: people, facilities, and organizations. Additionally, CIDNE is the primary means by which HUMINT collection team (HCT) reporting is fused into the theater intelligence database (BCT/HUMINT officer [S-2X]/military intelligence company/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 operational environment 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 on industry standards. TiGR, addressed above and which the COIST will have, is capable of pulling and displaying CIDNE information.

- **Ground Movement Target Indicator (GMTI) Tracking:** Tracking can be done using GMTI-type indicators that can observe all the objects moving in the area of interest. GMTI measurements supplied by the sensor are assumed to belong to the road network. On the basis of this assumption, several techniques have been studied to take this information into account. GMTI products should be requested from the brigade S-2 through the BN S-2 as part of the company ISR plan. The COIST does not have the capability to receive and interpret direct GMTI feeds.
- **Microsoft Internet Relay Chat (mIRC) (or Jabber chat):** mIRC is a system that allows the COIST to both monitor multiple situations at once and communicate instantly across the battlefield with anyone who is connected. Chat is a primary means of communicating in theater and is the most common means for communicating with theater-level assets, such as full-motion video. mIRC is similar to any instant messaging application found on the Internet. COIST personnel can monitor a number of chat rooms depending on their preferences. The COIST needs someone to monitor mIRC at all times because of the time-sensitive information that moves across it. Monitoring mIRC will not be the only job this individual performs, but the assigned Soldier will be responsible for checking it constantly. It is suggested the Soldier monitoring mIRC has a maximum of five windows on his computer open at any one time to ensure information overload does not occur. Many units are beginning to transition to Jabber chat—both systems have similar capabilities.
- **Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE) systems:** BAT collects fingerprints, iris scans, facial photos, and biographical information on persons of interest into a searchable database. It is used for tactical operations, detainee operations, base access, improvised explosive device (IED) forensics operations, and local hire screening and intelligence. HIIDE collects and matches fingerprints, iris images, facial photos, and biographical contextual data of persons of interest against an internal database. HIIDE is interoperable with BAT for biometrics data exchange back to the Department of Defense biometrics data repository.

Intelligence, Surveillance, and Reconnaissance Request Procedures

When the COIST requests ISR assets, it should request a capability and not an asset (i.e., “A company requests full-motion video,” not “I need a Shadow/Predator”). The reason for this is that if the COIST requests an asset and that particular asset is not available, the COIST will not receive any support. If the COIST requests a capability (such as IR or full-motion video), it will get support from whatever asset is available with that capability. Additionally, units should include a task and purpose and how/when the information needs to be collected.

All ISR requests will be sent up to the BN, consolidated, and, if necessary, requested from brigade. The COIST needs to be as specific as possible when

explaining why it needs a particular capability. The demand for ISR assets is extremely high, and the COIST needs to be able to convince higher headquarters what it needs is a priority and all other organic assets have been exhausted.

Maps

There are several environments where standard 1:50,000 maps or even satellite imagery collected years ago are insufficient, inaccurate, or simply not available. The COIST can assist Soldiers and patrols by requesting the most updated map and imagery data through the BN S-2. Additionally, Soldiers operating in these areas will instinctively scout them to increase their familiarity with new surroundings and must record the information they find and report it for appropriate dissemination (i.e., within the company as well as to higher and adjacent units). They do this by improving either existing maps or creating usable sketch maps of key areas. Then, to prepare units that may have to patrol or fight in this area in the future, the COIST should update its maps of the area and disseminate this information up, down, and laterally. Maps can be updated in TiGR, and updates can be viewed by anyone with TiGR access.

Sketch maps: overlays

This basic map skill should be known and practiced at the squad level. A Soldier can produce an adequate sketch map using a sheet of paper, pencil, straight edge, and any known reference point. The process can be as simple as tracing grid lines from an existing map and adding details such as new trails, bridges, or anything of importance that is not on the issued map. For example, a 1:50,000 map may not contain a series of irrigation canals that severely restrict cross-country mobility alongside an important main supply route. When this is known, the COIST might designate this location as a potential site for future enemy ambushes.

Graph paper is particularly useful for creating sketch maps. In this case, a patrol can be dispatched to the area with the current map, paper and pencils, straight edge, and other tools such as the Precision Lightweight GPS Receiver, Defense Advanced GPS Receiver, compass, and graph paper and sketch in the details about the irrigation canals and bypass routes. The COIST can then reproduce this sketch map on overlays on separate sheets of paper for dissemination within the company and to higher and adjacent units. The next step is to update the maps within the company command post.

Field sketches

The field sketch is closely akin to a sketch map, but in the absence of a digital camera, it will include sketches of an objective, key facility, or other important area to aid commanders in planning. An example would be an observation post producing a sketch of a compound suspected of containing enemy forces. This sketch can be given to the commander to identify details that require additional planning, aid the assault force in identifying the target building, and possibly even save time by eliminating the need for a full leader's reconnaissance.

Field sketches are obviously not as useful as digital photographs in terms of presenting a picture and they are certainly more difficult to disseminate, but they are another tool available for collectors to pass on information to those who need it.

Conclusion

The COIST will have access to several systems and tools to aid in the collection, analysis, reporting, and dissemination of information. These systems and tools can help to build an accurate intelligence picture within the company AO. However, to be used effectively and as significant enablers, Soldiers and leaders assigned to the COIST must be familiar with their operation, characteristics, and capabilities.

Chapter 4

Company Intelligence Support Team Battle Rhythm

Battle rhythm and operational tempo (OPTEMPO) are critical aspects of both command post (CP) and company intelligence support team (COIST) operations. An established, effective, and understood battle rhythm assists in efficiency and shortens the time required to share information. The commander is responsible for establishing the COIST battle rhythm. Although the purposes and missions of the CP and the COIST are different, the two entities are collocated. Even with a necessary and clear delineation of duties and responsibilities, some overlap and redundancy will occur between the CP and the COIST. This potential overlap occurs primarily because at the company level commanders do not have staffs; therefore, the company battle staff becomes those personnel in the unit who operate the CP and the COIST. This chapter begins by looking at the overall company battle rhythm and then focuses on COIST and intelligence-specific considerations.

Successful continuous operations at the company level are more demanding than at higher-level organizations. The unit requires a tactical standing operating procedure (SOP) allowing rest, especially for critical personnel. At company level, the commander and first sergeant will find it very demanding to try to rest. Their rest plan must be a priority for the organization to be led effectively and for their units to be successful on the battlefield.

The cycle of recurring events within a CP/COIST focuses the leaders and Soldiers on meeting information and action requirements. Company personnel are normally required to attend battalion (BN) and company recurring meetings, which has an impact on company CP/COIST operations and schedules and must be incorporated into the small unit's battle rhythm. Examples of recurring events include the following:

- Shift changes
- Battle update briefings to the commander
- BN battle updates without the commander
- BN targeting meetings
- BN reports
- BN commander's collaborative sessions
- Company CP officer in charge (OIC) and noncommissioned officer in charge (NCOIC) shift change briefings and collaborative sessions

The company CP and COIST OIC and NCOIC must achieve battle rhythm for updating and viewing information and understanding how to use it to affect operations. A well-established battle rhythm aids the commander and leaders with the CP and COIST organization, information management and display, decision making, and fighting the battle. Battle rhythm demands careful planning and design. Many competing demands must be deconflicted. Even subordinate platoons

and sections affect a company battle rhythm based on their needs and unit procedures.

The company CP and COIST should be staffed for 24-hour operations; however, the company must also conduct cyclical missions. SOPs establish methods of ensuring the right personnel are available for either cyclical or 24-hour operations. Regardless of the method used, practice during exercises will determine the strengths and weaknesses of headquarters personnel for CP and COIST operations and the training required for additional personnel who may be used to staff the CP and COIST during continuous or sustained operations. Such knowledge allows leaders to focus on the critical areas and personnel requiring additional training.

In planning, company and COIST leaders must consider battle rhythm requirements of subordinate platoons, sections, and squads. Depending on the situation, the company may schedule missions that allow platoon or section/squad rotations to maintain their battle rhythm.

Absence of Battle Rhythm

Without procedures establishing battle rhythm, leaders and units reach a point of diminished returns. This point typically occurs between 72 and 96 hours of continuous operations. As leader fatigue sets in, information flow, planning process, execution, and sustainment suffer, often greatly. Symptoms of diminished battle rhythm include the following:

- Leader fatigue
- Leaders not fully aware of critical decision points
- Leaders not available at critical decision points
- Disjointed timelines between various levels of command

Presence of Battle Rhythm

Battle rhythm allows units and leaders to function at a sustained level of efficiency for extended periods. Effective battle rhythm permits an acceptable level of leadership at all times. It can focus leadership at critical points in the fight or during particular events. Procedures and processes facilitating efficient decision making and parallel planning are critical to achieving battle rhythm. Every component of battle rhythm contributes uniquely to sustained operations.

Training

It is difficult, if not impossible, to establish battle rhythm while simultaneously conducting operations. Preplanning makes battle rhythm happen. Planning, preparing, and training before deployment lay a solid foundation for viable battle rhythm during operations. Commanders must ensure all company personnel are trained on CP setup and operations and they understand the team concept required to conduct CP and COIST operations during combat operations for extended periods. Additionally, company commanders must coordinate with BN staffs during training to deconflict staff operations and requirements counterproductive to the company battle rhythm.

Battle Rhythm Elements

Battle rhythm is a multifaceted concept that includes the following elements:

- Sleep/rest plans
- Trained second- and third-tier leadership in CPs and COISTs
- Synchronized upward multiechelon timelines
- Parallel planning
- Established processes and SOPs

Command Post Personnel Depth

Established processes and SOPs relieve many antagonistic effects of extended operations. SOPs that establish and maintain battle rhythm by facilitating routine decisions and operations are a step in the right direction. Soldiers trained to act appropriately in the absence of leaders or orders can relieve commanders and leaders of many of the time-consuming tasks that rob them of essential rest. Examples of tasks noncommissioned officers (NCOs) and junior officers can accomplish for the commander include the following:

- Battle summaries and updates during a fight
- Intelligence updates before, during, and after a battle
- Sustainment updates before, during, and after a battle
- Updates to the next higher commander
- Shift change briefings

Noncommissioned Officer and Junior Officer Responsibilities

At the company level, all personnel are critical to the success of the operation and provide valuable contributions. It is imperative commanders ensure each Soldier understands the importance of even the most menial tasks, such as CP security and tactical operations center setup and teardown. Given the amount of personnel in a company, 24-hour operations, and force protection requirements, commanders must utilize all personnel available to successfully accomplish CP and COIST operations. The improper use of personnel produces the following results:

- Key leaders become exhausted.
- CP and COIST operations-trained personnel become exhausted.
- The initiative of trained subordinates is stifled, and the incentive to train is diminished.

The following techniques ensure proper use of personnel:

- Appropriate tasks are assigned to junior NCOs and specialists.
- Effective training and SOPs instill trust in officers and confidence in junior NCOs and specialists.
- Effective command guidance conveys to the company that the operation is a team effort and all personnel available contribute to the effort.

Continuous Operations and Timelines Synchronization

Timelines for the operation at hand must allow for not only the next operation but also extended continuous operations. Synchronized, multiechelon timelines assist units in achieving battle rhythm. If units do not address critical events at least one level up and down, disruption results. An example of an unsynchronized timeline is a BN rehearsal that conflicts with platoon precombat inspections or other events in its internal timeline. Lower echelon units as well as platoons and sections seldom recover from a poor timeline directed by a higher headquarters. Company commanders must coordinate with their BN staffs on developing SOPs that include planning, rehearsal, and execution timelines one level below BN to prevent these conflicts.

