RQ-4 Global Hawk and U-2 Dragon Lady are Air Force's primary high-altitude ISR aircraft, Beale Air Force Base, California, September 17, 2013 (U.S. Air Force/ Bobby Cummings)

Achieving Secrecy and Surprise in a Ubiquitous ISR Environment

By Adam G. Lenfestey, Nathan Rowan, James E. Fagan, and Corey H. Ruckdeschel

Sun Tzu could not have prophesied the future any better when he stated, "All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."[1] How can today's military planner execute a successful operational deception when the eyes of the world are always watching?

The notion of military offset strategies has been widely discussed in recent years. The first Department of Defense (DOD) offset strategy was envisioned to mitigate the Soviet Union's numerical advantage in conventional forces through a credible nuclear deterrent. When the Soviet Union, and to a lesser extent China, became nuclear powers, a new offset strategy was required. The second offset strategy consisted most prominently of antiaccess/area-denial (A2/AD) capabilities, such as precision navigation and timing (PNT), precision-guided munitions, and advanced intelligence, surveillance, and reconnaissance (ISR).[2] The second offset could be said to have culminated in 1991 during Operation

Lieutenant Colonel Adam G. Lenfestey, USAF, is Deputy Director of Space Programs and Operations at the Office of the Under Secretary of Defense for Intelligence. Commander Nathan Rowan, USN, is Commanding Officer of the USS *Billings* (Blue) LCS 15. Lieutenant Colonel James E. Fagan, USAF, is Chief of Strategic Engagement in the Political-Military Affairs Bureau at the Department of State. Major Corey H. Ruckdeschel, USA, is Chief U.S. Pacific Command Deliberate Planner for Joint Force Space Component Command at U.S. Strategic Command.

U-2 Dragon Lady delivers critical imagery and signals intelligence to decisionmakers during all phases of conflict, Sierra Nevada Mountain Range, California, March 23, 2016 (U.S. Air Force/Robert M. Trujillo)

Desert Storm, which was the first major U.S. combat operation since Vietnam.

To signal our warfighting superiority to the Iraqi regime and bolster American public confidence leading into this campaign, several capabilities key to the second offset strategy were declassified: high-resolution aerial and satellite imagery, precision strike, and stealth technology. The 1991 U.S.-led coalition against Iraq quickly achieved air superiority and began an extended campaign of precision strikes, enabled by air and space reconnaissance, against Iraqi critical warfighting infrastructure and forward-deployed forces in Kuwait, such as Republican Guard units. Under the blanket of air supremacy, the United States massed ground forces in Saudi Arabia while deceiving the Iraqi regime to believe it intended an amphibious landing in Kuwait. The ground war began when the now-famous "left hook" (the attack from the western desert rather than the anticipated amphibious assault from the southern shores of Kuwait) caught Iraqi forces completely by surprise. The combination of PNT, advanced ISR, and precision strike, coupled with a massed ground attack enabled by operational secrecy and surprise, resulted in a resounding victory over what was the world's fourth-largest military.

As the implications of second offset technologies became known and battlefield-proven over the ensuing decades, the world took notice. Governments around the globe sought for themselves the sort of results the United States realized against Iraq—in some cases to reproduce these U.S. advantages and in other instances to counter them. Entrepreneurs, likewise, realized the potential market value of rapid global ISR capabilities and began to develop them for commercial sale. By 2015, commercial remote sensing (CRS) satellites, also known as Earth observation services, had become a $1.8 billion-per-year industry comprising 14 percent of operational satellites worldwide, while military surveillance satellites composed an additional 8 percent.[3] The global aerial imaging industry, meanwhile, "including helicopters, fixed-wing aircraft, multi-rotor unmanned aerial systems [UAS]," and so forth, was valued at $1.1 billion in 2014 and is forecast to grow to $3.3 billion annually within 10 years.[4]

A strong U.S. CRS industry presents undeniable benefits to U.S. and coalition warfighters, policymakers, and interagency partners through innovation, cost-sharing, and its inherently unclassified nature. Yet once a U.S.-based CRS provider is licensed to operate, DOD has little ability to affect its activities or prevent its products from falling into hostile hands. Also, while U.S. industry remains preeminent in most areas of space-based CRS such as resolution, large constellations for rapid revisit, and advanced sensor phenomenologies, foreign government and CRS systems are advancing rapidly. Along with the exponential proliferation of small UAS and handheld smart devices, these trends pose a serious challenge to the traditional military principles of secrecy and surprise.

