Winter 2017
Volume 31, No. 4
AFRP 10-1

Senior Leader Perspective

Features

Departments

Improving Outcomes

Intelligence, Surveillance, and Reconnaissance Assessment

Brig Gen Timothy D. Haugh, USAF
Lt Col Douglas W. Leonard, USAF

The seemingly insatiable appetite of US DOD combatant commands (CCMD) for intelligence, surveillance, and reconnaissance (ISR) has driven the growth of a massive theater ISR enterprise. Despite this tremendous investment, one that has seen DOD expenditures rise six-fold from 2001 to 2012, the then Air Force deputy chief of staff (DCS) for intelligence, surveillance, and reconnaissance (DCS-ISR), Lt Gen Robert Otto, remarked that the department satisfies fewer CCMD intelligence needs today than at the height of the Iraq surge.[1] How did the DOD get in this remarkable position? The department, it appears, has been a victim of its success. The now retired chairman of the joint chiefs, Gen Martin Dempsey,

wrote: "The current joint force of ISR personnel, sensors, platforms, and networks is so vast, diverse, and distributed that managing their effective employment represents a large and growing challenge for the Department of Defense." He added, "Currently, ISR sensor and PED (Processing, Exploitation, and Dissemination) requirements and associated resources (systems, software, and people) are managed separately, resulting in mismatches in collection, processing, and analysis capacities."[2] Qualitative and quantitative ISR assessment linked closely to a coherent ISR strategy will permit commanders and planners to better align these disparate capabilities and avoid duplication or "mismatches." Commanders can then determine the effect of ISR on theater operational outcomes in the forms of opportunity cost and return on investment while ensuring the closure of intelligence gaps linked to those same objectives.

Current State of Platform Strategy

Since 2001, the DOD has invested significantly in ISR platforms and PED analysts. Unfortunately, the methodology underlying ISR strategy development did not keep pace. Concepts such as special operations forces (SOF) find, fix, finish, exploit, and analyze, mission type orders, and time-dominant fusion show great promise but have not yet approached the scale necessary to reform theater collection and analysis.[3] The rapid fusion of all available intelligence to meet the supported commander's intent ties these disparate approaches together, suggesting an important paradigm shift: success in operational ISR requires not platforms, but a wide variety of inputs analyzed and disseminated for war-fighter consumption as rapidly as possible. At present, each theater interacts independently with the national intelligence community (IC) and the DOD to garner collection for local warfighting needs. The management of this collection falls into a number of different stovepipes loosely organized around collection domain (air, space, sea, land, or cyber) or phenomenology (geospatial, signals, human, or signatures-based). Consequently, theater components compete to maximize gross collection without linking each point of collection to an appropriate lacuna in knowledge (intelligence gap) or supported commander desired effect (operational outcome). Recent conceptual advancements in the national IC, such as activity-based intelligence (ABI), object-based production (OBP), and structured observation management (SOM), when combined with recent advancements in automated algorithms to optimize collection from national assets, should force a corresponding change in the DOD approach. However, DOD doctrine, beyond the statements of some of the leading thinkers outside the formal publication process, does not yet consider these shifts. The complexity of ISR support to operational commanders demands such a reconsideration beginning with a more robust, qualitative ISR assessment operating at the tactical (intelligence production and sensor performance), operational (platform effectiveness and integration), and strategic (resource allocation and future purchasing and programming) levels.

Current State of Assessment

Within the DOD, organizations assess ISR for three primary reasons:

1. Did services acquire the right ISR capabilities in the right number, performing as designed?
2. Were the available theater airborne ISR capabilities apportioned correctly?
3. Was theater airborne ISR employed effectively?[4]

Traditionally, the under secretary of defense for intelligence (USD[I]) assesses service ISR acquisition strategy; USD(I), and JCS/J32 assess apportionment and allocation between CCMDs; and CCMDs and their air components assess the employment of ISR within theaters. The authors of this article propose a three-level pyramidal structure for ISR assessment that links individual intelligence products and sensor performance to operational outcomes and the closing of intelligence gaps as well as the operational (theater effectiveness) and strategic (resource decisions and platform allocation) efforts. Tactical entities such as US Air Force ISR wings and US Army military intelligence brigades must contribute to this process in ways never codified. Space constraints dictate a focus on those tactical and operational levels for the air component in this article, although the methodology will draw on the best practices put forth by USD(I) in strategic-level effectiveness as well.

A number of studies have attempted to improve ISR assessment, yet none have significantly advanced the doctrine for assessing ISR effectiveness at the operational or tactical levels. Operationally, the CCMD and the combined forces air component commander conduct airborne ISR assessment under the authority of the joint forces commander (JFC). Joint Publication (JP) 2-01 describes the process simply: "The joint force J-2, through the CCMD joint intelligence operations center (JIOC), helps the JFC by assessing adversary capabilities, vulnerabilities, and intentions, and monitoring the numerous aspects of the operational environment that can influence the outcome of operations. The J-2 also helps the JFC and staff decide what aspects of the operational environment to measure and how to measure them to determine progress toward accomplishing a task, creating an effect, or achieving an objective."[5] CCMDs, including coalition or joint task forces, are responsible for creating priority intelligence requirements and collection requirements, while the CFACC's air operations center tasks and directs airborne ISR platforms, sensors, PED, and fusion elements to collect, process, and disseminate intelligence to satisfy CCMD requirements.[6] To date, much of the theater ISR assessment has focused on measures of performance (MoP), which generally consist of quantitative measures focused solely on an individual domain (air) and phenomenology (most often geospatial). Some of the most common measures appear in the following list:

1. Number of ISR sorties planned and executed
2. Sensor availability
3. Number of images collected
4. Essential elements of information satisfied
5. Number of full-motion video hours

6. Number of intelligence products produced by intelligence discipline

These measures are easily quantifiable, but rarely contribute to answering the critical effectiveness questions: Did ISR advance the supported commander's desired operational outcomes (measured in opportunity cost and return on investment) or close intelligence gaps (measured in terms of knowledge advancement on an objective scale)? Why then do CCMDs and air components rely on MoP? RAND Corporation's previous study on ISR assessment states the issue clearly: "(T)he most often reported complaint from intelligence producers and consumers alike—too much emphasis on 'bean counting' of sorties flown, hours spent observing, and percentage of targets collected and too little on whether the ISR effort is actually supporting the commander's objectives. The reason for this emphasis, of course, is that the former is fairly easy to calculate and the latter quite difficult to determine, especially given the time pressures of an ongoing campaign."[7]

The intelligence cycle and associated tasking processes have earned significant description in joint and air component doctrine, but little exists on ISR assessment.[8] As documented in a RAND study in 2008 (and still true today), the USAF's AOC doctrine cites that the Intelligence, Surveillance, and Reconnaissance Division in the AOC should "monitor and evaluate the ISR strategy for effectiveness in meeting overall ISR requirements, JFC/JFACC (Joint Forces Air Component Command) PIR, and supporting JFC/JFACC strategy and plans,"[9] but provides no methodology to accomplish those tasks. JP 2-01 mandates that "all intelligence personnel and consumers" generate "timely feedback to the joint force J-2 staff regarding both successes and problems with the functioning of the intelligence process."[10] JP 2-01.3 provides a basic framework for operational assessment via MoP and measures of effectiveness (MoE) but stops short of any specific approach for ISR.[11] As noted in the RAND study, the rapid pace of operations coupled with the enormous difficulty of assessing product value at the operational level for such a wide-ranging and complex DOD ISR enterprise has caused a drift away from doctrinal requirements.

The greatest portion of the DOD's massive growth in ISR platforms has been through the USAF. The Air Force has committed to ISR as one of its five core missions with the Air Force Distributed Common Ground System (AF DCGS) serving as the primary exploitation weapon system for those missions and a useful representative of the explosive growth of USAF ISR generally. The AF DCGS support to airborne ISR missions increased by more than 1,900 percent from 2001 to 2015 as the Air Force flew 80 percent of all operational ISR hours and provided exploitation for 58 percent of all DOD-affiliated ISR in the second quarter of fiscal year 2016.[12] Such remarkable, almost unconstrained growth, when combined with an industrial age collection management process, has created systemic inefficiencies that demand immediate attention. Recent USD(I) studies may provide a useful methodological baseline but the air component, assisted by the CCMDs and the JCS/J32, should take a prominent role as the owner of a preponderance of theater assets and as the collection operations manager in several ongoing conflicts. Traditionally, USAF tactical advances emerge directly from the operator level in the form of tactics bulletins. Unfortunately, ISR assessment has not been a popular subject for edgy thinking; only one tactics bulletin since 2001 referenced holistic ISR assessment.[13] The

enormity of the problem, perhaps, and its linkage back to national-level processes has made it seem unapproachable. A strong framework should assist in identifying areas for more pronounced and specific tactical advancement.

