



HANDBOOK



No. 13-09

May 13

CoIST

Company Intelligence Support Team

UPDATE

Lessons and Best Practices

U.S. UNCLASSIFIED
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. government efforts.

The information contained in this product is provided for informational purposes only and is not necessarily approved U.S. Army policy or doctrine.

This product is designated for official use by U.S. government personnel and their approved contractors. It cannot be released to allies, coalition partners, or the public without the 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 Regulations 380-5, section 5-2. Official military personnel, civil service/government personnel, and approved contractors of the United States may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official U.S. government 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 or approved contractor facilities and cannot be released to allies, coalition partners, or the public without the consent of CALL.

CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents 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, government officials, and approved contractors have access to CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" materials.

Regulations strictly forbid posting CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents to Army Knowledge Online or other Department of Defense (DOD) websites 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. DOD 5400.7-R, DOD Freedom of Information Act Program, September 1998, provides guidance on the release, safeguard, and unauthorized disclosure of FOUO information.

Appropriate disciplinary action may be taken against those responsible for the unauthorized release of FOUO information. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against those responsible for the release; in addition unauthorized releases by contractor personnel to unauthorized persons may warrant action relative to the contractor under the Federal Acquisition Regulation (FAR).

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.

U.S. UNCLASSIFIED
For Official Use Only

CENTER FOR ARMY LESSONS LEARNED

SUPPORTING THE WARFIGHTER



Company Intelligence Support Team (CoIST)

DIGITAL VERSION AVAILABLE

A digital version of this CALL publication is available to view, download, or reproduce from the CALL restricted website, <<http://call.army.mil>>. Reproduction of this publication is welcomed and highly encouraged.

Common Access Card (CAC) or Army Knowledge Online (AKO) login is required to access the digital version.

This publication is located online at:

**[https://call2.army.mil/toc.aspx?document=7101&
filename=/docs/doc7101/13-09.pdf](https://call2.army.mil/toc.aspx?document=7101&filename=/docs/doc7101/13-09.pdf)**



Foreword

The complexity of operations, the ability to collect information and provide it at the lowest level at almost real time, and our increased expectations of junior leaders have reinforced the requirement for CoIST in the current fight. As we prepare our company commanders for future conflicts, they must continue to have an enhanced intelligence capability at the small unit level.


In conventional operations, intelligence is passed from higher to lower headquarters. 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 or other decentralized operations, information generally flows in the opposite direction. Small units provide ground truth and raw information, without the assistance, analysis, and filtering of higher level intelligence staff support. In either centralized or decentralized conditions, the unit's CoIST enables the company to maintain situational awareness, develop situational understanding, and produce intelligence to drive operations.

CoISTs, whether called by that name or troop intelligence support team or the company S-2 sections, support decentralized operations, whether they involve COIN or decisive action. We will use CoIST as the standard theme in this handbook. This is a re-write of the first CoIST handbook based off lessons learned and tactics, techniques, and procedures of CoIST.

Key concepts covered in this publication include the following:

- Commanders' Guidance and Selection for CoIST.
- CoIST Mission, Task, and Purpose.
- CoIST Manning.
- CoIST Setup and Organization.

- CoIST Battle Rhythm.
- Integration of CoIST Operations in Platoons through Brigades.
- CoIST Targeting.
- CoIST Systems and Tools.
- Maneuver vs. Non-maneuver.



WILLIAM B. HICKMAN
Brigadier General, USA
CG, JRTC and Fort Polk

Company Intelligence Support Team (CoIST)	
Table of Contents	
Chapter 1. Commander Guidance and Selection Process for Company Intelligence Support Teams	1
Chapter 2. Mission, Task, and Purpose	9
Chapter 3. Organization and Duties	19
Chapter 4. Physical Layout	25
Chapter 5. Battle Rhythm	31
Chapter 6. Networking	39
Chapter 7. Targeting	49
Chapter 8. Systems and Tools	59
Chapter 9. Maneuver vs. Non-Maneuver	67

Center For Army Lessons Learned	
Director	COL Thomas H. Roe
CALL Analysts	MAJ Cyrus K. Russ Thomas P. Odom, LNO, JRTC Operations Group
Authors	COL John M. Haynicz, JRTC LTC Eric A. Land, JRTC MSG William T. Beckman (Ret), JRTC Ralph Inman, JRTC Operations Group Intel Team, CI2C Nicholas J. Francois, JRTC
Coordinating Organizations	Fort Huachuca Military Training Team Fort Huachuca CI2C Fort Huachuca National Training Center

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

Commander Guidance and Selection Process for Company Intelligence Support Teams

“If it does not hurt, then it is not the right Soldier for the CoIST.”

The brigade commander must take the first step in building company intelligence support teams (CoISTs) making them a priority for all subordinate commanders in the brigade combat team (BCT) with the commander’s staff supervisor being the BCT S-2; CoISTs are therefore a BCT command priority, executed through command channels, with intelligence channel assistance. A command memorandum is the best tool for making that clear.

The BCT Commander Sets the Tone

Example of a CoIST POLICY MEMORANDUM

SUBJECT: BCT Commander’s Company Intelligence Support Team Policy

1. References:

- a. TC 2-19.63. Company Intelligence Support Team.
- b. CoIST: Company Intelligence Support Team Handbook: October, 2012. Published by the Center for Army Lessons Learned.
- c. BCT Company Intelligence Support Team Standard Operating Procedures.

2. Intent: This document outlines the brigade commander’s intent for CoISTs throughout the brigade combat team (BCT).

3. Mission: The BCT CoIST program prepares CoIST to facilitate the collection, analysis, processing, and coordination of all-source intelligence across the BCT to support targeting, influence the operational environment (OE), support company-level operations, and build the bottom-up intelligence needed on today’s battlefield. The CoIST mission is to serve as the primary source of information and intelligence that the company commander needs to make timely, accurate decisions.

4. Staffing:

- a. All companies should staff CoIST with at least six Soldiers from their organic MTOE. Each CoIST will have at least one officer, one noncommissioned officer (NCO), and four additional Soldiers. These Soldiers should have 11B, 19D, or 13B military occupational

specialties (MOS) if at all possible. If necessary, other personnel within the Company MTOE can be used. Commanders will select CoIST members based on a high level of motivation, ability to use technical equipment, and a general aptitude for integrating intelligence information into tactical operations. To provide continuity, personnel selected to serve in the CoIST will remain in that position through the deployment unless a move is specifically authorized by the battalion commander. Commanders will ensure CoIST operations are the primary duty for selected personnel and will limit assigning additional duties that detract from the primary mission.

b. As of FY12 the CoIST is allocated a 35F to each company within the maneuver battalion.

5. Training Objectives:

a. At a minimum, all CoIST cell members will attend the 40-hour basic CoIST course offered as a Fort Huachuca mobile training team (MTT) or as a resident course provided by the home station trainers (HST) at the MTC or CI2C. CoIST members will also receive four hours of basic TIGR training and four hours of Axis Pro.

b. In addition to the basic analyst tasks, BCT S-2 shops will train their CoIST on aspects of the intelligence fight peculiar to their particular area of operations (AO). Examples of these would be:

- i. The prebriefing and debriefing process.
- ii. Threat groups and enemy TTP of a particular AO.
- iii. Effective database search techniques for a particular AO (i.e., entity-based searches vs. geography-based searches).
- iv. SR assets capabilities that operate within the AO.

As the analytical skills of the CoIST improves, the battalion S-2 teaches CoIST more complicated tasks such as intelligence preparation of the battlefield, development of most likely and most dangerous enemy courses of action, and writing of company intelligence requirements. Lastly, each CoIST will assign individuals to serve as subject-matter experts on biometrics automated tool set (BAT), tactical site exploitation and forensics, collection asset capabilities, and product fusion pushed to the battalion as well as other companies.

6. Equipment: CoIST receives automation equipment required to conduct 24-hour operations in conjunction with company command posts (CPs). The company CP provides additional desk and workspace required to incorporate additional automation equipment and product/information sharing space. The minimum acceptable equipment list includes the following:

- a. Three laptops—two CSI and one SIPR, both with AXIS Pro.
- b. Printer/copier/scanner combo.
- c. Digital camera.
- d. Video projector.
- e. One System Remote Viewing Terminal (OSRVT).
- f. BAT.
- g. Handheld Interagency Identity Detection Equipment (HIIDE) per platoon.
- h. Cellular Exploitation (CellEx).

7. Brigade and Battalion Support: Brigade and battalion support to CoIST will include requesting and facilitating required training, acquisition of designated automation requirements, and developing standard operating procedures (SOP) to ensure information flow to and from CoIST cells throughout the BCT.

Selection Process

The first step in fielding CoIST begins with command guidance like the example given in the previous section. The second step in ensuring the guidance is followed in the selection of the CoIST personnel. CoIST is fundamentally people-centric, meaning it is not a technology-driven endeavor. The mission of the CoIST is to serve as the primary source of information and intelligence that the company commander needs to make timely, accurate decisions. Without quality Soldiers, the CoIST, regardless of technology, will fall short of those expectations. There are some basic requirements and recommended qualities for CoIST personnel. These include the following:

- Security Requirements: Must have SECRET clearance.
- Personal and professional attributes:
 - GT score of 110.

- Previous employment experience.
- Self motivated.
- Proficient in basic computer operation.
- Demonstrate ability to operate with little to no supervision.
- Complete tasks on time and to standard.
- Demonstrate ability to think critically and analytically.

Finding Soldiers who meet these criteria is best done through a phased selection, as follows:

- Phase 1, Team core selection: Company leadership selects Soldiers who, along with the assigned S-2 analyst, will form the core of that unit's CoIST. These Soldiers fill the role of OIC and/or NCOIC.
- Phase 2, S-2/Company CDR evaluate: The S-2/CDR evaluates all selected Soldiers as potential analysts.
- Phase 3, Training and team integration: The S-2 shop conducts a week long workshop to provide the CoIST sustainment training.
- Phase 4, Sustainment training: Upon completion of the training, the CoIST will meet weekly for sustainment training.
- Phase 5, Team backfill: The companies introduce the remaining two individuals to the CoIST training, as they become available.

