Employing ISR
SOF Best Practices

Special operations forces (SOF) victories in the war on terror have driven a transformation in the relationship between operations and intelligence. Today, intelligence *is* operations. Perhaps the most famous example was the death of Abu Musab al-Zarqawi. The airstrike that killed Zarqawi was only a fraction of the effort to find and accurately target him.[1] The true operational art behind that strike was a multidisciplined intelligence, surveillance, and reconnaissance (ISR) endeavor coupled with agile SOF that patiently laid bare the Zarqawi network and resulted in a find-fix-finish operation. It took more than 600 hours of ISR to track and observe the network that yielded the target.[2] Airborne ISR was a critical and necessary piece, but it alone was not sufficient to target Zarqawi. Instead, it was focused and directed by a robust all-source intelligence network employing human intelligence (HUMINT), detainee intelligence, and signals intelligence (SIGINT). This collection and intelligence analysis was part of a network of personnel, systems, and mechanisms woven into the daily operations of and directed by a joint special operations task force (JSOTF). The Zarqawi strike was merely the most publicized of *hundreds* of *successful* counternetwork operations that used the new combined arms team of operations and intelligence, which highlights surveillance and reconnaissance as its most effective tool.

The JSOTF tactics behind this new combined team deserve some scrutiny because they empower tactical-level operations for offensive irregular warfare (IW). This article discusses some of the tactics, techniques, and procedures based on the collective experience with JSOTFs engaged in counterinsurgency and counternetwork operations in Iraq and Afghanistan from 2004 to 2007. Some of the SOF best practices in using ISR may be applicable and valuable to conventional forces.

The SOF–ISR combination was effective because it unified operations and airborne collections with all other intelligence disciplines under a single commander. The JSOTF employed airborne ISR as an integral part of operations and clearly understood that

By MICHAEL T. FLYNN, RICH JUERGENS, *and* THOMAS L. CANTRELL

Soldiers advise Iraqi special operations forces during combat operation in Baghdad

Combat Camera Group Pacific (Johansen Laurel)

intelligence was the primary combat multiplier capability needed to fight the enemy. From this operational framework, some important lessons emerged when employing ISR:

- use the find-fix-finish-exploit-analyze targeting model
- synchronize ISR to all-source intelligence
- pass ISR (weight the main effort)
- conduct ISR processing, exploitation, and dissemination as far forward deployed as possible
- emphasize exploitation and analysis
- unify organization.

Low-contrast Enemy

These lessons emerged from trial and error tempered by 6 years of constant contact with an enemy whose nature demanded new approaches. Today's enemy is a low-contrast foe easily camouflaged among civilian clutter, unlike high-contrast targets such as airfields and warships.[3] The insurgent's primary strength has always been to hide in complex terrain such as mountainous or urban environments. The global communications revolution has given this insurgent a new complex terrain—an "electronic sanctuary"—in which actions can be hidden among the innumerable civilian signals that constitute daily cell phone and Internet traffic.[4] It is from this new sanctuary that the enemy coordinates activities from dispersed networks in order to self-synchronize, pass information, and transfer funds. In this way, the insurgent has become "networked coalitions of the willing" that come together temporarily and are thus difficult to destroy.[5] Drawing support from their networks, they remain low contrast until time to strike and then quickly blend back into the population.

Use F3EA

An aggressive targeting model known as *find, fix, finish, exploit, and analyze* (F3EA) features massed, persistent ISR cued to a powerful and decentralized all-source intelligence apparatus in order to *find* a target amidst civilian clutter and *fix* his exact location (see figure). This precision geolocation enables surgical *finish* operations that emphasize speed to catch a fleeting target. The emphasis on the finish was not only to remove a combatant from the battlefield, but also to take an opportunity to gain more information on the globalized and networked foe. *Exploit-analyze* is the main effort of F3EA because it provides insight into the enemy network and offers new lines of operations. Exploit-analyze starts the cycle over again by providing leads, or start points, into the network that could be observed and tracked using airborne ISR. A finishing force unified with airborne ISR and an exploit-analyze capability is able to be persistent, surgical, and rapid in operations against the insurgent's network. Airborne ISR became the pacing item for operations, but it had to be cued by the meticulous work of a robust, all-source, and collaborative intelligence network.

