'Reach-Back'—A New Approach To Asymmetrical Warfare Intelligence

By Capt. Phillip Radzikowski

"You don't know what you don't know." This cliché has been used countless times to describe the global war on terrorism. Unfortunately, it is an apt description: When it comes to the intelligence community, most Army officers really *don't* know what they don't know.

Throughout the Army, company commanders are hungry for accurate, fast and reliable intelligence. Battalion commanders are pushing their intelligence (S-2) shops to produce intelligence far beyond their capabilities. Brigade military intelligence companies (MICO) are working at maximum capacity, trying to provide actionable intelligence for their battalions and companies while also working to develop trends, stay ahead of insurgents' planning, and prepare staff estimates and decision briefs. Inside this entire mélange, it is easy for a commander to succumb to tunnel vision and not look beyond the unit's organic capabilities.

Outside this swirl of intelligence development, however, is an underutilized—and invaluable—support network that is of operational advantage from within the intelligence community. This weapon is "reach-back" support.

Reach-back support is a relatively new concept. It provides operational warfighting units—battalions and brigades—the opportunity to reach outside of their traditional avenues of information flow and use national intelligence community assets to gather information to fill "gaps" in tactical intelligence.

Traditionally, company commanders develop the ground situation through patrol reports, atmospherics and general situational awareness. Their reporting tells the true story on the ground. The battalion intelligence officer and his shop process, track and attempt to identify patterns of insurgent networks and groups that will help drive targeting operations. Ultimately, targeting is refined at the brigade and battalion levels and then executed at the company level. The brigade MICO expands upon the battalion S-2's assessments and evaluations and creates broader network analysis of insurgent group development. The MICO has the added responsibility of incorporating the broader intelligence community's assets into the fight. Traditionally, this works. The problem is that, traditionally, the U.S. Army has not been fighting an insurgency.

During combat with an insurgency, the battlefield transforms at an inconceivable speed. Enemy tactics, techniques and procedures (TTPs) evolve, networks move and key individuals change rapidly. For companies, battalions and brigades to keep up and stay ahead of the insurgent execution curve requires the support of an intelligence network that can gather and leverage national information assets immediately and effectively. Reach-back support is the answer.

Reach-back support is the ability for forward-deployed units (battalions and brigades) to refer specific intelligence-oriented questions to continental United States-based agencies for support. The U.S. government's intelligence community has an enormous amount of collected information, including relevant warfighting information, which is compartmentalized for added security. This means that if an individual performing an intelligence function doesn't know about the availability of certain information, then he or she cannot use it—that potentially valuable information is rendered useless.

With reach-back support, when members of a tactical unit identify a gap in their own intelligence, then that gap becomes a question. The unit then poses the question to a reach-back support agency that will have a team of intelligence analysts address that specific problem and produce a "product" that addresses that specific gap.

Reach-back and IEDs

Perhaps the most exemplary form of reach-back support is in combating improvised explosive devices (IEDs). In 2003, IEDs began to appear in Iraq. Soon they became the deadliest weapon of insurgents. Easy to make, easy to use and extremely effective, the IED concept quickly morphed into many different TTPs: suicide-borne, deep-buried, explosively formed penetrator, victim-operated, remote-controlled and so on.

To combat the problem, DoD created the Joint Improvised Explosive Device Defeat Organization (JIEDDO); its charter was to "defeat the IED as a weapon of strategic influence." To do this, JIEDDO developed three lines of operations: defeat the device, train the force and attack the network.

Unfortunately, and not surprisingly, as certain types of IEDs were defeated, new TTPs emerged. As the U.S. military's training and tools improved, so, too, did the insurgent's arsenal of IED tactics, techniques and procedures. IEDs are simply the end state of a large, sophisticated network of insurgents, logisticians, financiers, emplacers, triggermen, communications specialists and leaders, and the only way to effectively counter IEDs is to capture and/or kill the network of individuals who employ them.

Eventually, JIEDDO recognized that equipping and training the force was not sufficient to combat the threat of IEDs. In 2006, JIEDDO created the Counter-IED Operations Integration Center (COIC) to do just that. COIC is a Joint fusion and analysis center for the Department of Defense. Using net-centric methods of information sharing and analysis of existing intelligence material—including patterns of life of key individuals and TTP trends that can be passed on to units in daily contact with insurgents—the center serves as the network attack aspect of JIEDDO and provides battalions and brigades with packaged information that can be used kinetically to attack insurgent networks.

COIC consists of five sections: operations (OPS) lab, mission integration division (MID), network integration division (NID), operations research and systems analysis (ORSA), and the "Red Team." Their functions and capabilities range from direct communication to units (OPS lab) and an expertise that spans the entire intelligence community (MID) to designing software that allows units to further exploit information as intelligence (NID), providing the insurgent point of view into all products that are requested (Red Team), and identifying trends and gaps among friendly and enemy operations (ORSA).