Basic CoIST intelligence training will comprise the following:

- Five-day MTT.
- CI2C Home Station Training (FORSCOM program).
- Advanced software capabilities of PowerPoint, Word, Excel, etc.
- Data mining – critical analysis of data sets.
- Analytical platforms – TIGR Net, Google Earth, and CIDNE.
- Essential intelligence products – baseball cards, patrol pre/debriefs, database and info management, etc.
- Basics of pattern and enemy trends analysis.
- Target country cultural overview.

- Product standards – how to create high-quality products with relevant information and timely/accurate reporting.
- Basics of battlefield ISR using IST, TSE, and TQ.

Selection Phases in Detail

Phase 1: Company Selection (Team Core Selection)

Company commanders and 1SGs will select their candidates for the CoIST program. Selectees will complete a CoIST selection packet before they arrive for the initial interview. The packet includes:

- Proof of SECRET clearance.
- Enlisted Record Brief (for GT Score).
- Letter from the Soldier stating qualifications for the CoIST program, what they think the impact of the program will be for them and the unit they're representing, as well as any strengths they perceive they bring to the table. (This is a writing sample to show Soldier's ability to write professionally.)

Phase 2: Initial Interview (S-2 Evaluation)

Soldier's packet is reviewed by CoIST board. Board members include:

- S-2 OIC.
- Assistant S-2.
- S-2 NCOIC.
- Company commander or 1SG.

Phase 3: Assessment

The assessment is a test of basic abilities that are the foundations to analytic work.

- Computer skills assessment on basic functions, Word, Excel, and PowerPoint.
- Critical thinking and writing.

Computer skills assessment:

- Microsoft Word PE.
 - Open Microsoft Word document.
 - Type: The quick brown fox jumps over the lazy dog.

- Change sentence font from Calibri (Body) to Times New Roman.
- Change font size from 11 to 13 point.
- Make the word “quick” bold.
- Underline the word “jumps.”
- Italicize the word “lazy.”
- Center sentence on page.
- Turn “bullets” on re-type sentence twice utilizing bullet format.
- Microsoft Excel PE.
 - Open Microsoft Excel.
 - Set borders.
 - Insert new column between columns A and B, highlight new column in red.
 - Insert new row between rows 3 and 4, highlight new row in yellow.
 - Merge cells C3 and D3, highlight in green.
 - Delete row/column.
 - Type “Goblin” in cell E5.
 - Copy cell E5 to cell D4.
 - Highlight cell D4 in blue.
 - Type “1” in cell A1.
 - Fill in numbers 1-10 in cells A1 through A10.
 - Delete rows 3, 5, 7, and 9.
 - How many rows do you have filled in?
 - Type “2” in cell B1.
 - Create a formula to automatically add values of cells A1 and B1, with the result displayed in C2.
- Microsoft PowerPoint PE.
 - Open Microsoft PowerPoint.
 - Create blank slide.

- Insert a text box and type “Goblin.”
- Insert a photo; then crop photo.
- Create new slide.
- Insert a table created in Excel PE.
- Create new slide.
- Insert and utilize symbols, i.e., arrows, boxes, circles.
- Hide second slide.
- Display in presentation mode (slideshow).

Critical Thinking and Writing: Soldier will be given current news articles pertaining to one topic. Soldier will produce a written essay on what the articles are about, the impact the topic has, and how the topic will affect a given subject. Soldier will be given a data set and will be expected to analyze the information for patterns. Soldier will then produce a written essay with logical deductions from his analysis.

Guidance issued:

- Read the following articles.
- What is the strategic and/or theater-level implication?
- If you were in that theater of operations today, based on this information, what would be some of your tactical recommendations to your combatant commander?
- What do you think the North Koreans are trying to achieve?
- How is this BCT serving as the PACOM QRF?
- Write it in 12 point, Times New Roman, Double Spaced, no more than one page.

Example analytical exercise: In this case the CoIST board supplied three news articles from current world affairs to the candidate to read and evaluate. The candidate had to assess what the articles meant and suggest what the “next step” would be. At the time, the board used three articles from the Korean Peninsula as it was leading in the news. Those analysts who had kept up with current affairs had an edge on the exercise as they could put it into context. Those who didn’t follow current affairs had to rely on the articles alone. The exercise allowed the candidate to demonstrate an ability to synthesize information into a single picture in a professionally

written product to summarize that information finishing with predictive analysis.

Phases 4 and 5: Selection and Backfill

Candidates selected enter training as specified above. Those candidates who don't pass the selection process will be returned to their companies. The companies may then present another candidate. It may be advisable for companies to have more than one candidate in mind for the selection process

Conclusion

This chapter gives an example of a brigade commander memorandum that can be used to establish the CoIST within the brigade and then discussed the mission of the CoIST and gave examples of ways to choose members for the CoIST. These are not the only methods, but they provide guidance when establishing and choosing Soldiers for the CoIST.

Chapter 2

Mission, Task, and Purpose

The mission of a company intelligence support team (CoIST) is to serve as the primary source of information and intelligence that the company commander needs to make timely accurate decisions.

Company leaders must review, interpret, and evaluate huge volumes of data on a daily basis to ensure relevance and relationships. CoISTs are by mission devoted to streamlining that process. Time wasted on irrelevant information can mean lives wasted. CoISTs are an information management and analysis funnel for what can be an overwhelming flood of data from patrol debriefs, intelligence summaries (INTSUMs), link diagrams, and be-on-the-lookout (BOLO) lists just to name a few. Although the commander will determine and direct the exact requirements for the CoIST, specified and implied tasks usually include intelligence, surveillance, and reconnaissance (ISR); patrol pre-briefings and debriefings; predictive analysis; targeting; and tactical site exploitation (TSE).

The CoIST provides a 24/7 analytical, production, and dissemination capability that gives the company commander options to exploit enemy vulnerabilities. The CoIST is responsible for taking large volumes of collected combat information derived from multiple sources and turning it into actionable intelligence at the company level. Analysis is focused on the company operational environment (OE), with the ability to report and help populate the overall battalion and brigade combat team common operational picture (COP).

If managed properly, a CoIST assists the commander in managing battlefield effects and operational expectations across all direct actions (DA). Although the CoIST is co-located with the command post (CP) its members are not part of the CP, they are there to track key events that happen while any missions are ongoing. The duties the CoIST cell has to conduct are as follows:

Data Collection and Analysis

Collect data and conduct pattern analysis to include the following:

- Conduct patrol debriefs and analyze information gathered.
- Collect all electronic data such as the biometrics automated toolset and handheld interagency identity detection equipment (BAT/HIIDE) and cellular exploitation (CellEx) from returning patrols and disseminate.
- Track and analyze all significant activities.

- Generate analytical assessment and mission summary products for the commander and the battalion S-2.
- Conduct analysis of intelligence, forecast enemy actions (predictive analysis), and prepare the threat situational template (SITE MP) to include the threat's most likely course of action (MLCOA)/most dangerous course of action (MDCOA).
- Proposes targets to the commander for review and nomination through data mining and tying individuals to Significant Activities (SIGACTs).
- Battle track enemy SIGACTs to develop enemy patterns and tactics, techniques, and procedures (TTP).

Report and Exchange Information

Facilitate the exchange and dissemination of intelligence such as information flow to the company and to and from the battalion S-2 in the form of INTSUMs or Graphic INTSUMS (GRINTSUM), also carry out intelligence sharing with adjacent units, while performing the following:

- Dissemination of combat information and actionable intelligence.
- Maintain updated intelligence boards for outgoing patrols.
- Conduct mission pre-briefs and debriefs with all of patrols if feasible.
- Produce, process, and analyze information/material from TSE.
- 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 (AI).
- 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 and maintain clear communications with the battalion S-2 and adjacent companies through the use of a primary, alternate, contingency, and emergency (PACE) plan.
- Establish battle rhythm with the S-2 to pass information to and from the battalion on a regular basis.

Support Operations

CoIST should conduct daily commander's update brief (CUB) on intelligence-related matters to include the following:

- Intelligence preparation of the battlefield (IPB) for company operations.

- Provide information operations (IO) and civil military operation (CMO) recommendations to the commander.
- Support situational development and maintain understanding of the OE.
- Recommend company priority intelligence requirements (PIR) and specific information requirements (SIR) to the commander.
- Conduct assessment of effects and exploitation following a mission.
- Provide predictive analysis for the commander to develop COA and named AIs (NAI).
- 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, such as, ISR request of high level asset capabilities.

Support Targeting

Manage the company's lethal and nonlethal targeting. Company level targeting is the overall synthesis of all sources of intelligence—battalion and sister-companies 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 OE.

- Provides SA and Situational Understanding (SU) for the commander.
- Proposes targets to the commander for review and nomination.
- Utilizes ISR to target lethally and non-lethally.
- Produces company-level high-value individual (HVI) and high-value target (HVT) list.
- Develops the company-level target packets, and requests higher level assets and/or effects in support of lethal and nonlethal operations.
- Requests classified products and sensitive information from the BN S-2 for inclusion in the target packet.
- Works with the commander to further develop targets and identify gaps in the current intelligence picture (CIP).

- Supervises the company's ISR program. Based on the commander's guidance regarding company level PIR, develop an ISR collection matrix, using company level assets before requesting higher level assets. List below is an example of some assets that may be on your FOB.
- Networks with elements on your FOB and uses non-standard ISR assets.
 - Air Weapons Team (AWT).
 - Surveillance Weapons Team (SWT).
 - Nongovernmental Organizations (NGO).
 - Human Intelligence Collection Team (HUMINT) or (HCT).
 - SIGINT.
 - UGS.
 - Female Engagement Team (FET).
- Conducts planning, synchronization, and request for company and higher level assets.

Patrol Briefs

Manage the patrol pre-brief and debrief processes for the company. The patrol pre-brief is not to be confused with the patrol order given by the patrol leader from the commander. The commander and the platoon leader should work with the CoIST in the planning process for the development of their order. The pre-brief is given by a member of the CoIST to the patrol prior to departing the forward operating base (FOB), combat outpost (COP), or joint security site. During this process, outgoing patrols are briefed on the following:

- Pre-Brief.
 - Specific information requirements.
 - Possible TQ guidance.
 - Define the operational environment.
 - Describe the effects of terrain and weather.
 - Describe operational effects.
 - Evaluate the threat.
 - Determine the threat courses of action.