Brigadier General Michael T. Flynn, USA, is Director of Intelligence (J2) at U.S. Central Command. Colonel Rich Juergens, USA, is Commander of Joint Task Force–Bravo in Honduras. Major Thomas L. Cantrell, USAF, is a student at the Joint Advanced Warfighting School.

to detect, identify, and track him in this low-contrast environment.

An all-source intelligence network must cue airborne ISR. The most effective airborne sensors are full-motion video (FMV) and SIGINT. However, when applied against the low-contrast enemy, these sensors must have a narrow field of view, and that means they are not effective as wide area search tools. As such, airborne ISR requires a start point provided by other sources. HUMINT and SIGINT are prolific providers of start points for airborne collection. The enemy is so well hidden that it takes multiple sources of intelligence to corroborate one another. SIGINT, for example, can locate a target but may not be able to discern who it is. FMV can track but not necessarily identify. HUMINT can provide intent but may not be able to fix a target to a precise location.

the global communications revolution has given this insurgent a new complex terrain—an "electronic sanctuary"

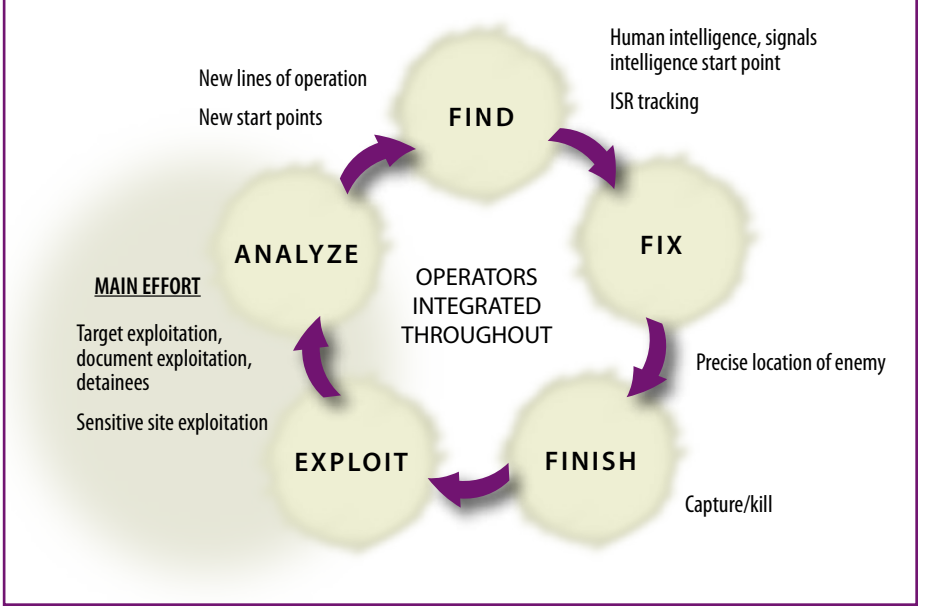
Synchronize ISR

Persistent and high-fidelity intelligence is the key to defeating a foe whose primary strength is denying U.S. forces a target. In contrast to major theater operations where the purpose is to find and destroy ships, tank formations, or infrastructure, the most difficult task in insurgencies is finding the enemy. Airborne ISR has become critical to this war because it offers persistent and low-visibility observation of the enemy as well as an ability to focus the spotlight on low-contrast foes, so they can be captured or killed.

However, these disciplines working together are able to focus the spotlight on low-contrast foes, so they can be captured or killed.