Assessment Framework: Decision Advantage and the Three Rights

In concert with the growth of ISR platforms and sensors, the USAF has moved to revolutionize intelligence analysis. The Air Force DCS-ISR called for such rapid change in *Air Force ISR 2023: Delivering Decision Advantage*:

> The fundamental job of AF ISR Airmen is to analyze, inform, and provide commanders at every level with the knowledge they need to prevent surprise, make decisions, command forces, and employ weapons. Maintaining decision advantage empowers leaders to protect friendly forces and hold targets at risk across the depth and breadth of the battlespace—on the ground, at sea, in the air, in space, and in cyberspace. It also enables commanders to apply deliberate, discriminate, and deadly kinetic and non-kinetic combat power. To deliver decision advantage, we will seamlessly present, integrate, command and control (C2), and operate ISR forces to provide Airmen, joint force commanders, and national decision makers with utmost confidence in the choices they make.[14]

Lieutenant General Otto's vision extends beyond a simple satisfaction of collection requirements to a focus on producing intelligence products driving supported commander's decisions and actions. Subsequently, then Maj Gen Jack Shanahan, at the time the commander of Twenty-Fifth Air Force, centered his ISR-focused organization on the *Three Rights*: "Right Intelligence, Right Person, Right Time: Delivering the right ISR to the right person at the right time. . . our job is to turn data into information, information into knowledge and knowledge into actionable intelligence that results in better decisions."[15] These two senior leader vectors overlay with USD(I)'s ISR Task Force-recommended framework for ISR assessment: outcomes (decision advantage) and closing intelligence gaps (Three Rights) provide a foundation for advancing air component ISR assessment tradecraft by emphasizing the result of the intelligence cycle, the intelligence product.

Assessment must begin with the tactical product (See figure). Operational-level assessors, in the case of the air component residing largely in the AOC, simply do not have the manpower, time, or expertise to adequately link specific products to tactical or operational ISR objectives, strategic-level PIRs, or similar commander questions. The tactical production element, therefore, must take on this element of assessment at the wing or brigade level. This assessment must begin as qualitative, examining the specific information passed in a product for its value to operational effects in the battlespace, measured in terms of knowledge advancement on an objective scale. This assessment begins at the producer level via automated fields in production control software and in combined intelligence and operational briefs and debriefings. In other words, the entire process depends on a structured data environment whereby intelligence production links to the information state of an intelligence object. Each intelligence product, then, contributes to the maintenance (in the case of indications and warning) or increase (in the case of target development) in knowledge regarding that object. The wing or brigade can then take all entries in the aggregate and assign qualitative values, developed in concert with the operations research and lessons learned community, to each product.

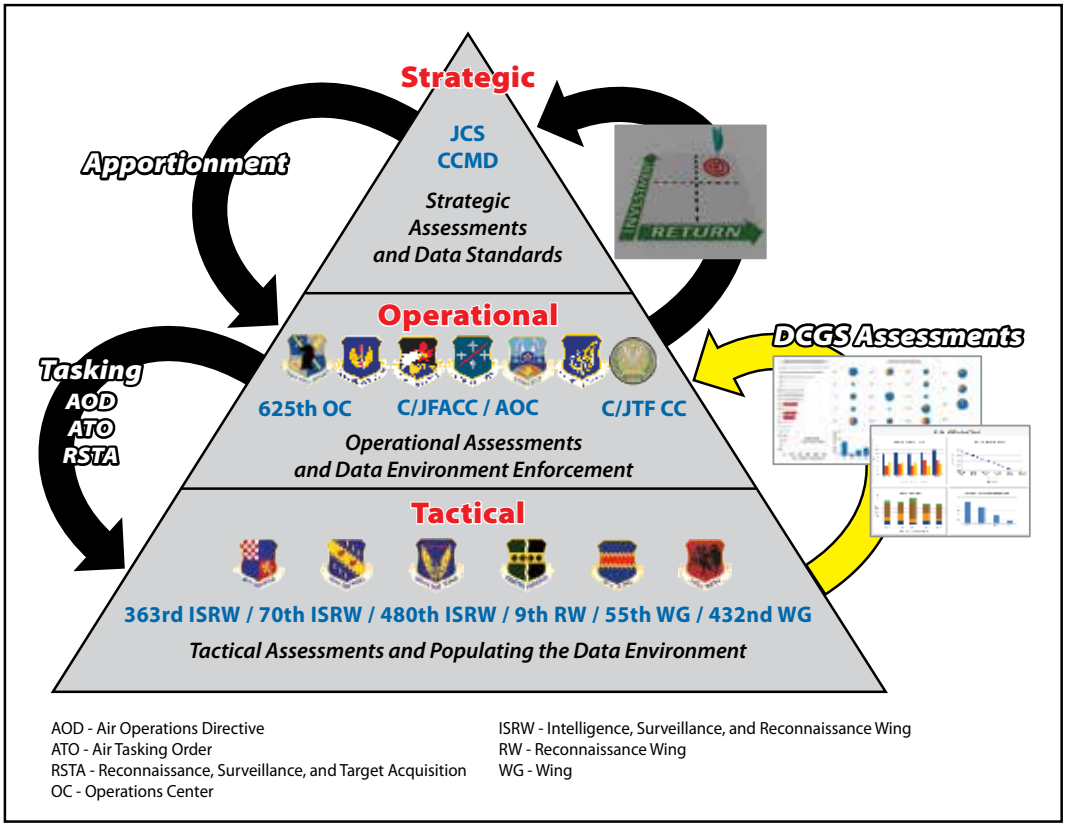


Figure. ISR assessment levels

The process will require heavy involvement from forward ISR elements such as ISR liaison officers, and ISR tactical controllers, to assist in the development of appropriately narrow and focused ISR objectives at the operational and tactical levels. Tactical-level product assessment will then feed the larger operational-level assessment of sortie and sensor effectiveness, inform resourcing decisions on ISR platforms and allocation, and feed directly back into the daily process of ISR command and control. The accumulation of tactical level inputs, when compared at the operational level, will serve as comparative validation of the effectiveness of each input. The levels of assessment, then, remain locked together and focused at the operational level.

CCMDs must share responsibility with air components in linking ISR strategy and resulting intelligence production to outcomes and closing intelligence gaps. Effective linkage requires a clear connection between the supported commander's intent and the ISR strategy. While this might appear obvious, traditional industrial age ISR collection management practices, technology, and data structures mandate a focus on individual intelligence collection disciplines such as signals intelligence (SIGINT) or geospatial intelligence (GEOINT) vice an emphasis on the resulting

fused intelligence product.[16] An assessment process based, at least in part on production, will require some changes to guidance, particularly on the sourcing of intelligence reporting. The national IC has made significant strides in tracking the intelligence used to inform senior leader decisions. The clearest example is the presidential daily briefing (PDB). The PDB is meticulously sourced, generating a relatively simple evaluation over time on collection sources informing presidential decisions, the ultimate in strategic outcomes and decision advantage. This approach is not limited just to the PDB. The IC has established standards that require sourcing for all finished intelligence production. CCMDs, JTFs, and components should mimic this practice to identify what intelligence products and collection sources influence senior leader decision making. The DOD, via the Office of the Secretary of Defense (OSD) and joint staff, should mandate sourcing for CCMD and JTF daily briefings and finished intelligence products. This sourcing should link to the originating collection source. Clearly, this data collection comes at a cost, but ultimately the CCMD's benefit from validating effective ISR strategy and employment through demonstrable, intelligence-informed CCMD and JTF senior leader decisions. Sourcing provides easily quantified measurement of decision advantage at the operational level and assists in the tactical-level assessment of products as described above.

The expert assessors in the ISR Task Force have identified other indirect measures that can inform operational-level ISR assessment.[17] A robust operational-level process must be introspective and begin with operational effects. Ultimately, the process must provide the supported commander with the answers to the questions he posed related to the battlespace, typically expressed as PIRs. The ISR assessment process must operate at the tactical level, sometimes in SIGINT, GEOINT, or other subdisciplinary stovepipes, but accumulate at the operational level for translation back into command-level language. In short, each intelligence report and ISR sortie must circle back to the operational effects it generates.

If the supported commander is a ground element, traditional operations orders and fragmentary orders capture the appropriate information in either the situation or enemy disposition. However, an appropriate assessment process requires some connective tissue from PIRs, typically general and difficult to use as an objective measure, and the conduct of ISR and the accompanying analysis. ISR objectives, as mentioned above, can provide these linkages from the commander's intent to operational efforts and ultimately to tactical objectives and the actual collection. These objectives will emerge from a close collaboration between components, the appropriate theater-level command and control entity (in this case, the AOC), and the intelligence production element with the greatest analytical understanding of the theater and problems in question. Assessment must remain firmly anchored in an understanding of the changes to intelligence objects prioritized by their proximity to these operational and tactical objectives.

Full accomplishment of such a linkage between production and theater-level objectives for the air component must occur within the AOC. Consequently, the AOC must prioritize such assessment for those practices to take root and generate useful conclusions. At present, AOCs have an operational assessment team (OAT) that could fill this role. An OAT is comprised of operational research analysts dedicated to the science and art of assessing operational activities. Traditionally, these experts

have focused on assessing the effectiveness of close air support planning and execution and munitions effectiveness. Instrumenting the ISR processes within the AOC and collecting the right data can also enable these experts to assist in ISR assessment.[18] Admittedly, changing this emphasis will not be easy, but recent successes highlight the potential opportunity.