- Key intelligence items to discuss during the patrol pre-brief include the following:
 - Last 24-48 hours significant activities in the area of responsibility (storyboards or graphic intelligence summary).
 - Current IED threats and locations of concentrated IED attacks.
 - Route status.
 - ISR collection assets and priorities.
 - Current assessments and future expectations.
 - High-payoff target/High Value Targets (HPT/HVT).
 - Updates on key personalities (centers of gravity [COG], 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.
- CoISTs are vital to debriefs. At the conclusion of a mounted or dismounted patrol, leaders, Soldiers and host-nation forces (if applicable) must be debriefed by their CoIST in their respective unit to ensure information and intelligence is 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 OE and is decisive in the targeting process (lethal/nonlethal).

- General village assessments and debriefs of a key leader engagement (KLE) with an SOR allow the company commander and his CoIST to focus their efforts in developing village stability operations (VSO) and/or District Stability Framework (DSF) and refining the lines of effort (LOE) from the company and higher.
- To have an effective patrol debrief, the CoIST must have a standardized patrol debrief format, consistent with the reporting requirements of higher headquarters and what SIRs were given at the pre-brief. 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 horizontally and vertically. Additionally, this data will feed the intelligence cycle, continue the IPB process, and ultimately begin the next operation cycle for the company, BN, and BCT.
- Patrol debrief tactical ground reporting. The primary system the CoIST can use to capture this data is the Tactical Ground Reporting (TIGR) System. (**Note:** See Chapter 8 for data capture details.)
 - The database allows the CoIST or analysts the ability to upload debrief reports, assessments, and media; organize debriefs geographically; and allow adjacent units the ability to query the database utilizing filters. In addition to uploading the database, this system allows other intelligence collectors the opportunity and ability to share and synchronize intelligence. It is imperative that Soldiers understand that patrol debriefs are what feed the intelligence that drives the company operation cycle.
 - Reports need to be entered directly into TIGR summary and not as an attachment to the patrol report, which make it unsearchable. During a debrief, the CoIST must get an honesty trace from the patrol to verify the route taken out and back. Additionally, all media and events occurring during the patrol must be associated with that patrol. All this is done to ensure the data is searchable for later use. Debrief 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 (preferred method):
 - ◆ 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 asks questions (least preferred method):
 - ◆ Pros: Less time-demanding for CoIST since debrief is written.
 - ◆ Cons: May miss important information from other points of view.
- Ultimately, the CoIST must analyze this data and answer the commander's PIR to update the ISR plan and answer any request for information (RFI) or intelligence gap. Key intelligence items to discuss during the patrol debrief include the following:

- * Answers to PIR, SIR, 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.
 - * Sources of Influence (SOI) assessments, observations, and notes from Key Leader Engagement (KLE).
 - * Updates to ISR matrix and PIR.
 - * Updates to patrol-level PMESSII, ASCOPE, and other related assessments.
 - * Updates to town/village assessments.
 - * Host-nation security force assessments.
 - * HIIDE upload to BATS database.
 - * Updates to intelligence database (TIGR).
- If conducting mission or patrols with host-nation forces, the CoIST should be prepared to debrief them as well because these forces usually have a more in depth knowledge of the area and see the operational environment in a different way than our Soldiers. Debriefing host-nation forces is often time consuming due to language barriers. There are several techniques that can be used in debriefing host-nation forces. The CoIST must ensure shared information meets operational security requirements regardless of which method is used to debrief the host-nation forces.
- * Debrief US and host-nation forces at one time:

- ◆ Easiest to accomplish when there are fewer OPSEC requirements.
- ◆ Allows US to understand local point of view during the process.
- ◆ Can cause confusion if different operational terms are used between the parties.
- * Debrief US and host-nation forces separately:
 - ◆ Allows US forces to speak without limited restraint.
 - ◆ Does not allow both parties to build on each other's observations.
 - ◆ Can cause confusion if debriefs vary in content.
- * Train host-nation forces to conduct debriefs and obtain a finished debrief from host-nation leadership:
 - ◆ Least time consuming for CoIST.
 - ◆ Allows host-nation forces to understand the process and importance of debriefs.

Support Detainee Operations

CoIST support to detainee operations is twofold:

- Ensure departing patrol units are armed with complete detainee packets and the knowledge to properly complete the forms.
- Ensure returning patrols have completed forms correctly and gather any remaining statements or forms.
- Maintain detainee packet data, copies of complete packets, and track the current location and status of the company's detainees.

Support Tactical Site Exploitation

The CoIST must ensure units depart on patrols trained and equipped with the proper TSE paperwork and equipment.

- DA Form 4137, Chain of Custody.
- CALYX.
- HIIDE.
- Digital camera.

- Evidence bag.
- Pen and paper for sketches.
- Gloves.

Upon completion of the patrol and following debriefs the CoIST sorts through photos collected, downloads biometric data from HIIDE to BAT and then syncs it to the BAT database. It is here the CoIST, once again, begins its data synthesis to update its targeting. The CoIST submits document and media exploitation material to higher headquarters in a timely manner.

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

- TSE/TQ plan must be involved in the CONOP.
- TQ involves direct questions only.
- TQ does 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 TQ involves threats directed at the detainee or his family.
- CoIST CANNOT run a source or an approach on any detainee brought in with TSE! It is unlawful and will result in UCMJ action.

Conclusion

The CoIST is not staffed, equipped, or authorized by a modified table of organization and equipment (MTOE), 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 a selection process 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 organic specialized staff (except newly authorized 35F) personnel to perform this mission and must constitute CoIST out of hide. Regardless of how large or how well staffed, 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, as of October 1, 2011, an MTOE change to maneuver units places one 35F Intelligence Analyst at the company level.

Chapter 3

Organization and Duties

The company commander is a key player in all aspects of company operations. This is especially true when it comes to the structure, manning, and integration of the company intelligence support team (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 have the following attributes:

- Possess or be eligible for 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 8).
- Possess operational experience to understand what information is important and how to present it.

It is also important the CoIST has sufficient 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), and special IR (SIR); commanders cannot allow their IR to stagnate.
- Follow the standing operating procedure (SOP).
- Maintain regularly scheduled communication with higher headquarters' staff.
- Maintain and retain CoIST personnel once they have been trained.
- Minimize distracter tasks for the CoIST.

Recommended CoIST Manning Chart

Six CoIST personnel:

- One CoIST noncommissioned officer in charge (NCOIC)
- One analyst
- Four Soldiers

Figure 3-1. Manning chart

CoIST Officer in Charge (OIC)

The CoIST OIC is the senior Soldier assigned to the CoIST. He receives direct guidance and direction from the company commander and executive officer (XO) and assists and participates in the company planning process engaging with the S-3 officer on future and current company operations.

Primary OIC tasks include the following:

- Complete oversight of CoIST operations.
- Establish unit CoIST SOP.
- Coordinate with company commander in development of commanders critical IR (CCIR), PIR, and IRs.
- Continuous integration with company operations and company planning process.
- Over sees production and dissemination of CoIST products.
- Maintain communications with battalion S-2 officer and collection manager.
- Coordinates company active and passive counterintelligence effort.
- Engages with company operations on force protection effort.
- Serves as company collection manager overseeing processes and dissemination of Battalion PIRs and company special operational requirements (SOR).
- Coordinates with headquarters company to request additional intelligence resources in accordance with company collection effort.
- Attends targeting boards and meetings to coordinate company nominations with battalion targeting.

- Ensures CoIST members are tasked appropriately and identifies priorities of work.
- Manages current and emerging targets, and ensures target packets are created to facilitate servicing of targets.

CoIST Noncommissioned Officer in Charge (NCOIC)

The CoIST NCOIC (or chief) is the senior enlisted Soldier assigned to the CoIST. He receives guidance and direction from the XO and CoIST OIC. Assists the watch officer in building the common operational picture (COP) and supervises CoIST in order to effectively support future and current operations.

Primary NCOIC tasks include the following:

- Supervise CoIST operations and personnel.
- Ensure briefs are conducted for outgoing patrols.
- Ensure debriefings are conducted for all patrols.
- Assist OIC in requesting and integrating organic/non-organic support into the company's collection effort.
- Produce intelligence briefs for company commander.
- Supervise intelligence briefs to support operations.
- Ensure debriefs are integrated into the collection effort.
- Supervise production/dissemination of intelligence reports.
- Supervise production of unit target packages.
- Supervise production of local area maps, imagery, and products within company capability.
- Request intelligence products from battalion S-2.
- Supervise detainee tracking for further exploitation.
- Rapidly process, disseminate, and exploit information.
- Coordinate with higher, adjacent, and supporting units on intelligence-related matters.
- Maintain communications with battalion S-2 and supported units.
- Publish daily changing of primary and alternate challenge and passwords, signs and countersigns. Take appropriate action if they are compromised.

- Supervise intelligence preparation of the battlefield (IPB) of the company area of operations (AO) and individual missions.
- Ensure all products are up to date pertaining to IPB, collections, analytical tools, target dossiers, CoIST journals, battalion reports (intelligence summaries, tactical site exploitation [TSE], supplementary reports, situation reports).
- Supervise and review analysis of events and combat reporting to support the battalion intelligence effort.

CoIST Analyst

Primary Soldier analyst tasks include the following:

- Assist in operational planning, company targeting boards, and mission preparation.
- Prepare and maintain IPB for company AO and individual missions.
- Prepare and maintain targeting packages.
- Produce and disseminate required intelligence reports for supported, supporting, and adjacent units.
- Maintain the TIGR and company database.
- Assist in production of intelligence briefs to support operations.
- Input information gathered into the appropriate system for analysis, production and dissemination.
- Prepare and maintain CoIST intelligence boards.
- Prepare and maintain link analysis on lethal and non-lethal targets.
- Produce local maps, imagery, and products within capability.
- Conduct honesty trace (friendly pattern analysis).
- Track detainees for further exploitation.
- Ensure all special material is forwarded to battalion for exploitation.

CoIST Collection Analyst

Primary collection analyst tasks include the following:

- Assist OIC and NCOIC in development of company intelligence collection plan.
- Track enemy activity on enemy situation map.

