No. 18
February 2018

The Mitchell Forum

Rethinking the Information Paradigm:
The Future of Intelligence, Surveillance, and Reconnaissance in Contested Environments

By Col Herbert C. Kemp, PhD, USAF (Ret.)

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact on current and emerging policy debates. The views expressed in this series are those of the author, and not necessarily those of the Mitchell Institute.

Abstract

Over the course of several decades, the US Air Force intelligence, surveillance, and reconnaissance (ISR) enterprise has undergone a remarkable transformation as it has evolved from a forward deployed industrial age operation to a globally networked information age operation.

The enterprise has enjoyed great success since September 2001, particularly with respect to distributed operations in support of the United States' counterterrorism operations. However, rapidly changing trends in the lethality of future air defense environments, the challenges to long haul datalinks in contested environments, and the accelerating avalanche of data in modern combat all point to the need for the ISR enterprise to undergo another revolution to meet the demands of 21st century multi-domain warfare.

This paper traces the evolution of the ISR enterprise to its present form, explores the evolving challenges and technologies affecting both the enterprise and the future operating environment, and offers potential avenues of modernization to meet the needs of a very challenging future.

Introduction

The Air Force intelligence, surveillance, and reconnaissance (ISR) enterprise has achieved a remarkable degree of success in its current globally distributed form. From its technological roots in the Cold War, the ISR enterprise grew and adapted to the dynamic needs created by the counterinsurgency wars the nation has been fighting since 2001. It succeeded through continuous (if not always painless) innovation and through sheer mass as the enterprise grew on an industrial scale to address urgent operational needs. While counterinsurgency requirements will remain important, the ISR enterprise of today may not be well matched to the demands of the highly contested environments expected in potential future combat with peer or near-peer competitors. The current ISR enterprise relies on two fundamental capabilities: the capability to fly sensors wherever they are needed to collect the intelligence required, and the capability to quickly exploit and disseminate that intelligence across a globally distributed enterprise. Both these capabilities are potentially at risk in highly contested environments.

A Brief History of Distributed ISR Operations

While counterinsurgency requirements will remain important, the ISR enterprise of today may not be well matched to the demands of the highly contested environments expected in potential future combat with peer or near-peer competitors.

Decades ago, when film cameras and "store-and-dump" electronic collectors were the main sensors flown on reconnaissance aircraft, exploitation of the collected intelligence could not occur until after the aircraft landed. This was the way the Air Force conducted ISR operations through much of the Vietnam War. However, by 1970, the USAF employed a U-2 aircraft in Vietnam to collect signals intelligence (SIGINT) data and transmit it to a ground station using the SENIOR BOOK system.[1] By the mid-1980s, U-2 aircraft with more advanced multi-INT capabilities were in use in Europe to support NATO operations, employing line-of-sight datalinks to in-theater ground stations to transmit data in near-real time.[2] A separate capability, SENIOR STRETCH, and later SENIOR SPAN established the first beyond-line-of-sight operation via the Extended Tether Program.[3]

With the end of the Cold War, these capabilities were returned to the continental United States (CONUS) and were reconstituted in the mid-1990s as Deployable Ground Stations (DGSs) 1 and 2, located at Langley AFB, Virginia, and Beale AFB, California, respectively. Together with the U-2 aircraft and its sensors, the Air Force established a capability designated the Contingency Airborne Reconnaissance System (CARS).[4] While the CARS ground stations were initially designed to be deployed to the supported theater, a new capability called Mobile Stretch (MOBSTR) made it possible to deploy a MOBSTR ground relay station forward to receive the U-2 downlink and then retransmit the data via satellite relay to a DGS in CONUS. This enabled the Air Force to establish an initial capability for distributed operations supporting operations in the Balkans and Southwest Asia by the late 1990s.[5]

By the turn of the century, distributed ISR operations were becoming normalized, although capabilities, operating practices, and command relationships continued to evolve as the Air Force learned how to operationalize the concept of units that could be operationally employed without being physically deployed. The initial DGSs at Beale and Langley, along with fixed ground stations at Osan AB, Republic of Korea (ROK) (DGS-3), and Ramstein AB, Germany (DGS-4), comprised the initial baseline for the Air Force Distributed Common Ground System (DCGS), which has continued to expand to meet emerging requirements.