During a recent crisis in the US Central Command (CENTCOM) area of responsibility (AOR), the deputy coalition forces air component commander (D-CFACC) requested intelligence products from the US Air Force ISR enterprise at various classification levels. Producing intelligence at multiple classification levels is routine for the expert enlisted intelligence analysts assigned to AF DCGS, but the timeline and intent behind the D-CFACC request made this request stand out. He needed the intelligence to negotiate basing rights with a coalition partner. Within hours of the first sortie in the new area of operations, AF DCGS analysts provided GEOINT products at five different classification levels to contribute to these negotiations. The successful outcome of these senior leader negotiations was at least partially enabled by effective ISR sorties and intelligence products tailored to the senior leader intent. This was a successful outcome, but the standard assessment process had no means to capture this success. Instead, the CFACC's intelligence team developed a separate reporting mechanism to track the thousands of intelligence reports provided to coalition partners and reported these results to CENTCOM and OSD monthly, though that mechanism included only raw numbers without an effort to link those specific products back to supported outcomes or gaps. Modification of previously static processes can occur, particularly when the supported commander is producing successful outcomes. SOF has been moving toward the tracking of successful outcomes for more than a decade, identifying the right data to report, capture, and analyze to validate ISR apportionment. It is time for CCMDs, JTFs, and AOCs to follow suit by capturing and reporting indirect measures to inform ISR assessment.

Closing Intelligence Gaps (Right Intelligence, Right Place, Right Time)

Employing ISR effectively to close the highest priority intelligence gaps is a shared responsibility between CCMDs, the national IC, CFACCs, ISR platforms, PED, and intelligence fusion analysts. Each organization has a critical role to play. The CCMD plays the most important role by identifying the highest priority intelligence problem in the form of PIRs. Cogent PIRs are the first link in crafting an effective ISR strategy. Developing the strategy to effectively employ ISR is a team sport comprised of CCMD ISR planners, CCMD intelligence analysts, AOC planners, ISR platform operators, AF DCGS planners, IC representatives, and intelligence fusion analysts. ISR strategists and collection planners should evaluate all potential sources of intelligence based on timeliness, phenomenology, the availability of analytical assets, and relevant platform availability when aligning collection. Ideally, analytical elements such as AF DCGS should not "chase" airborne ISR collection but instead should analyze and exploit any and all sources available that will successfully answer the questions posed by the supported commander, questions ultimately posed as operational and tactical objectives more easily translated into real

analytical priorities for a production element. In short, collection is not about information from the air domain; it is about information for the air domain. The management of these air assets is a necessary and important subcomponent of the process that also falls under the responsibility of the AOC with the support of tactical production elements such as AF DCGS. When evaluating the ability of airborne ISR to satisfy intelligence requirements, ISR assessors consider the effectiveness of the intelligence product to satisfy a CCMD PIR as decomposed via a regularized taxonomy to operational and tactical ISR objectives. While this seems intuitive, ISR is rarely evaluated against the ability to produce intelligence products that close intelligence gaps. General Shanahan's "go-do" provides a starting point: right intelligence, right place, and right time.

During a review of combatant command and AOC assessment approaches, each CCMD focused on quantitative reporting. The focus on quantity devalues the CCMD's PIR, ISR strategy, and ISR objectives and returns ISR assessment to the trap identified by RAND, "too much emphasis on 'bean counting.' "[19] Now is the time to break this cycle. A number of best practices have emerged that will advance the tradecraft necessary to adequately assess ISR production against the desired metric of the three rights:

1. US European Command (EUCOM) tasking to AF DCGS to provide a tailored postmission summary of each sortie's ability to satisfy priority ISR problem sets. Many of these products have already elevated to the commander of EUCOM, the secretary of defense, and one to the president of the United States.
2. Unified approach in the US Pacific Command Theater between Pacific Air Forces/ISR, 613th AOC, and AF DCGS to craft dynamic lines of effort tailored to JFACC intelligence needs and theater PIRs and specifically called out and linked in all theater-generated intelligence products, a powerful first step toward holistic ISR assessment.
3. A partnership between US Air Forces Central Command (AFCENT), the 497th ISR Group, 693th ISRG, and 363rd ISRG to assess effectiveness of ISR sorties in the CENTCOM AOR to produce fused intelligence products immediately ingestible into AFCENT and supported JTF targeting processes, particularly during the most recent campaign against the Islamic State of Iraq and Syria.
4. The 693rd ISRG national tactical integration (NTI) analyst experimentation with big data methods to assess the effectiveness of SIGINT sensors. NTI analysts used national IC-developed modeling tools intended for intelligence analysis to transform more than 10,000 lines of sortie data into a product capable of linking collection to prioritized PIR.

ISR assessment tradecraft has stagnated for years, but the technology and interest are now present to generate a renaissance. Senior leadership must embrace and institutionalize these emerging practices immediately to optimize ISR employment in all theaters.

Advancing ISR Assessment Tradecraft: Air Components Postured to Lead

Many of the preconditions necessary for success in ISR assessment are now present. The arrival of Air Combat Command (ACC) as the owning ISR major command presents an important organizational backbone even as senior leadership at both the operational and strategic levels recognize the inadequacy of contemporary measurements. ACC and theater air components are uniquely postured to develop this tradecraft in support of the CCMDs; while decision advantage and the Three Rights provide the starting point. Several straightforward steps should enable huge leaps in the tradecraft:

1. Generate a US Air Force Warfare Center (USAFWC) process to collect, store, and advocate advanced ISR assessment tradecraft, to include invitations to SOF ISR professionals, with an eye toward influencing changes in both Air Force and joint doctrine.
2. ACC would lead the writing of an updated ISR assessment concept of operations as the basis for codification of detailed ISR assessment practices in a future 3-3 volume assembled by the USAFWC.
3. ACC would partner with component major commands (MAJCOM), nonappropriated funds, combat support agencies, and the Office of the Director of National Intelligence to codify requirements for the appropriate sourcing of intelligence products, as well as the tagging and tracking of intelligence information. These efforts should link closely with the IC Information Technology Enterprise projects to deliver interoperable data repositories and collection capabilities while enabling advanced ABI tradecraft such as OBP and SOM.
4. ACC would partner with component MAJCOMs and NAFs on near-term material solutions to ensure data interoperability between intelligence production databases and AOC baseline systems for operational and ISR assessment.
5. AF-A2 (ISR) and AF-A3 (operations, plans, and requirements), along with ACC, advocate to OSD and the Joint Staff for a policy to link CCMD ISR platform apportionment and allocation, at least in part, to the CCMD's ability to effectively assess ISR based on operational outcomes (decision advantage) and ability to satisfy ISR objectives derived from PIRs (Three Rights).

Conclusion

As the United States moves to deal with instability in the Middle East, Africa, and Central Asia, it also must confront a rising tide of near-peer military competitors. At the same time, ISR collection technology has proliferated sufficiently to remove the substantial advantage the United States has enjoyed for decades. The primary American advantage in the future will rest on the ability of US decision makers to understand and react to emerging situations more rapidly than leaders in opposing states and groups. The key to building that decision advantage, though, is the ability to dynamically employ ISR across all domains and collection phenomenologies for

the benefit of the war fighter and the strategic decision maker. The DOD has reached a saturation point of ISR information; the time has come to harness the full capability of collection resources through improved ISR assessment at all levels: tactical, operational, and strategic. This new approach will require the use of improved qualitative understanding of individual products, a deliberately linked operational assessment process that considers the full scope of response options to enable supported commander-driven operational outcomes, and the efficient closure of intelligence gaps through an integrated big data approach. The sources and platforms currently in use across the collection domains are sufficient in quantity; assessment will make them sufficient in quality. ✪

Notes

1. House, *Performance Audit of Department of Defense Intelligence, Surveillance, and Reconnaissance*, House Permanent Select Committee on Intelligence, April 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/isrperformanceaudit%20final.pdf; and Lt Gen Robert P. Otto (remarks, *Defense Connect Online*), 8 April 2015.

2. Gen Martin E. Dempsey, "[intelligence, surveillance, and reconnaissance] ISR Joint Force 2020 White Paper," (Washington, DC: Chairman of the Joint Chiefs of Staff [CJCS], June 2014), 3, 6, http://dtic.mil/doctrine/concepts/white_papers/cjcs_wp_isr.pdf.

3. Michael T. Flynn, Rich Juergens, and Thomas L. Cantrell, "Employing ISR SOF [special operations forces] Best Practices," *Joint Force Quarterly* 50, 3rd Quarter 2008, 56–61, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA516799; Capt Jaylan Michael Haley, "An Evolution in Intelligence Doctrine: The Intelligence, Surveillance, and Reconnaissance Mission Type Order," *Air & Space Power Journal* 26, no. 5 (September–October 2012), 33–48, http://www.au.af.mil/au/afri/aspj/article.asp?id=99; and Jason B. Brown and David Vernal, "Time Dominant Fusion in a Complex World," *Trajectory Magazine*, November 2014, http://trajectorymagazine.com/got-geoint/item/1840-time-dominant-fusion-in-a-complex-world.html.

4. Dean Milne and Ryan Yoho (intelligence, surveillance, and reconnaissance task force [ISRTF] contract support), and interview by the author, 28 March 2015.

5. Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, 5 January 2012, IV–15, http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf.