In addition, the COIC also conducts training of deploying units to help teach the reach-back methodology of support. COIC realizes that in order to attack the network, deploying units must know that there is a large amount of information available and that the COIC can help turn that information into intelligence.

COIC Products

Requests for support (RFS) to COIC vary according to a number of factors. Whenever a unit is required to leave its traditional area of responsibility, it will request reach-back intelligence support to assist its internal intelligence preparation of the battlefield prior to the mission. This request generally comes from units that are new to certain operating areas within Iraq, during reliefs in place and during out-of-sector missions.

As units mature into their area of operations, they begin to map insurgent networks. Invariably, units on the ground are the best gauge of atmospherics. Although very diligent and effective, units sometimes develop gaps and require network analysis from the COIC, which provides another look at the problem and develops and analyzes known insurgent IED networks that operate within a specific region.

Generally, killing or capturing the leaders of organizations alone will not lead to the defeat of the network, but analyzing a leader's contacts and other compartmentalized intelligence discipline reporting can lead to identifying key personnel in their networks. This personality "profile" lays out how the key individual has developed and organized his networks both geographically and with network diagrams and provides the names and locations of key personnel.

Not all requests are in response to upcoming operations or ongoing analysis. Some requests are in response to significant actions that occur and reflect the commander's desire to immediately ascertain as much information as possible for the area surrounding the attack. For example, a request for support of this nature would elicit a product that attempts to identify ingress/egress routes from deep-buried IED locations that killed two Coalition forces soldiers. The COIC will "surge" to turn information surrounding catastrophic significant actions into actionable intelligence as quickly as possible.

Other COIC products include cultural perspectives and technological support. The former (a Red Team responsibility) might inform on emerging and evolving threat TTPs, attack claims made by insurgent groups, and local-national cultural views and opinions concerning actions of Coalition forces. The latter might request a 3-D dashboard fly-through model of Tarmiyah to help a battalion conduct premission rehearsals.

The RFS Process

When an operational unit identifies an intelligence gap or has a problem it cannot answer, the S-2 will write an RFS, which is sent via e-mail to the COIC division support team (DST). The DST will vet the request against the catalogue of federated defense partners and try to answer with what is currently "on the shelf." If the work has already been completed by another agency (or previously by COIC), then the product will be sent to the requesting unit. Most RFSs are generated at the battalion and brigade levels, though some are generated at the division and corps levels, while others are initiated at the COIC. Once the request for support is in COIC, the OPS lab will log it into the RFS tracker. The RFS manager will then announce the new RFS at the daily "mission board" brief, which also includes recent IED operations. Within two hours of the mission board posting, COIC meets to assign individual tasks and responsibilities.

There is no finite timeline to determine how long it takes to answer an RFS fully. The driving force behind project completion is the latest time of value, typically 10 to 14 days. No earlier than four days prior to completion, the lead analyst will schedule a critical review of the in-progress product—a slide-by-slide review of the work to date to ensure that the product is up to the COIC standard, that it is customer-centric and user-friendly, and that it accurately defines the answer to the question.

Not less than one day prior to the latest time of value, the same product is "Red Teamed." This is the approval review. Generally, there have been modifications of the product from the previous stage, and the product is reviewed again in its entirety for accuracy and thoroughness. Upon completion of the Red Team review, the product is sent to the requester. It is also posted for reference by the entire intelligence community for future use and collaboration.

Tapping into the COIC is easy, as the COIC exists to support combat units. There are a number of ways that deployed units (or units deploying soon) can tap into the COIC for reach-back support via its SIPRNET web site: www.coic.smil.mil. On the web site, users can navigate their way to the web-based COIC appliances. E-mail is the easiest, clearest way to submit a request. Because each OPS and MID team is divided into geographically based teams, the analysts and the OPS lab leaders can be e-mailed directly to initiate work. E-mail addresses can be found at www.coic.smil.mil. In addition, division support teams conduct visits to deployed brigade combat teams. The purpose of the visits is to work with brigade intelligence analysts and help fill gaps in their analysis.

Don't know what you don't know? That's no longer an excuse. □

CAPT. PHILLIP RADZIKOWSKI served with the 4th Stryker Brigade Combat Team, 2nd Infantry Division, as the brigade assistant S-3, then as a liaison officer with the COIC for 14 months during the brigade's deployment to Iraq. He worked exclusively with the COIC to help fill intelligence gaps in fighting insurgency. An Infantry Captains Career Course graduate, he now serves on the Army Staff at the Pentagon.