- Monitor unit unmanned aerial systems (UAS).
- Assist in briefing patrols on company collections focus of effort.
- Track “be-on-the-lookout” (BOLO) vehicles.
- Assist in debriefs to support the collection effort.
- Process unit imagery support requests to battalion S-2.

CoIST Common Skills

CoIST member common skills include the following:

- Operate digital camera and video assets.
- Operate CoIST suite, BATS/HIIDE, OSRVT Suite, and related software.
- Enter personnel profile data into BATS system.

CoIST Duties in the Company

Primary team duties in a company include the following:

- Man the company CoIST as the intelligence watch at all times.
- Track enemy activity.
- Maintain intelligence journal.
- Update pattern analysis products.
- Brief and debrief patrols, convoys, and guard rotations.
- Maintain all intelligence information boards in the command post.
- Maintain enemy situation map.
- Perform quality control on Intel TIGER database entries and products.

Conclusion

A CoIST is by definition a small team. Delineation of duties and use of SOPs will help the team function, especially under the strain of continuous operations. That said CoISTs are small enough that every team member from OIC to analyst should be cross-trained and functional in every team position within 90 days of forming the team. Cross training builds redundancy and flexibility necessary in combat. Finally, as a CoIST builds and cements itself as a team, care must be taken that it not become too internally focused. Cross training with company command post personnel and exchange duties with adjacent CoISTs and battalion S-2s should also be integrated into the long-term training and sustainment plan.

Chapter 4

Physical Layout

The CoIST must stay current on all operations and should be co-located with the company command post (CP) from which it can communicate directly with the battalion S-2 as well as units on patrol. This proximity to the CP's radios increases CoIST situational awareness as it continues intelligence collection and analysis. Remember the CoIST serves as a functional component of the CP; it is not meant to run the company CP. Control measures must be established so sensitive material is only seen by those with appropriate access. The CoIST also requires close access to the company decisionmaker (commander, first sergeant, or executive officer).

Pictures in this chapter depict a way to lay out a CoIST for operations in a tactical environment. The graphics depict what a CoIST should produce and disseminate. They show 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.

The analytical section of the CoIST is the area 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.

The CoIST should establish a patrol tracker separate from the operations patrol tracker. The patrol tracker helps the CoIST identify patterns and signature tactics, techniques, and procedures (TTPs) the company may be creating. During the patrol pre-brief, the briefer should recommend certain actions to the patrol leader, such as leaving at a different time or taking a different route.

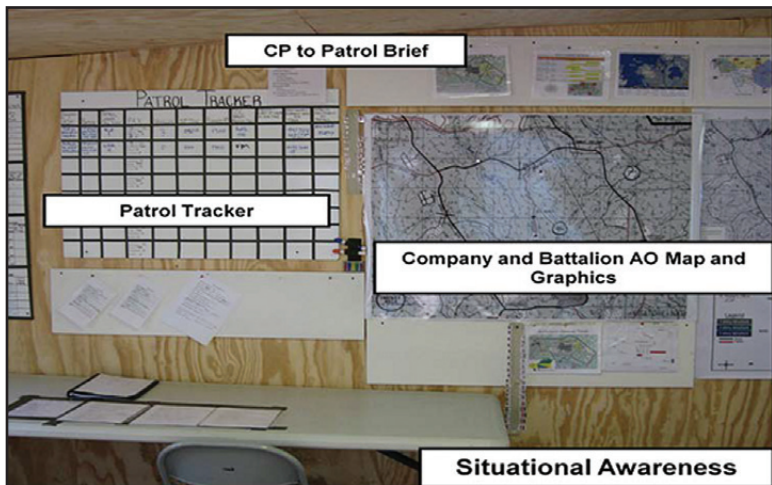


Figure 4-1. CP to patrol brief

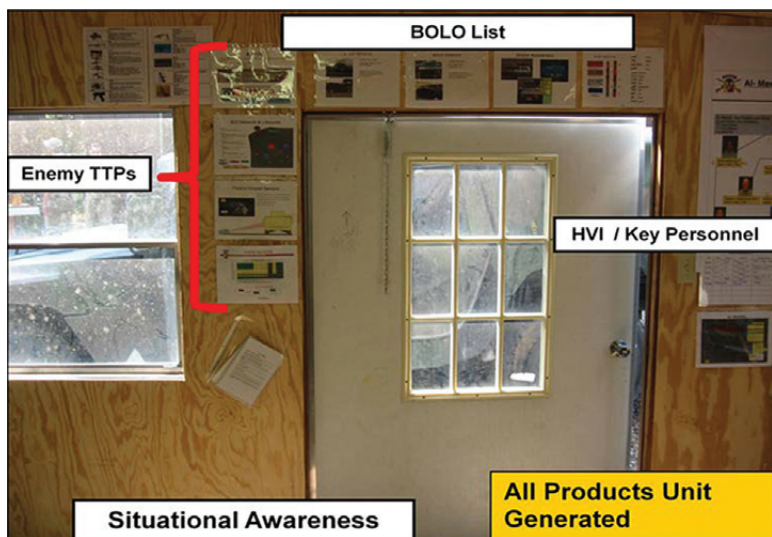


Figure 4-2. All products unit generated

Products include the following:

- Enemy situation.
- Contacts, location, movement.
- Identity.
- BDA.
- Might include detainee/EPW status.
- Targets (HVT/HPT).
- Significant activity (SIGACT).
- Light and weather data.
- Signal operating instructions data.



Figure 4-3. SIGACT tracking for SA

SIGACT tracking includes the following:

- Company combat power.
- Company assets tracker.
- Attachment combat power.

- Route status tracker.
- Medical facilities tracker.
- Fire support assets available.
- Air assets available.
- Unit locations and activities.
- Combat power and status of assets.
- Analytical materials.
- Pattern and link diagrams, be on the lookout for (BOLO) lists, etc.
- Imagery, overlays, etc.
- Synchronization matrix.
- Essential elements of friendly information (EEFI).
- Supply status.

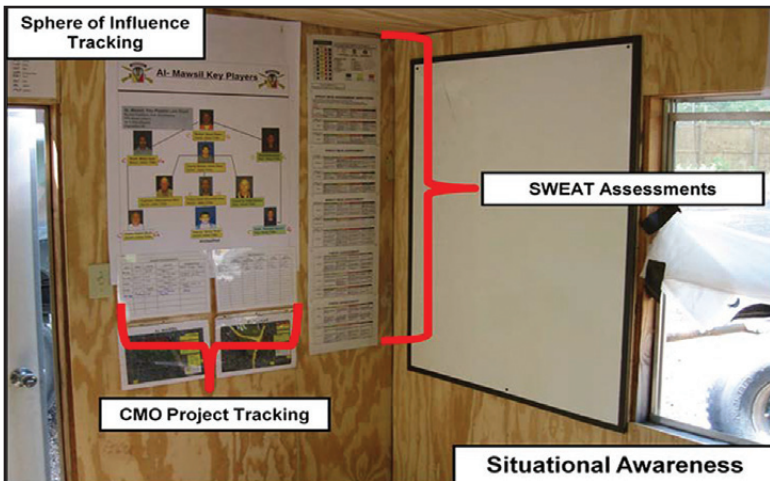


Figure 4-4. Sphere of influence tracking

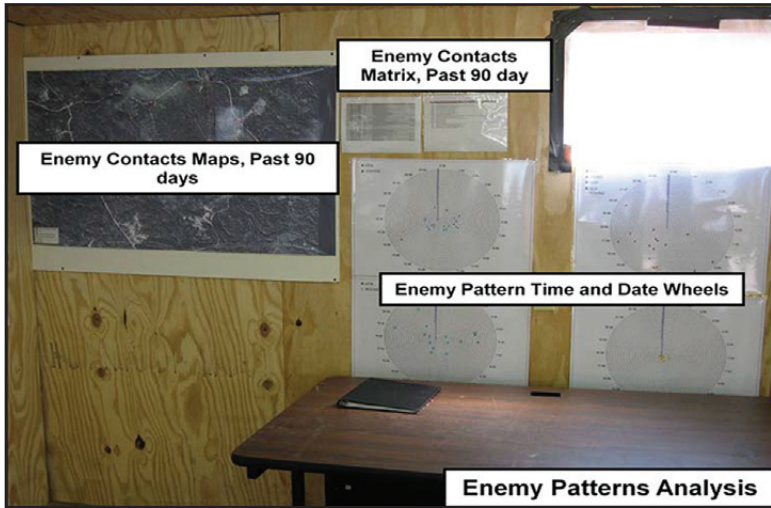


Figure 4-5. Enemy patterns analysis

Debrief returning patrols:

- Debriefing is one of the most critical tasks that the CoIST can conduct.
- Debriefing goal is to discover what indicators were present prior to, and after events, as well as answering commander's requirements.

Missions should not be considered over until a debriefing is conducted.

- Events are tracked in CP.
- CoIST members prepare debriefing as patrol returns.
- Patrol leadership and members of patrol participate in debriefing, with CoIST focused on gathering answers to SIRs given during pre-briefing.
- Debriefing is not complete until the debrief is input into TIGR so that adjacent units can access the information.



Figure 4-6. Debriefing area

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 CoIST. 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 priority intelligence requirement (PIRs), specific information requirements (SIR), specific operational requirements (SOR), and indicators. Additionally, the commander must set clear priorities to assist the CoIST in executing 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 5

Battle Rhythm

Battle rhythm and operational tempo (OPTEMPO) are critical to both command post (CP) and company intelligence support team (CoIST) operations. An established, effective, and understood battle rhythm boosts efficiency and speeds information sharing. Certain leaders must work together in building battle rhythms to meet OPTEMPO. The commander and his CoIST leaders and NCOs must work as a team in establishing the CoIST battle rhythm. Although the roles and missions of the CP and the CoIST differ they are collocated as partners in maintaining situational awareness (SA). Do not attempt a two-for-one on CP teams and CoIST; they will both need to be filled from hide.