6. Joint Publication 2-0, *Joint Intelligence*, 22 October 2013, 2-6; Air Force Tactics, Techniques, and Procedures 3, no. 3, Air Operations Center (AOC), *Operational Employment: Air Operations Center*, 31 January 2014, 6-89–6-124, https://fas.org/irp/doddir/dod/jp2_0.pdf.

7. RAND Project Air Force, *Methodology for Improving the Planning, Execution, and Assessment of Intelligence, Surveillance, and Reconnaissance Operations*, 2008, 14.

8. See, for example, Joint Publication 2-0, chap. 4, Section E; Joint Publication 2-01, chap. 3; Air Force Tactics, Techniques, and Procedures (AFTTP) 3-3, AOC Sections 6.6 and 6.7; and Air Force Basic Doctrine (AFBD) Annex 2-0, *Global Integrated Intelligence, Surveillance, and Reconnaissance Operations*, 29 January 2015, 16–24.

9. RAND, *Methodology,* 12. See also AFBD Annex 3-0, *Operations and Planning*, 5 November 2012, 106–107; and AFTTP 3–3, AOC, 6–124.

10. Joint Publication 2-01, 3-65–3-66 (quotation on 3-66).

11. Joint Publication 2-01.3, *Intelligence Preparation of the Operational Environment*, 21 May 2014, 6-16–6-21.

12. Distributed Common Ground System (DCGS) mission increase numbers were calculated from Air Combat Command (ACC) and 480th Intelligence, Surveillance and Reconnaissance Wing (480 ISRW) archived mission data. Percentage of allocation was calculated from Joint Staff fiscal year 2016 Global Force Management Allocation Plan.

13. Capt Ryan Skaggs, *561st Joint Tactics Squadron Flash Bulletin* 11-02, "ISR Mission Type Order Planning and Execution," 10 January 2011. For a related and foundational discussion, see also Lt Col Jason Brown and Maj Max Pearson, "Theater Intelligence, Surveillance, and Reconnaissance Concept of Operations," *USAF Weapons Review* (Fall 2008): 18–25.

14. Lt Gen Robert P. Otto, *Air Force ISR 2023: Delivering Decision Advantage*, November 2013, 6.
15. Maj Gen John N.T. Shanahan, *25th AF Strategic Plan 2015*, February 2015, 1.
16. For further discussion on this and related points, see Col Jason Brown, "Strategy for Intelligence, Surveillance, and Reconnaissance" (master's thesis, Air War College, Air University, 14 February 2013). Data management, in particular, remains an important emphasis item that falls outside the scope of this paper. For an example see the Headquarters ACC/A2 "ISR Assessment Functional Concept" (currently in draft) and the office of undersecretary of defense for intelligence OUSD(I) "ISR Assessment and [Idea]: A Practical Perspective" (currently in draft) for a more detailed discussion of data management practices and concepts.
17. ISRTF Requirements and Analysis Division, "Improving ISR Effectiveness Assessments," January 2014. See also *Deputy Director, J-7, Future Joint Force Development, the Joint Staff*, "Iron Bullet 15-3 Global ISR Enterprise Management Seminar Quicklook Report," 3 December 2015.
18. USAF AOC doctrine expects that the operational assessment team will participate in all operational assessments, but, in practice, ISR assessments occur within the ISR Division. See *Air Force Basic Doctrine Annex* 2-0, 24; and AFTTP 3-3.AOC, 6-124.
19. RAND, *Methodology*, 14.

Brig Gen Timothy D. Haugh, USAF

Brigadier General Haugh (BA, Lehigh University; MS, Southern Methodist University; MS, Naval Postgraduate School; MS, Industrial College of the Armed Forces) serves as the director of intelligence, US Cyber Command. He has served in a variety of intelligence, cyber, staff, and command assignments. His staff assignments include the Office of the Secretary of Defense, Air Staff, and the Combined Air Operations Center. Brigadier General Haugh commanded the 480th Intelligence, Surveillance, and Reconnaissance Wing, Joint Base Langley–Eustis, Virginia; the 318th Information Operations Group, Joint Base Lackland–San Antonio, Texas; 315th Network Warfare Squadron, Fort Meade, Maryland; and Detachment 2, 544th Intelligence Group, Sabana Seca, Puerto Rico.

Lt Col Douglas W. Leonard, USAF

Lieutenant Colonel Leonard (BS, USAFA; MA, Florida State University; PhD, Duke University) serves as the commander of the 27th Intelligence Squadron, Joint Base Langley–Eustis, VA. He has served in a variety of intelligence assignments at the unit level and served on staffs at Air Combat Command and Headquarters Air Force. Lieutenant Colonel Leonard previously commanded Detachment 5, 544th Intelligence, Surveillance, and Reconnaissance Group, Chantilly, VA.
.

Lethal Autonomy

What It Tells Us about Modern Warfare

Maj Thomas B. Payne, USAF

By now, most military leaders have heard about the development of autonomy in weapon systems and are aware of the vocal opposition from outside the DOD.[1] Autonomy in weapon systems has been under development and controversial for many years.[2] Now, however, robotics and autonomous systems have been highlighted by the DOD as a centerpiece of the "third offset" strategy.[3] This strategy seeks to ensure continued asymmetric combat advantage for the United States, with a particular focus on the incorporation of future technologies not easily replicated by competitor states or nonstate entities.[4] The upcoming years are therefore a critical time in the research, development, and deployment of lethal autonomous weapon systems (LAWS) in the United States and throughout the world.[5]

The DOD's push, along with recent technological developments, have triggered a broad and public discussion of concerns with LAWS, including direct opposition to their development. These concerns are of three general types: (1) the belief that risks associated with such new weapons outweigh benefits, (2) concerns about whether lethal autonomy violates the international law of war, and (3) doubts regarding the moral propriety of machines apparently making "discretionary" decisions to take a human life.[6]

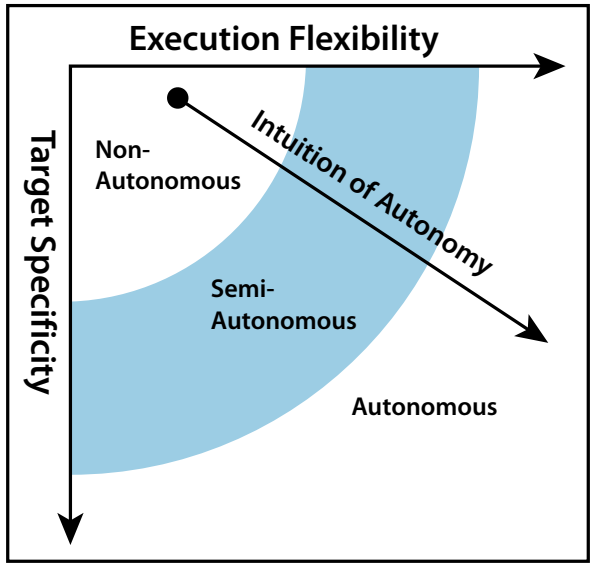


Figure. Continuum of Autonomy

Defining Autonomy

There are various ways to discuss *autonomy* in weapon systems. Outside of the technical literature, the term is less descriptive and more evocative—that is, terming a weapon system autonomous does less to describe how it operates than it does to invoke ideas and concerns about its decision making and predictability.[7] The definitions of the terms, and even the taxonomy of existing systems, are not always consistent among authors on the subject.[8] Although precise definitions are critical for design and engineering purposes, understanding the debate about autonomy requires an acknowledgement of these differing uses of the term, typically centered on ethically relevant subprocesses of the system as a whole; targeting, goal-seeking, and the initiation of lethality.

The perception of policy-relevant autonomy has two underlying elements. On the one hand, it references the target specificity given to the system in geographic, temporal, or descriptive characteristics. Thus, systems that are given a highly specific target designation by a person (that is, air-to-air missiles that attempt to identify

a specifically selected target by location, or the presence of jamming signals, or most defensive systems) are not considered autonomous.

On the other hand is execution flexibility, where systems that have tight constraints on available actions are considered nonautonomous. Examples include a land mine, trip-wire explosive, or defensive gun emplacement, as opposed to a robotic tank ordered simply to "guard a perimeter," which most would consider autonomous. Devices with limited targeting but broad execution flexibility, such as a robot programmed to hunt down a particular individual in a geographic region, seem to encounter the same risk/benefit analysis and ethical intuitions as the notional "fully autonomous system" or "robot soldier."

Therefore, broad targeting specificity and expansive execution flexibility both tend to result in the characterization of a system's behavior as autonomous. Both characteristics raise real or perceived concerns about the locus of decision making and predictability of the system.

Key Issues

There is a wide variety of topics related to the development and employment of lethal autonomous weapon systems. The numerous issues of this debate can be usefully divided into ones regarding (1) risks and potential benefits, (2) legal issues, and (3) moral/ethical concerns (see table). Positions vary in terms of nuance, but much of the primary discussion centers on whether a ban (international or unilateral to the United States) on the research, development, and deployment of LAWS is appropriate.