Airborne ISR's effectiveness grows exponentially when it is cued to and driven by other sources of intelligence rather than operating alone. Without a robust, collaborative intelligence network to guide it, sensors are often used in reactive modes that negate their true power and tend to minimize their full potential. These intelligence disciplines provide

Use of Find, Fix, Finish, Exploit, and Analyze (F3EA)



a start point into the enemy network that can be exploited through persistent and patient observation. With this type of start point, one can mass ISR with confidence that assets are not being wasted.

Mass ISR

Intelligence, surveillance, and reconnaissance are most effective against low-contrast enemies when *massed*. The insurgent's ability to hide in plain sight demands persistent collection in order to detect his presence. Persistent collection requires long dwell times and must be focused using multiple sensors on discrete parts of the network in order to achieve the fidelity of information required for targeting.

when the enemy is massed, ISR can be spread about; when the enemy is dispersed, ISR must be massed

When the enemy is massed, detection is made simpler and ISR can be spread about; conversely, when the enemy is dispersed, detection potential is reduced and ISR must be massed to be effective.[6]

Inherent in massing is rejecting the commonly held practice of "fair-sharing" ISR among multiple units. Massing implies focus and priority. Selected parts of the enemy's network receive focus, which should be unwavering for a specified time. This is counterintuitive to those who feel the need to fair-share assets as a way to cover more space and service more priorities. The problem with a low-contrast and fleeting foe, however, is that enemy actions are not easily predictable. Without prediction, the next best things are redundancy and saturation. Piecemeal employment of ISR assets over a large geographic area theoretically allows for efficient targeting but often at the expense of effectiveness. Several tactics can be applied to improve ISR effectiveness against the insurgent.

The *Unblinking Eye* provides an opportunity to learn about the network in action and how it operates. It is long dwell, persistent surveillance directed against known and suspected terrorist sites or individuals. The purpose of this long dwell airborne stakeout is to apply multisensor observation 24/7 to achieve a greater understanding of how the enemy's network operates by building a pattern of life analysis. This is an important concept and has proven itself time and again with hundreds of examples of successful raids.

Nodal analysis is spatially connecting relationships between places and people by tracking their patterns of life. While the enemy moves from point to point, airborne ISR tracks and notes every location and person visited. Connections between those sites and persons to the target are built, and nodes in the enemy's low-contrast network emerge. Nodal analysis has the effect of taking a shadowy foe and revealing his physical infrastructure for things such as funding, meetings, headquarters, media outlets, and weapons supply points. As a result, the network becomes more visible and vulnerable, thus negating the enemy's asymmetric advantage of denying a target. Nodal analysis uses the initial start point to generate additional start points that develop even more lines of operation into the enemy's network. The payoff of this analysis is huge but requires patience to allow the network's picture to develop over a long term and accept the accompanying risk of potentially losing the prey.

Vehicle follow is tracking vehicle movements from the air. These are important in illustrating the network and generating fix-finish operations. A recent Office of the Secretary of Defense study over a multimonth period found that vehicle follows were important to building pattern of life and nodal analysis.[7] Vehicle follows were surprisingly central to understanding how a network functions. They are also among the most difficult airborne ISR operations to conduct and often require massing of assets to ensure adequate tracking.

Airborne ISR effectiveness increases by an order of magnitude when massed. A single combat air patrol (CAP) of ISR is defined as one platform 24/7 over a target. Use of three CAPs is generally the best practice for massing on a target set during the fix and finish phase of the operation. This allows mass not only in space but also in time, which equates to persistence. It is not enough to have several eyes on a target—several eyes are needed on a target *for a long period*. Three CAPs permit persistent surveillance of a target while simultaneously developing the network's pattern of life through nodal analysis and vehicle follows. It gives the finishing force commander more options than merely killing or letting an observed enemy go; with sufficient ISR, a ground force commander can demonstrate much greater operational patience, thus allowing a larger insurgent network to emerge.