DOD has begun to invest in a third offset strategy, designed to "offset shrinking U.S. military force structure and declining technological superiority in an era of great power competition."[5] Third offset investments are necessary because potential adversaries, and in some cases the private sector, are approaching parity with the U.S. national security community in key areas of second offset capability. Yet while the proposed third offset strategy will develop new asymmetric U.S. military capabilities, it will not remove our responsibility to consider fundamental warfighting principles. As foreign and commercial ISR capabilities proliferate, our ability to leverage secrecy and surprise for battlefield advantage is in danger of being severely degraded or lost altogether. We must take prudent near-term steps to address this concern.

Improving Counter-ISR

To leverage secrecy and surprise in today's operating environment, DOD needs to improve its counter-ISR posture in five specific ways:

- identify friendly force signatures that require obfuscation
- develop passive and active denial and deception capabilities
- update DOD policy regarding aerial and space-based collection on militarily sensitive sites
- work with U.S. industry, the interagency communuty, and Congress to manage proliferation of militarily relevant CRS collection against friendly forces
- engage on a military-to-military basis with partner nations to develop bilateral and multilateral agreements and norms for operational and transactional controls on CRS collection.

Identify Signatures. First and foremost, planners need to understand the true nature of friendly force exposure to modern ISR collection during military operations. DOD should baseline the current temporal, spatial, and spectral signatures of conventional military forces as they will operate in land, maritime, and air domains in major deliberate planning scenarios. This study should evaluate current operation and contingency plans, focusing on deployment from garrison, transport, joint reception, staging, onward-movement, and integration in theater, and the associated logistics footprint. It should assume a robust, nonfriendly ISR presence both prior to and during combat operations. Combatant commands should evaluate the results of the signature study to identify and prioritize the operational signatures we must hide to preserve secrecy and/or manipulate to facilitate surprise. The commands may also find it necessary to revise portions of some deliberate plans against robust A2/AD scenarios.

Develop Countermeasures. DOD should baseline the current state of its denial and deception capabilities, identifying all such existing investments across all conventional military components and assessing their potential for employment in standing operation and contingency plans. This baseline should include all appropriate special handling caveats required to achieve a comprehensive picture of the existing pockets of excellence across the enterprise. Ultimately, unless these capabilities are scalable in sufficient numbers to meet combatant commander needs and available for regular training and exercise, they will be suboptimally employed when needed most.

The military Services should reinvigorate tactics, techniques, and procedures (TTPs) to manage operational signatures, train forces to employ those TTPs, and exercise them regularly. The Services will also likely need to develop new camouflage, concealment, and deception or other counter-ISR capabilities. It may even be necessary to adjust the DOD steady-state force posture to achieve a robust presence in A2/AD areas by combining secrecy and surprise with dispersal and displacement of forces, hardening of key infrastructure, and rapid reconstitution capabilities.[6]

Combatant commanders should also seek ways to mitigate the predictable operational signatures of deploying forces. Ubiquitous ISR makes surprise in mass extremely challenging, which is why the United States invested in the second offset decades ago. Now that U.S. adversaries are nearing ISR parity, to regain battlespace advantage senior commanders may need to distribute authority in new ways, such as disaggregating surface action groups at sea.[7] As a historical example, in the Battle of Austerlitz, Napoleon was successful in creating self-sustaining battalions that allowed him to surprise and attack the enemy on multiple axes with a minimal logistics and command and control footprint. It is imperative that combatant commanders find innovative ways to emulate this technique in a modern environment.

In terms of defensive measures, the United States is being outpaced in operational denial and deception, such as the use of decoys and dummy weapons systems. Decoy (systems that look, emit, and act like the real system) and dummy (ones that look *enough like* the real system) platforms are extensively used by U.S. adversaries to complicate our targeting cycle. Previous operations in Kosovo and Serbia saw the United States targeting dummy surface-to-air missile (SAM) sites that were nothing more than plywood sheets constructed and painted to look like real weapons. Recently, companies in Russia, China, and India have begun to make life-size inflatable SAM and aircraft replicas that match real-world dimensions and paint schemes. These inflatables can be quickly erected, interspersed with real systems, and relocated to create confusion against adversary analysts.