Standing Operating Procedures Utilization

SOPs must be practiced and reviewed during professional development and sergeants' time. The existence of an SOP will not resolve troop-leading challenges unless the SOP is practiced often and internalized by unit members. Checklists are critical, as many leaders will often find themselves rushed, physically fatigued, distracted, and deprived of sleep. Checklists ensure each step is considered even when leaders are exhausted.

Company Intelligence Support Team-Specific Battle Rhythm

The COIST must establish an internal SOP and battle rhythm that outline both recurring cyclic events, such as meetings and shift changes, and also incorporate the intelligence battle rhythm of its higher headquarters. While the exact times and requirements may vary from unit to unit, the following outline can be used as a baseline template to assist companies in developing a predictable, routine, and sustainable tempo to COIST operations:

- Daily:
 - Facilitate and collect patrol debriefs (senior COIST Soldier).
 - Conduct mission prebriefings and debriefings for patrols and operations (COIST analysts).
 - Review and analyze patrol debriefs (COIST OIC/NCOIC).
 - Conduct data processing, and update maps, templates, and graphics (COIST analysts).

- Supervise detainee packets (COIST OIC/NCOIC).
- Provide deception recommendations as required (COIST OIC/NCOIC).
- Exchange data with the BN S-2 and brief the commander (COIST OIC/NCOIC).
- Collect, report, and disseminate through pertinent channels site exploitation and weapons intelligence (senior COIST Soldier).
- Update all trackers and graphs (senior COIST Soldier).
- Update intelligence board for outgoing patrols (senior COIST Soldier).
- Contact adjacent units for intelligence sharing (COIST OIC/NCOIC).
- Update biometric information.
- Weekly:
 - Analyze week's events (COIST OIC/NCOIC).
 - Conduct pattern analysis for the last 30 days (COIST analysts).
 - Refine enemy situational template (COIST analysts).
 - Forecast enemy actions (COIST analysts).
 - Identify potential targets (COIST analysts).
 - Identify and update company, troop, and battery named areas of interest (senior COIST Soldier).
 - Update company, troop, and battery priority information requirements (COIST OIC/NCOIC).
 - Update sewer, water, electricity, academics, trash, medical, and security; and area, structures, capabilities, organizations, people, and events assessments (COIST analysts).
 - Brief commander (COIST OIC/NCOIC).
- Monthly:
 - Analyze month's events (COIST OIC/NCOIC).
 - Analyze patterns for the last 30 days (COIST OIC/NCOIC).

- Produce detailed monthly intelligence summary (INTSUM) (COIST OIC/NCOIC).
- Brief company leadership (COIST OIC/NCOIC).

Intelligence Battle Rhythm

The intelligence battle rhythm is designed around the brigade combat team (BCT) and BN battle rhythm. The intelligence battle rhythm will be adjusted as required by theater and operational requirements. The following schedule can be used as a baseline template to inform and assist companies in planning for and developing a predictable and recurring intelligence:

- Company/BN:
 - 0800 – Shift change slides information cutoff (S-2)
 - 0830 – Shift change slides due to BN battle captain (CPT)
 - 0830 – Company fusion cell (CFC)/S-2 net call via Adobe Connect
 - 0900 – BN shift change
 - 1000 – BN battle update assessment (BUA)/staff synchronization (synch) meeting (S-2)
 - 1300 – BN intelligence, surveillance, and reconnaissance (ISR) synch meeting (S-2, CFC)
 - 1700 – BN collection planning session (S-2, CFC)
 - 1800 – Company collection plan due to BN (CFC)
 - 1900 – CFC INTSUM information cutoff (CFC)
 - 2000 – CFC INTSUM due to BN
 - 2000 – Shift change slides information cutoff (S-2)
 - 2030 – Shift change slides due to BN battle CPT
 - 2030 – BN INTSUM posted
 - 2100 – BN shift change
- Brigade (BDE)/Sensitive compartmented information facility (SCIF):
 - 0800 – BN shift change slides information cutoff
 - 0800 – SCIF shift change slides information cutoff (SCIF NCIOC, operations, fusion, S-2X, collection management and dissemination [CM&D], and signals intelligence [SIGINT])

0900 – BN shift change slides due to BDE
0930 – BDE shift change
0930 – BDE shift change slides due to SCIF
1000 – SCIF shift change
1030 – S-2 conference call via Adobe Connect
1100 – BCT BUA/staff synch meeting (S-2)
1400 – BDE ISR synch meeting (S-2, ISR, targeting, and military intelligence company)
1530 – BCT daily targeting meeting (S-2, ISR, and targeting)
1830 – BN collection plan/asset status update to BCT (ISR)
1830 – SCIF huddle (SCIF NCIOC, fusion, S-2X, CM&D, and SIGINT)
1900 – BN INTSUM information cutoff
2000 – BN shift change slides information cutoff
2000 – SCIF shift change slides information cutoff (SCIF NCIOC, operations, fusion, S-2X, CM&D, and SIGINT)
2030 – BN INTSUM due to BDE (S-2)
2100 – BN shift change slides due to BDE
2130 – BDE shift change
2130 – BDE INTSUM posted
2130 – BDE shift change slides due to SCIF
2200 – SCIF shift change

Figure 4 illustrates the company-level intelligence cycle.

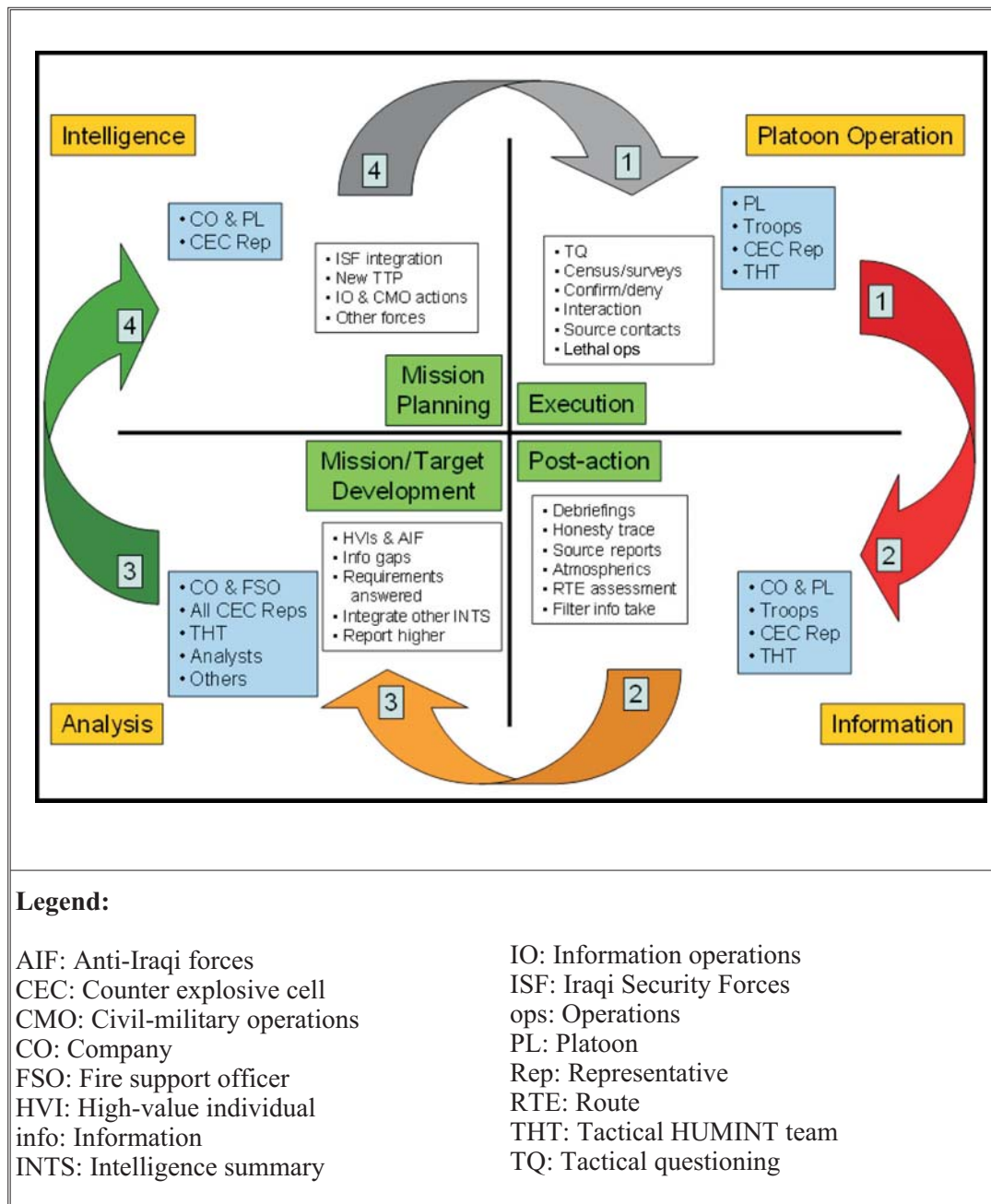


Figure 4. Company-level intelligence cycle

Conclusion

Successful continuous operations at the company level are more demanding than at higher-level organizations due to available personnel and mission requirements. Battle rhythm and OPTEMPO are critical aspects of both company CP and COIST operations. Although the purposes and missions of the CP and the COIST are different, the two entities are collocated. Even with a necessary and clear

delineation of duties and responsibilities, some overlap and redundancy will occur between the CP and the COIST; therefore, the company battle staff becomes those personnel in the unit who operate the CP and the COIST. The relationship between OPTEMPO, battle rhythm, and the unit intelligence cycle necessitates the development of SOPs and tactics, techniques, and procedures that account for and encompass all COIST and intelligence-specific considerations.

Chapter 5

Integration of Company Intelligence Support Team Operations: Platoon Through Brigade

For the company intelligence support team (COIST) to be effective, its activities, analysis, and reporting must be carefully integrated from bottom to top and from top to bottom. Integration encompasses open, two-way information exchange from the platoon level to the brigade combat team (BCT) level. There should be no confusion as to if or how the COIST replaces or negates the need for battalion (BN)- and BCT-level intelligence sections. It absolutely does not! Instead, the COIST is most effective when its work is complementary, supporting, and coordinated with the efforts of existing higher echelon intelligence sections' planning and collection efforts. Although intelligence, synchronization, and reconnaissance (ISR) efforts are undertaken at all levels—company to BCT—one of the primary intelligence-gathering vehicles available at the small-unit level is the patrol. For this illustration of COIST through BCT integration, the patrol will be used to illustrate the connections necessary to achieve complete integration.

Intelligence cells reside at all levels—from BCT to company. At the BCT level, there will be an S-2 section that conducts detailed intelligence analysis of the BCT area of operation (AO). Additionally, the BCT staff serves as a conduit or link to echelon-above-BCT intelligence-gathering systems and platforms. Based on the BCT's mission and commander's intent, the S-2 section in conjunction with the entire BCT staff develops an ISR plan or matrix to answer the commander's priority intelligence requirements (PIRs), assist in targeting, and gather intelligence and indicators to drive tactical operations and orders to subordinate units. These orders and operations can take the form of specific information requirements (SIR) and specific orders and requests (SOR). The SIR and SOR are then allocated against available collection assets, which can be from higher echelons, organic, or passed to subordinate units. In some configurations (e.g., Stryker BCT) the BCT may also have a reconnaissance, surveillance, and target acquisition squadron with additional assets and expertise to assist in intelligence analysis as well as for planning and conducting ISR.

