
U.S. Air Force (Eric Harris)

RQ-4 Global Hawk was designed for intelligence, surveillance, and reconnaissance

ISR Support to Operational Access
Winning Initiative in Antiaccess and Area-denial Environments

By ANDREW ROBERT MARVIN

When General Martin Dempsey released the Joint Operational Access Concept (JOAC) in January 2012, it represented a strategic shift within the Department of Defense (DOD) following more than a decade of focus on irregular warfare in Iraq and Afghanistan. In the JOAC, General Dempsey called for the development of strong solutions to counter enemy efforts to deny the U.S. military both the ability to reach a joint operational area (antiaccess) and, once it has reached that area, its ability to freely maneuver toward an objective (area denial). Together, these antiaccess/area-denial (A2/AD) tactics represent a substantial threat to the current American way of war, which is characterized by long buildups, sizable logistics footprints, and unhindered access to intelligence, surveillance, and reconnaissance (ISR).

Execution of A2/AD against U.S. forces assumes the enemy successfully employs advanced conventional weapons and cyber capabilities, some relatively novel and some familiar to planners. Potential foes have many weapons, but their plans will hinge on just a few of them. These few weapons will form the enemy's high-value target (HVT) list. American ISR must focus on finding these HVTs fast enough and far enough away from a joint task force (JTF) to allow for their successful targeting and destruction.

Andrew Robert Marvin is a Management Consultant for IBM Global Business Services in Chantilly, Virginia, where he conducts quantitative assessments of military operations and intelligence, surveillance, and reconnaissance assets. He also researches the application of social media in emergency management.

DOD

Remains of Iraqi Scud missile shot down by MIM-104 Patriot tactical air defense missile outside of Riyadh during Operation *Desert Storm*

The thinking about ISR employment in an A2/AD environment is not mature. The JOAC spends only a few paragraphs out of 70 pages on intelligence. Other valuable works on A2/AD, such as Mark Gunzinger and Christopher Dougherty's valuable description of possible operations in the Persian Gulf,[1] discuss maneuver more than intelligence. DOD leadership must ensure that ISR and processing, exploitation, and dissemination (PED) capabilities properly support and map to an operational access campaign or the concept will fail. This success must start with more thinking and debate on intelligence missions in A2/AD environments.

The intelligence function's task in an operational access campaign will be tough. Not only must intelligence find HVTs central to A2/AD, but it must do that in a high-threat environment where ISR assets can be destroyed or spoofed. Assuming a collection platform succeeds and actually survives long enough to exfiltrate its data, analysts must then produce and disseminate all-source intelligence rapidly enough for friendly firepower, which is also vulnerable to A2/AD assets, to use it. The intelligence function must juggle these tasks as well as traditional responsibilities such as intelligence preparation of the operational environment, situational awareness, and counterintelligence. To make matters more challenging, a JTF executing an operational access campaign could face competition for scarce intelligence collection and production assets from other contingency operations as well as demands from political leaders who need to stay abreast of the situation. During Operation *Odyssey Dawn*, the Air Force's only Joint Surveillance Target Attack Radar System unit was already committed to flights in Afghanistan when it was called to provide aircraft and crews to support operations in Libya, putting additional stress on an already heavily used capability.[2]

This article proposes a framework for analyzing intelligence support, and ISR in particular, in support of the JOAC. While the intelligence mission is universal—to drive operations through the provision of actionable information to commanders—its tools are not. What worked in Afghanistan, or even in Libya, might not work in a future operational access campaign. By thinking about operational access theory, we can imagine exactly what we want ISR to do, freeing ourselves (just enough) from past paradigms, doctrine, field manuals, and joint staff acquisition processes that are either overprescriptive or unhelpfully vague when applied to future problems. Finally, in addition to putting forward the *attributes* of good operational access ISR (the *what* in these future campaigns), this article seeks to contribute to the *how* side of the equation by offering methods to assess and measure the size and composition of a future intelligence warfighting function.

The Future Battlefield

When Operation *Iraqi Freedom* transitioned from invasion to counterinsurgency, it took several rotations for ISR capabilities to adjust from tracking Republican Guard divisions to finding insurgent high-value individuals (HVIs). While not all A2/AD threats are as elusive as HVIs, there is reason to believe they will challenge existing ISR capabilities. In the JOAC, air defense tops the list of potential aerial-denial threats. Integrated air defense systems (IADS) are largely static, relying on large radar sets, ground control intercept stations, and large surface-to-air missiles (SAMs) that are difficult to move. Some of these assets can be identified and plotted preconflict. For instance, a SAM battery defending a key airfield is unlikely to move once detected. The United States made short work of air defenses in Iraq and Libya during recent conflicts, yet these nations had antiquated IADS. Newer SAMs, even long-range missiles such as the Russian S-400, are more mobile than the decades-old SA-5s fielded by Libya.