Massing ISR in time and space has operational results that should not be ignored. The Office of the Secretary of Defense study concluded that massed and persistent collection was an important element of success in SOF operations.[8] Conventional forces tend to cover disparate targets for a shorter period than SOF, which tend to focus collection on a smaller number of targets for much longer. The conventional force approach reveals a desire to service a large number of targets and units instead of developing the pattern of life of an enemy network. The tendency to think of persistence in terms of space rather than time

Soldier engages Taliban with AT4 rocket in Afghanistan

982d Combat Camera Company (Michael L. Casteel)

results in sprinkling assets in multiple areas rather than focusing them on a limited number of locations.[9] This method attempts to support a large number of units, rather than a handful of units, with sufficient collections capability to be effective and operationally potent. This is a difficult paradigm shift to make, but in a scarce ISR environment some units may need to go without to ensure that a smaller number can be effective against the higher priority targets. The alternative is to make all units suboptimal.

Conduct Forward PED

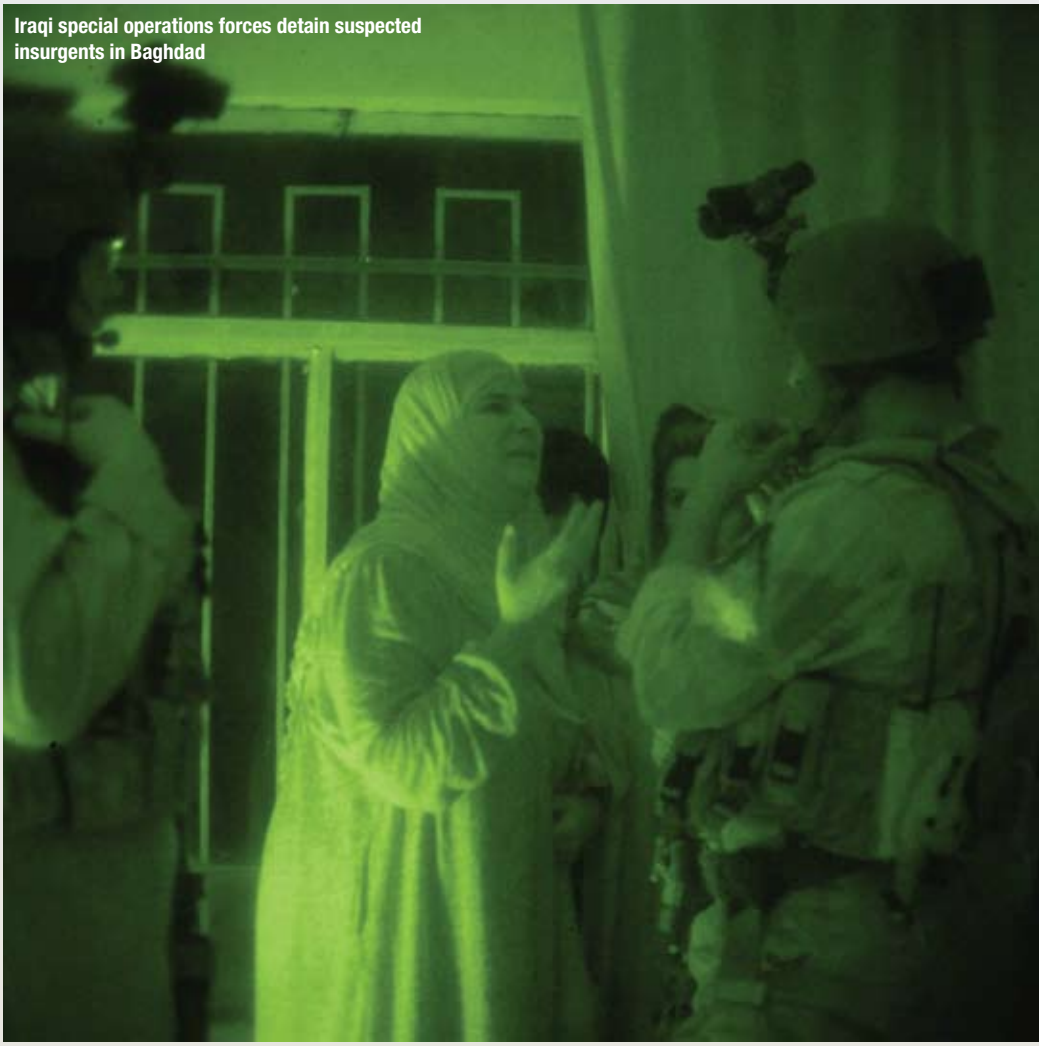
A critical enabler in employing ISR was having forward processing, exploitation, and dissemination (PED) integrated into the Tactical Operations Center (TOC). The Air Force has excelled at building state-of-the-art reachback PED nodes. But the speed and intuition required to cross-cue, target, plan, and react amidst multiple streams of intelligence and operations in a highly fluid battlespace require a forward PED presence able to interact in that environment. The reachback nodes simply do not have the situational awareness one gains by physically being forward with supported operations and other intelligence personnel.[10] A certain balance between the efficiency of reachback and the effectiveness of being deployed can be attained by sending small "reach-forward" elements to orchestrate and integrate the overall PED effort. PED became critical and far more effective to fast-moving decisionmaking simply by being forward.