The BN will also have an S-2 section. This section is not as robust as the BCT-level S-2 section, but it does have the capability to conduct detailed intelligence preparation of the battlefield (IPB). The BN S-2 section in conjunction with the entire BN staff develops an ISR plan or matrix to answer higher and BN-level PIRs and assist in targeting and the gathering and analysis of available intelligence to drive tactical operations and orders to subordinate companies and specialty platoons. As at the BCT level, BN PIRs can be addressed by requesting higher-echelon assets—using organic BN assets such as scout and sniper platoons—or they can be passed to subordinate companies in the form of maneuver orders, SIR, and SOR.

At the company level there is no organic organizational intelligence analysis section, but as stated throughout this handbook, most company-size elements are organizing COISTs to fulfill this requirement. Within its capability, the COIST conducts IPB and assists the commander in the development of company-level PIRs and a company level-ISR plan. This plan will support the collection of information on the company commander's PIRs as well as incorporating the PIRs, SIR, SOR, and maneuver orders of the BN and BCT commanders. The SIR and SOR

CENTER FOR ARMY LESSONS LEARNED

developed can then be addressed by requesting ISR assets from higher echelons or by using company-level organic assets.

The PIR and ISR plans from BCT to company are linked as PIRs, SIR, and SOR. Maneuver orders from higher commanders can become company-level PIRs, SIR, SOR, or tasks. At the company level these requirements can be passed to patrols during patrol prebriefings and collected back at patrol debriefings and reported to higher headquarters.

To be effective, the COIST must understand how to conduct effective patrol briefs and debriefs and report, analyze, and exploit the information and intelligence derived from these reports to develop enemy estimates, conduct pattern/predictive analysis, and support the targeting process. These processes and systems must be established and trained on to facilitate quick reporting and enable both company and higher-level organizations to conduct timely intelligence-driven operations throughout the AO.

It is essential at the platoon level that leaders and Soldiers debrief their respective intelligence sections/teams and provide information for the development of refined intelligence in support of the ISR efforts at company, BN, and BCT levels to ultimately answer their commanders' PIRs.

The patrol brief is the key delivery method for sharing intelligence with or on adjacent and subordinate units prior to departing the forward operating base, combat outpost, or joint security site. Depending on terrain and where the company headquarters is located, the patrol brief can be issued by either the BN S-2 or the COIST. Intelligence shared during a patrol brief should not be limited to lethal targeting or effects but should also focus on nonlethal effects. As the counterinsurgency (COIN) environment matures, it is essential that commanders and leaders focus on nonlethal targeting and the operational environment (political, military, economic, security, social, information, infrastructure, physical environment, and time [PMESSII-PT]) or area structures, capabilities, organizations, people, and events (ASCOPE).

During the patrol brief, COISTs and S-2s must submit requests for information (RFIs) and SOR to the patrolling unit. These RFIs and SOR allow Soldiers the opportunity to answer intelligence gaps and assist in answering the commander's PIRs. Refined collection focus aids in the support of ISR plans. The ISR plan/matrix should be continually updated as intelligence is collected. Additionally, it is crucial that units have a task and purpose and understand the reporting requirements and SOR they are being tasked with.

The patrol brief should be thought of as an abbreviated IPB brief. The S-2/COIST conducting the prebrief must:

- Describe the effects of terrain and weather.
- Define the operational environment.
- Describe operational effects.

- Evaluate the threat.
- Determine the threat courses of action.

Key intelligence items to discuss during the patrol prebrief include the following:

- Last 24–48 hours significant activities in the area of responsibility (storyboards or graphic intelligence summary).
- Route status.
- ISR collection assets and priorities.
- Current assessments and future expectations.
- High-payoff target list (HPTL) (distribute and brief).
- Updates on key personalities (spheres of influence [SOI]), groups, events, and threats).
- Collection priorities (ISR matrix and intelligence synchronization matrix) in support of the commander's PIRs.
- Be-on-the-lookout list.
- Updated ISR matrix (intelligence requirements, SIR, SOR, named areas of interest [NAIs]) in support of the commander's PIRs.
- Updated biometric files for the Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE) systems at patrol level.
- Updated graphics (routes, imagery, objectives, NAIs, and targeted areas of interest [TAIs]).
- Updated assessments of the operational environment in regard to PMESSII-PT and ASCOPE.

Patrol debrief tactical ground reporting

At the conclusion of a mounted or dismounted patrol, leaders and Soldiers must debrief their respective unit and intelligence counterparts to ensure information and intelligence are not lost. The patrol leader along with his entire patrol must debrief every piece of information even though it might not seem important or of intelligence value. Routine information often provides indicators of the operational environment and is decisive in the targeting process (lethal/nonlethal). General village assessments and debriefs of a key leader engagement (KLE) with an SOI allow the company commander and his COIST or the BN commander's staff the ability to focus their efforts in developing the target synchronization matrix and refining the lines of effort (LOE).

To have an effective patrol debrief, the COIST must have a standardized patrol debrief format consistent with the reporting requirements of higher headquarters. This checklist allows for a detailed debrief and ensures all information collected by the patrol is captured. When a successful debrief is conducted, the COIST can analyze the information, develop it into an intelligence product, and distribute the product to the BN S-2. Additionally, this data will feed the intelligence cycle, continue the IPB process, and ultimately begin the next targeting cycle for the company, BN, and BCT.

Two systems the S-2/COIST can use to capture this data are the Combined Information Data Network Exchange (CIDNE) and the Tactical Ground Reporting (TiGR) System. (**Note:** These databases are addressed extensively in Chapter 4.) The databases allow analysts the ability to upload text debriefs, assessments, and media; organize debriefs geographically; and allow adjacent units the ability to query the database utilizing filters. In addition to uploading the database, these systems allow other intelligence collectors the opportunity and ability to share and synchronize intelligence. It is imperative that Soldiers understand that patrol debriefs and operation debriefs are what feed the intelligence and targeting cycle.

TiGR and CIDNE are two databases for the entry of company information; however, they have very different functions. CIDNE is for the receipt of formal reports such as a KLE or a civil affairs report. TiGR, on the other hand, is a tool that provides context to the report. As an example, “This KLE happened and this was the result” is a typical CIDNE report. “This KLE happened after a sophisticated attack delayed the patrol, and the village elder had been killed a day before” is a TiGR report on the same incident. The two systems are used together to enable the level of detail a COIST should provide to the company commander.

Reports need to be entered directly into TiGR and not as an attached text report. An honesty trace must be used. Additionally, photographs and significant activities occurring during the patrol must be associated with that patrol. All this is done to ensure the data is searchable for later use. Debriefing checklists are helpful, but a debrief is not a check-the-block affair, and there must be room for free text within the debrief to portray the context and meaning of the information presented. Ensure the debrief format captures data that will pass the basic tests such as:

- Is this report searchable through text?
- Is this report searchable through geography?
- Can this report be viewed with other similar reports (i.e., is it filterable through the system)?
- Is it written in a format that is conducive to the use of the search tools provided? (For example, one-word answers to questions are almost worthless due to the inability of TiGR to run Boolean searches. As a result, paragraphs and sentences are required to provide context to the report, which then facilitate subsequent searches.).

There are several methods of debriefing patrols, and units should be prepared to use whichever technique best supports the situation. Each method can be modified as necessary, but there are pros and cons associated with each technique:

- Debrief the entire patrol at one time:
 - Pros: Provides the best information and all points of view.
 - Cons: Takes time, and requires a large secure area.
- Debrief squad leader and key leaders:
 - Pros: Faster, gets leader input, and requires less space.
 - Cons: Does not get all points of view.
- Platoon leader and platoon sergeant debrief patrol, then debrief COIST:
 - Pros: Frees up COIST, and gets all points of view.
 - Cons: May take longer, requires training, and information may get lost in translation.
- Platoon leader writes up debrief, and COIST reads and ask questions:
 - Pros: Less time-demanding for COIST since debrief is written.
 - Cons: May miss important information from other points of view.

Ultimately, the S-2/COIST must analyze this data and answer the commander's PIRs to update the ISR plan and answer any RFIs or intelligence gaps.

Key intelligence items to discuss during the patrol debrief include the following:

- Answers to PIRs, SIR, SOR, and observed actions and inactions in NAIs.
- Route taken/route tasked and status of routes.
- Observations of populace:
 - Key engagements
 - Items discussed
 - Attitudes observed
 - Photographs taken
 - Unusual sounds or odors
 - New graffiti/enemy propaganda
 - Changes to terrain or physical environment

- Changes to operational graphics or observations from route/main supply route.
- SOI assessments, observations, and notes from KLE.
- Updates to ISR matrix and PIRs.
- Updates to patrol-level PMESSII-PT, ASCOPE, and other related assessments.
- Updates to town/village assessments.
- Host nation security force assessments.
- HIIDE device upload to BAT database.
- Updates to intelligence databases (Command Post of the Future and TiGR).

Target Development/Prioritizing Lethal and Nonlethal Targets

It is imperative that all members of the target working group review all target nominations and understand how the enemy network ties into the AO/area of influence (AI) and adjacent units' AOs and AIs. Identify and establish a working relationship with other agencies operating in your AO (i.e., explosive ordnance disposal, weapons intelligence team, and special operations forces) and share your targeting lines with these organizations to see how they fit into their targeting lines of operation (LOO)/LOE and targeting matrices. Synchronized targeting LOO/LOE facilitates an excellent joint effort to defeat the network and get in front of the enemy's decision cycle. Consider, within the constraints of protection and operational security, sharing the targeting LOO/LOE with the host nation security forces. It is an opportunity to bring both host nation police and army leaders together and share intelligence. This can also be conducted jointly with military transition teams or security transition teams to fully integrate the coalition force/host nation security force targeting cycle.

To increase the ability of host nation security force partners to conduct unilateral or bilateral operations, units are encouraged to distribute targeted personalities' names (HPTL) and photographs to the host nation security forces and strive to conduct joint targeting with them.

Synchronization and Integration of Intelligence, Surveillance, and Reconnaissance and Collection Assets

ISR synchronization has a significant impact on integrating lethal and nonlethal targets/fires. ISR synchronization is critical regardless of mission, but the importance is greatly increased with the size of the operational environment. To aggressively deter enemy actions, particularly with indirect fires, units need to detect the enemy before he can deliver assets. The challenges are that often this is placed solely in the hands of a very junior COIST/S-2 and is not synchronized with BCT and above-level assets. Units need to know what assets are available, request them based on predictive analysis, and most importantly, synchronize the effort to provide the best ISR coverage. This should be a significant part of the targeting

process at all levels, with focused emphasis on NAI refinement and the use of all available assets, including the myriad of nonstandard ISR platforms such as unit snipers, combat logistics patrols, and rotary- and fixed-wing flight crew debriefings and reports.