Potential Benefits

Military Capabilities

The potential value of LAWS in armed conflict is uncontroversial.[9] With nonlethal military systems, traditional automation provides an immediate force multiplier by taking repetitive or analytically arduous tasks and removing the need to hire, train, and support personnel to perform them. Autonomous action is even more valuable as complex systems, incorporating learning algorithms and contextual awareness, allow for the automation of much more numerous and difficult tasks requiring judgment and situational awareness, such as automated flight control.[10] Additionally, autonomous systems will likely be capable of reacting substantially faster than humans. The initial reaction advantage of autonomous systems could snowball through cycles of reaction, creating a potentially insurmountable advantage in warfare.[11]

Leverage Civilian Technology

The focus on LAWS is also potentially beneficial for the United States because it capitalizes on current advances in civilian autonomous technology. The United States is a global leader in this area, and one of the imperatives of military technology is to maximize areas where an asymmetric advantage is available that is difficult for opponents to replicate. Investment in these areas of research and development (R&D)

may drive the development of industrial capacity and commercial innovation in a virtuous cycle. Military and civilian developments in autonomous capability therefore have a positive symbiotic relationship.[12]

Table. Taxonomy of the debate

Category of Concern		*Specific Issue*	*Critical of LAWS*	*Supportive of LAWS*
Benefits and Risks	*Benefits*	Military capabilities	Risk related to error and adversary action may outweigh benefits	Provides significant, and perhaps decisive, military advantage
		Leverage civilian technology	Arms race with competitors not able to master technical side of militarization of civilian technology	Takes advantage of areas of US technology leadership; strengthens persistence of advantage
		Ethical improvements	Will not be capable of ethical decision making	May improve on precision weaponry in protecting civilians
	Risks	Likelihood of war/ Jus ad bellum	Lack of casualties will encourage leaders to engage in unlawful war	Generic objection that applies to development of any substantial military advantage
		Arms race	Triggers a wider arms race	Peer development and civilian technology will result in LAWS
		Asymmetric warfare	Increases likelihood of strikes on civilians	Excessively generic objection; seems to blame victims for illegal attacks
		Hacking/subversion	Allows for hacking/ subversion	Allows continued operations without communications
		Loss of command and control	Runaway escalation due to fast LAWS on both sides	LAWS likely restrictive rules of engagement; free-ranging persistent LAWS improbable
		Judgment errors	Decision making of the system is unpredictable	Reliability and predictability will reach human levels; no more required
Legal Issues	*Weapons Law*	Per se	Because inherently indiscriminate, per se illegal	High-intensity conflicts make even unreliable LAWS conditionally legal
		Distinction	Unable to distinguish civilians	No negative emotions, human-level decisions
		Proportionality	Cannot balance military advantage and collateral damage	Commander who sets into motion makes judgment, as current practice
	Accountability		No one held responsible for commission of war crimes	Excessive focus on criminal; same as other weapon malfunctions
Moral / Ethical Issues			Demeaning to humanity for LAWS to determine death	LAWS don't make decision; commander who sets in motion does

Source: Multiple sources.

Potential Improvements in Ethical Warfare

Both opponents and supporters of a ban on LAWS highlight the potential for autonomous technology to facilitate compliance with the law of armed conflict—at least in some areas. LAWS are not susceptible to emotional effects such as shock or anger that may result in abuses by human soldiers. The presence of LAWS in mixed teams with human soldiers, particularly if LAWS have independent capacity to judge ethical conduct, may also temper the willingness and ability of those soldiers to engage in inappropriate or unlawful conduct.[13]

The use of autonomous weapon systems under circumstances where all or almost all of the potential targets are lawful, or have already been vetted, may arguably also provide humanitarian benefits. For example, if the alternative is between using a bomb and a robot soldier, the LAWS might be legally and ethically desirable, even if the autonomous system's ability to distinguish noncombatants is unreliable. In this sense, autonomous decision making at the moment of lethal action may be an improvement on the precision of weapon systems, eliminating some of the error created by imperfect intelligence and distance in time between the initiator and target.[14]

Potential Risks

Likelihood of War/Moral Hazard

A common concern is that the existence of LAWS encourages inappropriate aggression. Although sometimes couched in terms of jus ad bellum, or the legal theory of just war, this concern does not actually question the propriety of war initiation.[15] Rather, the argument is that LAWS would create a moral hazard for national leadership. If you suppose that current or future leaders are willing and desire to engage in unlawful war-making but are inhibited by the likelihood that it will result in military casualties, either for moral reasons or because of spin-off effects of those casualties, then LAWS might minimize these casualties and thus result in unlawful aggression.[16] A counterargument, however, is that this objection is excessively generic. Any weapon system that minimizes casualties, or gives a substantial advantage to one side in armed conflict, would seem to trigger this same moral hazard.[17]

Uncontrolled Arms Race

LAWS may also trigger wider arms races. This argument takes two forms. First, because of the tremendous tactical advantage associated with the development of LAWS, peer and near-peer competitors will be forced to develop increasingly sophisticated autonomous capabilities for their own weapon systems. Second, asymmetric competitors, such as international terrorist organizations, who would otherwise lack organic R&D to develop such systems, will gain access to the technology once it becomes widely used in warfare. In addition to the inherent instability associated with arms race dynamics, competitors in both cases may have less incentive or less capacity to control the behavior of LAWS.[18] Therefore, even the most ethical

development of LAWS by the United States may result in the development and fielding of indiscriminate LAWS.[19]

A number of counterpoints have been presented to this risk. First, some argue an arms race is already in progress, with peer and near-peer competitors developing autonomous weapon systems, and US efforts are required simply to remain competitive. These nations will arguably refuse to adopt, or successfully evade enforcement of, any potential multilateral ban. Second, asymmetric competitors may be capable of leveraging technological development in the civilian sector, since some argue weaponization of some civilian technologies will be relatively easy.[20]

Asymmetric Warfare

The replacement of soldiers by LAWS also has the potential to increase attacks on civilian targets, particularly in the United States itself. Enemies of the United States, it is argued, will see no political or strategic benefit in attempting to fight if the United States is not suffering human casualties. These opponents are therefore incentivized to carry out attacks on civilian rather than military targets.[21]

Of course, as critics note, any generic technological advantage that makes US service members less susceptible to enemy attack appears to create the same risk. In the same vein, one DOD analyst notes that this argument essentially "blames the victim" by discouraging the protection of soldiers because of the enemy's presumed willingness to violate the laws of war by assaulting civilians. Finally, considering the history of nuclear strategy as well as terrorist targeting, both of which focus substantially on civilians, both near-peers and asymmetric opponents seem willing to place civilians in jeopardy if it serves strategic ends; therefore, the presence or absence of US casualties on the battlefield is arguably irrelevant.[22]

Hacking/Subversion

The reliance on autonomous systems increases the military's vulnerability to hacking or the subversion of software and hardware. The replication of software, as well as the complexity and interdependence involved with widespread use of autonomous weapon systems could significantly magnify harm if a security vulnerability or exploitable system malfunction were acquired by an adversary. Potential consequences could include mass fratricide, civilian targeting, or unintended escalation.[23]

One response to that argument, however, is that on-board autonomous capability may actually *counter* subversion or hacking of current and future remote systems. For example, an autonomous friend/foe system might refuse to fire on friendlies when receiving a spoofed set of instructions or an autonomous flight system might continue protective flight of a remotely piloted aircraft if the control link is disrupted. Of course, even weapon systems that do not include autonomous capabilities rely heavily on computer hardware and software. This automation does not seem markedly less susceptible to hacking and subversion, and the presence of autonomy may make a system more resilient than an equally computerized but less internally controlled nonautonomous weapon system.[24]

Loss of Command/Control

The literature also identifies a risk that the large-scale adoption of autonomous weapon systems may result in runaway escalation. The very interdependence, complexity, and flexibility of the system that allows it to perform complex mission sets may result in unpredictable and unintended lethality. In addition, the danger of uncontrolled escalation is significantly greater precisely because the speed with which LAWS are capable of decision making and action—one of the primary military advantages—creates a potential time delay between failure and corrective action. Finally, unlike idiosyncratic human decision making, software control systems may be replicated throughout the fleet of LAWS, and so the damage potential of a simultaneous failure by all similar LAWS in the inventory must be considered, not only the consequences of a single system failure. Some analysts of LAWS envision an armed conflict that begins without either party intending it because of an initial error snowballing into a full-scale response, triggering automated response in a vicious cycle.[25]

The counterargument is that there is nothing inherently more destructive about autonomous weaponry; it is simply conventional weaponry directed by an autonomous system. Thus, it is not clear why autonomous systems would be more susceptible to inadvertent escalation than humans under the same circumstances. Some also question the plausibility of a scenario in which numerous free-ranging autonomous weapon systems come into contact with one another while empowered to engage in conflict independent of explicit human tasking or authorization.[26]

Judgment Errors/Accuracy

The final and most frequently cited risk is in the area of reliability and predictability. For various reasons, almost all involved in LAWS analysis recognize the difficulties inherent in ensuring reliable decision making.[27] Proponents of a ban generally take the position that the decision making of an autonomous weapon system is fundamentally or irreducibly unpredictable, thereby foregoing the need for research to determine future reliability. For example, some argue that because no software can include an exhaustive description of all possible circumstances, it is impossible for an autonomous system to behave predictably outside highly controlled circumstances. Others argue that the technology required for flexible autonomous operations will, by needs, be based on learning or self-altering algorithms, which may develop unpredictable behavior patterns invisible to the original designers.[28] Finally, there are concerns that, even if developed, ethical decision making would be a premium system not deployed by potential state and nonstate opponents of the United States in a prospective arms race, even if the United States reliably employed it.[29]

Some experts, however, believe that an autonomous decision-making system may plausibly reach a level of reliability and predictability comparable to a human soldier. The proponents of the technology argue that requiring absolute or logically

certain predictability from LAWS holds it to a higher standard than that applied to humans and risks failing to use a potentially more reliable system because it is not perfectly reliable.[30] The question of decision-making performance is, however, inextricably linked to a large number of disputes regarding the legality of LAWS. The nature and performance of the autonomous system in making critical decisions about the propriety of the use of lethal force are the central issues addressed next.