DOD should consider investing in similar systems for our own use to take advantage of the very adversary ISR that currently presents such a challenge. The Allies used dummy systems in World War II to confuse German intelligence by providing false numbers and disposition of forces. Effective ISR work can negate the confusion caused by dummy and decoy systems, but this takes time that can be used to friendly advantage. While some investment within DOD has likely already occurred, effective implementation will require a coordinated effort to develop, field, operate, and maintain such systems on a strategically or operationally relevant scale.

Passive measures likely will not be able to counter 100 percent of adversary

United Launch Alliance Atlas V rocket carrying second Mobile User Objective System satellite for U.S. Navy lifts off from Space Launch Complex-41, Cape Canaveral Air Force Station, Florida, July 9, 2013 (Courtesy Pat Corkery)

ISR capabilities, however. In addition to direct counter-ISR capabilities, DOD should develop unique information operation TTPs to create doubt in the intelligence collected by near-peer competitors, working to sow inconsistencies in the data generated from different sources of collection. We should create and leverage adversary uncertainty to ensure U.S. decision advantage, since it takes time to develop sufficient confidence in intelligence analysis to enable quality decisions. This requires us to hone our skills in currently underutilized mission areas. Currently, information operations are often improperly planned and executed in military operations, typically because they are difficult to simulate during planning and exercises, and thus their effects are hard to predict.[8] However, such active measures will become essential tools to complicate adversary kill chains in a robust ISR environment.

Cyber operations, for example, can paralyze an adversary's ability to defend and counterattack. The Russian war with Georgia in 2008 made heavy use of cyber attacks on Georgian command and control, finance, and governmental networks before and during combat. These attacks delayed a Georgian defensive reaction to Russian troops crossing the border into South Ossetia, since Georgian forces were dependent on electronic networks for command and control, targeting, fires, and logistics. However, cyber weapons can be costly to develop and maintain. A nation must first develop cyber tools to penetrate and surveil adversary networks. Upon identifying critical nodes, additional tools must be emplaced for activation at the desired time. These tools must be built to remain undetected yet accessible to the owner. Even then, the operator cannot be certain a given cyber effect will be executable when desired. The target may have an intelligence collection value that supersedes its neutralization, or the action against the target may bring about undesired secondary and tertiary consequences. Additionally, once a cyber weapon is used, it is exposed and is potentially open to the adversary to analyze, modify, and reuse against the originator.

Cyber operations may not need to include penetration of protected adversary networks, however. Instead, cyber operators could focus on third-party sources of information and intelligence such as social media, which has developed into a method of rapid information dissemination where it is often difficult to validate individual users or the accuracy of their information. Manipulation of social media will not fool dedicated, analytic government agencies indefinitely, but it could provide valuable maneuver space, as it takes time and resources to disprove misinformation and determine facts. Such operations can be compared to aerial chaff

dispersed to confuse radar. Advanced radars may be able to work through the clutter and relocate the initial target, but by the time this occurs, the target has likely escaped and possibly placed itself in a position of relative advantage.

DOD may also require new force projection capabilities with smaller footprints. For example, the use of drones has already rapidly transformed the way we go to war. Drones can be employed in all warfighting domains and can be far less detectable than conventional forces. They provide extended surveillance capabilities with a minimal forward logistics footprint and provide real-time data that allow commanders to assess the battlespace and potentially apply combat power, dramatically expanding the capabilities of an otherwise small and isolated unit.[9] Incorporation of drones into conventional operations can greatly improve economy of force while maintaining the element of surprise.

Update Policy. To this point, we have discussed ways to mitigate detection by hostile ISR. There are significant cases, however, where the nonfriendly ISR capability is, in fact, within our policy influence in various ways. For example, U.S. law grants the Secretary of Commerce authority to license CRS space systems,[10] and the U.S. National Security Council CRS policy requires the Secretary of Commerce, prior to granting any such license, to consult with the Secretary of Defense for national security concerns and with the Secretary of State for foreign policy and international obligations.[11] Each Secretary can direct the inclusion of license conditions, including operational controls such as limits on spatial and spectral resolution, special collection modes, geographic restrictions, or latency requirements. These can be enduring conditions or can be activated for a specified duration. The cumbersome interagency process by which this license adjudication occurs is currently under review by the National Security Council in light of a rapid increase in the number and complexity of CRS license requests in recent years.

