“Why COIST Matters”
Victor R. Morris

Introduction

“Do you even COIST, bro?” was the question a young command post non-commissioned officer (NCO) asked one of his Soldiers. The question arose during situational exercise lane training (STX) involving platoon level patrols in the company sector. The young soldier asked his leader how he knew about the enemy’s employment of IEDs and the “hot spot” locations, which are essential to countering asymmetric threats, maintaining situational awareness and contributing to bottom-up refinement. There have been numerous debates regarding the applicability of Company Intelligence Support Teams or COISTs and the “way ahead” in future conflicts. Opinions such as “COIST is for COIN”, “COIST is not doctrine”, and “Intel is for analysts” have been widespread. In contrast, there have been positive reviews from Specialist through Brigadier General about the efficacy of COISTs in training and combat.

One of the current challenges involving COISTs stems from an overall military shift. This shift involves the reduction of counterinsurgency operations world-wide, increase of Decisive Action Training Environment rotations (DATE) and global employment utilizing Regionally Aligned Forces (RAF). The DATE rotations support conducting Unified Land Operations in a Hybrid Threat Environment. There is a perception that COISTs are only relevant in an irregular warfare model during counterinsurgency and stability operations. Other challenges to COIST future applicability involve a lack of doctrine and ineffective task organization. The current company COIST model is not conducive to effectively engaging diverse combinations of regular and irregular forces simultaneously. Future security challenges will include multi-faceted, uncertain, complex and chaotic environments, and will require more support to information and intelligence requirements at all echelons. The initial, sustainment and pre-deployment training must be a command priority and must for formalized for future management during Army Force Generation (ARFORGEN) cycles. Finally, teams must become better integrated into company command posts during training and be better supported through more emphasis on overall mission command. COISTs must not only be maintained for future conflicts, but adapted to be better integrated and transitional within company mission command systems during Unified Land Operations involving a hybrid threat.

Background

The complexity of irregular warfare necessitated the need to have more enhanced intelligence capability at the small unit level. In conventional operations, intelligence is disseminated from higher to lower headquarters based on the presence of intelligence gathering resources. In counterinsurgency or other decentralized operations, information flows in the opposite direction, where small units gather raw
information based on their operational environment. Recent counterinsurgency operations assessed that company formations needed the ability to produce intelligence to drive their operations and support higher echelon common operational picture (COP) development. This assessment was refined and given the designation “COIST” with the following mission: serve as the primary source of information and intelligence that the company commander needs to make timely accurate decisions (CALL COIST Handbook). Post-deployment after action reviews (AARs) and training assessments dictated the employment of COISTs and greatly enhanced the company’s ability to analyze, produce and disseminate accurate information and intelligence in a counterinsurgency environment. They also facilitated better situational awareness and more effective lethal and non-lethal targeting in support of the commander’s intent and overall mission.

The Shift: Unified Land Operations

In response to the current and future changes, the combat training centers and TRADOC collaborated on the development of a training model called the Decisive Action Training Environment (DATE). The current model is designated as DATE 2.1 and differs from past training rotations and pre-deployment Mission Readiness Exercises (MREs) utilized to prepare units for Iraq and Afghanistan. The model was designed to prepare tactical organizations to execute a wide range of operations as part of Unified Land Operations. The DATE model presents a complex training environment that is designed to train operationally adaptable units. The ground operations provide the ability for the unit to build competency with mission essential tasks, while refining standard operating procedures from the last fourteen years of combat. Next, the model drew on aspects of the contemporary operational environment, while incorporating aspects of emerging threats and security challenges. The threat to the brigade’s mission involves an emerging category of threats and activities that do not fit into the traditional understanding of conventional and unconventional war. Lastly, the DATE includes Joint, Interagency, Intergovernmental, and Multinational (JIIM) partners and a multifaceted host nation security force that presents the brigade with integration challenges and opportunities. This paradigm shift to encompass Decisive Action, Army Core Competencies and Mission Command has created debate about the applicability of COISTs during Unified Land Operations.