Things to consider when requesting ISR:

- Understand the air tasking order and the ISR cycle (usually 72-hour cycle). This is normally refined by the brigade aviation element and brigade collection management and dissemination process managers.
- Understand the brigade's collection priorities and what unit has priority of assets by type (human intelligence [HUMINT], signals intelligence [SIGINT], unmanned aircraft system [UAS], etc.).
- Utilize the BN commander's priorities from targeting meetings and target working groups, and ensure ISR assets (ground/aerial) are tied not only to PIRs but also to the target synchronization meeting.
- Synchronize ISR with an NAI or TAI, and request the asset during times of combat operations or when it is thought the enemy is active in the specified geographic area.
- Ensure all assets have a task and purpose and have clear reporting requirements (SOR).
- Validate the collector requested is the correct asset to provide observation of the NAI.
- Justify the need for collection systems by having companies and the BN staff attach a concept of the operation (CONOP) to the ISR request. The CONOP allows the collection manager to prioritize collection systems and will aid the requesting BN with obtaining the asset needed to support the mission.

The COIST needs to address the following questions with the commander and the BN staff:

- What intelligence sources are in the unit's area of operation (HUMINT, SIGINT, etc.)?
- How long does it take to get the information from subordinate collectors?
- Does the architecture for data storage support rapid recall and manipulation? Are the following connections available, adequate, and functioning: joint network node, command post node, and SECRET Internet Protocol Router node access point?
- What ISR and technical systems are available to find, fix, and finish targets?
 - When are they available?

- Are any mutually exclusive?
- How do we maintain coverage if one system is withdrawn or inoperative?

Conclusion

The COIST must disseminate and distribute intelligence products daily both up and down the chain of command.

The COIST must ensure all collectors understand the commander's PIRs and know how to answer them. This includes all patrols, Soldiers, and enablers (HUMINT collection teams, UAS, and SIGINT teams).

The COIST must ensure patrol leaders/Soldiers understand the capabilities of enablers and how and when to request them. It is also imperative patrol leaders/Soldiers understand how to control assets once allocated in support of their AO.

Patrol briefs are the key delivery method for sharing intelligence with adjacent and subordinate units.

The COIST must receive and integrate intelligence products submitted daily from patrols and collectors. These products allow the COIST to refine intelligence estimates and update enemy assessments. Additionally, the COIST must receive the platoon leaders' assessments of their respective AOs.

The COIST is the company-level entity and entry point into fully integrated top-to-bottom and bottom-to-top intelligence and information exchange. The COIST does not replace or replicate the functions of higher-level intelligence cells but instead informs, coordinates with, and complements overall BCT and BN intelligence plans and collection efforts. The interrelationship, nesting, and integration of PIRs, SIR, SOR, and ISR planning and collection facilitate and necessitate the deliberate, thoughtful, and proactive integration of intelligence exchange and integration from the platoon level to the BCT level.

Chapter 6

Company Intelligence Support Team Targeting

As discussed previously, a company-size element has very limited resources. At the brigade combat team (BCT) and battalion (BN) levels are adequately staffed sections to cover baseline requirements while at the same time contribute to staff planning meetings, working groups, and boards. The current operational environment has placed added emphasis on the targeting process in both lethal and nonlethal constructs. The BN and BCT target working group reviews all target nominations and attempts to understand how the enemy network ties into the area of operation (AO) and area of influence (AI) and adjacent units' AOs and AIs. At these above company-level headquarters, synchronized targeting line of effort facilitates efforts to defeat enemy networks and get in front of the enemy's decision cycle.

The company intelligence support team (COIST) is the company-level entry point into the targeting process. The COIST, in addition to in-house analysis and targeting, feeds information gained from patrols and engagements to the company's higher headquarters. This information is used to inform and assist the BN and BCT targeting cycle. At the COIST, the key to successful targeting is separating the important from the unimportant and then focusing and directing limited company and external resources where they can best and most positively influence the company area of responsibility (AOR).

Targeting at the company level is actually sorting and prioritizing information from patrols and engagements until there is enough information to act on with an acceptable level of certainty. Company-level targeting is not limited to lethal means such as direct and indirect fires but should be all-encompassing and include all available assets such as building projects, security for host nation personnel, Medical Civic Action Program, and host nation police and military assistance. Many units use the fire support officer to lead the COIST. In these cases, the COIST may be expected to assume lead planning and responsibility at the company level for targeting, employing enablers, and other operations as directed by the commander.

Company Intelligence Support Team Target Development Support

A target is an entity or object considered for possible engagement or action by lethal or nonlethal means. It may be an area, complex, installation, force, equipment, capability, function, individual, group, system, entity, or behavior identified for possible action to support the commander's objectives, guidance, and intent.

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. The purpose of targeting is to disrupt, delay, or limit threat interference of friendly activities; it requires coordinated interaction between operations and intelligence personnel. Based on the commander's guidance and targeting objectives, the staff determines what targets to engage and how and where to engage them. Targets should be assigned to the best systems to achieve the desired effects. Targeting is based on the enemy's assets that provide them an advantage,

friendly scheme of maneuver, and tactical plans. Targeting options can be either lethal or nonlethal.

Targeting in stability operations requires a detailed understanding of social networks, insurgent networks, actions, and civil considerations. In stability operations, there is greater emphasis on the effects of combat operations on the local government, army, police, and civilian population. The consideration of second- and third-order effects is critical. For example, it makes sense to separate the insurgent forces from the local population. If friendly forces conduct a successful cordon and search and find a room full of improvised explosive devices (IEDs), the first order of effect is to potentially disrupt IED attacks. However, the second order of effects that must be addressed could be civilian concerns over damage caused by the cordon and search. If civilian concerns are not addressed, friendly forces may have to deal with demonstrations that will drain the combat power needed for other operations. If the population's security and facility needs are not addressed, insurgent forces and weapons could/will return to the area, the third-order effect.

Targeting Meeting

The targeting meeting provides the company with a means to focus and synchronize the unit's efforts based on the current enemy situation, current unit success, and operation orders and fragmentary orders from higher echelons. It is also a means of assessing current lethal and nonlethal effects to determine if a change to the current plan is needed. The end state of a targeting meeting is the commander's decision for what to target, how to detect the target, how to deliver assets against the target, and how to assess the results of operations. The targeting meeting at the company is a regularly recurring event to keep the unit continuously focused on command priorities and to confirm whether the desired effects are being achieved. Targeting meetings can also be hasty meetings prior to missions to ensure the unit receives all relevant information and the commander's most current and up-to-date guidance.

Pretargeting Meeting

To conduct successful targeting meetings, the COIST must have information prepared to share with all participants of the meeting. The COIST inputs for the pretargeting meeting are the following:

- Light and weather data (received from higher headquarters).
- Terrain data in the form of maps or imagery.
- High-value target list (HVTL) with link and pattern analysis.
- Current and proposed priority intelligence requirements (PIRs), specific information requirements (SIR), and specific orders and requests (SOR) (received from higher headquarters and refined by company).
- Enemy course of action (COA) and event template.

- Battalion intelligence, surveillance, and reconnaissance (ISR) plan for the next 72 hours.
- ISR assets available.

COIST inputs for the targeting meeting include the following:

- Light, weather, and terrain data.
- Current enemy situation template, incident overlay, and link and pattern analysis.
- Status of nonorganic ISR assets requested by the company.
- Battle damage assessment of attacked targets as required (last 12–24 hours), highlighting changes in enemy capabilities.
- Current and proposed PIRs, SIR, SOR, and high-value targets (HVTs).
- Enemy COA for the targeting period.

The COIST compiles data for the target packet from information received from higher echelons and information gathered by unit missions. The target packet should be an all-source product with vetted, validated information in support of the designated desired effect. This packet can be used for lethal and nonlethal targets. As the information is gathered, the COIST will assemble the information and create a packet for the HVT or the high-value individual (HVI). This product, if properly formatted, allows patrols to carry a reference guide on any mission. For nonlethal targets, its format can be used to keep files on important personnel in the unit AOR and can be used as a quick reference for units if there is a planned engagement or meeting with the individual. This is a working document and should be updated as any new information on the HVT or HVI is obtained. Subsequent pages will contain all other data known about the individual, including copies of the source reports. Targeting factors that should always be considered are the following:

- Effective targeting demands accurate and well-organized intelligence.
- Plan for site exploitation.
- Be prepared for a follow-on mission.
- Have an information operations message prepared for missions.
- Beat the enemy to the media.
- Update target packets upon completion of the mission.
- Targets do not always have to be physical. (Think of ways to “steal” the enemy’s support base and safe haven.)

In addition to the target packet, there are other analytic products and tools to assist the COIST and the unit in developing information for the AOR. Other products the

COIST can maintain to assist with the targeting effort are a link diagram, HVTL, and be-on-the-lookout (BOLO) list.

Diagram Human Networks

Hostile individuals may blend with the population, but they will have a network of other individuals who will assist them. An example of when a link diagram is useful is an IED network. An IED explosion is the culmination of a networked operation that supported the IED. Someone emplaced the IED and may have initiated it. All of those “someones” make up a network. Some members of networks are more important than others; using the IED network example, financiers may support many operations. The IED maker builds many IEDs. Both will likely have contacts linking them to multiple IED incidents. Both of these individuals are important to the organization, whereas an individual who emplaces the IED is more easily replaced and less important. Additionally, it is important to remember that when an individual from the network is removed from the network, someone else must assume the duties of that individual.

Diagramming human networks as they emerge in intelligence operations helps the unit see how the threat is organized. Diagrams will show which individuals are working together. The diagram should show both professional relationships and blood relationships as they are identified. Such diagrams will show missing links or unknown persons whose existence is deemed probable if not certain. The diagrams may have a name of an individual but no picture or a picture with no name. Units must update these link diagrams as information becomes available. Link diagrams can include information on individuals, such as the types of cars they drive and the locations of their houses.

The key to link diagrams is to show the relationships between the hostile individuals. Link diagrams must be current to be useful. Update the diagram to show individuals who have been killed, captured, or recently released from jail. There are software programs such as Analyst Notebook and Analyst and eXploration of Information Sources Professional to build the diagrams. Microsoft PowerPoint also works well if the unit has no access to these programs. An example link diagram is shown in Figure 6.

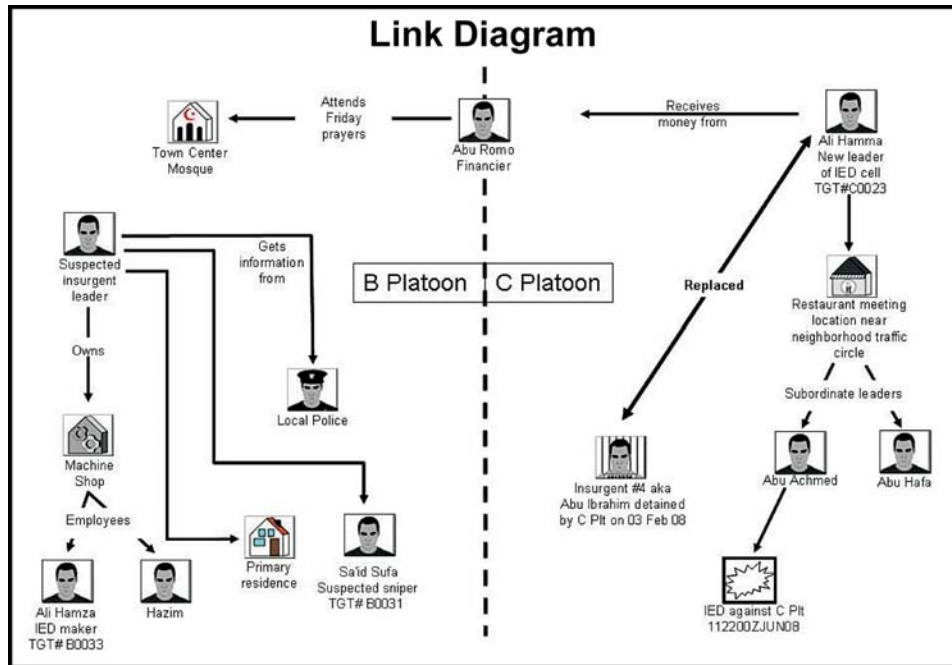


Figure 6. Example link diagram

High-Value Target List

The HVTL is initially developed at the BCT or higher echelon and sent to the company. Sometimes the targets that are of high value to higher echelons are not of high value to the company; many will not even be in the company's AO. The opposite is equally true. The company may be very interested in an individual who shoots at company Soldiers routinely. The individual is probably not an insurgent cell leader and the activities are not of high interest to higher echelons; however, the activities make him a HVI for the company. The company will take the initial HVTL and tailor it to the individuals affecting the company's AOR.