Forward PED became tightly integrated into the operations tempo. The JSOTF and its subordinate task forces dynamically retasked ISR assets as the operational situation developed in order to quickly react to the emergence of fleeting targets. The forward PED element was critical to this. These PED professionals directed the sensor following the target and as the situation changed would confer with operations personnel as to the best response. PED would rewind and review key events on the fly with operators to assess whether a trigger event had been met, while a reachback element kept eyes on the real-time video and communicated updates to the TOC. All the intelligence disciplines conferred and contributed their part to help the operator decide whether to conduct a raid, call an airstrike, bring in another collection asset, or continue to observe. The finishing force conducted real-time face-to-face consultation among operations, collections, and intelligence personnel to exploit opportunities.

Forward PED personnel developed a continuity in analysis that was crucial in targeting the low-contrast foe. For example, airborne FMV was often like a law enforcement stakeout, and these specialists became intimately familiar with a target's habits and characteristics. FMV analysts engaged in an Unblinking Eye atmosphere developed a target intimacy to the degree that they could easily recognize something unusual and in some cases even detect a visual signature of how the target walked, traveled in groups, or engaged other people.[11] The ability to recognize a target's gait, dress, companions, parking patterns, and so forth became high-confidence targeting indicators because of the hours of pattern of life observation. This created an intimacy with the target that made the FMV sensor all the more powerful. Airborne surveillance in some ways is like HUMINT in that it provides a means of direct observation that previously had to be conducted by a specialized surveillance operative under significant risk.[12] Like a private investigator, airborne FMV can stake out an insurgent's house by using the relative safety altitude provides. This high-tech asset excels at the low-tech effect of observing the activity of individuals.

Airborne ISR is the centerpiece of the F3EA because it is tightly synchronized with a finishing force. This force is tightly coiled like a snake and ready to take advantage of fleeting opportunities that are so often found on the insurgent battlefield. These operators do not employ "whack-a-mole" tactics, but exercise operational patience in applying ISR

all the intelligence disciplines conferred and contributed their part to help the operator decide whether to conduct a raid, call an airstrike, bring in another collection asset, or continue to observe



Iraqi special operations forces detain suspected insurgents in Baghdad

U.S. Navy (Michael B.W. Watkins)

to gain greater insight into the network. They have learned that gathering greater fidelity on the network is often more important than a short tactical gain. They allow the target to ripen—and when judgment dictates that they have observed enough, they strike. This flows into the exploitation phase and drives the next steps in the operational campaign against the network. Multiple targets may be struck at once and, in some cases, yield an abundance of highly useful information on the murky enemy. The JSOTF took care to exploit sites properly because they understood that the information derived during the exploit-analyze phase would lead to more targets.