The Doctrine Dilemma

There have been improvements during the last eight years involving the development and implementation of COIST doctrine, but the concept is still not formalized in many company formations. It is imperative that doctrinal references be used as the basis for COIST training, AARs and standard operating procedure (SOP) development. A current doctrine review and its support to COIST operations are below:

- **25 November 2008**: Field manual 2-19.4, 1-24, Brigade Combat Team (BCT) Intelligence Operations. This section briefly mentions the need to form COISTs based on capability requirements and access to perishable information. It also highlights the fact that these teams are ad hoc and optional.

- **23 March 2010**: Field Manual 2-0 Intelligence fails to address COIST operations in detail.

- **9 November 2010**: Training Circular 2-19.63 Company Intelligence Support Team. Aside from various CALL handbooks published May 2013, this is a very detailed doctrinal publication involving COISTs. Although it was published in 2010, it acts as the doctrinal foundation for our COIST, Attack the Network, Counterinsurgency and staff training courses.

- **15 April 2014**: The revision to FM 2-0 Intelligence highlights COISTs in BCT intelligence operations (Chapter 2). Paragraphs 2-7 through 2-10 provide an overview of COIST and their
contribution to intelligence sharing, enemy assessment, troop leading procedures, and mission execution. The manual also states that the MI Company may augment selected maneuver companies with MI Soldiers to form the nucleus of the COIST.

- **10 February 2015:** ATP 2-19.4, 1-24, Brigade Combat Team (BCT) Intelligence Operations. This document has been updated from the previous 2008 version and clearly frames the CoIST’s role & responsibilities.

**Evaluating the Threat**

Hybrid threats are not new and there are myriad examples throughout history of how adversaries organize into conventional and irregular forces. A *hybrid threat (HT)* is defined as the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually beneficial effects (TC 7-100). The term “hybrid” has recently been used to illustrate the increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict. Contemporary hybrid warfare involves a multiplicity of actors employing a combination of hybrid instruments facilitated by 21st century technologies and combinations of conventional and irregular forces. Hybrid threats are characterized by the combination of forces, which can further be defined as conventional military, insurgent (cellular networks) or criminal organizations. To be a hybrid, these forces cooperate in the context of pursuing their own internal objectives, which further complicate the unit’s mission and need for increased situational awareness and understanding. A recent example of this threat can be seen in Buenos Aires, Argentina. On August 10, 2014, Troops of Apolo Task Force, Third Army Division, discovered a complex illegal structure which operated in La Esperanza village, Buenos Aires municipality, Cauca. On site, troops fought against a group of guerrillas and when they retreated, troops searched the area and located a 200 m² structure which had been adapted to manufacture explosives and process coca paste. This facility was reported to be the property of the Revolutionary Armed Forces of Colombia (FARC). This event is evidence of the close relation between drug trafficking and FARC, and the way this criminal structure intends to strengthen its capabilities by using explosive devices. Below are some of the goals associated with hybrid threats:

- Removal of forces from their area of operations.
- Degrade and exhaust forces rather than cause a direct military defeat.
- Use of a dynamic variety of conventional and unconventional methods to create multiple dilemmas.
- Prevent opponents from segregating the conflict into easily assailable parts. In many cases military action is the least important of the hybrid threat’s activities.
- Rapidly form, transform, adapt and abolish cells based on requirements, environment and opponents.
- Simultaneously inject themselves into all of the operational variables in the OE (PMESII-PT).
- Adhere to ensuring security, accomplishing the task, maintaining adaptability, and remaining connected to the people.
- Preserve bases to train, self-sustain, prepare for future missions and evolve organizational capability.
- Initiate strategic consequences of denying an enemy a secure area, or making it politically untenable to remain.
- Create a dilemma where an army is vulnerable to conventional attack when it disperses to combat irregular forces within the population, and cede control of the operational environment and
population if they remain concentrated.