Also, mobile systems that combine transporter, erector, launcher, and radar (TELAR) into one vehicle have grown more sophisticated. Mobile SAMs can operate autonomously or take cues from surviving target acquisition or even civil air control radar. If not initially destroyed in garrison, these weapons can become a persistent threat to U.S. aircraft, preventing the deployment of slower aircraft such as unmanned aerial systems (UASs) and AC-130 gunships, while forcing jets to operate at higher altitudes. If U.S. ground forces are engaged, such systems can pose a significant threat to aircraft performing the demanding close air support mission.

Surface-to-surface missiles (SSMs) with ranges in excess of 1,000 nautical miles pose a serious antiaccess threat under the terms of the JOAC. Potential SSM threats can follow either cruise or ballistic trajectories and can be launched from land, sea, or air. Even with conventional warheads, these weapons can threaten the staging areas needed for a campaign. Given proper targeting (including fully autonomous terminal stages), high speed, and sizable warheads, such weapons can even threaten U.S. carriers. Truck-mounted missiles or transporter erector launchers (TELs) can provide this missile the same capability to hide, launch, and disappear ("shoot and scoot") that modern SAM TELARs possess.

America's record in countering mobile SSMs is mixed. Iraqi Scuds were high prior-

ity targets during Operation *Desert Storm*. To find them, the coalition scoured potential launch areas with both special operations forces (SOF) and tactical aircraft loitering over kill boxes. These efforts likely had some impact. Scud attacks declined from 4.3 per day during the war's first week to 1.5 per day thereafter, but evidence suggests the coalition actually destroyed few TELs but many decoys.[3] After the war, Saddam Hussein still had a sizable Scud force to declare to United Nations weapons inspectors.

While ISR has improved significantly since 1991, experience in Libya and Iraq indicates that killing fleeting targets is still difficult. During the 2008 battle for Sadr City, rocket attacks launched by Iraqi insurgents proved so difficult to interdict that ground forces resorted to walling off sections of the city to prevent further attacks. Future foes may take their cues from Sadr City's rocket teams and hide their TELs in complex terrain instead of the flat environs of Anbar Province. Enemy IADS and air forces will likely be tougher as well. Under existing ISR regimes, search and strike sorties dedicated to neutralize these potent weapons would be sorely missed as a range of other A2/AD threats engages U.S. forces.

Intelligence Fundamentals for JOAC

The JOAC's response to evolving IADS, SSM, and other A2/AD threats is to count on increased cross-domain synergy of U.S. warfighting capabilities in order to gain a temporary exploitable advantage over the enemy—a swift effort to open the portal wide enough to allow victory. The JOAC calls for combat power both applied directly against enemy A2/AD threats and employed across great distances by way of a hardened long-distance supply chain.

While cross-domain synergy implies a variety of shooters (emerging capabilities may, for instance, allow SOF, submarines, or cyber assets to effectively neutralize an enemy IADS), the task and purpose are clear: enemy A2/AD assets need to go down long enough to support maneuver against an objective. This hard requirement creates two intelligence missions: effective search and actionable fusion.

Effective search refers to the collection of A2/AD asset signatures to support targeting by available firepower or soft-kill capabilities. While a range of sensors from imagery to human intelligence may detect a given A2/AD asset, any sensor must meet certain criteria to be effective. These criteria are access, capacity, resolution, and persistence.

Access equates to a sensor's effective reach. A high-gain receiver may be able to detect certain signals from hundreds of miles away, while a SOF surveillance team's range may be limited to line of sight and thermal imager resolution. Given the consequences of being ranged by U.S. firepower, future enemies are likely to devote significant combat power to counter reconnaissance and destroy American ISR assets. Mines can keep submarines at bay, and aggressive rear area security can neutralize SOF strategic reconnaissance efforts. SAMs might not be the only threat to air-breathing ISR assets. The Russians have designed air-to-air missiles such as the R-37 and R-172 with ranges in excess of 100 nautical miles. These "AWACS killers" could threaten U.S. ISR assets, keeping airborne sensors away from a battlefield and reducing their access. We speak of access as effective reach because range is not the only way to gain access. American ISR assets can also evade enemy counter-reconnaissance by methods such as survivability (operating from a platform that can absorb or evade enemy punishment) and clandestine emplacement (an unseen SOF team or a stealth platform).