Standing Operating Procedures (SOP)

Successful continuous operations at the company level are more demanding than at higher-level organizations. Why? Because small units by definition must do more with less when it comes to personnel. Efficiency is the key and nothing improves efficiency more than a standing operating procedure (SOP). The unit requires a tactical SOP (TACSOP) allowing rest, especially for critical personnel. The rest plan must be a priority for the company to be led effectively and for their units to be successful on the battlefield.

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

- Shift changes.
- Battle update briefings to the commander.
- Battalion S-2 synchronization meeting.
- Battalion targeting meetings.

Nested Battle Rhythms

The CoIST OIC and NCOIC must nest a battle rhythm with the S-2 and the commander for updating and viewing information and understanding how to use it to affect operations. A well-established battle rhythm aids the commander and CoIST leaders in information management, wall products, and decisionmaking in order to understand the operational environment (OE). Battle rhythm demands careful planning and design, and competing

demands must be de-conflicted. Even subordinate platoons and sections affect a company battle rhythm based on their needs and unit procedures.

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. The CoIST must maintain 24-hour operations.

Without an established battle rhythm the CoIST will suffer, missing key decisions and losing key information, which may lead to unsuccessful mission and unnecessarily putting Soldiers in harm's way. With the battle rhythm in place the CoIST will see things more clearly and better analyze the information being brought to the CoIST. Procedures and processes facilitating efficient decisionmaking and parallel planning are critical to achieving battle rhythm. Every component of battle rhythm contributes uniquely to prolonged operations.

Get it Right in Training

It is difficult to establish battle rhythm while simultaneously conducting operations; SOPs are a must to establish the battle rhythm. Planning, preparing, and training before deployment lays a solid foundation for a viable battle rhythm during operations. Company commanders must coordinate with the battalion S-2 and S-3 sections 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:

- Established processes and SOPs.
- Trained second- and third-tier leadership in the CoIST.
- Lateral and horizontal information dissemination.
- Parallel planning.
- Synchronized upward multi-echelon timelines.
- Shift change.
- Sleep and rest plans.

Command Post Personnel Depth

Established processes and SOPs relieve many antagonistic effects of extended operations. SOPs that establish and maintain battle rhythm to facilitate 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:

- Troops in contact (TIC) summaries and updates during a fight.
- Intelligence updates before, during, and after a TIC.
- Sustainment updates before, during, and after a TIC.
- Updates to the next higher commander.
- Shift change briefings.
- Daily intelligence updates to keep commander's situational awareness at the highest level.

Continuous Operations and Timelines Synchronization

Timelines for the operation at hand must allow for not only the next operation but also extended continuous operations. If units do not address critical events at least one level up disruption will result. 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 battalion staffs on developing SOPs that include planning, rehearsal, and execution timelines one level below battalion to prevent these conflicts.

CoIST SOP and Battle Rhythm

The CoIST must establish an internal SOP and battle rhythm that outlines recurring cyclic events, such as meetings and shift changes, and also incorporates 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 pre-brief and debriefs 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 battalion 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 wall/board for outgoing patrols (senior CoIST Soldier).
- Contact adjacent units for intelligence sharing (CoIST OIC/NCOIC).
- Update and synchronize biometric information. (CoIST analysts).
- Send up daily INTSUM/GRINTSUM with last and next 24-hour assessments. (CoIST analysts).
- Weekly:
 - Analyze week's events (CoIST OIC/NCOIC).
 - Conduct pattern analysis for the last seven 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 (NAIs) (senior CoIST Soldier).
 - Update company, troop, and battery priority information requirements (PIRs) and specific information requests (SIRs) (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 battalion 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 battle rhythm:

Company/Battalion:

0800 – Shift change slides information cutoff (S-2).

0830 – Shift change slides due to battalion battle captain (CPT).

0830 – Company fusion cell (CFC)/S-2 net call via Adobe Connect.

0900 – Battalion shift change.

1000 – Battalion battle updates assessment (BUA)/staff synchronization (synch) meeting (S-2).

1300 – Battalion intelligence, surveillance, and reconnaissance (ISR) synch meeting (S-2, CFC).

1700 – Battalion collection planning session (S-2, CFC).

1800 – Company collection plan due to battalion (CFC).

1900 – CFC INTSUM information cutoff (CFC).

2000 – CFC INTSUM due to battalion.

2000 – Shift change slides information cutoff (S-2).

2030 – Shift change slides to battalion battle CPT.

2030 – Battalion INTSUM posted.

2200 – Battalion shift change.

Brigade Sensitive Compartmented Information Facility (SCIF):

0800 – Battalion shift change slides information cutoff.

0800 – SCIF shift change slides information cutoff (SCIF NCIOC, operations, fusion, S2X, collection management and dissemination [CM&D], and signals intelligence [SIGINT]).

0900 – Battalion shift change slides due to brigade.

0930 – Brigade shift change.

0930 – Brigade 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 – Brigade ISR synch meeting (S-2, ISR, targeting, and military intelligence company).

1530 – BCT daily targeting meeting (S-2, ISR, and targeting).

1830 – Battalion collection plan/asset status update to BCT (ISR).

1830 – SCIF huddle (SCIF NCIOC, fusion, S2X, CM&D, and SIGINT).

1900 – Battalion INTSUM information cutoff.

2000 – Battalion shift change slides information cutoff.

2000 – SCIF shift change slides information cutoff (SCIF NCIOC, operations, fusion, S2X, CM&D, and SIGINT).

2030 – Battalion INTSUM due to brigade (S-2).

2100 – Battalion shift change slides due to brigade.

2130 – Brigade shift change.

2130 – Brigade INTSUM posted.

2130 – Brigade shift change slides due to SCIF.

2200 – SCIF shift change.

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 the CoIST operations. Although the purposes and missions of the CP and the CoIST are different, the two entities are co-located. Even with a necessary and clear delineation of duties and responsibilities, minimal overlap and redundancy must occur between the CP and the CoIST. The relationship between OPTEMPO, battle rhythm, and the unit intelligence cycle necessitates the development of SOPs and TTPs that account for and encompass all CoIST and intelligence-specific considerations.

Chapter 6

Networking

As stated in the opening chapter of this handbook, the success of a company intelligence support team (CoIST) begins with a brigade commander's commitment to the program. The staff supervisory agent for CoIST throughout a brigade combat team (BCT) naturally devolves to the brigade S-2 as the senior intelligence officer within the BCT. BCT S-2s look after battalion S-2s, and in following that pattern, battalion S-2s and their sections serve the same role for CoISTs. A CoIST remains that company commander's intelligence "shop," the battalion S-2 section helps train, support, and sometimes resource the CoISTs in its subordinate units.

The overall goal of the CoIST is twofold:

- Aid the company commander in his military decisionmaking process (MDMP) by extending a common operational picture to the company.
- Assist the battalion S-2 in providing a flow of bottom-up intelligence to higher headquarters.

For the company intelligence support team (CoIST) to be effective, its activities, analysis, and reporting must be carefully integrated to flow horizontally and vertically. Integration encompasses an open two-way information exchange from the platoon level across companies 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 and BCT-level intelligence sections. It absolutely does not! The battalion S-2 section is by organization and capabilities the nexus for CoIST operations throughout a battalion sector.

While the CoIST is a company asset, its effectiveness is contingent on its ability to process raw information into actionable intelligence for the company sector into a picture that will assist the company commander in his MDMP. The quality of CoIST-developed intelligence directly affects adjacent and higher units. So it is important that the company commander and battalion S-2 establish and adhere to a well-defined battle rhythm that integrates the CoISTs with the battalion S-2. Ultimately the CoIST works for the company commander but has "due outs" to the battalion S-2. Battalion intelligence sections have very limited manpower; proper integration with subordinate CoISTs can expand those capabilities threefold.

Advocacy for the CoIST Network

Given the potential boost in the battalion intelligence system from adding CoISTs, it stands to reason that the greatest advocate for CoIST should be

the battalion S-2. CoIST adds a network of analytical cells to a battalion intelligence system. At the company level, the press of immediate events may somewhat blind a company commander to the positive effects of a successful CoIST for many months. The commander and first sergeant may wonder why they gave up four to six of their smartest Soldiers toward this effort. Worse still, they may start pulling them back toward what they consider more important duties.

The S-2, however, should always be looking at the larger battalion intelligence fight and therefore recognize the value of the CoIST network. The battalion 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 taskings CoIST members encounter. Finally, the S-2 will know the origin of effective intelligence and must ensure that company and battalion commanders are aware of what successes have resulted from the hard work of the CoIST. Only by sharing the successes of effective CoIST can the battalion bring about a general understanding of the importance of their efforts.

Overall, the successful implementation of CoIST involves extensive effort on the part of the battalion S-2. If the S-2 fails to do the required preparatory work, his own use of the CoIST network will likely fail. S-2s must put in the required planning to ensure the fused intelligence picture is pushed to the company level. CoIST must understand that no matter what their geographic disposition, their efforts are not isolated, and a failure to implement the guidance and SOP of the Battalion 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 and 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. Critical to that understanding is grasping that CoIST is NOT a single entity; rather CoIST is a network that offers horizontal and vertical situational awareness.

Battalion Intelligence Section

The battalion S-2 is therefore central to the success of CoISTs in subordinate units. The S-2 must create systems so the CoIST network provides the S-2 section analyzed intelligence products rather than raw information. CoIST and the CoIST network become knowledge management drivers for efficiency rather than uncontrolled gushers of unanalyzed data. The first will reduce the overall workload on the battalion S-2 analysts and lead to the creation of better intelligence products at all levels. The second will drown the battalion S-2 section. Avoiding that effect requires the S-2 to provide the following five things to the CoIST network:

- Advocacy (discussed above).

- Guidance.
- Standing operating procedures (SOP) from the brigade level down.
- Involvement in training.
- Feedback.

Clear Guidance

While the CoIST works for the company commander, the company is in fact the best intelligence asset in the battalion's possession. As a result the company is often tasked to answer battalion-level information requirements (IRs). The information that a battalion commander needs to succeed can be broad and extremely complicated. The S-2 must work to break this broad swath of necessary information into clear, specific IR and then work with the S-3 to task these to the appropriate units. Ideally they will be pushed to the company as part of the battalion daily fragmentary order (FRAGO) in the form of special operational requirements (SOR) or intelligence tasking.