**Training to Counter the Threat**

COISTs must possess core competencies associated with engaging actors in a hybrid environment. The below tasks are associated with offensive, defensive and stability operations in a static or mobile command post during operations. The core competencies can also be aligned with a COIST framework consisting of the following spheres: Mission, Purpose and Function, Task Organization, Core Tasks, Situational Development and Understanding, Support to Targeting and Assessment. The framework is nested in the Mission Command and Intelligence Warfighting Functions for complimentary effects. The below list is not all inclusive and is subject to change based on the mission and commander’s discretion.

**Traditional or Conventional Threat**: Regular Military Forces as a threat the regulated armed forces of a state or alliance of states with the specified function of military offensive and defensive capabilities. These forces may have matching capabilities across all war-fighting functions.

**COIST Core Competencies**: Intelligence Preparation of the Battlefield (IPB) involving detailed terrain analysis, various intelligence disciplines to included TECHINT, OSINT, SIGINT, GEOINT and HUMINT, template and company graphic management (analog and BFT), PIR, SIR, CCIR management, ISR program management, proper enabler utilization (task/purpose), information assurance management (cyber defense), airspace/ground integration, planning on the move contribution and direct support to the orders process, which is condensed during high-tempo operations.

**Irregular or Unconventional Threat**: Irregular forces as armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces (JP 3-24). These forces include: paramilitary, insurgent, guerrilla, terrorist and criminal elements. At the tactical level, they can apply tactics, techniques, and procedures (TTPs) common to regular forces but do so with asymmetric applications. The definition of irregular warfare highlights population centric engagement and intention to damage an opponent’s influence over that population.

**COIST Core Competencies**: IPB with an emphasis on understanding trends, patterns, human networks (to include criminal), culture and perceptions of the community within the environments, various intelligence disciplines, Weapons Technical Intelligence (WTI), OSINT with a social media emphasis, SIGINT, GEOINT and HUMINT. All of the above competencies support situational awareness and support to targeting.

**Lessons Learned**

James K. Greer’s article from the Small Wars Journal entitled “The Network vs. the BCT: Organizational Overmatch in Hybrid Strategies” analyzes the concept of more modular approaches at the tactical level specifically involving “cellular companies.” In summary, he suggests that we must become a cellular network in order to respond to future threats. This is accomplished through a deviation from the current relatively fixed company identity to a “cellular company” that operates off of rule sets enabled by a robust information and intelligence cell. This cell is an augmentation of the information mission command system. He also states that the company should be able to gain or lose modules many times in a day without losing the coherence of operations, as tasks and engagements are conducted simultaneously and sequentially.

As an Infantry Company Commander during OIF 09-10, we conducted operations in a similar model. For example, we had one platoon conducting route security patrols (C-IED), one platoon conducting host nation security force EOD training, one platoon conducting indirect fire disruption patrols in a targeted
area of interest, and one platoon designated as a company or battalion quick reaction force. Based on the situation and operations tempo, these patrols could be happening sequentially or simultaneously. Additionally, each module has its own set of enablers, which had to be planned and managed properly. The “dynamic re-tasking” occurred when host nation security forces required tactical support from U.S. forces. Typically, Commanders were given six to eight hours to dynamically re-task the company to support host nation battalion level operations. This re-tasking meant consolidating and re-organizing the platoons or “cells” back at the operating base and finalizing the troop leading procedures. The majority of the time the mission was to conduct a company level clearance of an urban area. In other offensive terms, we conducted company movements to contact whilst partnered with host nation forces. The threat was asymmetrical at the time, but this can easily be applied to a more conventional or hybrid threat. The OPORD was completed and briefed within three to four hours of the company WARNO. The company essentially went from conducting de-centralized stability operations to centralized offensive operations in six hours with direct support from the headquarters section. COIST employment begins with the company command team and the commander’s mission command philosophy and system management.

Mission Command Systems: COIST 2020 Initiatives

The solution to effective and adaptable companies lies within mission command. ADP 6-0 defines Mission Command as the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander’s intent to empower agile and adaptive leaders in the conduct of unified land operations. Additionally, mission command system consists of five components: personnel, networks, information systems, processes and procedures, facilities and equipment. All of these components are contained in the company command post module. That module is contained in the headquarters section with the commander as the backbone of mission command.