Following 9/11, as the US entered combat operations in Afghanistan and later in Iraq, the distributed ISR enterprise grew to accommodate increased demand, including major expansion of capabilities to exploit full motion video (FMV) from the rapidly proliferating number of MQ-1 Predator and later MQ-9 Reaper missions being flown. While FMV had been a part of the ISR mission before 9/11, the demand expanded rapidly after 9/11, concurrently with the demand for exploitation and processing of multi-INT data feeds from U-2 and RQ-4 high-altitude platforms.[6] To support the global enterprise, the

Air Force reorganized DCGS "…as a global ISR weapons system versus a set of organic nodes that are only associated with one region."[7]

Today's ISR enterprise is a global operation that supports combat operations in Southwest Asia, as well as worldwide peacetime aerial reconnaissance missions. Manned systems such as the U-2 and various RC-135 variants continue to perform well, but the trend toward remote piloted systems is clear. Remotely piloted aircraft (RPAs) were flying 60 Combat Air Patrols (CAPs) daily in early 2016 and the Air Force had decided to increase this to 70 CAPs in the near term and eventually to 90 CAPs.[8] The bulk of data exploitation is performed within the Air Force DCGS, which at present includes 27 processing sites worldwide, with a wing operations center at Langley AFB to manage global operations.[9] However, the system is also highly linear, with a defined mission thread from each sensor to one or more human analysts. Moreover, current processing and exploitation systems are manpower intensive, with most of the "touch labor" applied early in the analytical process.[10] These distributed models require the Air Force to maintain multiple long-haul, high-bandwidth communications and datalinks that may be vulnerable in future conflicts.[11]

The bulk of data exploitation is performed within the Air Force DCGS, which at present includes 27 processing sites worldwide, with a wing operations center at Langley AFB to manage global operations. However, the system is also highly linear, with a defined mission thread from each sensor to one or more human analysts.

The ISR enterprise has performed remarkably well in supporting peacetime reconnaissance operations. So, why change? Simply stated, the enterprise has become exquisitely well suited to supporting the global war on terror in relatively uncontested air defense environments, and often under circumstances that are not heavily dependent on the speedy synthesis of existing information with baseline knowledge, also known as "time-dominant fusion." In its present configuration, however, the enterprise may not be well suited to provide ISR support to combat operations in highly contested environments. To better frame the problem, it is important to examine the future combat environment, as well as the demands that the ISR enterprise will have to meet to support command and control and the operational capabilities to fight and win in a future multi-domain battle.

Understanding the Future Battlespace

There is general agreement among military and security analysts that future conflicts will be fought in a range of highly lethal environments. Highly capable, mobile, long-range surface-to-air missiles already threaten both penetrating aircraft and non-penetrating aircraft that usually operate from standoff orbits. Long-range surface-to-surface mobile missiles threaten US bases, fixed radars, and command and control systems. One author went so far as to suggest that the proliferation of long-range mobile missiles by potential adversaries might even have achieved another revolution in military affairs.[12] The emergence of offensive and defensive electronic countermeasures plus cyber capabilities will augment the impact of kinetic weapons in modern warfare. Sensing and operating in this future battlespace will require a very different ISR enterprise.

Networks and long-haul datalinks are potentially vulnerable to jamming and intrusion; the US cannot assume continuous connectivity. As noted by the Air Force Research Laboratory (AFRL), "Complex electronic warfare environments that degrade command, control, communications, and computers will disrupt timely collection and dissemination of ISR information."[13] Moreover, these effects extend to both airborne and space-based systems.

In addition, future contested environments will feature increasingly compressed decision cycles, affecting both combat aircraft and their supporting ISR assets.[14] Continuing time compression of decision cycles is already exceeding human decision capacity in cyberspace, and could eventually overwhelm human capacity in a physical battlespace. This phenomenon is a dominant feature of missile defense activities today and a similar shortening of decision cycles in other aspects of air warfare can be expected as well.