Capacity refers to the amount of data a sensor can gather and process. For imagery sensors, this might be expressed in gigapixels, or square meters. For signals efforts, the number of channels monitored might be a relevant metric. Capacity is critical because of the familiar "empty battlefield" effect brought on by increasing weapon lethality. Between World War I and the 1973 Yom Kippur War, battlefield density decreased by a factor of 16.[4] Historian Trevor Dupuy measured 40,000 meters of battlefield per soldier in the latter conflict. This trend will likely continue in A2/AD conflicts. Longer range IADS and tactical missiles can attack from far off, thereby defeating U.S. ISR access in a linear fashion—weapons push away from a sensor kilometer by kilometer. Range is even harsher in its effect on capacity, however. As a weapon's effective range doubles (as the SA-17 doubled the range of the legacy SA-6 SAM), its potential hiding space on the battlefield quadruples. This fact might drive the United States to adopt ISR assets that can rapidly collect over a large area (whether geographic or electromagnetic).

Resolution refers to the ability to distinguish target signature from background noise. Research into HVI targeting in Iraq and Afghanistan found three critical elements of resolution: identity, geospatial, and temporal. *Identity* resolution shows what a target is—a church versus a barracks, a civilian versus an enemy agent. For fixed sites, identity resolution may be sufficient for targeting since imagery methods of geolocation are well refined and facilities do not change rapidly. For a runway, it is probably sufficient to see if it is still present a few days before a missile strike. Mobile targets such as HVIs and TELARs need good geospatial and temporal resolution. *Geospatial* resolution tells exactly where a target is (in a particular county or at a particular street corner). *Temporal* resolution lets us know when the other two attributes have been detected. This could be hours or minutes ago. Closer is better, of course, but weapon capabilities and dynamic targeting procedures would determine specifically how accurate ISR resolution must be.

Persistence refers to the length of time a sensor can collect data. Sensors with high persistence can access the battlefield for a long time. If a sensor was fast and had an infinite *capacity* (that is, it could collect on the entire battlefield at once) and exquisite resolution, it would not need persistence—all relevant HVTs would become visible at a scan of the sensor. Of course, no such sensor exists, and current systems need to invest time scanning the battlefield either searching for a particular HVT or stalking an existing one, waiting for its signature to change. In the stalk mode, a signals intelligence aircraft can wait for an enemy radio net to activate or a UAS can wait for an HVI to depart a safe house, opening the opportunity for a strike.

We have already shown that key A2/AD threats (such as mobile SAMs and SSMs) possess both low signature and high mobility. Finding a static, nonemitting TEL on a battlefield is a tall order. Missile launch may give sensors better detection odds, but ISR's goals should be predictive (or "left of the plume"), not a forensic examination of a successful enemy attack.

Effective search is the toughest problem facing intelligence support to the JOAC. Its success is tied to precious sensors that must effectively balance multiple dimensions. Search must be coordinated

with (and occasionally compete against) other military activities, and their ISR platforms must survive enemy efforts to thwart sensor access by destruction, denial, or deception. Still, effective search is not sufficient for intelligence success; actionable fusion must take place to ensure collected intelligence delivers value to an end user—usually a commander or a shooter—who is responsible for delivering firepower via land, sea, air, or cyber platform.

In existing intelligence doctrine, collection ostensibly delivers lists of answers to questions written in the form of priority intelligence requirements. Commanders allegedly write these requirements and then consume and synthesize collected intelligence to make decisions regarding the course of the battle. In actuality, intelligence staff officers usually write up requirements, which are often not synchronized with adjacent echelons. Additionally, shooters are likely to be even more voracious consumers of intelligence than their commanders. They are more numerous, of course, and hold the responsibility to actually execute the commander's plan by fighting and defeating the enemy. The intelligence that these shooters need may be highly perishable—a ballistic missile TEL may be set up for less than 30 minutes before it shoots from a presurveyed location. Aggressive time selection standards will demand fast actionable fusion that aids the shooter in finding and killing its target. The end result of actionable fusion is not a detailed briefing. It is a smoking crater.

In this scenario, intelligence analysts and the processing, exploitation, and dissemination infrastructure must work relentlessly on reducing the sensor-shooter link to meet tough dynamic targeting standards. Actionable fusion requires deliberate placement of each communications link, storage system, dissemination path, and approval mechanism that touches collected data. In an A2/AD scenario, the JTF intelligence function can neither pass erroneous information to a shooter nor let a fleeting target slip through the cracks. Intelligence support to time-sensitive targeting must be a battle drill practiced as rigorously and regularly as the application of lethal fires. To the greatest extent possible, its elements should not be simulated, and national agencies expected to support an intelligence effort during war should be present in training. Likewise, the analysis and PED feeding actionable fusion should not be a pickup game of individual augmentees and hastily assigned reachback analysts. Commanders and intelligence professionals should work out the people, processes, and technology beforehand given what we know about past experience and potential future combat scenarios.