There is no standard number of individuals to be placed on the list; however, it should be prioritized with the most important individuals on top. The list should be maintained daily and information added or modified as it becomes available. If a target is detained, remove the individual from the active list, but keep the information so if the individual returns to the AOR, the data will still be available. The list can be managed in several different ways but should have an active and inactive component. If an individual has not been reported on in a set amount of time, remove him from the active list and place him on the inactive list.

The following information should be placed on the list at a minimum:

- Target number. When an individual becomes significant enough to be placed on the HVTL, he should receive a target tracking number and have a target packet started.
- Name. Include the individual's full name and any aliases.

- **Position.** What does the unit believe this person does? This information is a brief explanation of where the individual fits into the threat picture in the AOR and why he is a HVT.
- **Address.** Any known or suspected residences the individual may use. There may be several, and as more information becomes available, the unit can confirm or deny the validity of the addresses.
- **Phone number.** Individuals will likely have more than one phone number and may change numbers frequently.
- **Picture.** Include a picture of the individual, if available.
- **Remarks.** This information is a freeform column where the unit can link associated reports to the individual, make notes about the individual, or put in a physical description. Even with a picture, a physical description helps because it describes height, weight, style of dress, and behavior. It can also have the latest date of information about the individual.

Be-On-the-Lookout List

The BOLO list tracks vehicles involved in hostile activity or belonging to individuals involved in hostile activities. If a unit finds a suspicious vehicle, the BOLO list is a quick-reference document to see if the vehicle has been previously reported in hostile activity. A BOLO list is a spreadsheet that contains the following information:

- Make and type of vehicle.
- Model.
- Color.
- License number.
- Driver and passengers of the vehicle (names of hostile individuals associated with the vehicle).
- Activity; why the vehicle is wanted.
- Date the vehicle was last seen.
- Last location by grid or route name.

If local cars are not the same type of cars that would be seen in the United States, a book with pictures of the local cars should also be assembled.

Targeting Standing Operating Procedures

Units will develop targeting standing operating procedures (SOPs) to refine, streamline, and improve the overall company targeting process. An example company-level targeting SOP follows.

Lethal Targeting Operations

- The COIST will develop company-level targets based on the commander's PIRs/IRs.
- Lethal operations must be conclusively researched through all SECRET Internet Protocol Router (SIPR)/Non-Secure Internet Protocol Router sources.
- At a minimum, the COIST will provide three separate reports before committing to lethal operations:
 - SIPR (Combined Information Data Network Exchange) contains theater reporting through human intelligence (HUMINT), signals intelligence, and significant activities. Historical and recent reporting may be gained through this means.
 - Local sworn statements:
 - * Sworn statements and reporting through host nation police agencies are an acceptable means of identifying lethal targets.
 - * HUMINT collection teams may provide sworn statements for lethal operations.
 - Local detention facilities. Statements furnished to U.S. Army interrogators may also be used to identify lethal targets.
- All lethal target operations must be approved through BN operations and the BN S-2 and assigned a target tracking number before operations.

Lethal targeting packets will at a minimum include the following:

- Cover with target number, date, and name of individual who assembled/updated the packet.
- Target overview.
- Personal description with known associates.
- Link diagram.
- Imagery of the object/target.
- Reporting information.
- Site exploitation plan.

Nonlethal Targeting Operations

Nonlethal operations encompass all civil affairs, engineering, medical, political, and social structures. Nonlethal operations are not only an effort to win hearts and minds but may be used to shift local power from anti-coalition forces to a local population that supports anti-insurgency activity.

All nonlethal targeting operations must be approved through BN operations and assigned a target tracking number before execution.

Nonlethal targeting packets should include at a minimum:

- Cover with target number, date, and name of individual who assembled/updated the packet and classification.
- Imagery with physical description, biographical information, background, and engagement goal.
- Known relationships and associations.
- Notes from previous engagements.
- Intelligence updates.
- Related civil-military operations projects.
- Engagement worksheet.
- Historical notes.

Conclusion

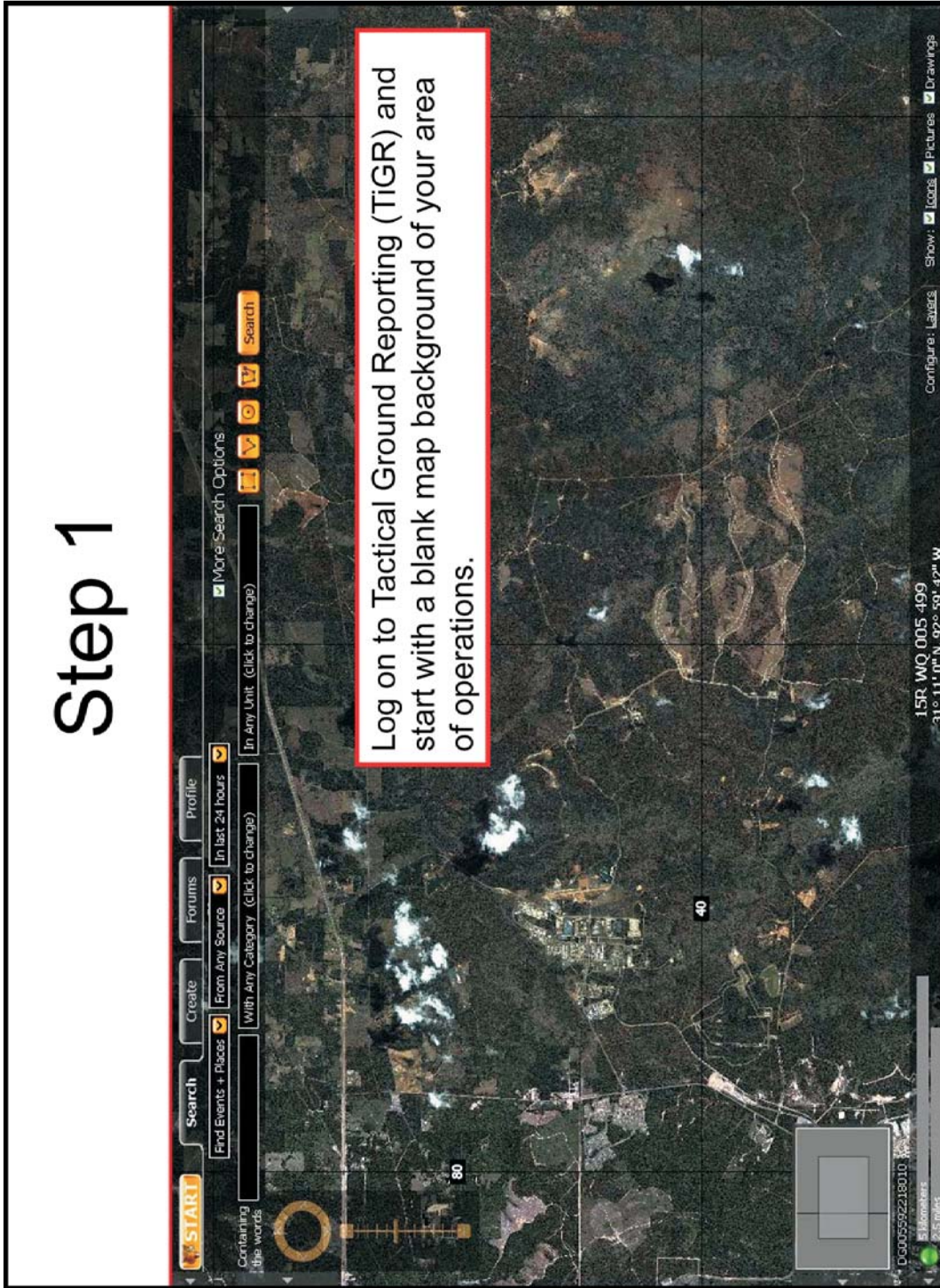
The COIST is the company-level entry point into the targeting process. The COIST records and analyzes information gained from patrols and engagements to the company's higher headquarters. This information is used to inform and assist the BN/BCT targeting cycle. At the COIST, the key to successful targeting is separating the important from the unimportant and then focusing and directing limited company and external resources where they can best and most positively influence the company AOR. Targeting at the company level is actually sorting and prioritizing information from patrols and engagements until there is enough information to act on with an acceptable level of certainty. Company-level targeting is not limited to lethal means, such as direct and indirect fires, but should be all-encompassing and include all available assets.

Appendix A

Ten-Step Tactical Ground Reporting System Debrief

The slide presentation on the following pages graphically demonstrates an example ten-step method to employ the Tactical Ground Reporting (TiGR) system when debriefing patrols. The presentation addresses preparing the system, initiating a report, entering a patrol narrative, creating a record of the patrol's route, attaching media, affiliating the debrief, and saving the report.

Step 1



Step 2

The screenshot shows a software interface for military intelligence. At the top, there are navigation buttons: **START**, **Search**, **Create**, **Forums**, and **Profile**. Below these are search filters: **Find Events + Places** (From Any Source, In last 24 hours), **With Any Category** (click to change), and **In Any Unit** (click to change). A search bar contains the text "Containing the words".