The airborne platforms in operational use today are, in the main, not survivable in highly contested environments. The RC-135, U-2, and RQ-4 were never intended to penetrate defended airspace and must operate at standoff ranges. The same holds true for battle management systems such as the E-3 Airborne Warning and Control System (AWACS) and E-8 Joint Surveillance Target Attack Radar System (JSTARS). Development of longer range sensors may permit collection from greater standoff distances for a time, but in the future contested battlespace long-range air defense missiles may well push current standoff systems beyond their effective range, at least for imaging sensors.[15, 16]

Current penetrating systems may likewise be less survivable in highly contested environments. A recent study by NATO's Joint Airpower Competence Center highlighted the vulnerabilities of RPAs in contested environments with respect to both kinetic and non-kinetic threats. The study indicated that radar cross-sections of −35dBm to −45dBm (i.e., reflecting only 0.01 percent to 0.001 percent of incoming radar energy) would be required to penetrate modern integrated air defense systems without detection, noting that only fifth generation combat aircraft currently exhibited these characteristics. Moreover, current datalinks were assessed as being vulnerable to electronic threats in this environment.[17]

Sensing the future battlespace will in essence depend on two types of information: information that can be collected from outside the battlespace and information that must be collected inside the battlespace.

Considerations for Developing a Future ISR Architecture

Developing an ISR architecture capable of delivering information superiority and supporting decision advantage in the hostile environments of future wars requires a fundamental rethinking of how the United States military senses and shapes battlefields and conflict zones. For ease of discussion, the key considerations can be grouped into the categories of sensing, networking, and understanding.

Sensing the Battlespace

Sensing the future battlespace will in essence depend on two types of information: information that can be collected from outside the battlespace and information that must be collected inside the battlespace. Standoff airborne platforms with long-range sensors as well as space-based systems can collect from outside the battlespace. Although long-range air defense missiles may force current airborne imaging platforms out of standoff range, passive radio frequency (RF) systems may remain effective in most scenarios over longer ranges. In the longer term, new technologies may be developed to address the shortfall in long-range standoff imaging. For example, one long-range sensing technology in development makes use of synthetic aperture laser radar, which would be able to identify targets through "…geometric imaging at ranges and resolutions exceeding the geometric limits of conventional apertures."[18]

Given the anticipated reduced survivability of currently operating aircraft, penetration of a highly contested conflict space would clearly require platforms that are low observable, utilize low probability of intercept/low probability of detection communications, and rely mainly on passive sensors. Passive RF sensors with a wide field of view would be suitable for target detection and location.[19] Passive electro-optical/infrared (EO/IR) sensors would have utility as well, but would require higher bandwidth for data transmission. Beyond purpose-built ISR platforms, the designs for fifth generation jet combat aircraft and advanced bombers include a more ubiquitous capacity for passive RF collection, giving these platforms the capacity to penetrate highly contested environments while functioning as nodes in a highly evolved resilient network.[20] Hence, many of the sensors and networks in the ISR enterprise would not necessarily be dedicated ISR resources.

A trend toward employment of larger numbers of smaller systems and aircraft offers great promise for improved responsiveness and reduced vulnerability. One emerging capability is the proliferation of constellations of small imaging satellites ("smallsats") with acceptable resolution and high revisit rates. In the Air Force's evolving concept of "sensing as a service," commercial smallsat constellations with EO, IR, multispectral imaging, hyperspectral imaging, and radar capabilities are now on orbit, featuring periodicity of one to 10 minutes and resolution potentially down to half a meter. This capability would offer utility in detection of both mobile and camouflaged targets, while the ubiquitous nature of the smallsat constellations would potentially enable a higher degree of survivability than smaller numbers of large satellites.[21] At the same time, the new Air Force remote piloted aircraft (RPA) flight plan addresses various concepts for greater numbers of small, low-cost, expendable RPA types for improved performance and survivability in contested environments.[22]

The cyber domain represents an increasingly lucrative source of data that can be accessed from outside a physical battlespace, and presents a rich source of intelligence for the Air Force ISR enterprise.[23] The ubiquitous nature of open source data and the web itself allows collectors to go beyond penetration of networks to gather intelligence. For example, Dutch investigators accessing social media and cell phone records were able to establish a track and chronology for the Russian SA-11 transporter-erector-launcher that shot down a Malaysian airliner over Ukraine in 2014 by locating multiple images collected by cell phones and posted to social media at various times and locations.[24] For the Dutch investigators, this involved a tedious, time-consuming, labor-intensive search. However, when such tasks are addressed as big data problems, advanced algorithms could enable exploitation of ubiquitous social media (to include metadata) to add context, augment ISR data, and identify times and locations of key events and actors. Moreover, given suitable advances in big data analytics, data from unclassified networks could be used to cue ISR sensors and drive collection plans, all within operationally relevant times.[25] The recent establishment of an algorithmic warfare team within the Department of Defense (DOD) indicates that such capabilities are coming into operational use. One early application appears to be automating the task of identifying mobile missiles found in imagery coverage of large areas.[26] This would suggest that smallsats with sub-meter resolution and high revisit rates could be combined with algorithmic search capabilities to constitute a potentially powerful capability to manage the high volume of data in a future conflict zone.