Implications

As we evolve the operational access concept in response to A2/AD threats, we need to size the force to ensure that the Armed Forces and combat support agencies have the proper tools in the numbers needed to defeat these threats. As we have seen, the ISR stakes are high in any A2/AD scenario due to the speed at which an enemy can deliver firepower and the vulnerable concentrations (for example, ships, airfields, and forward operating bases) U.S. forces will present on the battlefield. For combat units and logistics, there is a great deal of background to assist in force-sizing. A mechanized infantry battalion can nominally cover four kilometers of frontage in the defense, and fighter wings and carrier groups can hit a certain number of targets per day depending on distance, munitions, and tankers available. The logistics community can plan using consumption rates for fuel, food, and munitions under certain circumstances. Even if these planning factors are somewhat off the mark, they give a solid starting point for planners thinking about future forces. Sizing ISR is more problematic. The Intelligence Community has fewer rules of thumb, and much systemic intelligence data are classified and hard to access. ISR application is not formulaic; 25 gallons of diesel may fill up a Humvee, and 18 standard pallets may fit on a C-17, but there is no equivalent solution that *x* number of ISR hours will detect an SSM in a wooded environment.

The result of poor forecasting techniques and a dearth of hard data is that ISR and PED support to JTFs can be wildly off the mark. Operation *Iraqi Freedom* began in 2003 and was supported mainly by Air Force Predator UASs that were augmented by a handful of short endurance, low-resolution UASs operated by the Army. By 2008, the UAS presence on the battlefield had grown by a factor of 25.[5] Human intelligence (HUMINT) capabilities expanded rapidly as well. At the start of *Iraqi Freedom*, brigades fielded one small HUMINT team each. By 2008, it was not uncommon for battalions to have two teams apiece, sourced both from the brigade's organic military intelligence company and augmentees from general support military intelligence or battlefield surveillance brigades. At the Army's intelligence center at Fort Huachuca, Arizona, a forest of buildings rose from the desert to train newly minted HUMINT specialists. Hastily hired contract instructors augmented the Active-duty cadre at the fort and made this training surge possible.

There are similar stories for signals intelligence and analytic efforts. A common explanation for this disconnect was that U.S. land forces had prepared to fight a mechanized foe that was easy to find but hard to kill. In Iraq (and Afghanistan), these forces instead faced an irregular threat of insurgents who were unable to hold ground against overwhelming American firepower, yet they were devilishly difficult to find.

ISR capabilities present at the outset of Operation *Iraqi Freedom* were largely determined by two methods: subject matter expert (SME) assessment, where a group of experienced professionals gives its experienced opinion on matters, and modeling and simulations (M&S), a largely computerized process of wargaming possible scenarios. Both have their place as assessment tools. SMEs can deliver answers quickly and leverage large amounts of personal experience. M&S can deliver detailed answers to concrete questions, such as the outcome of battles between mechanized units. Both have shortcomings when applied to ISR force-sizing.

SME input is critical to any assessment. As a standalone capability, subject matter expert results are quick and usually trusted. Very good M&S include input and validation from SMEs, particularly when exact measurements of a modeled attribute are not available. Another sizing method called operations assessment also requires either

as a standalone capability, subject matter expert results are quick and usually trusted

SME input or direct observation to build understanding and gain expertise. However, SMEs are not perfect. For instance, they are highly subjective to "success story" bias. When interviewed, operators and intelligence professionals tend to amplify the importance of a given ISR or PED capability if they have seen it succeed once or have viewed a success story vignette, often on a PowerPoint slide. These vignettes may not be representative of an ISR asset's performance, but because they often create a compelling narrative, they can be powerful platforms to drive the adoption and proliferation of certain capabilities. Additionally, context matters. Two brigade commanders interviewed regarding their tenures in Afghanistan gave different answers when asked to gauge the effectiveness of ground moving target indicator (GMTI) support. Success bias might affect these differences, as might incompetent (or particularly skilled) intelligence analysts. Finally, one unit could have gotten better results because its terrain is better suited for GMTI collection. None of these factors automatically invalidates SME input, but they demonstrate that it may not stand alone without follow-on analysis.