The U.S. National Space Policy (NSP) states that "a robust and competitive commercial space sector is vital to continued progress in space." One theme of the NSP is to encourage U.S. commercial industry growth, both to support government needs and compete favorably in the global market. The NSP has borne fruit: the U.S. CRS industry leads the world market in all but a single niche market (synthetic aperture radar), and it is growing rapidly in size, scope, and complexity. New commercial entrants are bringing high-resolution electro-optical, synthetic aperture radar, multispectral and hyperspectral imagery, and large constellations that provide extremely frequent coverage of the Earth.

DOD evaluates each new license based on sensor capabilities and planned operating modes, but it lacks formal implementing guidance or operational context to assess the likely national security impact of new concepts. In concert with the study of operational signatures described above, the department should develop a set of theoretical minimum time, space, and spectrum sensor system parameters that enable an operator to detect militarily sensitive signatures. DOD should then leverage these parameters, along with the operational effect determined by the combatant commands, as it adjudicates future CRS license requests. In addition, the department should evaluate the operational effectiveness of limited-duration operational controls such as geographic restrictions or temporary resolution limits.

Our potential adversaries, as well as commercial providers, have also recognized the potential applications of drones for ISR. However, unlike space assets, drones are tactically countered by a variety of means. Combatant commands and military Services should identify sensitive locations that should be off limits to drone overflight and should use established air traffic management means to restrict access by friendly collectors. DOD should develop policy regarding the use of tactical countermeasures to prevent collection by hostile or third-party drone operators, including readily available kinetic and nonkinetic options.

Manage Proliferation. While DOD can place some operational controls on U.S.-based systems through the licensing process, the U.S. Government currently lacks clear statutory authority for transactional controls, such as the ability to restrict sale of remote-sensing data and products to specific actors of concern. Federal law prohibits some entities, such as those on the State Department's Denied Party or Treasury's Office of Foreign Assets Control lists, from directly tasking collection from domestic CRS imagery providers. However, even assuming effective enforcement of this prohibition, CRS images are rarely proprietary to an individual customer. Once a CRS provider loads an image to an archive for commercial sale, it is nearly impossible to prevent its sale to actors of concern. This is largely due to the prevailing interpretation of the Berman Amendment, which "stipulates that transactions involving 'information and informational materials' are generally exempt from the purview of the presidential regulation."[12] The amendment was intended to facilitate U.S. sale of entertainment programming, participation in academic conferences, and other such pursuits overseas during the Cold War. However, archived satellite imagery currently is regarded to fall into the broad category of information and informational materials despite any latent national security implications it may entail. This prevailing interpretation of the Berman Amendment causes DOD to be more conservative in licensing CRS operations than it might be if it had recourse to curtail dissemination of sensitive satellite data to actors of concern after collection.

DOD should work within the interagency community and with Congress to develop regulatory and legislative change proposals for transactional controls that could better prevent proliferation of militarily relevant CRS collection against friendly forces, while still enabling a flourishing CRS market. One potential solution would require CRS operators whose systems reach a threshold capable of detecting critical operational signatures, as identified in the aforementioned studies, to enroll in the National Industrial Security Program (NISP) as a condition of their license. NISP is a

partnership between government and industry to safeguard classified and controlled but unclassified national security information in the possession of private industry and academia.[13] As such, the NISP could facilitate handling and release procedures for CRS imagery if governed by transactional controls. It is commonly argued that implementing transactional controls would place the U.S. domestic CRS industry at a disadvantage to foreign competition. This argument is weak, however, because most significant foreign CRS competitors already operate under transactional controls within their host nations.

Engage Allies. World governments generally fall into one of three categories of overhead ISR consumption. In a few cases, they rely primarily on indigenous national technical means, perhaps augmented by CRS. In other cases, they form consortia or public-private partnerships to produce dual-use indigenous systems that meet their national needs and sell excess capacity in the CRS market to offset their cost of ownership. In the remaining cases, they simply form imagery-sharing agreements with allies or buy CRS products from any provider that meets their needs.

The United States is on friendly terms with most, if not all, significant CRS provider nations and has established bilateral/multilateral defense agreements with many of them. Foreign CRS providers approaching peer capability with U.S. systems are nearly universally subject to operational and transactional controls by their host governments. In the current global environment, it is fair to say there are no significant foreign CRS systems that operate under less regulation than their U.S. counterparts. To ensure the competitiveness of U.S. industry while better protecting national security, DOD should work within the interagency community, as well as through bilateral and multilateral military-to-military engagements, to establish a set of international norms for operational and transactional controls among CRS provider nations. These controls should be designed to prevent the exploitation of CRS by hostile entities to target friendly military operations and critical infrastructure.