The S-2's work does not end here, however, as he must ensure that the company tasked with the IR understands 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 that these battalion-level information requirements are answered in a timely and effective manner.

SOP

The battalion S-2 owes the CoIST a detailed SOP on all aspects of CoIST operations. Again, the format and quality of information posted by one CoIST directly affects the success of adjacent CoISTs and thus must be managed from the higher level. The SOP required generally falls into four broad categories:

- Primary, alternate, contingency, and emergency communications (PACE).
- Reporting requirements.
- Intelligence synchronization products.
- Data basing and knowledge management guidelines.

Some common examples of procedures the battalion S-2 owes the CoIST are the following:

- Battalion pre-brief and debrief formats in the SOP.
- Targeting product formats in the SOP.

- Daily intelligence summaries (INTSUM) and graphic INTSUM (GRINTSUM) formats in the SOP (or whatever format is used to pass information between company and battalion level).
- Data entry SOP for the various TIGR system functions (significant activities [SIGACT], HUMINT reports, SIGINT 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 paperwork of detainees.
- Other SOP a battalion S-2 might determine applies to a specific AO.

The battalion 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 SOP. The basic guideline is the SOP 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 this SOP is an extensive amount of work for the battalion S-2 section but is necessary to ensure a smooth flow of information throughout the battalion sector.

Training

A typical maneuver battalion only has school-trained military occupational specialty (MOS) 35F intelligence analysts within the battalion S-2 section. While mobile training teams (MTT) provide a baseline of training to most CoISTs, often the Soldier who receives the MTT training is replaced before the unit hits theater. So to counter this, the S-2 section must step up to ensure these individuals receive basic analytical training.

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

- Instruction in the battalion standard debriefing process.
- Classes in the threat groups and enemy tactics in a particular area of operation (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 intelligence surveillance and reconnaissance (ISR) assets that operate within the AO.

Most often the S-2 section will be busy training for their mission and won't have time to train the CoIST. This is why it is imperative that the company commander select the right individuals to man the CoIST and keep them in place throughout initial training to completion of the deployment.

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 IRs should also be taught. If the battalion S-2 takes a hands-off approach to the training of the CoIST, their effectiveness will be greatly diminished upon arrival in the combat zone.

Feedback

The battalion S-2 owes the CoIST clear and useful feedback on all products it produces. When a CoIST believes they are operating in a vacuum and no one is looking at the work they present, this will invariably produce substandard products. Feedback on whether products such as debriefs and area assessments are meeting the intent for the battalion can easily be entered through the comment feature on TIGR but is best offered in a discussion between the S-2 and the CoIST. This discussion usually takes the form of a meeting (either face-to-face or over a digital communications system) between the S-2 section and CoIST to discuss the information that has come from each company sector during the week and also the status of any IRs that have been answered or remain unanswered. The more feedback the CoIST receives on their piece of the intelligence effort, the better the results will be for both the company and the battalion.

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 PIR/SIR as well as incorporating the battalion and BCT commanders PIR/SIR. The SIR and SOR developed can then be addressed by requesting ISR assets from higher echelons or by using company-level organic assets first.

The battalion can conduct detailed IPB. The battalion S-2 section in conjunction with the S-3 develops and proposes an ISR plan to the battalion commander. ISR assets are used to answer battalion PIR/SIR, assist in targeting process and analysis of available intelligence to drive tactical operations. 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. At the BCT level the S-2 section mirrors the battalion S-2 section. The manning at the BCT differs by having additional personnel to conduct a more in-depth analysis. Also the BCT is the liaison to division and higher for gaining external ISR assets and confirming targeting packets.

PIR, SIR, and the Intelligence System CoIST to BCT

The intelligence system is built to meet and service intelligence requirements that support commanders. Company PIR is derived from the battalion PIR, which comes from the BCT PIRs. Once the company commander has established his PIR, the CoIST then creates company level SIRs to be given at the patrol pre-brief. If any SIRs are answered by the patrol during the debriefing this may answer PIR at the higher levels. Maneuver orders from higher commanders can become company-level PIR/SIR. Information can be collected back at patrol debriefings on SIRs and reported to the battalion section.

CoIST must understand how to conduct effective patrol pre-briefs and debriefs. This will allow CoIST to report, analyze, and exploit information and glean intelligence derived from these reports. With this the CoIST will develop enemy estimates, conduct pattern, trend, and predictive analysis, which supports the targeting process. The final outcome is to answer company commander's PIR and conduct timely intelligence-driven operations throughout the AO.

The main tool that will be used for pre-brief and debrief is TIGR. The CoIST will start by opening a report after each pre-brief happens and log any SIR given to the patrol. Upon return of the patrol the CoIST will have a copy of the SIR given to the patrol to assist them with debriefing. Debriefing should be an 80 percent to 20 percent mix with the patrol doing 80 percent of the talking. Once done debriefing with all the patrol members, the report in TIGR must be completed. This should not be an Excel or Word attachment and must be typed right into the report summary block to ensure it is searchable. After the report is saved it is now instantaneously viewable by everyone in theater.

Intelligence shared during a patrol brief should not be limited to lethal targeting or effects but should also focus on nonlethal effects. As the COIN environment matures, it is essential that commanders and leaders focus on nonlethal targeting and the operational environments (political, military, economic, security, social, information, infrastructure [PMESII]) or area structures, capabilities, organizations, people, and events (ASCOPE).

During the patrol pre-brief, CoIST and S-2s must submit SORs to the patrolling unit. These SORs allow Soldiers the opportunity to answer intelligence gaps and assist in answering the commander's PIR/SIRs. CoIST must continue to refine their collection focus to aid in the support of the ISR plans. The ISR plan 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 from the S-2 or company commander.

CoIST Synchronization and Integration of ISR and Collection Assets

The other half of the intelligence system is organized around managing collection assets to develop needed information. In that regard, ISR is much like Fires, which is organized about achieving effects on targets and systems that will reach those targets. The CoIST then serves a function like a Joint Fires Observer at company level. The CoIST develops intelligence from information at the same time managing information collection assets through ISR synchronization. This ISR synchronization supports integration of lethal and nonlethal 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 must detect the enemy before the unit can deliver fires against him. Synchronizing ISR can fall in the lap of a junior CoIST whose members do know or understand how to synchronize with battalion and BCT S-2s.

It falls to the battalion S-2s to ensure that the CoISTs in the battalion network grasp the fundamentals of ISR synchronization. Units need to know what assets are available and request them based on capabilities needed for the mission and must synchronize the effort to provide the best ISR coverage. This should be a significant part of the lethal/nonlethal 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.

The CoIST should always try and use company assets first when developing an ISR matrix. When the CoIST needs ISR assets from outside the company, 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 when the latest time information of value (LTIOV).

All ISR requests will be sent up to the battalion consolidated, and, if necessary, requested from brigade. The CoIST needs to be as specific as possible when explaining why it needs a particular capability.

Considerations when doing ISR planning:

- What do you know?
- What don't you know?
- What do you think?
- What are you doing about what you don't know?

Things to consider when requesting ISR include the following:

- 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 manager.
- 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 battalion 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 lethal/nonlethal 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 pertaining to the SORs.
- 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 battalion 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 battalion with obtaining the asset needed to support the mission.

The CoIST needs to address the following questions with the company commander and the battalion staff:

- What intelligence sources are in the unit's area of operation?
- How long does it take to get the information from subordinate collectors?
- Does the architecture for data storage support rapid recall and manipulation?
- 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

Understanding CoISTs means first grasping that CoIST is not a single team operating in support of a company commander. CoIST is a network of teams operating in support of all the company commanders in a given battalion. As a battalion network of teams, the battalion S-2 and S-2 section serve as the central net control for that network. A single CoIST may succeed in providing localized intelligence to its company commander and an array of disconnected CoISTs may all achieve similar successes. A network of three to five CoISTs trained, mentored, and controlled by an active battalion S-2 and section can do far more.

Chapter 7

Targeting

As discussed previously, a company-size element has very limited resources. At the battalion and brigade combat team (BCT), S-2 sections are staffed to cover baseline requirements while at the same time contribute to staff planning and working groups. The current operational environment has placed added emphasis on the targeting process in both lethal and nonlethal constructs. The battalion and BCT target working group reviews all target nominations and attempts to understand how the enemy network ties into the area of operations and interest (AO/AI) with adjacent units' AOs and AIs. At headquarters above company-level, a synchronized targeting line of effort facilitates the defeat of enemy networks.

Targeting at the Company

The CoIST takes information from patrols and engagements, extracts the intelligence, and forwards that analysis to higher headquarters. This intelligence helps the battalion and BCT targeting cycle. At the CoIST, the key to successful targeting is separating the important from the unimportant and then focusing company assets and external resources to influence the company area of responsibility (AOR).

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

CoIST Target Development Support

A target is an entity or object considered for possible engagement or action by lethal or nonlethal means. It may be a person, place, or thing 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! The purpose of targeting is to disrupt, delay, or limit enemy interference with 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 appropriate systems to achieve the desired

effects. Targeting is based on the enemy's assets that provide them an advantage, scheme of maneuver, and tactical plans.

Targeting in stability operations requires a detailed understanding of social networks, insurgent networks, actions, and civil considerations. 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 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.

Pre-targeting Meeting

To conduct successful targeting meetings, the CoIST must prepare information to share with all participants. The CoIST inputs for the pre-targeting meeting include:

- 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 and special information requirements (PIR/SIR) (received from higher headquarters and refined by company).
- Enemy course of action (ECOA) and event template.
- Intelligence surveillance and reconnaissance (ISR) plan for the next 72 hours and assets available.
- Enemy COA for the targeting period.

The CoIST gets the battalion target packet, based on information gathered by unit missions. The target packet should be an all-source product with vetted and validated information from two separate reports/sources in support of the desired effect. As data is gathered, the CoIST assembles the information and creates a target packet for the HVT or HVI and performs updates as information changes or becomes available. For nonlethal targets, the same format serves to keep files on important personnel in the unit AOR and as a quick reference for units if there is a planned engagement

or meeting with the individual. 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 after 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.