A red box highlights the following text:

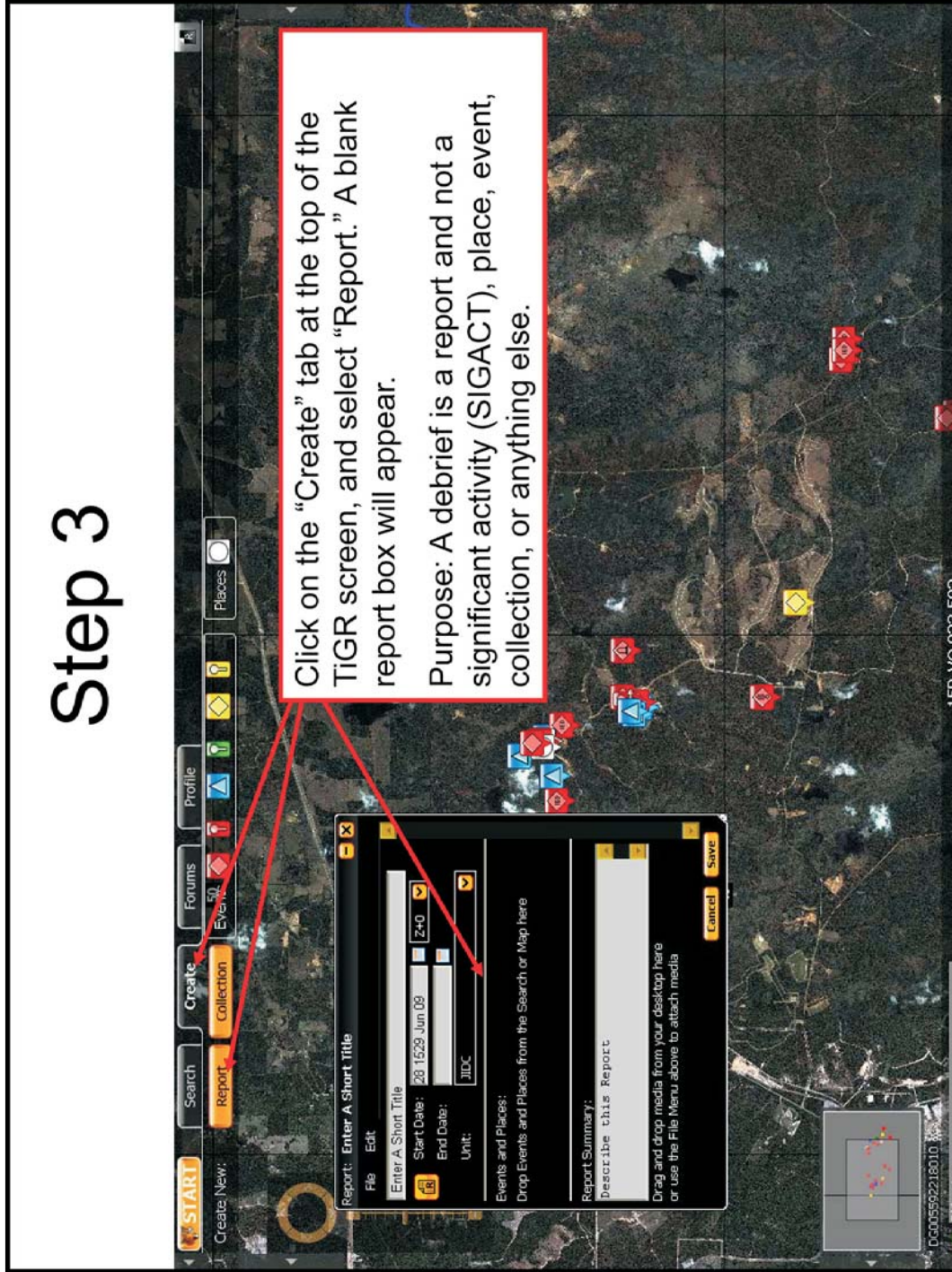
Run a search for all events and places during the time frame in which the patrol occurred. This will cause these events to populate your map.
 Purpose: We may have to affiliate some of these events with the debris.

The map below shows a satellite view of a forested area with several red and blue markers. A red arrow points from the highlighted text to the search filters. A list of search results is visible on the right side of the map:

- 2 hours ago: A-2-12 FA/ASBCT(2-ID)
- 3 hours ago: C/2-23 IN/ASBCT(2-ID)
- 3 hours ago: IDF @ Torch CP
- 4 hours ago: B/4-9 INF/ASBCT(2-ID)
- 4 hours ago: 3rd P/T takes SAF
- 5 hours ago: A/4-9 INF/ASBCT(2-ID)
- 5 hours ago: A CO 4-9 IN ATTACKED BY MORTAR
- 5 hours ago: A CO JCOB takes YBIEB
- 6 hours ago: Weapon cache
- 7 hours ago: C/2-1 INF/ASBCT(2-ID)
- 7 hours ago: 4x155mm Pressure Plate
- 9 hours ago: C/2-1 INF/ASBCT(2-ID)
- IDF POO

At the bottom right, there is a scale bar (0 to 2.5 miles), a location indicator (15SR WQ 011.489, 31° 10' 26" N, 92° 59' 18" W), and a "500 Per Page" dropdown menu. The bottom right corner also contains icons for "Layers", "Pictures", and "Drawings".

Step 3



Step 4

The screenshot shows a software interface with a map background. A dialog box is open in the center, titled "Report: DEBRIEF 2/B/3-199". The dialog has several fields: "Title" (containing "DEBRIEF 2/B/3-199"), "Start Date" (28 1629 Jun 09), "End Date" (28 1829 Jun 09), and "Unit" (JIDC). Below these fields are sections for "Events and Places" and "Report Summary". A red box highlights the "Title" field and the text below it: "Purpose: We will use this time information later to evaluate any patterns our friendly forces may be setting for the enemy. Also, standardized titles will help us recall this data later." The interface also includes a top menu bar with "START", "Search", "Report", "Create Collection", "Events", "Forums", "Profile", and "Places". A bottom status bar shows coordinates "15R VQ 940 495" and "31° 10' 47" N, 93° 3' 45" W".

Enter your title in the title block according to your battalion's standard, and then enter the time frame for the patrol in the "Start Date" and "End Date" blocks.

Purpose: We will use this time information later to evaluate any patterns our friendly forces may be setting for the enemy. Also, standardized titles will help us recall this data later.

Step 5

Enter your patrol narrative in the block titled "Report Summary."

Purpose: This is the searchable block of TiGR, and all information that is or may be relevant should be entered here. To optimize this data entry:

- Maximize use of specificity, especially regarding proper names and locations.
- Use proper grammar and sentence structure and not Army bullet comments (using descriptive language will facilitate more possible and better searches later).

Report: DEBRIEF 2/18/3-199

File Edit
 End Date: 28 1829 Jun 09
 Unit: JIDC

Events and Places:
 Drop Events and Places from the Search or Map here

Report Summary:
 2/18-199 SP-D FOR EARTHQUAKE AT 1529 AND HEADED EAST ALONG ROUTE 100. AS WE MOVED TOWARD SULLIVAN WE NOTICED A LARGE AMOUNT OF GARBAGE STREAM ACROSS THE ROAD NEAR IP CHECKPOINT. AT 1545 WE ENTERED SULLIVAN FROM THE NORTH ENTRANCE. WE NOTICED THAT THERE WERE FAR FEWER INDIVIDUALS AT THE MARKETPLACE THAN WAS NORMAL FOR THE AREA. OPT KIM DECIDED TO CONDUCT A SLE WITH OMAR BIN ZAID HADI AT THE MARKET, TO DECIDE WHAT WAS HAPPENING IN TOWN

15R VQ 907 503
 31° 11' 12" N, 99° 5' 53" W

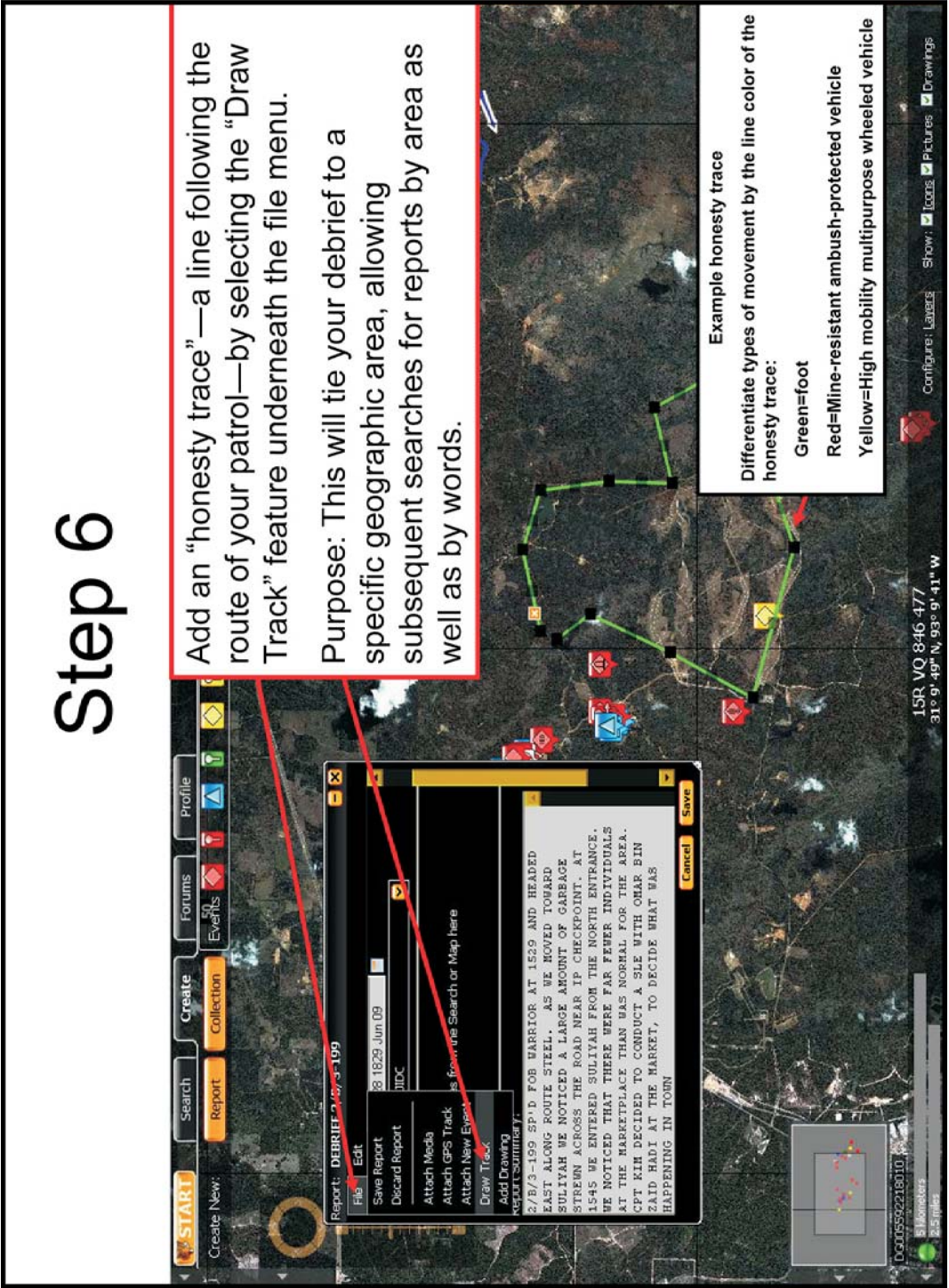
5 Kilometers
 2.5 Miles

Configure Layers Show Layers Pictures Drawings

Step 6

Add an "honesty trace"—a line following the route of your patrol—by selecting the "Draw Trace" feature underneath the file menu.