Exploit and Analyze

F3EA differs from other targeting models because of its emphasis on exploit-analyze as the main effort. This recognizes the importance of intelligence in fighting the low-contrast foe and aggressively supplying multisource start points for new ISR collection. More than the other phases, this feeds the intelligence-operations cycle in which intelligence leads to operations that yield more intelligence leading to more operations. The JSOTF emphasis on raids is essential to gather intelligence on the enemy network; simply killing the enemy will not lead to greater effectiveness against their networks. In fact, capturing the enemy for purposes of interrogating is normally the preferred option. The bottom line of exploit-analyze is to gather information and rapidly turn it into operational action by applying it to defeat the enemy's network.

Target exploitation and *document exploitation* are important law enforcement–type activities critical to F3EA. Documents and pocket litter, as well as information found on computers and cell phones, can provide clues that analysts need to evaluate enemy organizations, capabilities, and intentions.[13] The enemy's low-contrast network comes to light a little more clearly by reading his email, financial records, media, and servers. Target and document exploitation help build the picture of the enemy as a system of systems and as such enables counternetwork forces to attack it holistically.

Detainee intelligence is another law enforcement–like function crucial to revealing the enemy's network. The ability to talk to insurgent leaders, facilitators, and financiers on how the organization functions offers significant insight on how to take that organization apart. In terms of analysis and developing targeting lines of operation, detainee intelligence is the key to the "slow, deliberate exploitation of leads and opportunities, person-to-person" that drive operations.[14] Intelligence from detainees drives operations, yielding more detainees for additional exploitation and intelligence. A tight connection between interrogators and detainee analysts on one hand and all-source intelligence, collections, and operators on the other is critical to take advantage of raw information.

the ability to talk to insurgent leaders, facilitators, and financiers on how the organization functions offers insight on how to take that organization apart

Unify Organization

F3EA is best employed under a unity of organization to ensure speed of decision and speed of action. All elements required for success in F3EA were under the single direction of the JSOTF commander. A conscious effort was made to eliminate organizational seams between key functions that drive the F3EA process. Early in the war on terror, an intelligence organization may have led find and fix efforts but had to pass finish to a SOF unit. This represented an "organizational blink" where responsibility for actions on the target had to be passed across a seam to another organization. The time and spin-up required when that seam was crossed slowed the ability to finish the enemy. After the finish and site exploitation, interrogation and follow-on document or media exploitation were conducted by still other units, creating additional blinks in yielding timely intelligence that could be fed back into the targeting cycle. Analysis was another disparate effort, relying on skills and expertise that were mostly geographically dispersed, making face-to-face collaboration difficult. No matter how good the intelligence gain was, requesting support from multiple organizations for these different functions was neither timely nor did it provide the necessary agility.

The JSOTF created a unity of organization by bringing elements of the interagency community behind the F3EA functions into a common Joint Operations Center. The organizational imperative was simple: get the best people and bring them together face to face in a single location collaborating on a target set while orchestrating reachback support to their national offices. This effectively decentralized those national agencies, pushing the needed intelligence to the tactical level where it was most useful. These specialists collaborated and fused in a flattened environment where horizontal communication is favored over the vertical. Airborne ISR crews and operators worked closely with intelligence analysts while ISR PED personnel coordinated with interrogators, all in a fast-moving fused process facilitated by sharing the same physical space. As a result, a fleeting target was not passed around from one organization to another, but moved rapidly "in house" for full analytical, operational, and exploitation impact. The result was that a target could go from observation to action within minutes, providing the agility that counternetwork and counterinsurgency forces require.