A Chinese proverb states, "The best time to plant a tree was 20 years ago. The second-best time is now." This problem cannot be solved quickly, and no doubt DOD would have been well served to consider and implement counter-ISR measures over the last 20 years had we known how rapidly the field would develop. That said, DOD should begin to take action to ensure we do not lose the military principles of secrecy and surprise as our adversaries approach parity in second offset capabilities. We should begin by identifying the spatial, spectral, and temporal signatures that most expose friendly forces' intent and plans. Armed with these new insights, DOD should prioritize, develop, and employ denial and deception capabilities to deny adversary collection and create strategic ambiguity. In parallel, we should update DOD policy to mitigate our exposure to, and work across, government and industry to develop new techniques to manage proliferation of sensitive collection by non-hostile actors. Lastly, we should engage with our allies in military-to-military channels to develop bilateral/multilateral agreements and norms for operational and transactional controls among CRS provider nations.

None of these recommendations is a panacea. Independently, their effects likely will not generate the desired effects against near-peer adversaries. However, in concert, these recommendations have the potential to re-enable operational secrecy and surprise in a ubiquitous, nonfriendly ISR environment. JFQ

Notes

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1971).

[2] Robert Tomes, "Why the Cold War Offset Strategy Was All About Deterrence and Stealth," *War on the Rocks*, January 14, 2015, available at <http://warontherocks.com/2015/01/why-the-cold-war-offset-strategy-was-all-about-deterrence-and-stealth/>.

[3] Satellite Industry Association, "State of the Satellite Industry Report," September 2016, available at <www.sia.org/wp-content/uploads/2016/09/SSIR16-2016-09-23-Update.compressed.pdf>.

[4] Transparency Market Research, "Aerial Imaging Market—Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2015–2023," available at <www.transparencymarketresearch.com/aerial-imagery-market.html>.

[5] Terri Moon Cronk, "Work Calls for Third Offset Strategy to Bolster Future of Warfighting," Department of Defense, September 10, 2015, available at <www.defense.gov/News/Article/Article/616806/work-calls-for-third-offset-strategy-to-bolster-future-of-warfighting>; and MacKenzie Eaglen, "What Is the Third Offset Strategy," *Real Clear Defense*, February 16, 2016, available at <www.realcleardefense.com/articles/2016/02/16/what_is_the_third_offset_strategy_109034.html>.

[6] Elbridge Colby and Jonathan F. Solomon, "Avoiding Becoming a Paper Tiger: Presence in a Warfighting Defense Strategy," *Joint Force Quarterly* 82 (3rd Quarter 2016); and Timothy A. Walton, "Securing the Third Offset Strategy: Priorities for the Next Secretary of Defense," *Joint Force Quarterly* 82 (3rd Quarter 2016).

[7] Kit De Angelis and Jason Garfield, "Give Commanders the Authority," U.S. Naval Institute *Proceedings* 142, no. 10 (October 2016), 364, available at <www.usni.org/magazines/proceedings/2016-10/give-commanders-authority>.

[8] James R. McGrath, "Twenty-First Century Information Warfare and the Third Offset Strategy," *Joint Force Quarterly* 82 (3rd Quarter 2016).

[9] Michael Hastings, "The Rise of the Killer Drones: How America Goes to War in Secret," *Rolling Stone*, April 16, 2012, available at <www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416>.

[10] Title 51, U.S.C. §601, Pub. L. 111-314, "Land Remote Sensing Policy," December 18, 2010, available at <www.congress.gov/111/plaws/publ314/PLAW-111publ314.pdf>.

[11] Title 15, CFR, Part 960, "Licensing of Private Remote Sensing Systems," available at <www.ecfr.gov/cgi-bin/text-idx?SID=3e52af0c3e0563ad8891ca35e3ba0758&mc=true&node=pt15.3.960&rgn=div5>.

[12] Bruce Craig, "Sleeping with the Enemy? OFAC Rules and First Amendment Freedoms," *Perspectives on History*, May 2004, available at <www.historians.org/publications-and-directories/perspectives-on-history/may-2004/sleeping-with-the-enemy-ofac-rules-and-first-amendment-freedoms>.

[13] Defense Security Service, "Industrial Security," available at <www.dss.mil/isp/>.