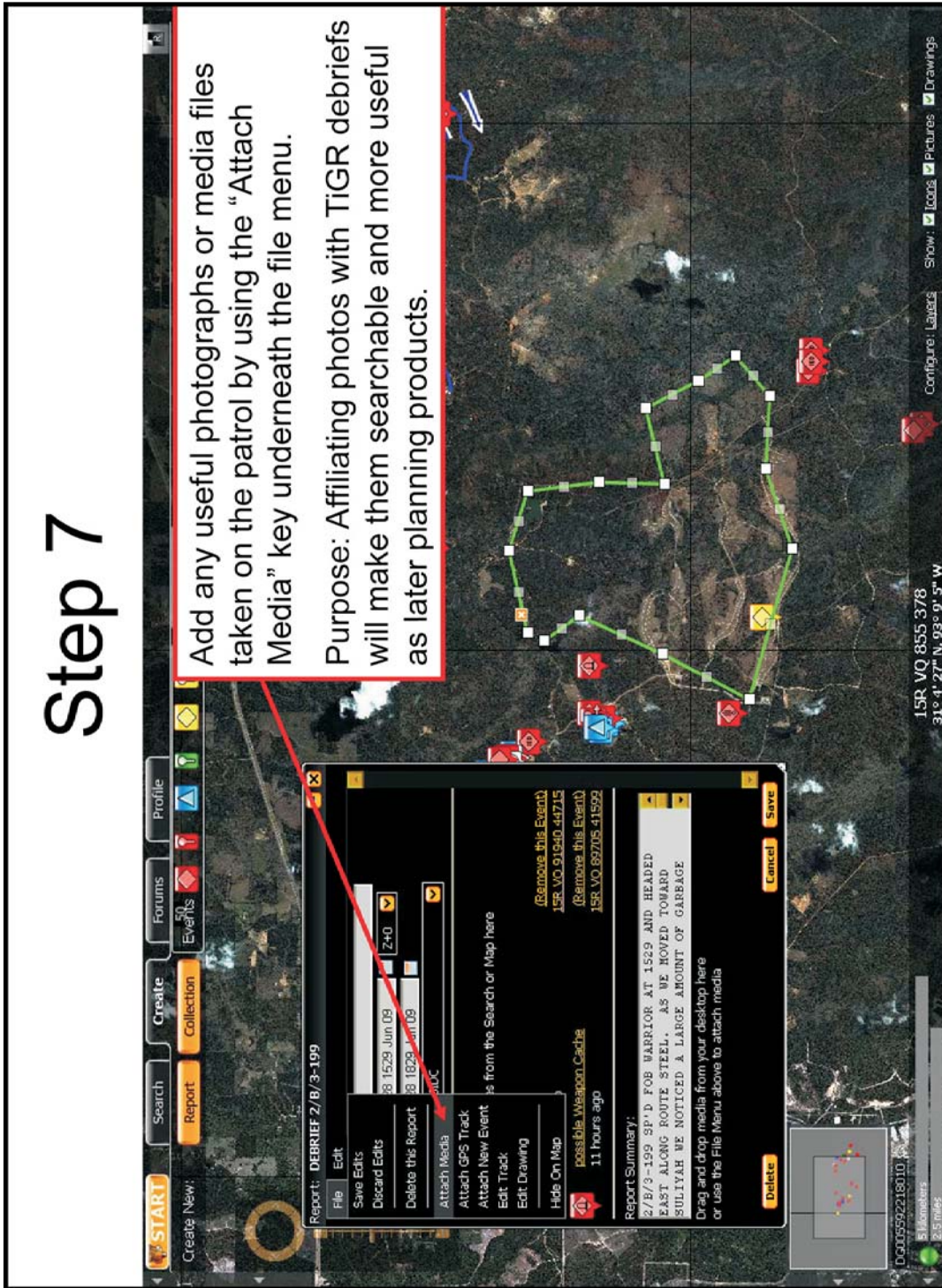
Purpose: This will tie your debrief to a specific geographic area, allowing subsequent searches for reports by area as well as by words.



Step 7

Add any useful photographs or media files taken on the patrol by using the "Attach Media" key underneath the file menu.

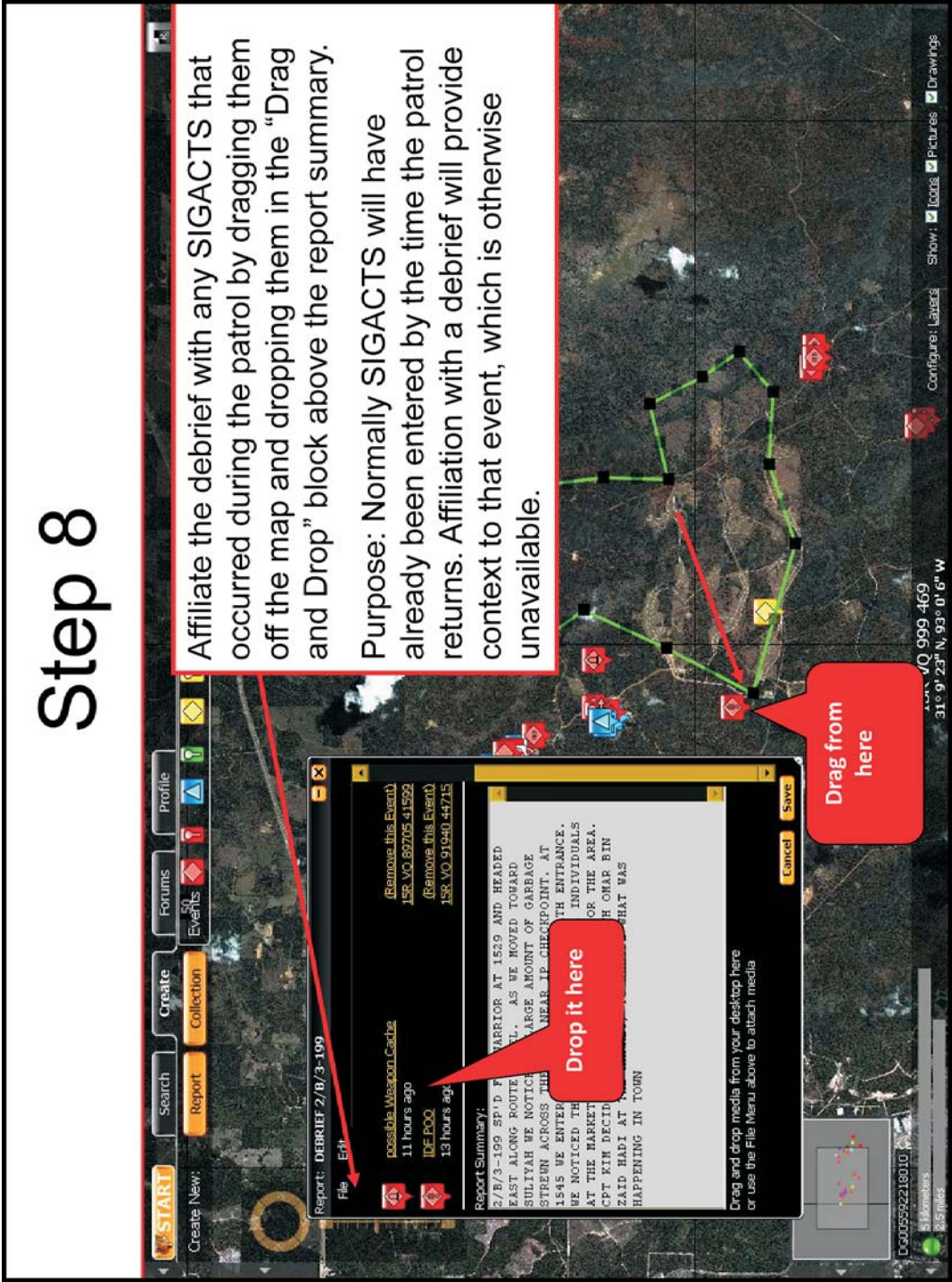
Purpose: Affiliating photos with TiGR debriefs will make them searchable and more useful as later planning products.



Step 8

Affiliate the debrief with any SIGACTS that occurred during the patrol by dragging them off the map and dropping them in the "Drag and Drop" block above the report summary.

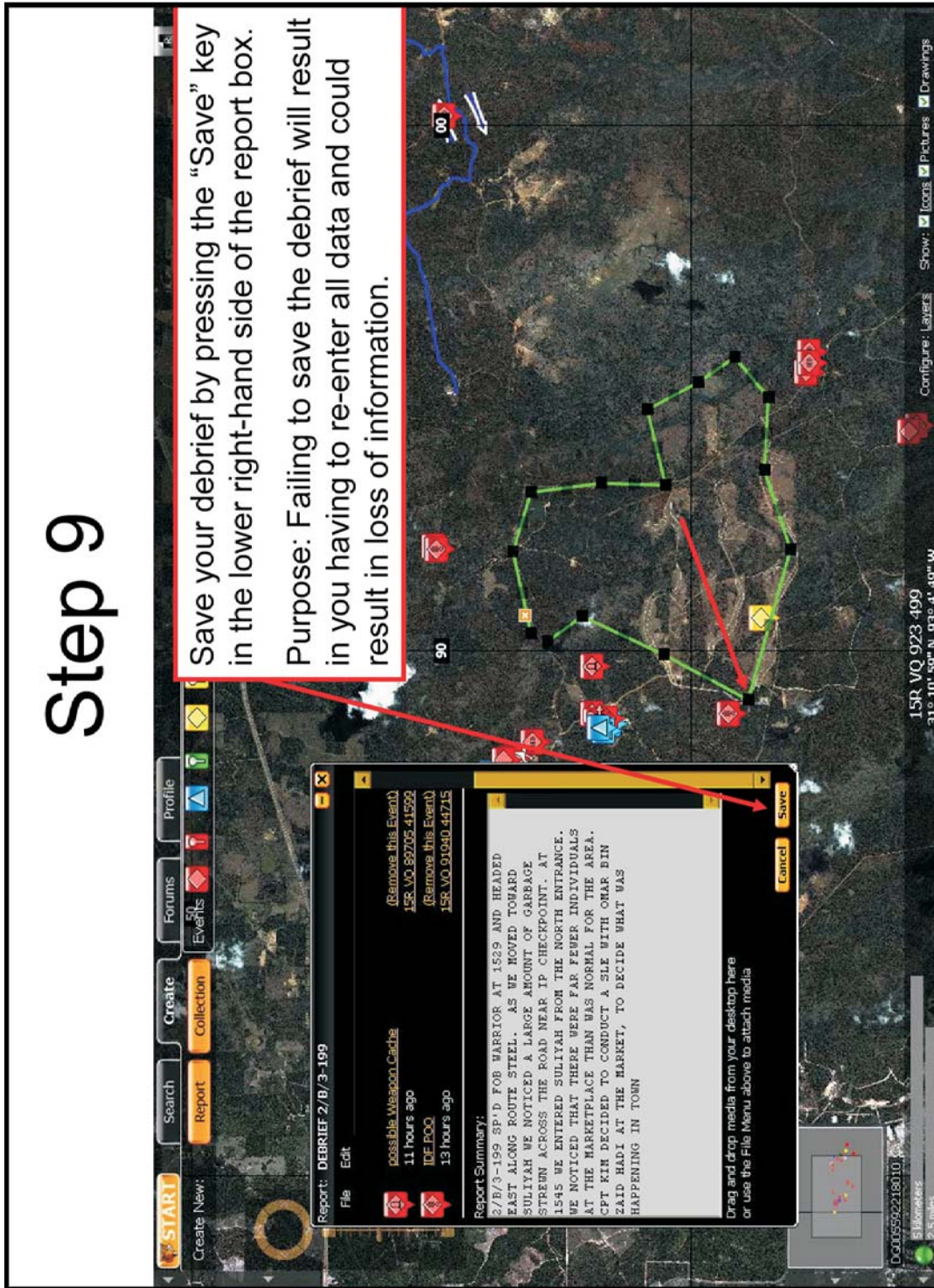
Purpose: Normally SIGACTS will have already been entered by the time the patrol returns. Affiliation with a debrief will provide context to that event, which is otherwise unavailable.



Step 9

Save your debrief by pressing the "Save" key in the lower right-hand side of the report box.