The cyber domain represents an increasingly lucrative source of data that can be accessed from outside a physical battlespace, and presents a rich source of intelligence for the Air Force ISR enterprise.

Resilient Networks and the Role of Autonomy

As noted earlier, in recent conflicts the Air Force has enjoyed air, space, and information superiority. Tactical communications in the battlespace have been relatively free from jamming and interference. Long-haul datalinks have securely moved massive amounts of ISR data from aircraft and platforms operating in forward areas to DCGS ground stations well outside the area of conflict. Command and control systems have been able to operate with little interference from the enemy. These advantages are less likely to prevail in the future contested battlespace, and the operational and technical architectures of future networks must address anticipated conditions.[27]

To be sure, thought leaders in air warfare are already seeking and developing new technologies and operational art to achieve success in the contested battlespace. Recognizing the nonlinear nature of future conflicts has led to discussions of achieving "local and temporal domain superiority" and shifting from the traditional kill chain to a more nonlinear "kill web."[28] The concept of "fusion warfare" focuses on employment of multi-domain capabilities to set the conditions for success at the times and places needed, for example.[29]

Whereas the current ISR enterprise rests on an underlying assumption of continuous global connectivity, a better assumption for the future would acknowledge the probability of discontinuous, interrupted long-haul communications. In such an environment, the enterprise must assume the attributes of a complex adaptive system, with significant implications for operational and technological autonomy. In a complex adaptive system, "[r]ather than being centrally controlled, control over the coherent structure is distributed as an emergent property of the interacting agents."[30] Key properties of complex adaptive systems include nonlinearity and unpredictability. In such a disaggregated system, combat aircraft and ISR aircraft that can communicate with each other would self-organize within the elements of the network that remain available in that time and space in order to prosecute the attack. By using linked data, each actor within the self-organized group would maintain awareness of information sufficiency and information gaps resulting from network access or denial. Algorithms hosted on each platform and node within the self-organized grouping could present risk-based courses of action depending on threat levels, operational priorities, and rules of engagement. Such an organizing principle would leverage and be consistent with previously articulated concepts of the "Combat Cloud."[31]

Improving Understanding by Rethinking the Information Paradigm

Today, the dominant information paradigm in the ISR enterprise consists of a linear path from sensor to analyst to end user, with much of the human touch labor applied early in the process. For example, an EO image acquired by an airborne platform is transmitted via datalinks to a ground station, at which point a human analyst begins to exploit the image; exploitation may range from adding internet chat or voiceover in the case of FMV to more extensive imagery analysis, precise mensuration, detailed reporting, and intelligence production. As the exploited image product moves up the chain, all-source analysts begin to add value with intelligence obtained from other sources to begin to develop finished intelligence. Such a manpower-intensive process is sustainable in low-intensity counterinsurgency warfare and remains valid for non-time-dominant requirements, but may not necessarily scale to meet the needs of high-intensity conflict.

To operate at machine speed, and thus match the operations tempo of future conflicts, the ISR enterprise must flip the paradigm. Rather than have human operators perform manual exploitation of intelligence data at the start of the process, a better approach would use machines at the front end and involve humans later in the process.

To operate at machine speed, and thus match the operations tempo of future conflicts, the ISR enterprise must flip the paradigm. Rather than have human operators perform manual exploitation of intelligence data at the start of the process, a better approach would use machines at the front end and involve humans later in the process. Onboard processing and data correlation would support both disaggregated self-organizing elements within the battlespace and analytic elements located outside the physical battlespace. Much of the information collected in the battlespace could be sent to other sensor and shooter platforms without having to travel to a remote ground station and back. Of course, the data could be shared both with other platforms in battle and with remote ground stations, but the attribute to note here is that information would have different value as it travels from the point of collection to multiple end-points, with multiple off-ramps and on-ramps for information within the network.

In such an approach, a human analyst could operate at a workstation that presents an integrated display consisting solely of all automatable data, which might lead the analyst to make an informed decision to apply imaging sensors that in turn would require more touch labor. In essence, this could move imagery sensors from a discovery role to a role more closely associated with confirmation and targeting. That said, as noted earlier, in certain circumstances imagery platforms may be unable to penetrate the battlespace; primary reliance could then shift to standoff electronic sensors and other non-imaging sensors. In functional terms, this potentially means a shift from direct observation of targets of interest to indirect observation based on an aggregation of inferential data to identify and locate objects of interest in a given area of conflict.