Speed of decision was achieved because this unity of organization was under common direction and priority. The commander's intent was the most important thing driving the intelligence and operations teams on focused common lines of operations that could change as the battlespace changed. This unity created an environment where decisions could be rapidly made, whether to retask ISR assets, conduct a raid, or switch focus based on a critical piece of HUMINT. The JSOTF's F3EA process was therefore very rapid—its ability to decide and its authorities to act were flattened with no need to seek higher permissions, and this made it fast enough to be effective against the enemy. Unity of organization communicates intent, minimizes friction, drives focus and priority, enhances collaboration, and drives prioritized, persistent, and focused approaches to attack an enemy network. Without it, the agility of striking multiple targets per night or swiftly moving from the patient and methodical find to those moments of madness in fix and finish are beset by too much friction to be feasible.

Recommendations

Counternetwork operations as described here cannot win a counterinsurgency, but they can provide the space and time needed for wider stability operations to enable political solutions. The significance in these tactics is that they not only maintain a rapid operations tempo against the enemy, but also are designed to gather the maximum information possible on the enemy network. Armed with this information, the JSOTF turns up the gain on the low-contrast network and can smartly target

those important and low-redundancy nodes on which the enemy depends.[15] Persistence, speed, and unity are required to be successful.

The tactics described here can be applied at the brigade combat team (BCT) level. National agencies have recognized the power of decentralizing their capabilities and putting them into the hands of those who most need them. Most agencies are pushing their reach-forward teams to the lowest level possible. Decentralized control of airborne ISR at the BCT level also makes sense for those who have the operations-intelligence synergy to accurately point airborne ISR and have the forces poised to take advantage of find and fix. This demands robust air planning and control capability at the brigade level.

Increasing airborne ISR and devolving control requires greater joint integration at lower levels. The brigade aviation element (BAE) provides organic 24-hour operational capability to plan and coordinate full-spectrum aviation operations (including unmanned aerial systems) throughout a BCT's area of responsibility. It includes the capability for airspace control and tailored intelligence analysis. The Air Force Theater Air Control System (TACS) elements should be increased and linked to the BAE to facilitate planning and integrate control of these decentralized air assets. The new Air Force Doctrine Document 2–3, *Irregular Warfare*, recognizes the need in some cases to "delegate some aspects of planning and decision making to subordinate Airmen positioned at lower levels within the TACS. . . . Increasing the role and authority of subordinate Airmen may provide more innovative and effective uses of Air Force capabilities."[16] Lower-level TACS should include forward PED elements employed and integrated wherever possible. ISR should be allocated more to BCTs that emphasize exploit-analyze, mass ISR, have robust planning and control capability, and weave these elements into a unity of effort that relentlessly drives lines of effort against the enemy network.

Airborne ISR, specifically FMV and SIGINT, is so essential to counterinsurgency and counternetwork operations that it is clear the Services are behind in providing adequate resources to deployed forces. Evidence from the last 6 years of combat operations combined with lessons learned, testimonials, and combatant command integrated priority lists should be more than enough evidence that our FMV and SIGINT fleet needs to grow by orders of magnitude. As Air Force Deputy Chief of Staff for Intelligence Lieutenant General David Deptula related in a speech last year, the "Department of Defense should aspire to put an end to the situation in which sensor systems and the means to interpret . . . are chronically low density/high demand assets."[17] A good starting point is to enable Air Force Special Operations Command with a robust fleet of airborne ISR. Special Operations Command and the Theater Special Operations Commands alone require at least 30 orbits of dual sensor FMV/SIGINT to meet their war on terror commitments. Beyond Iraq and Afghanistan, these assets will prove invaluable in IW arenas where "through, by, with" concepts will require U.S. enablers to make host nation counterinsurgency effective. An IW ISR fleet could act as a testbed for new tactics, techniques, and procedures (TTP) that could be codified and proliferated throughout the Department of Defense and promote smarter and more precise operations against low-contrast opponents.