Legal Issues

There are two areas of legal contention regarding autonomous weapon systems. The first area is the weapon system's ability to comply with US obligations under international humanitarian law and rules of engagement (ROE).[31] This is essentially an operational concern: Will the functioning of the weapon systems comply with the appropriate requirements? The second concern is less focused on function, but instead questions whether the use of LAWS will make it more difficult to hold parties accountable for misconduct during armed conflict.[32]

Operational/Functional Laws

There are generally three areas of operational law that arguably affect consideration of LAWS. First, there is the set of legal norms that governs the appropriate justification for the initiation of armed conflict, called jus ad bellum, as noted above.[33] However, when critics and defenders address initiation of armed conflict, the critical issue is the potential for moral hazard rather than the law, as discussed previously under "Risks." The second area of operational law classifies weapons themselves as lawful or unlawful. Finally, law governs conduct of operations during war, or jus in bello.[34]

Weapons Law

A weapons evaluation for compliance with the laws of armed conflict considers first whether a weapon is prohibited per se, or prohibited under all circumstances, under the law of war. This status adheres to weapons that are banned pursuant to treaty as well as to weapons that cannot comply with legal requirements under any circumstance or method of use.[35] The first principal legal requirement is that the weapon does not cause suffering or injury beyond that required for a military purpose. For example, the use of glass ammunition is prohibited, without further evaluating the specific circumstances of use, because its use is considered to inflict unnecessary suffering. The second legal requirement is that weapons must be capable of being employed in a fashion to distinguish between military and civilian targets (which might be impossible either because of an incapacity to target or to control effects).[36]

Although some proponents of a ban on LAWS argue that such systems are per se illegal on the basis that they can never adequately distinguish between lawful and unlawful targets, opponents argue that this assertion ignores many lawful use scenarios.[37] They point out that even "dumb" bombs and indirect artillery fires are not per se illegal, since they can be used under circumstances in which civilians are

not present; for example, to target a cluster of tanks in an unpopulated area. Likewise, even autonomous weapons without any capability to distinguish between combatants and civilians might be used under limited circumstances in combat zones without noncombatants.[38] The resolution of this disagreement seems to turn on the likelihood of any scenario in which LAWS can perform at least equal to a human, with opponents of a ban pointing to the uncontroversial current use of over-the-horizon, or sensor-based, targeting as an analogy, and proponents of a ban arguing that these scenarios are extremely limited or unlikely.[39]

The second aspect of a weapon evaluation is based on the specific proposed uses of the weapon. In this case, each of the proposed uses of the weapon must be evaluated for the weapon system's compliance—under those sets of circumstances—with the law of war. This contextual evaluation primarily relies on the weapon system's ability to comply with the principles of distinction and proportionality during actual operational use.[40]

Law of Armed Conflict/Jus in Bello

Although a variety of principles form the basis of the law of armed conflict (the DOD identifies five), most consideration of autonomous weapon systems has focused on the foundational principle of distinction and its related principle of proportionality.[41] The requirement to take feasible precautions is also frequently raised, but has generated little meaningful debate.[42]

Distinction

Distinction is the requirement that warring parties distinguish between military and civilian objects and personnel during the course of conflict and is considered customary international law.[43] The primary concern, as discussed before, is that even if LAWS in principle are not per se indiscriminant, in practice they will simply be unable to distinguish between combatants and civilians.[44] The difficulty of this task is agreed, by all sides of the debate, to be a particularly acute concern in the context of irregular warfare. In these conflicts, combatants may be embedded within the larger civilian environment, which creates extremely complex decision-making scenarios.[45]

In addition, because LAWS lack empathy or human emotion, they are now, and may be in the future, unable to effectively determine the intentions of individuals on the battlefield, critical to distinguishing combatants and noncombatants. Consider, for example, complex situations involving noncivilian noncombatants legally entitled to protection, such as surrendering, wounded, or incapacitated fighters.[46]

Defenders of the technology, at least in terms of its potential, point out that future autonomous weapon systems may be more capable of distinguishing between combatants and civilians than human soldiers. Because LAWS' capabilities are not degraded by the same stress and emotional intensity that affects the judgment of soldiers in combat, and because LAWS have no need for self-defense, they can respond more tolerantly to ambiguous circumstances than similarly situated soldiers. For example, they might delay their response to threatening actions until the initiation of active hostility.[47] Also, governments interested in improving the accuracy of distinctions made by

such systems could employ shared standards of testing, as well as leveraging the benefit of evaluation by ethicists of complex or difficult distinction decisions.[48]

Proportionality

Proportionality is the requirement that military action not cause excessive damage to civilian lives or property in relation to the military advantage to be gained from the action.[49] On one hand, many argue the proportionality judgment that is required by this rule is inherently complex and flexible and thereby fundamentally beyond the capabilities of an autonomous system. When a decision maker considers the allowable collateral impact of a single action (like dropping a bomb), proportionality requires understanding and integration of the surrounding circumstances of the immediate battlefield, as well as an overall strategic understanding of the goals of the military action in question. Additionally, determining whether collateral impact is excessive is arguably fundamentally inaccessible to LAWS because it embeds an irreducibly human judgment of reasonableness, which is a sort of rough-and-ready appeal to the human faculty of common sense and shared human values.[50]

On the other hand, technology defenders envision the commander activating the LAWS making proportionality judgements about the expected collateral impact resulting from activation of the entire system, drawing on previously established reliability measurements developed for that purpose.[51] When some critics have pointed out that such judgments are time-sensitive and cannot simply be preprogrammed, ban opponents have responded that ensuring their continued viability simply requires time limits to avoid the aging of these judgments.[52]

Collateral damage estimates for current weapon systems are regularly made using objective data and scientific algorithms. Some supporters of LAWS thereby argue that modern warfare regularly involves individuals executing a kinetic action (that is, dropping a bomb or firing a missile) with little or no capability or requirement to assess the specific conditions of the target immediately before its destruction or to perform an instantaneous proportionality assessment.[53]

As previously noted, the commander who sets the LAWS in motion, plays a critical role in the legal responsibility for its resulting action. However, there remain questions whether that commander, or any other individual, could be held appropriately accountable for war crimes committed by such a weapon system.[54]

Accountability and Liability

Critics of LAWS have raised legal objections relating to the chain of accountability for the actions of these systems. Because machines are not ethical actors, if an autonomous system carried out an action illegal under the laws of war (a war crime), holding someone responsible for that decision could be difficult or impossible.[55] Opponents of a ban counter that there is a long tradition of command responsibility for the actions taken by subordinates. If LAWS were used by a commander with the intention to commit a war crime, then the commander could be held responsible for that crime.[56] Likewise, if the LAWS were intentionally designed or manufactured with the purpose of being used to commit war crimes, or with reasonable knowledge

that they would be so employed, then the designers or manufacturers could also bear criminal liability.

However, while this intent might generate responsibility, arguably war crimes are most likely to occur as a result of an unintended action by the autonomous system, not as an element of deliberate design. Although commanders are responsible for the reasonably foreseeable actions of subordinates, critics are concerned that commanders, designers, and manufacturers will be excused from such responsibility because of the fundamentally complex and unpredictable nature of autonomous decision making. In this view, victims of war crimes committed by LAWS will lack redress, creating a fundamental lack of justice and responsibility associated with the use of these weapons. For this reason alone, some argue, LAWS should be banned.[57]

Of course, some note that Soldiers ordered to perform an otherwise lawful mission could commit war crimes as well.[58] While this still leaves some person criminally responsible for the misconduct, LAWS' defenders counter that this analysis places an excessive focus on individual criminal liability.[59] They point out that the law has effectively managed responsibility for a variety of circumstances involving not fully predictable outcomes, such as the law regarding pet behavior or criminal negligence.[60] Moreover, the law of state responsibility would seem to allocate legal responsibility and an obligation to provide appropriate redress to the belligerent state employing the LAWS, arguably making the establishment of individual culpability less urgent.[61] The question of whether noncombatant victims of LAWS-related violence—whether intentional, collateral, or accidental—can receive justice leads to a larger question about the moral propriety of LAWS.