Purpose: Failing to save the debrief will result in you having to re-enter all data and could result in loss of information.



Step 10

The screenshot shows a software interface with a report window titled "DEBRIEF 2/8/3-199". The report content includes:

- File:**
 - Start Date: 28 Jun 09
 - End Date: 28 1829 Jun 09
 - Unit: JIDC
- Events:**
 - IDF POO (13 hours ago): possible Weapon Cache
 - 15R VO 91040 44715 (11 hours ago)
 - 15R VO 8975 41599
- Report Summary:**

2/8/3-199 SPD FOB WARRIOR AT 1529 AND HEADED EAST ALONG ROUTE STEEL AS WE MOVED TOWARD SULTYAH WE NOTICED A LARGE AMOUNT OF GARBAGE STREAMING ACROSS THE ROAD NEAR IP ... [Click for the rest of this Summary.](#)
- Comments:**

< 1 minute ago [21td tfl](#) added:
GOOD START BUT I NEED A LOT MORE DETAIL, AND REMEMBER THAT IN THE STANDARD ARABIC MUHAMMAD IS THE ONLY PROPER SPELLING OF THE NAME
- Created by:** [21td tfl](#), 2 minutes ago [This Version]

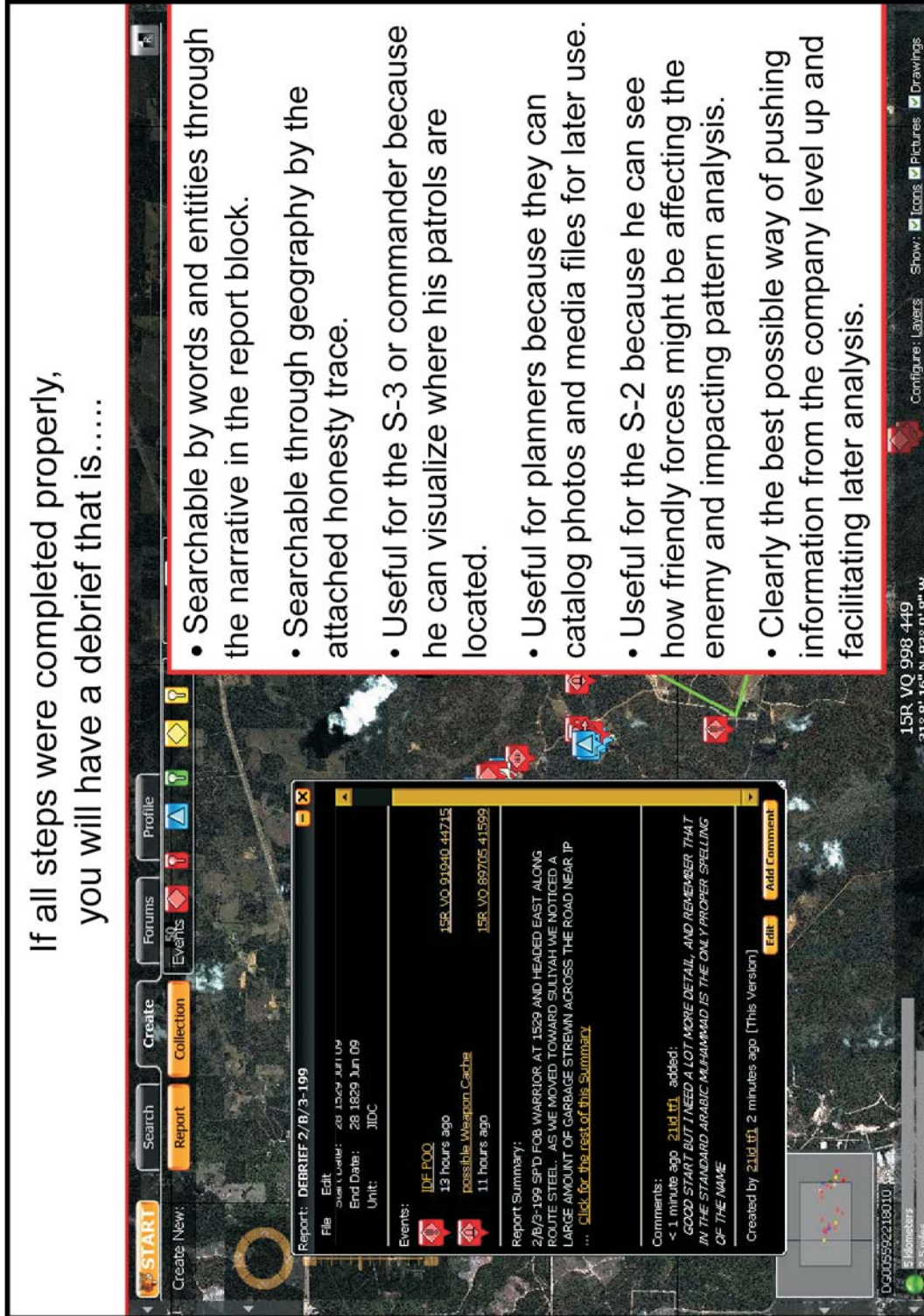
Buttons for "Add Comment", "edit", "Layers", "Icons", "Pictures", and "Drawings" are visible. A text box on the right side of the interface contains the following text:

S-2 reviews debrief and adds any feedback necessary utilizing the "Add Comment" key in the lower right-hand side of the completed debrief.

Purpose: Frequently, debriefs will be entered that are incorrect, poorly written, or formatted in an unsearchable manner. Also, company intelligence support teams will appreciate knowing that battalion and higher headquarters actually received and used their debrief.

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

- Searchable by words and entities through the narrative in the report block.
- Searchable through geography by the attached honesty trace.
- Useful for the S-3 or commander because he can visualize where his patrols are located.
- Useful for planners because they can catalog photos and media files for later use.
- Useful for the S-2 because he can see how friendly forces might be affecting the enemy and impacting pattern analysis.
- Clearly the best possible way of pushing information from the company level up and facilitating later analysis.



PROVIDE US YOUR INPUT

To help you access information quickly and efficiently, Center for Army Lessons Learned (CALL) posts all publications, along with numerous other useful products, on the CALL Web site. The CALL Web site is restricted to U.S. government and allied personnel.

PROVIDE FEEDBACK OR REQUEST INFORMATION

<<http://call.army.mil>>

If you have any comments, suggestions, or requests for information (RFIs), use the following links on the CALL home page: “Request for Information or a CALL Product” or “Give Us Your Feedback.”

**PROVIDE TACTICS, TECHNIQUES, AND PROCEDURES (TTP) OR
SUBMIT AN AFTER-ACTION REVIEW (AAR)**

If your unit has identified lessons learned or TTP or would like to submit an AAR, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

NIPR Email address: call.rfimanager@conus.army.mil

SIPR Email address: call.rfiagent@conus.army.smil.mil

Mailing Address: Center for Army Lessons Learned, ATTN: OCC, 10 Meade Ave., Bldg 50, Fort Leavenworth, KS 66027-1350.

TO REQUEST COPIES OF THIS PUBLICATION

If you would like copies of this publication, please submit your request at: <http://call.army.mil>. Use the “Request for Information or a CALL Product” link. Please fill in all the information, including your unit name and official military address. Please include building number and street for military posts.

PRODUCTS AVAILABLE "ONLINE"

CENTER FOR ARMY LESSONS LEARNED (CALL)

Access and download information from CALL's Web site. CALL also offers Web-based access to the CALL Archives. The CALL home page address is:

<<http://call.army.mil>>

CALL produces the following publications on a variety of subjects:

- **Combat Training Center Bulletins, Newsletters, and Trends**
- **Special Editions**
- *News From the Front*
- **Training Techniques**
- **Handbooks**
- **Initial Impressions Reports**

You may request these publications by using the "Request for Information or a CALL Product" link on the CALL home page.

**COMBINED ARMS CENTER (CAC)
Additional Publications and Resources**

The CAC home page address is:

<<http://www.leavenworth.army.mil>>

Battle Command Knowledge System (BCKS)

BCKS supports the online generation, application, management, and exploitation of Army knowledge to foster collaboration among Soldiers and units in order to share expertise and experience, facilitate leader development and intuitive decision making, and support the development of organizations and teams. Find BCKS at <<http://usacac.army.mil/CAC/bcks/index.asp>>.

Center for Army Leadership (CAL)

CAL plans and programs leadership instruction, doctrine, and research. CAL integrates and synchronizes the Professional Military Education Systems and Civilian Education System. Find CAL products at <<http://usacac.army.mil/CAC/CAL/index.asp>>.

Combat Studies Institute (CSI)

CSI is a military history "think tank" that produces timely and relevant military history and contemporary operational history. Find CSI products at <<http://usacac.army.mil/CAC/csi/RandP/CSIPubs.asp>>.

Combined Arms Center-Training: The Road to Deployment

This site provides brigade combat teams, divisions, and support brigades the latest road to deployment information. This site also includes U.S. Forces Command's latest training guidance and most current Battle Command Training Program Counterinsurgency Seminars. Find The Road to Deployment at <<http://rtd.leavenworth.army.smil.mil>>.

Combined Arms Doctrine Directorate (CADD)

CADD develops, writes, and updates Army doctrine at the corps and division level. Find the doctrinal publications at either the Army Publishing Directorate (APD) <<http://www.usapa.army.mil>> or the Reimer Digital Library <<http://www.adtdl.army.mil>>.

Foreign Military Studies Office (FMSO)

FMSO is a research and analysis center on Fort Leavenworth under the TRADOC G-2. FMSO manages and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. Find FMSO products at <<http://fmso.leavenworth.army.mil/recent.htm>> or <<http://fmso.leavenworth.army.mil/products.htm>>.

Military Review (MR)

MR is a refereed journal that provides a forum for original thought and debate on the art and science of land warfare and other issues of current interest to the U.S. Army and the Department of Defense. Find MR at <<http://usacac.leavenworth.army.mil/CAC/milreview>>.

TRADOC Intelligence Support Activity (TRISA)

TRISA is a field agency of the TRADOC G2 and a tenant organization on Fort Leavenworth. TRISA is responsible for the development of intelligence products to support the policy-making, training, combat development, models, and simulations arenas. Find TRISA Threats at <<https://dcsint-threats.leavenworth.army.mil/default.aspx>> (requires AKO password and ID).

United States Army Information Operations Proponent (USAIOP)

USAIOP is responsible for developing and documenting all IO requirements for doctrine, organization, training, materiel, leadership and education, personnel, and facilities; managing the eight personnel lifecycles for officers in the IO functional area; and coordinating and teaching the qualification course for information operations officers. Find USAIOP at <<http://usacac.army.mil/CAC/usaiop.asp>>.

U.S. Army and Marine Corps Counterinsurgency (COIN) Center

The U.S. Army and Marine Corps COIN Center acts as an advocate and integrator for COIN programs throughout the combined, joint, and interagency arena. Find the U.S. Army/U.S. Marine Corps COIN Center at: <<http://usacac.army.mil/cac2/coin/index.asp>>.

Support CAC in the exchange of information by telling us about your successes so they may be shared and become Army successes.

Center for Army Lessons Learned

10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350
<http://call.army.mil>



US Army
Combined
Arms Center

"Intellectual Center of the Army"

www.leavenworth.army.mil

U.S. UNCLASSIFIED
REL NATO, GCTF, ISAF, MCFI, ABCA
For Official Use Only