Targeting Meeting

A targeting meeting should end with the commander’s decision on 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 recurring event to keep the unit focused on commander priorities and to assess operational effects. Synchronization meetings outside the company with the battalion staff (S-2/S-3) serve to deconflict targets. Targeting meetings can also be hasty meetings prior to missions to ensure the unit receives all relevant information and the commander’s most current guidance. It is also a means of assessing current lethal and nonlethal effects to determine if a change to the current plan is needed.

Target Development/Prioritizing Lethal and Nonlethal Targets

All members of the target working group must 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 joint efforts to defeat the network. 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 (high-payoff target list [HPTL]) and photographs to the host nation security forces and strive to conduct joint targeting with them.

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 outlining an IED network. An IED explosion is the culmination of a network operation that supported the IED. Someone emplaced the IED and may have initiated it. All of those "someone's" 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 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 Axis Pro to build the diagrams. Microsoft PowerPoint also works well if the unit has no access to this program. An example link diagram is shown in Figure 7-1.

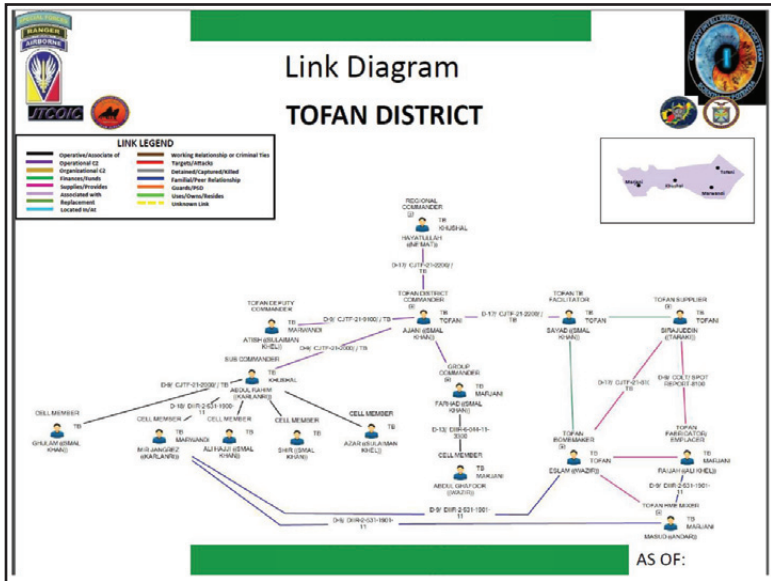


Figure 7-1. Example link diagram

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 HVTTL, 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. The following are examples of company-level lethal and nonlethal targeting SOPs.

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 (NIPR) sources.
- At a minimum, the CoIST will provide three separate reports before committing to lethal operations:
 - CIDNE is located on SIPR and contains theater reporting through HUMINT, SIGINT, and SIGACTs. 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.
 - * HCT 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 battalion operations and the battalion S-2 and assigned a target tracking number before operations. Lethal targeting packets will at a minimum include the following:

Lethal Targeting Operations (cont)

- 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 battalion 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, 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 battalion/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.

Chapter 8

Systems and Tools

To accurately conduct predictive analysis, the company intelligence support team (CoIST) must accurately track and analyze enemy activity. In addition to tracking events, the CoIST must update displayed Intel and brief the information to the commander and the unit with the most current Intel. There are many methods for collecting and tracking data on the enemy and events. The CoIST must track the data daily and analyze it by various methods. Daily tracking and analysis allows the CoIST to do pattern analysis covering weekly and monthly activities of the enemy.

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 establishes a knowledge management (KM) standing operating procedure (SOP) 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 AO.

Always remember that the most effective tool in the CoIST kitbag is the human brains of the team members and their willingness to think and analyze. No tool whether a piece of equipment or a software program can beat a thinking analyst.

Digital Cameras and Photographs

The digital camera is 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 provides detailed data and additional information and insight. For example, operational use of digital cameras has proven valuable to identify both friendly and enemy personnel.

Figure 8-1 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 8-1. Example digital photo

Digital cameras can also provide timely images of new graffiti, posters, and signs for translation/interpretation when 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 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. It is very important that CoIST 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 collectors and enablers 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 TTPs.

Video Camera

With video cameras getting small and light weight, they are as common as cameras are today on the battle field. 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, BCT level can see everything just as Soldiers on the ground saw it. All videos and pictures taken that are of relevance should be attached as media in the TIGR report or the AXIS PRO link diagram.

Unmanned Aircraft System (UAS)

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 it does provide 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 (HMMWV) so the operator can land the Raven when necessary, 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 make it simple to operate, however, it does require specialty-skilled operators who have acquired in-depth flight training from a Raven program manager or at the Ft. Benning, GA course.

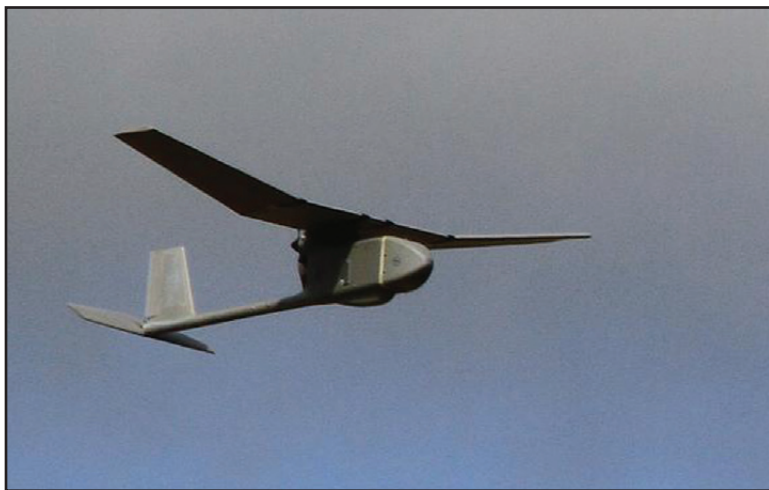


Figure 8-2. Raven UAS

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 125 kilometers, can fly for up to 6 hours, and operates at altitudes up to 15,000 feet. One advantage of the Shadow is that it is an in-house intelligence, surveillance, and reconnaissance (ISR) asset that can provide a battalion or brigade combat team (BCT) commander with tactical overwatch whenever needed. The CoIST can request use of or information from this BCT-level asset through the battalion 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 war fighters 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 platforms that operate on C/L/S or KU band. The OSRVT can watch footage of any platform that is within its broadcast area. The OSRVT is also small enough to be vehicle-mounted, enabling the commander on the objective to receive real-time information.



Figure 8-3. Shadow UAS

- **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 battalion 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 tactic, technique, or procedure (TTP) related to the specific device.
- **Analysis and Exploitation of Information Sources Professional (AXIS Pro).** This is the software that has replaced Analyst Notebook and is installed on each CoIST computer and Distributed Common Ground System–Army (DCGS–A). 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. CoIST will have CelLEX kits and possess the capability to conduct limited CelLEX. CoIST will use the CALYX computer for CelLEX. CALYX consists of the universal forensic extraction device (UFED) and NOMAD systems. The UFED pulls all the data from a cell phone in an easy to read report format. The NOMAD system is a pocket PC with all windows-based systems to save the data on, in a dismounted environment. DOMEX will support a wide range of intelligence activities to include all-source analysis, open-source exploitation (OSINT), HUMINT, SIGINT, geospatial intelligence (GEOINT), and measurement and signature intelligence (MASINT).
- **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 earlier in this chapter 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), PSI Jabber, and Transverse.** Chat tools on a CoIST system 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. These chat tools are similar to any instant messaging application found on the Internet. The CoIST needs someone to monitor chat rooms at all times because of the time-sensitive information that moves across it. Monitoring chat rooms will not be the only job this individual performs, but the assigned Soldier will be responsible for checking it constantly.
- **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. This data is used for tactical operations, detainee operations, base access, 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. The BAT must be used to transfer the data from the HIIDE to the database.

Maps

The CoIST can assist Soldiers and patrols by requesting the most updated map and imagery data through the BN S-2 and BCT GEOINT cell. Maps can be updated in TIGR, and updates can be viewed by anyone with TIGR access.

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 9

Maneuver vs. Non-Maneuver

Land owning units are not the sole benefactors of company intelligence support teams (CoIST). Non-land owning units also operate CoISTs with some differences based on missions and manpower. Non-land owning units require fewer personnel assigned to their CoIST; they may task CoIST out as an additional duty because they do not fulfill all the tasks of a land owner. In this chapter we will discuss units such as Military Police, Engineers, brigade sustainment battalions (BSBs), base defense operations centers (BDOC), and brigade special troops battalions (BSTB), as well as route clearance packages (RCPs) or anybody that is not a land owner. Non-maneuver units need to ensure that their CoIST cross talk with all land owner CoIST to capture near real-time data to pre-brief tactical convoy (combat?) operations (TCO). TCOs need to ensure they check-in with the CoIST at each FOB location to capture near real-time data (dissemination?) prior to departure. Think of a non-maneuver CoIST primarily as a collection asset for land owners versus operating as a full-fledged company S-2.

Non-land owner units routinely encountered the same, or similar, issues as land owners when it comes to using CoISTs. Still there are differences and for non-land owning CoISTs to succeed; we need to tailor their training to meet those differences. CoIST training as it stands now is maneuver focused, but is flexible enough to be adapted to non-maneuver units. BSBs often develop a single CoIST for the entire battalion, which usually consists of one or two soldiers from each company, collected under one company. Leadership typically consists of one or two NCOs, and no OIC. Additionally, while gathered under the administrative control of one company, the BSB S-2 provides most guidance instead of the company commanders. Most BSBs do not integrate CoIST support into transportation, maintenance, or medical operations beyond standard pre-brief/debrief of convoys. TTP may be to ensure there is a CoIST member embedded in each convoy.

Focal Points for RCP – BSTB CoIST**

Often the RCP is overlooked as a critical coordination and collection asset falling directly under the brigade. The RCP CoIST must directly interact with, and can serve as the ground truth for, the brigade counter improvised explosive device (C-IED) working group. The CoIST must also synchronize the intelligence picture amongst land owners, logistics elements, quick reaction forces (QRFs), and aviation (intelligence, surveillance, and reconnaissance [ISR] and non-typical ISR [NTISR]). Lastly, as a supporting unit, the RCP has the tertiary function as a collection asset for land owning units.