M&S are often touted as good capabilities to show future performance because they can be predictive. Indeed, when one has a great deal of data on a discrete situation (so many friendly tanks, so many rounds of ammunition, and so many opposition tanks), M&S can deliver some good answers. Unfortunately, ISR does not often present convenient factors such as coverage areas or consumption rates. Signal propagation rates may vary significantly depending on time of day, antenna placement, and aircraft altitude. Factors such as zoom and altitude also affect full-motion video area and resolution. Skill and experience are significant drivers of a sensor operator's ability to track a given target. Simulating such an environment relies on serial assumptions that dramatically reduce the chances of producing valid results. On the PED side, matters are even worse. M&S cannot hope to replicate factors that drive successful targeting, such as complex intelligence reporting (much of which is narrative) or the variance in quality among intelligence analysts. If one does attempt to account for these variances, inaccuracies can compound, skewing the results. As one study noted, applying M&S to intelligence employment is inherently challenging "because the generated results are often built on multiple nested and tenuous assumptions and approximations."[6]

Operations Assessment

For sizing ISR in support of the JOAC, an operations research technique known as operations assessment will likely outperform SME- or M&S-driven approaches. If appropriately employed alongside traditional sizing methods, it may yield results that are "less wrong" in the highly ambiguous world of forecasting ISR needs. Operations assessments start with developing a deep understanding of a unit's wartime mission and the operation of the ISR and PED assets that usually support them. SME input or direct observation is therefore important in the first stage of operations assessment, but rather than using this input as an endpoint for a staff briefing or position paper, operations assessments treat SME input as hypotheses to be tested with systemic data. This methodology proved successful in determining the key elements of HVI hunting in Iraq and Afghanistan and, later, the best way to kill indirect fire teams in Sadr City. In 2007, the Office of the Secretary of Defense hired a group of consultants to measure the performance of ISR and PED in supporting specific missions by examining key mission drivers (often determined through SME interviews and input) and substantial quantitative analysis. By reviewing thousands of storyboards, significant activities, intelligence reports, and sensor data records, the assessment team determined key drivers of success that led to several force-sizing decisions.[7]

Of course, while we have terabytes of operations and intelligence data from Iraq and Afghanistan, we are not currently fighting any countries that pose A2/AD threats. This does not invalidate the operations assessment approach, however. Certain elements of information will generalize. Some intelligence activities go on year round whether we are at war or peace. Measurement of those activities in peacetime, and the performance of key PED and ISR systems, could give insight into how they would perform in a shooting war against an enemy trying to destroy or spoof U.S. sensors. We do not know the performance of every IADS in the world, but we do have recent knowledge of how Libyan IADS reacted to U.S. forces and how successful our attacks, assessments, and followup strikes were. By the same token, we have never fought in many cities in the world, but we know how our sensors perform in urban environments and can extrapolate that to other urban areas.

SME input and M&S may play a part in these future operations assessments, but a brute force effort to model priority intelligence requirements and list critical attributes needed for the JOAC strategy will be doomed to failure. The terrain and domains, as the JOAC paper alludes, are simply too complex. The ISR focus for this threat should be informed by experts, driven by hypotheses, and supported by quantitative data. Such an effort, geared around the simple question of how we find and kill high-value targets in an A2/AD environment, would most likely yield answers, or at least candidates for more rigorous exploration. **JFQ**

NOTES

[1] Mark Gunzinger and Christopher Dougherty, *Outside-In: Operating from Range to Defeat Iran's Anti-Access and Area-Denial Threats* (Washington, DC: Center for Strategic and Budgetary Assessments, January 2012), available at <www.csbaonline.org/publications/2012/01/outside-in-operating-from-range-to-defeat-irans-anti-access-and-area-denial-threats/>.

[2] Gene Rector, "Joint STARS now supporting Libyan operations," *The Warner Robins Patriot*, March 25, 2011, available at <http://warnerrobinspatriot.com/view/full_story/12495900/article-Joint-STARS-now-supporting-Libyan-operations>.

[3] William Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets: Lessons from Vietnam and the Persian Gulf War* (Santa Monica, CA: RAND, 2001), available at <www.rand.org/pubs/monograph_reports/MR1408>.

[4] Trevor N. Dupuy, *The Evolution of Weapons and Warfare* (Indianapolis: Bobbs-Merrill, 1980), 307.

[5] Robert M. Gates, Remarks to Air War College, Montgomery, AL, April 21, 2008, available at <www.defense.gov/speeches/speech.aspx?speechid=1231>.

[6] Frank B. Strickland and Chris Whitlock, *Assessing the Value of Intelligence: Lessons for Leaders* (Washington, DC: IBM Center for the Business of Government, 2011), available at <www.businessofgovernment.org/report/assessing-value-intelligence-lessons-leaders>.

[7] Ibid.