Moral/Ethical Issues

The potential for autonomous weapon systems to make decisions about whether to take human life has generated discussion of risks and benefits, as well as legal concerns, but it has also raised more fundamental questions. Some, including Christopher Heyns, the United Nations Human Rights Council special rapporteur on extrajudicial, summary, or arbitrary executions, have indicated that the very notion of machines making the decision to take a human life is morally problematic.[62] As some describe, human dignity is at the core of the international law of human rights. Allowing a machine to make an independent judgment to take a life impugns that dignity.[63] Others argue that allowing machines to make the decision to kill treats human being as objects and denies their fundamental moral value.[64]

Ban opponents argue that moral intuition is based on excessive anthropomorphism of autonomous weapon systems, analogizing autonomous processing to human reasoning in a way that is unlikely to accurately reflect military technology within the foreseeable future. In their opinion, even a nondeterministic LAWS (that is, using a flexible learning algorithm) is not making a decision in an ethically meaningful sense any more than is an air-to-air missile or Patriot battery. Under this notion, the relevant decision to kill is made by the commander who assigns the LAWS its mission, sets limits in time and space, describes ROEs, and sets the LAWS into motion.[65] As discussed, still others accept the LAWS as a decision maker in a

morally relevant sense but argue that, when deployed, it will make better ethical decisions than a human Soldier.[66]

Autonomy May Highlight Broader Concerns

There are at least three major areas where the risks and ethical issues raised by critics of LAWS are not unique to these systems. Supporters of LAWS argue that critics only associate these issues with autonomy because they either have not considered or do not fully understand the array of technologies and doctrinal structures that— without autonomy—already generate the circumstances that give rise to critic's concerns. Specifically, even in the complete absence of autonomy, technological disparities result in a tremendous and increasingly disproportionate risk (civilian and military) between the United States and those enemies with whom we are currently engaged, producing the same moral hazard for decision makers. Likewise, along with reducing risk, stand-off weaponry of all types increasingly abstracts the initiator of lethal action from the individual killed in a way that raises fundamental questions regarding the dignity of individual human life. Finally, fragmentation of targeting and strike decision making is already characteristic of much operational tasking, and this mitigated character already complicates traditional notions of accountability and responsibility.

However, dismissal of these three critiques because they are not unique to LAWS is profoundly misguided. The fact that risk disproportion, lethal abstraction, and mitigated decision making are characteristic of modern US warfighting, independent of any particular technology, makes these critiques only more worthy of substantive engagement. Debate and discussion of autonomous weapon systems may bring into sharp focus risks and concerns—operational, legal, or ethical—which are characteristic of the entire host of evolving technologies and doctrines, and deserve engagement as constructive contributions on questions of national concern.

The United States' current conflicts with nonpeer nations and peoples have highlighted the disproportion in risk between us and our opponents, among both military members and civilian populations. While perhaps not significant in near-peer direct conflict (depending on the success of the third offset), such a disproportionate impact may distort the decision-making calculus of both military and civilian senior leaders, particularly in light of a US population who has little concern for enemy casualties or social impact on enemy nations. This heightened willingness of US leaders to intervene militarily may be reflected in the national conversation by flexibility in adherence to traditional notions of sovereignty (responsibility to protect) or by a broadening of national self-defense (anticipatory self-defense). Recent decades may reflect a growing willingness to seek the achievement of otherwise desirable political ends (replacement of a dictator or the prevention of ethnic abuses) via the application of military force precisely because its use risks so little in US military casualties and the societal impact that makes war "hell" is not felt domestically.

In addition to contributing to the diminished risk discussed above, stand-off weapons—from cruise missiles to RPAs—create an increasingly abstracted and technologically mediated interaction between the initiator of lethal action and the individual killed. Many, both inside and outside the military, find the personalization of

each decision to take a life the necessary sacrifice that humanizes the ruthless realities of combat. As the military continues to develop human-machine teaming concepts and technologies in a context much broader than LAWS, this moral insight may contribute to ensuring the final products reflect our national and personal values.

Finally, critiques of accountability of autonomous weapon activation suggest that the growing fragmentation of seemingly singular actions such as identify, target, or execute may have implications for accountability and responsibility, and that our traditional rules-based evaluations may not be keeping up with the changing character of war. While the military tradition of command attribution (making the commander responsible regardless of personal involvement) may function to counter ethical complacency resulting from diffusion of decision making across a bureaucratic organization, it doesn't resolve the absence of individual legal accountability identified by critics. Leaving aside autonomy, any modern kinetic strike may arise from a complex human-technological intelligence and targeting process, automated estimation of collateral impact, and group decision making, and may reasonably raise questions about the commander's understanding of the reliability of the technology involved. Even actions seemingly indicative of criminal negligence may become increasingly difficult to effectively prosecute, as each individual involved owns only a small portion of the overall compounded error.[67]

Summary

As seen in the table, the debate on LAWS is multifaceted with participants falling in a broad range from proponents supportive of LAWS development, to opponents seeking an outright ban—with many analysts falling between these extremes and focused on risk-awareness and comprehensive regulation. The discussion covers a wide variety of issues, including operational risk, legal factors, and overarching moral/ethical considerations. As commercial technology advances and the DOD continues to develop human-machine teaming and autonomy, LAWS will become ever more central to the US military's competitive advantage. It is increasingly important that military professionals, outside simply the technical arena, understand the grounds of discussion and the arguments being advanced. Even when the critique presented is not unique to LAWS, it may reflect a meaningful engagement with continuing developments characteristic of US warfighting. Understanding the intuitions being expressed, along with a willingness to be flexible where appropriate, will allow military and civilian leadership to guide the armed forces' development and employment of these and other weapon systems to ensure future warfare is conducted in a manner consistent with American values while still maintaining the technological advantages which are the backbone of the American way of war. ✪

Notes

1. Congressional Research Service Report R44466, *Lethal Autonomous Weapon Systems: Issues for Congress*, 14 April 2016, https://www.everycrsreport.com/files/20160414_R44466_47dffae4ebc5e9ea0800c8f1b062d9b9dce81436.pdf.

2. Consider the first autopilot, developed in 1912, as a sort of militarily relevant autonomous system (see Laurence R. Newcome, *Unmanned Aviation—A Brief History of Unmanned Aerial Vehicles* [Reston, VA: American Institute of Aeronautics and Astronauts, 2004], 16). Controversy and concern about autonomous weapons can be traced back far longer, well before the existence of any such system. For example, *Frankenstein, or The Modern Prometheus* by Mary Shelley, largely reflects many of the current concerns with the risks and unpredictable results of autonomous weapons development; *see also* the United Nations Office in Geneva, Switzerland), *Advance Copy of the Report of the 2015 Informal Meeting of Experts on LAWS*, 13–14 November 2014, 9, http://www.genf.diplo.de/contentblob/4567632/Daten/5648986/201504berichtexpertentreffenlaws.pdf.

3. Sydney J. Freedberg Jr., "Hagel Lists Key Technologies for US Military; Launches 'Offset' Strategy," *Breaking Defense*, 16 November 2014, http://breakingdefense.com/2014/11/hagel-launches-offset-strategy-lists-key-technologies/; and Zachary Keck, "A Tale of Two Offset Strategies," *The Diplomat*, 18 November 2014, http://thediplomat.com/2014/11/a-tale-of-two-offset-strategies/.

4. Deputy Secretary of Defense Bob Work, "The Third Offset Strategy and its Implications for Partners and Allies," delivered at Willard Hotel, Washington, DC, 28 January 2015, http://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies; and Secretary of Defense Chuck Hagel, " 'Defense Innovation Days' Opening Keynote," delivered at Newport, RI, 3 September 2014, http://www.defense.gov/News/Speeches/Speech-View/Article/605602; *see also* Robert O. Work and Shawn Brimley, *20YY: Preparing for War in the Robotics Age*, Center for a New American Security, January 2014, 10–16, Deputy Secretary of Defense Bob Work, "Reagan Defense Forum," https://www.cnas.org/publications/reports/20yy-preparing-for-war-in-the-robotic-age.

5. Deputy Secretary of Defense Bob Work, "Reagan Defense Forum: The Third Offset Strategy," delivered at Reagan Presidential Library, Simi Valley, CA, 7 November 2015, http://www.defense.gov/News/Speeches/Speech-View/Article/628246/reagan-defense-forum-the-third-offset-strategy.

6. Wendell Wallach, *Terminating the Terminator: What to Do About Autonomous Weapons*, Institute for Ethics and Emerging Technologies, 29 January 2013, http://ieet.org/index.php/IEET/more/wallach20130129; Human Rights Watch (HRW) and Harvard Law School's International Human Rights Clinic (IHRC), *Losing Humanity: The Case Against Killer Robots* (November 2012), https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots; HRW and IHRC, *Shaking the Foundations: The Human Rights Implications of Killer Robots* (May 2014), http://hrw.org/node/125251; HRW and IHRC, *Mind the Gap: The Lack of Accountability for Killer Robots* (April 2015), https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots; and HRW and IHRC, "Advancing the Debate on Killer Robots: 12 Key Arguments for a Preemptive Ban on Fully Autonomous Weapons" (May 2014), https://www.hrw.org/news/2014/05/13/advancing-debate-killer-robots.

7. HRW and IHRC, *Shaking the Foundations*, 1; Wendell Wallach and Colin Allen, "Framing Robot Arms Control," 126; Ian Anthony and Christopher Holland, "Governance of Autonomous Weapons," 424; Christof Heyns, Report of the Special Rapporteur, para. 38; and Paul Scharre and Michael Horowitz, An Introduction to Autonomy in Weapon Systems, 5–5; International Committee of the Red Cross (ICRC), Report of the ICRC Expert Meeting, 1; Department of Defense Directive (DODD) 3000.09, Autonomy in Weapon Systems, 13.