Intelligence Support to RCP

- Pre-briefs and debriefs.
- Route analysis and status updates.
- Enemy tactics, techniques, and procedures (TTP) along routes.
- Named areas of interest (NAI) recommendation and refinement.
- Most likely course of action (MLCOA) and most dangerous COA (MDCOA).
- Be On the Lookout lists (BOLO).
- Honest trace of cleared routes.
- ISR planning and refinement.
- Patrol schedule for units in the area of operations (AO).

Synchronization Requirements

- Gather collection criteria for battlespace owners along the route.
- Coordinate for NTISR support (including overwatch support from maneuver units).
- Synching RCP NAI, collection, BOLO responsibilities, and reporting criteria amongst scheduled ISR, logistics, and maneuver attachments.
- Reporting answers to maneuver PIR directly back to the unit.
- Daily updates from the brigade C-IED working group.
- Recommendations and refinement for C-IED products.

Focal points for the BSB and Engineer (Vertical and Horizontal) CoIST**

The BSB, forward support companies (FSC), and engineer assets often maneuver through the AO and can, at times, run missions that are very similar. With manning constraints, integrating a vertical or horizontal CoIST into the BSB CoIST can ease issues. Based on commander's intent, the team may be comprised of two to three full-time members augmenting the S-2, or four to six additional duty members serving primarily as briefers and liaisons while the heavy lifting is carried out by the S-2. This team will do limited analysis compared to a maneuver unit: they will, however, collect and maintain situational awareness for areas sometimes larger than a brigade AO. The bulk of time will be spend requesting AO updates and intelligence summaries (INTSUM) from the majority of the brigade

to provide situational awareness, while at the same time analyzing and assessing the enemy with regard to integrated RCP, ISR/NTISR, and convoy operations.

Focal points at the BSB Engineer and FSC CoIST**

Intelligence Support

- Pre-briefs and debrief, to include local national (LN) drivers.
- Tracking HUMINT collection team (HCT) interviews and assessments of LN drivers.
- Route analysis and status.
- RCP schedule and requirements.
- Enemy TTPs along routes.
- NAIs for brigade and lower.
- MLCOA/MDCOA.
- BOLOs.
- Biometrics on all local LN drivers.
- Honesty trace.
- Liaison with CoIST and S-2 during layovers.

Synchronization Requirements

- Gather collection criteria for land owners along the route.
- Coordinate for NTISR support (including overwatch support from maneuver units).
- Coordinating for ISR to cover gaps between logistics elements and RCP.
- Synching NAI, collection, BOLO responsibilities, and reporting criteria amongst scheduled ISR, logistics, and maneuver attachments.
- Reporting answers to maneuver PIR directly back to the unit.
- Requesting updates from the RCP.
- Tracking the RCP schedules and integrating collection and coordination measures.
- Providing contact information and schedule to CoIST/S-2 at layover positions and coordinating for debriefs/prebriefs at each location.

Focal Points for Aviation CoISTs**

Aviation CoISTs serve almost exclusively as collection and reporting assets to all CoIST under the brigade. Aviation S-2 spends the majority of their time focused on threats to aviation assets and on brigade-level collection and often do not have the time to focus collection down to the company level or to interact with each company individually. The S-2 can continue to brief the majority of the enemy side of the intelligence picture while the CoIST focuses on friendly operations and the enemy picture as seen by the ground. The CoIST fulfills that role by prioritizing and breaking collection requirements from CoIST down to indicators that are directly observable by aviation. The aviation CoIST becomes the subject-matter-expert (SME) on how each supported company conducts operations on the ground, and the expected enemy picture by the units on the ground.

Manning

Option 1:

- CoIST working in conjunction with S-2.
- Two personnel; alternating 12-hour shifts.
- Recommend NCOs (lowest acceptable paygrade is E-5) for both positions.

Option 2:

- CoIST representatives embedded in supported maneuver units.
- One CoIST representative embedded in each supported maneuver battalion.

Intelligence Support

- Ground enemy picture.
- SME on friendly TTPs and battle drills.
- Ground PIR broken into observable indicators for aviation.

Synchronization Requirements

- Gather collection criteria from battlespace owners and support units.
- Synch NAI, collection, BOLO responsibilities, and reporting criteria amongst supported units.
- Reporting answers to external PIR directly back to the unit.

MP CoISTs

MP companies can serve a wide range of missions. They can be land owners. They may be attached to maneuver units. They may operate at a detention center. Here we focus on MP CoISTs in a detached or a detention center role.

Focal Points for Detached MP CoIST**

As a detached element, the CoIST can operate effectively as a two Soldier element with one on shift at a time. Key tasks are coordinating with and passing intelligence to the detached platoons, ensuring maneuver is supporting them with the balance of intelligence functions, and managing the AO-wide national security force common operational picture (COP).

Manning

- Two Personnel; alternating 12-hour shifts.
- Recommend NCOs (lowest acceptable paygrade is E-6) for both positions.
- Trained CoIST representative (paygrade E-4 or E5) in each platoon.

Intelligence Support

- Daily intelligence synchronization meeting with detached platoons.
- Ensuring platoon integration into battlespace owner CoIST.
- Build national security force profile in each detached location.
- Assess national security force capabilities and training.
- Recommend to commander areas to shift or embed MP sections.
- Recommend friendly TTP and COAs based on the enemy COA for an area.

Synchronization Requirements

- Establish reporting timeline and conduct synch meeting with platoons.
- Share police-related intelligence picture with maneuver CoIST in the AO.
- Liaison with police transition teams and other embedded trainers and mentors to assess overall capabilities of security forces.
- Liaison with other agencies at the brigade level to work police-related issues.

Focal Points of a Detention Center MP CoIST**

As a detention center security element, key tasks include tracking the network in and around the facility, recommending HUMINT interviews, and periodically evaluating friendly TTPs against detainee threats and the enemy threat.

Manning

- Three to four personnel; alternating shifts.
- Recommend one NCOIC (paygrade E-6), one E-4, and one E-5.

Intelligence Support

- Daily intelligence synchronization meeting with S-2.
- Prebriefing and debriefing detention center shifts.
- Building attack-the-network products based on detainee networks.
- Assess capabilities and intent of organizations with detained members.
- Establish patterns of life for detainee population.
- Evaluate friendly TTPs and plans against MLCOA/MDCOA.

Synchronization Requirements

- Conduct synchronization meeting with adjacent land owners.
- Liaison with MP elements responsible for transporting detainees.
- Provide enemy network analysis to land owners and to higher S-2.
- Coordinate with HUMINT assets to evaluate detainees as possible sources.

Focal Points for BDOC CoIST**

Intelligence Support

- HVI/HVT.
- BOLOs.
- Biometrics updates.
- Predictive analysis with force protection in mind (IDF, PBIED, and SVBIED).
- Dissemination of TTPs laterally throughout all BDOC.
- Trend and pattern analysis at the entry control point (ECP).

- Nonlethal targeting for key leader engagements of individuals who support the FOB.
- MLCOA/MDCOA.
- Providing intelligence to the commander for force protection.

Synchronization Requirements

- Conduct BDOC sync meeting with adjacent BDOC elements.
- Conduct synchronization with co-located maneuver and logistics units.
- Pull enemy analysis and BOLO updates.
- Coordinate with S-2 on a daily basis to determine any assets (HUMINT, SIGINT, IMINT) that need special requirements or access to/from the installation.
- Evaluation of the defense plan in conjunction with the S-2 and adjacent BDOCs.
- Integration of QRF into BDOC briefing and intelligence COP.

**The focal points above are guidelines for establishing a non-land owning CoIST and can be added to or subtracted from.

PROVIDE US YOUR INPUT

To help you access information quickly and efficiently, the Center for Army Lessons Learned (CALL) posts all publications, along with numerous other useful products, on the CALL website. The CALL website 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: “RFI or a CALL Product” or “Contact CALL.”

**PROVIDE LESSONS AND BEST PRACTICES OR
SUBMIT AN AFTER ACTION REVIEW (AAR)**

If your unit has identified lessons or best practices 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 e-mail address: call.rfimanager@conus.army.mil

SIPR e-mail address: call.rfiagent@conus.army.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 “RFI 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

Access and download information from CALL’s website. 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 “RFI 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://usacac.army.mil/cac2/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/cac2/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/cac2/csi/csipubs.asp>>.

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 G2. 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/>>.

Military Review (MR)

MR is a revered 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.army.mil/cac2/militaryreview/index.asp>>.

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).

Combined Arms Center-Capability Development Integration Directorate (CAC-CDID)

CAC-CDIC is responsible for executing the capability development for a number of CAC proponent areas, such as Information Operations, Electronic Warfare, and Computer Network Operations, among others. CAC-CDID also teaches the Functional Area 30 (Information Operations) qualification course. Find CAC-CDID at <<http://usacac.army.mil/cac2/cdid/index.asp>>.

Army Irregular Warfare Fusion Cell (AIWFC)

AIWFC integrates and collaborates information exchange and analysis for irregular warfare (IW) activities in order to advocate DOTMLPF (doctrine, organization, training, materiel, leadership and education, personnel, and facilities) solutions addressing IW threats. AIWFC synchronizes and assists in the development of IW and countering irregular threats enterprises to support a coherent Army strategy that accounts for building partner capacity, stability operations, and the integration of unconventional warfare and counterterrorism. Find AIWFC at: <<http://usacac.army.mil/cac2/AIWFC>>.

Joint Center for International Security Force Assistance (JCISFA)

JCISFA's mission is to capture and analyze security force assistance (SFA) lessons from contemporary operations to advise combatant commands and military departments on appropriate doctrine; practices; and proven tactics, techniques, and procedures (TTP) to prepare for and conduct SFA missions efficiently. JCISFA was created to institutionalize SFA across DOD and serve as the DOD SFA Center of Excellence. Find JCISFA at <<https://jcisfa.jcs.mil/Public/Index.aspx>>.

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

<http://call.army.mil>



Center for Army Lessons Learned (CALL)

10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350

Combined Arms Center (CAC) • Ft. Leavenworth, KS



U.S. UNCLASSIFIED
FOR OFFICIAL USE ONLY