U.S. Joint Forces Command (USJFCOM) should codify these lessons learned into multi-Service TTPs and force modules. Unit type codes (UTCs) are alphanumeric codes uniquely identifying each type unit of the Armed Forces and represent discrete capabilities that joint planners use as the building blocks for modular, repeatable, and scalable resources for contingency and crisis action plans. ISR UTCs, for example, typically include platforms, pilots, and mechanics. Force modules are groups of UTCs that are functionally aligned and are typically employed together. USJFCOM should craft IW force modules that feature three CAPs of ISR with requisite PED UTCs and combined with operations and intelligence UTCs. Employing a force module in this way will ensure ISR is synchronized with operations and integrated with an all-source intelligence network. Being organized this way for war will cause the units comprising this force module to train together and build habitual relationships among combined arms teams of operations, intelligence, and collections. Thus, it would ensure these best practices would continue from the start of the next campaign rather than having to be learned.

Airborne ISR is most effective when it is massed, synchronized with operations, integrated with all-source intelligence, and employed under a unity of organization. Driven by this analytical and operational imperative, airborne ISR becomes an offensive counternetwork tool that enables a rapid tempo of operations. Without this focus, ISR devolves into a defensive tool conducting "whack-a-mole" tactics. Unlocking airborne ISR's true power involves employing this new combined arms team as a complete package to provide a more effective response to the type of enemy the war on terror might bring. **JFQ**

NOTES

[1] William B. Caldwell IV, Pentagon press briefing, June 9, 2006, available at <www.mnf-iraq.com/index.php?option=com_content&task=view&id=1236&Itemid=128>.

[2] Glenn W. Goodman, "ISR Now Synonymous with Operations," *Journal of Electronic Defense* 30, no. 7 (July 2007), 19.

[3] Edward N. Luttwak, "Dead End: Counterinsurgency as Military Malpractice," *Harper's Magazine* (February 2007), 36.

[4] David J. Kilcullen, "Counter-Insurgency Redux," *Survival* 48, no. 4 (Winter 2006/2007), 113.

[5] Thomas X. Hammes, "Countering Evolved Insurgent Networks," *Military Review* (July-August 2006), 19–20.

[6] U.S. Air Force, *Theater ISR CONOPS* (Washington, DC: Headquarters Department of the Air Force/A2CP, 2007), 18.

[7] Office of the Secretary of Defense, "EDGE FMV Study Results PowerPoint Briefing, October 2007, Interim Findings," 2007.

[8] Ibid.

[9] Michael L. Downs, "Rethinking the CFACC's Intelligence, Surveillance, and Reconnaissance Approach to Counterinsurgency," Master's thesis, Naval War College, 2007, 12.

[10] Gary E. Luck, "Insight on Joint Operations: The Art and Science," *A Common Perspective* 14, no. 2 (November 2006), 27.

[11] Robert D. Kaplan, *Hog Pilots, Blue-Water Grunts* (New York: Random House, 2007), 334.

[12] Brian A. Jackson, "Counterinsurgency Intelligence in a 'Long War': The British Experience in Northern Ireland," *Military Review* (January-February 2007), 80.

[13] Field Manual 3–24, *Counterinsurgency* (Washington, DC: Headquarters Department of the Army, December 2006).

[14] William B. Caldwell IV, weekly press briefing, June 8, 2006, available at <www.mnf-iraq.com/index.php?option=com_content&task=view&id=2018&Itemid=128>.

[15] Martin J. Muckian, "Structural Vulnerabilities of Networked Insurgencies: Adapting to the New Adversary," *Parameters* 36, no. 4 (Winter 2006/2007), 19.

[16] Air Force Doctrine Document (AFDD) 2–3, *Irregular Warfare* (Washington, DC: Headquarters Department of the Air Force, August 1, 2007), 9.

[17] Goodman, 20.