Detecting, identifying, and engaging targets in an environment in which visual and imaging cues are no longer dominant would require sophisticated signature management that addresses signatures in all detectable phenomenologies and incorporates them into systems that can rapidly identify targets based on these signatures.[32] To the extent that imaging sensors cannot be employed for target identification, the DOD may have to revise rules of engagement to permit risk-based kinetic targeting that relies solely on non-imaging signatures. In essence, a set of algorithms would establish the location and classification of the object with some stated level of confidence; the level of confidence required for targeting could vary with the potential threat and urgency of required action.

Conceptually, we often think of "intelligence, surveillance, and reconnaissance" in order to place primacy on the goal of producing intelligence. But functionally we should think in terms of surveillance, reconnaissance, and intelligence, in that order. In a future war, broad-area continuous surveillance would ingest massive amounts of data that would be characterized by machines and would inform machine-aided decisions to focus reconnaissance assets on specific targets of interest found in the sea of data. Downstream, humans aided by machines would produce intelligence to support operational planning and decision making. The bulk of data interaction would occur far upstream as data is exchanged platform-to-platform within the network, adapting continuously as various nodes gain or lose connectivity in dense jamming environments. This approach could evolve to the emergence of "…machine-on-machine decision-making…" simply because humans will no longer be able to function with the requisite decision speed.[33] Humans will set the rules and conditions, but the demands of operating at machine speed will necessarily lead to ever-greater reliance on machines rather than human operators.

While incremental change typically reinforces existing equities, radical discontinuous change often makes existing competencies irrelevant and almost always requires the development of new competencies. The advent of commercial digital cameras, which led to the rapid demise of film cameras, offers a classic commercial example.

Organizational Implications

In an ideal world, we would design and build the a system and then retire the old system, but we do not live in an ideal world. Moreover, the current ISR enterprise will likely have to continue to prosecute counterinsurgency and low-intensity counterterror missions for some time to come. The capabilities currently fielded have performed well in that role and can be expected to keep on doing so. However, developing new capabilities for the future fight in contested environments requires significant changes in technologies and organizational models.

Technological change can be characterized as one of two types. Incremental technological change is based on exploitation and development of existing technologies. This may require incremental modifications of organizational structure and procedures, but these are easily accommodated within existing organizations. Radical, discontinuous technological change, however, represents a different paradigm and historical organizational models have had difficulty in accommodating such change. In fact, most organizations actively resist radical discontinuous change because it disrupts established organizational equities. While incremental change typically reinforces existing equities, radical discontinuous change often makes existing competencies irrelevant and almost always requires the development of new competencies.[34] The advent of commercial digital cameras, which led to the rapid demise of film cameras, offers a classic commercial example. A military example from early in the 20th century reinforces this point. Some cavalry officers held the view that motorized transport represented a better way to move cavalry to the field; it did not occur to them that motorized vehicles would completely replace horse cavalry.

One could argue that the transition beginning in the late 1990s from in-theater ISR processing and exploitation to distributed ISR represented such a technologically disruptive event. Slow organizational acceptance by the institutional Air Force at the time to some extent hampered the instantiation of distributed ISR capabilities. As noted, the capabilities of AF DCGS were not fully realized until the system was reorganized to become a globally distributed system rather than a collection of regionally allocated nodes.[35]

The transition from the current linear ISR enterprise to a future complex adaptive system potentially represents another case of radical, discontinuous change. While the traditional approach to instantiating new systems and upgrades to existing systems relies on a series of new technology instantiations across the enterprise, such an approach could be counterproductive in this instance due to the radical, discontinuous nature of the new technology.

A better approach would be to use an ambidextrous organizational model: that is, an organization structured to concurrently execute existing business processes, while at the same time continuing to modernize them to the extent that incremental innovation permits. When business units are no longer competitive in an ambidextrous organization, they are simply retired. When radically new technologies emerge, the organization does not insert them into existing structures, but instead builds business units around the new technologies.[36] While technology-driven industries have successfully used ambidextrous organizational models, the model is not common in military or government settings.