Due to the nature of the future operational environment, the current state of company command posts and COIST cells are not effective due to a lack of effective integration. They should not only be combined, but augmented through experience and capability—not personnel. The efficacy of this technique comes from a synchronization of the five components of mission command in one module with intelligence as a centralized function. The module or node is the command post, the cells are the headquarters section/platoons, and the network is the company. One of the primary arguments with COIST training and employment involves creating cells “out of hide” and taking soldier from line platoons. All the mission-command capabilities are already present in the headquarters section of a maneuver company/troop/battery, which includes the 35 series MOS intelligence soldier, Armored, Infantry, and Stryker formations. Mission command capabilities can also be modified or augmented in non-maneuver companies as seen in Chapter 9 of the CALL COIST Handbook No. 13-09, May 2013. This is not to say that a soldier from the line cannot be transferred to or from the section, but the capabilities are already there and are adaptable. If you are conducting combined arms maneuver through high-tempo operations, the commander is fighting mounted through a multi-vehicle TAC or in a dismounted configuration. There is no “COIST vehicle” and those skill sets are executed via the personnel and systems present on the various TAC vehicles. If you transition to wide area security, the entire module along with the systems transitions to a tent or hard stand building. Company intelligence must be synchronized with current operations and reporting, based on all of the preparation and assessments conducted prior to the mission. The emphasis comes from a previous planning knowledge involving friendly maneuver, enemy courses of action, information requirements and enabler integration. Accurate reporting is decisive in high-tempo operations and must be concise for proper common operational picture development. Doesn’t it make sense for the soldiers collecting and analyzing the information before the mission, to report it during and after the mission?
All modular configurations of the command post must be able to receive, distribute and analyze information. They must also be able to recommend courses of action and integrate resources. All of this is accomplished through one mission command module that includes the company intelligence aspect. Intelligence is innate at the company level based on recent combat operations. There is no longer a need to differentiate Command Posts from COISTs because their missions are synonymous. We need to train with increased capability in mind, in lieu of increased personnel or equipment. Strong companies with strong leaders have the ability to “do more with less”.

Conclusion

In conclusion, companies have evolved from recent combat operations and must continue to evolve and adapt based on the future threats involving security. Time-honored concepts of conventional and unconventional war involving traditional methods have no meaning to a hybrid threat beyond their ability to be used against its opponents. The skill sets required to combat this threat must be standardized and maintained at the company level. Operations at the tactical level directly correlate to the success or failure of a campaign, where success is gained through enhancing the situational awareness in tactical units at the company/troop/battery level. All of the principles contained in this article are applicable to maneuver and non-maneuver companies alike. Whether you are utilizing Company Intelligence Support Team (COIST), Company-Level Intelligence Cell (CLIC), Company Intelligence Cell (CIC), or Intelligence Support Team (IST), you must be cellular and adaptive in order to support higher echelon requirements and the mission in a highly dynamic operational environment.

References

1. ATP 3-90.37 Combined Arms Counter-Improvised Explosive Device Operations.
1. ATP 3-21.11, SBCT Rifle Company 3rd QTR FY 15 (pending).
1. Training Circular 7-10 Hybrid Threat November 2010.
Victor R. Morris

Victor R. Morris is a former US Army Captain and Company Commander who served in the Armor and Infantry branches. He is currently a CIED and Irregular Warfare instructor at the US Army Europe’s Joint Multinational Readiness Centre (JMRC) in Hohenfels, Germany. The views expressed in this article are those of the author and do not reflect the official policy or position of FORSCOM, JIEDDO, the Department of the Army, the Department of Defense, the United States Government, any Government Agency, or Booz Allen Hamilton.


Links:
[1] [http://smallwarsjournal.com/author/victor-r-morris](http://smallwarsjournal.com/author/victor-r-morris)

Copyright © 2015, Small Wars Foundation.

Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our Terms of Use. Please help us support the Small Wars Community.