The Air Force could apply the ambidextrous approach to introduce discontinuous radical innovation into the next iteration of the service's ISR enterprise. The current enterprise, well attuned to the needs of counterinsurgency and other forms of low-intensity conflict, could continue to prosecute those missions unimpeded, and would continue to benefit from incremental modernization. However, the new ISR enterprise could be developed in CONUS; perfected through multiple demonstrations, exercises (such as Red Flag events); and then made operational in an overseas theater facing a highly contested threat environment. From there, the advanced capability could incorporate lessons learned and then be propagated across the other commands.

Conclusion

Change is always a difficult undertaking, particularly in large organizations that have come to depend on well-developed competencies that have proven effective in addressing current challenges. However, much of the ISR capability developed to fight the United States' wars since 2001 does not scale well to meet the challenges posed by multi-domain operations in contested environments. The approach to the future combat environment must be organized in a way that sustains counterinsurgency operations while concurrently providing the innovation space to develop radically new capabilities to address emerging threats. Such an approach will, no doubt, present programmatic challenges and may encounter institutional resistance. But speed and determination are essential if the Air Force ISR enterprise is to evolve to meet the needs of 21st century multi-domain warfare. ✪

Endnotes

[1] John W. Lent, *480th Intelligence, Surveillance and Reconnaissance Wing Heritage Pamphlet* (Joint Base Langley-Eustis, VA: 480th ISR Wing, May 1, 2012), http://www.25af.af.mil/Portals/100/Documents/AFD-120712-038.pdf?ver=2016-02-11-120759-263 (All web links accessed in February, 2018).

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Lt Gen David A. Deptula and Col James R. Marrs, USAF "Global Distributed ISR Operations: The Changing Face of Warfare," *Joint Force Quarterly*, Issue 54, 3rd Quarter 2009, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA515567.

[7] Lt Gen David A. Deptula, USAF (Ret.) "Intelligence, Surveillance and Reconnaissance in the Information Age," *Leading Edge*, June 9, 2015, https://leadingedgeairpower.com/2015/06/09/intelligence-surveillance-and-reconnaissance-in-the-information-age/.

[8] Phillip Swartz, "Air Force Expanding Flights, Training and Bases for Drones, Top General Says," *Air Force Times*, March 7, 2016, https://www.airforcetimes.com/story/military/2016/03/07/rpa-flights-increase-70-day-training-and-bases-grow-too-welsh-says/81454190/.

[9] Air Force Public Affairs, "Air Force Distributed Command Ground System," October 13, 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104525/air-force-distributed-common-ground-system.aspx.

[10] Defense Science Board, *Summer Study on Autonomy* (Washington, DC: Department of Defense (OUSD AT&L, 2016).

[11] K. Dewayne Brown, et al., "Model-Based Design for Affordability of a Netted Intelligence, Surveillance, and Reconnaissance Concept," *Johns Hopkins APL Technical Digest*, Vol. 33, No. 1, 2015, http://www.jhuapl.edu/techdigest/TD/td3301/33_01-Brown.pdf.

[12] William F. Bell, "Have Adversary Missiles Become a Revolution in Military Affairs?," *Air & Space Journal,* Vol. 28, No. 5*,* 2014, 45–70, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-28_Issue-5/F-Bell.pdf.

[13] US Air Force Research Laboratory, *ISR Science & Technology Strategy* (Wright-Patterson AFB, OH: Air Force Research Laboratory, 2013), 6.

[14] Air Force Maj Gen VeraLinn Jamieson and Lt Col Maurizio Calabrese, "An ISR Perspective on Fusion Warfare," *The Mitchell Forum*, No. 1, October 2015, The Mitchell Institute for Aerospace Studies, http://media.wix.com/ugd/a2dd91_df2f54c534b34ac1bac674b7379aa788.pdf.

[15] Bryan Clark and Mark Gunzinger, *Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum* (Washington, DC: The Center for Strategic and Budgetary Assessments, 2015), https://www.files.ethz.ch/isn/195138/CSBA6147-EW_Report_Final.pdf.

[16] David Walker, deputy assistant secretary of the Air Force for science, technology, and engineering, "Presentation to the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities," February 24, 2016, http://defenseinnovationmarketplace.mil/resources/HHRG-114-AS26-Wstate-WalkerD-20160224.pdf.

[17] Andre Haider, "Remotely Piloted Aircraft Systems in Contested Environments: A Vulnerability Analysis," (Kalkar, Germany: The Joint Airpower Competence Centre, September 2014), http://www.japcc.org/wp-content/uploads/2015/03/JAPCC-RPAS-Operations-in-Contested-Environments.pdf.

[18] Walker.

[19] Clark and Gunzinger.

[20] Deptula.

[21] Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance Lt Gen Robert P. Otto, "Commercial Space-Based GEOINT: An ISR Horizons Future Vision" (Washington, DC: HQ USAF, May 2015), http://www.defenseinnovationmarketplace.mil/resources/Commercial_GEOINT_Vision.pdf.

[22] Mark Pomerleau, "Only Half Ready for A2/AD, Air Force Looks to Unmanned," *C4ISRNet*, July 28, 2016, http://www.c4isrnet.com/story/military-tech/uas/2016/07/28/air-force-a2ad-unmanned/87628044.

[23] AFRL.

[24] Somini Sengupta and Andrew Kramer, "Dutch Inquiry Links Russia to 298 Deaths in Explosion of Jetliner Over Ukraine,*" The New York Times*, September 29, 2016, https://www.nytimes.com/2016/09/29/world/asia/malaysia-air-flight-mh17-russia-ukraine-missile.html?_r+0.

[25] Paul B. Symon and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data," *Joint Force Quarterly*, Vol. 79, October 1, 2015,. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/621113/defense-intelligence-analysis-in-the-age-of-big-data/.

[26] Marcus Weisberger, "The Increasingly Automated Hunt for Mobile Missile Launchers," *Defense One*, April 28, 2016, http://www.defenseone.com/technology/2016/04/increasingly-automated-hunt-mobile-missile-launchers/127864/.

[27] Robert K. Ackerman, (2016). "Air Force Cyber Faces Familiar Challenges," *Signal Magazine*, March 1, 2016, http://www.afcea.org/content/?q=Article-air-force-cyber-faces-familiar-challenges.

[28] Megan Eckstein, "Interview: Rear Admiral Manazir on Weaving the Navy's New Kill Webs," *USNI News*, October 3, 2016, https://news.usni.org/2016/10/03/interview-with-rear-adm-mike-manazir-weaving-the-navys-kill-web.

[29] Jamieson and Calabrese.

[30] Keith L. Green, *Complex Adaptive Systems in Military Analysis*," IDA Document D-4313, (Alexandria, VA: Institute for Defense Analyses, May 2011).

[31] Deptula, "Evolving Technologies and Warfare in the 21st Century: Introducing the Combat Cloud,*" Mitchell Institute Policy Papers*, Vol. 4, September 2016, The Mitchell Institute for Aerospace Studies, http://docs.wixstatic.com/ugd/a2dd91_73faf7274e9c4e4ca605004dc6628a88.pdf.

[32] Jamieson and Calabrese.

[33] Doug Wise, "Future Warfare Will Not Allow Meaningful Human Control," *The Cipher Brief*, January 15, 2017, https://www.thecipherbrief.com/future-warfare-will-not-allow-meaningful-human-control.

[34] Michael L. Tushman and Charles A. O Reilly, III, "Ambidextrous Organizations: Managing Evolutionary and Revolutionary Change," *California Management Review*, Vol. 38, No. 4, Summer 1996, 8, http://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Organizational_Learning_and_Change/Tushman_&_OReilly_1996_Ambidextrous_Organizations.pdf.

[35] Deptula.

[36] Charles A. O'Reilly, III, and Michael L. Tushman, "Organizational Ambidexterity: Past, Present and Future," *Academy of Management Perspectives*, Vol. 27, No. 4: 324–338, November 1, 2013, http://www.hbs.edu/faculty/Publication%20Files/O%27Reilly%20and%20Tushman%20AMP%20Ms%20051413_c66b0c53-5fcd-46d5-aa16-943eab6aa4a1.pdf.

About The Mitchell Institute

The Mitchell Institute educates the general public about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Col Herbert C. Kemp, PhD, USAF (Ret.), served 28 years as an Air Force intelligence officer. His assignments included command, staff, and diplomatic tours, serving in Asia, the Middle East, Europe, and Latin America. In his final active duty assignment prior to retirement in 2001, Kemp served as deputy director for surveillance and reconnaissance, Headquarters Air Force, Pentagon, Washington, D.C. He is currently the president and CEO of OneALPHA Corporation in Herndon, VA.

An Affiliate of the Air Force Association | www.mitchellaerospacepower.org