8. Consider the definition of defensive systems that are empowered to employ lethality in the absence of human action—the DOD considers them a variety of fully autonomous systems, while others distinguish them by their temporal or geographic targeting constraints from more fully autonomous systems. DODD 3000.09, *Autonomy in Weapon Systems*, 3, 13; Paul Scharre and Michael C. Horowitz, "An Introduction to Autonomy in Weapon Systems," (working paper, Center for a New American Security, Washington, DC, 2015), 13; and HRW and IHRC, *Losing Humanity*, 12, https://www.cnas.org/publications/reports/an-introduction-to-autonomy-in-weapon-systems. *See also* Defense Science Board, *Task Force Report: The Role of Autonomy in DOD Systems* (July 2012), 3–8, https://fas.org/irp/agency/DOD/dsb/autonomy.pdf; William Marra and Sonia McNeil, "Understanding 'The Loop': Regulating the Next Generation of War Machines," *Harvard Journal of Law and Public Policy* 36, no. 3 (1 May 2012), 6–7, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2043131; UNOG, *Advance Copy of the Report of the 2015 Informal Meeting of Experts on LAWS*, 11–12, http://www.unog.ch/80256EE600585943/(httpPages)/6CE049BE22EC75A2C1257C8D00513E26?OpenDocument; Eric Sholes, "Evolution of a UAV [unmanned aerial vehicle] Autonomy Classification Taxonomy," Aerospace Conference, *2007 Institute of Electrical and Electronics Engineers* (*IEEE*), 3 March 2010, 1, http://ieeexplore.ieee.org/document

/4161585/?reload=true; Wendell Wallach and Colin Allen, "Framing Robot Arms Control," *Ethics and Information Technology* 15, no. 2 (June 2013), 125, 132, https://philpapers.org/rec/WALFRA; and Ian Anthony and Chris Holland, *The Governance of Autonomous Weapons*, Stockholm International Peace Research Institute (SIPRI), SIPRI Yearbook 2014: Armaments, Disarmament and International Security, chap. 9, sec. II, 2014, 424–25, http://www.sipriyearbook.org/view/9780198712596/sipri-9780198712596-chapter-10-div1-3.xml?rskey=LIjQ3c&result=265&q=&print.

9. James Kadtke and Linton Wells II, *Policy Challenges of Accelerating Technological Change,* Center for Technology and National Security Policy, 12 September 2014, http://ctnsp.dodlive.mil/2014/09/12/dtp-106-policy-challenges-of-accelerating-technological-change-security-policy-and-strategy-implications-of-parallel-scientific-revolutions/; Work and Brimley, "Advancing the Debate," 19; Gordon Johnson, Tom Meyers, Russell Richards, et al., *Unmanned Effects* (*UFX*): *Taking the Human Out of the Loop,* iii, http://edocs.nps.edu/dodpubs/org/JFC/RAPno.03-10.pdf; United Nations Office at Geneva (UNOG), *Informal Meeting of Experts*, 5; and Heyns, Report of the Special Rapporteur, para. 50–51.

10. Work and Brimley, *20YY*, 9, 21–2; Freedberg, "Hagel Lists Key Technologies;" USAF, *Strategic Master Plan*; Johnson, Meyers, Richards, et al., *Unmanned Effects*, 4–5; and Defense Science Board, *The Role of Autonomy*, 41–42, 56–58.

11. Noel Sharkey, "Killing Made Easy: From Joysticks to Politics," in Patrick Lin, Keith Abney, and George A. Bekey, eds., *Robot Ethics* (Cambridge, MA: The MIT Press, 2012), 116; Schmitt and Thurnher, "Out of the Loop," 238; and Johnson, Meyers, Richards, et al., *Unmanned Effects*, 5.

12. Work and Brimley, *20YY*, 31; Anderson and Waxman, "Law and Ethics," 13; Defense Science Board, *The Role of Autonomy*, 69; Work, "Reagan Defense Forum;" Wallach and Allen, "Framing Robot Arms Control," 125–26; Work, "The Third Offset Strategy;" Hagel, " 'Defense Innovation Days;' " and Kadtke and Wells II, *Policy Challenges of Accelerating Technological Change*, 26.

13. Wendall Wallach, *Ensuring Human Control Over Military Robotics*, Institute for Ethics and Emerging Technologies, 29 August 2015, http://ieet.org/index.php/IEET/more/wallach20150829; Schmitt and Thurnher, "Out of the Loop," 62, 240; Brendon Mills, "Rosa's Dystopia: The Moral Downside of Coming Autonomous Weapon Systems," *Foreign Policy*, 18 June 2013, 1, http://foreignpolicy.com/2013/06/18/rosas-dystopia-the-moral-downside-of-coming-autonomous-weapons-systems/; Heyns, Report of the Special Rapporteur, para. 52, 54; and Ronald C. Arkin, *Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture*, Georgia Institute of Technology, Technical Report GIT-GVU-07-11, 6–7, http://www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf.

14. UNOG, *Informal Meeting of Experts*, 7; and Scharre and Horowitz, *Introduction to Autonomy*, 11–12.

15. The legal basis for just war analysis derives from the variety of sources including international agreements and unwritten customary international law. *Department of Defense Law of War Manual*, 39–49.

16. Sharkey, "Killing Made Easy," 122; Wallach, *Ensuring Human Control*; UNOG, *Informal Meeting of Experts*, 5; Wallach and Allen, "Framing Robot Arms Control," 125; and Heyns, Report of the Special Rapporteur, para. 57-58; HRW and IHRC, *Losing Humanity*, 39–41.

17. Schmitt and Thurnher, "Out of the Loop," 232; and Anderson and Waxman, "Law and Ethics for Robot Soldiers," 13. Arguably, using human lives as a calculated method to impose decision-making costs on politicians represents an actualization of the same moral problems posed by opponents of LAWS—in potential—when considering machine-determined lethal fires (see the "Moral/Ethical Issues" section). That is, human lives used as "means" to a political end, without individuation. *See also* Kenneth Anderson and Matthew C. Waxman, *Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can*, American University Washington College of Law, Research Paper No. 2013-11, 18, http://ssrn.com/abstract=2250126 (arguing moral equivalence to hostage taking to influence political decisions).

18. Such relations are unstable if they drain participants' financial capacity and thereby incentivize initiation of conflict in order to prevent further economic impact. *See also* Theresa Clair Smith, "Arms Race Instability and War," *Journal of Conflict Resolution* 24, no. 2 (June 1980), 253–84, https://www.jstor.org/stable/173849?seq=1#page_scan_tab_contents.

19. Wallach, *Ensuring Human Control*; HRW and IHRC, "Advancing the Debate," 18; Work and Brimley, *20YY*, 7–9; Wallach, *Terminating the Terminator*; Sharkey, "Killing Made Easy," 122; Heyns, Report of the Special Rapporteur, para. 88; and UNOG, *Informal Meeting of Experts*, 5.

20. Kadtke and Wells II, *Accelerating Technological Change*, 26; Schmitt and Thurnher, "Out of the Loop," *Harvard National Security Journal*, 238; Thurnher, "No One at the Controls," 80; Anderson and

Waxman, "Law and Ethics," 5, 13–17; Mr. Shawn Steene (Office of the Secretary of Defense, Strategy and Force Development [office responsible for DODD 3000.09, *Autonomy in Weapon Systems*]), interview by the author, winter 2015, The Pentagon, Washington, DC; and ICRC, *Expert Meeting on "Autonomous Weapon Systems,"* 6.

21. Sharkey, "Killing Made Easy," in *Robot Ethics*, 122; UNOG, *Informal Meeting of Experts*, 5; Mills, "Rosa's Dystopia," 2; and Heyns, Report of the Special Rapporteur, para. 87.

22. Steene, interview by the author.

23. Scharre, *Autonomous Weapons and Operational Risk*, 11, 14–15, 19–20, 23; Schmitt and Thurnher, "Out of the Loop," 242–43; and Heyns, Report of the Special Rapporteur, 98.

24. Kadtke and Wells II, *Accelerating Technological Change*, 46; Schmitt and Thurnher, "Out of the Loop," 242–43; Anderson and Waxman, "Law and Ethics," 5; and Duncan, "As More Devices Go Online."

25. Paul Scharre, *Autonomous Weapons and Operational Risk*, Center for a New American Security, Ethical Autonomy Project (February 2016), 1, 8–19, 23, 25–33, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Autonomous-weapons-operational-risk.pdf; Wallach and Allen, "Framing Robot Arms Control," 125; Work and Brimley, *20YY*, 31; Wallach, *Ensuring Human Control*; HRW and IHRC, "Advancing the Debate," 20; and ICRC, *Expert Meeting on "Autonomous Weapon Systems,"* 4, 8.

26. Schmitt and Thurnher, "Out of the Loop," 241; and United Nations Institute for Disarmament Research (UNIDIR), *Framing Discussions on the Weaponization of Increasingly Autonomous Technologies*, 6.

27. Parkins, "Killer Robots;" Wallach, *Terminating the Terminator*; UNOG, *Informal Meeting of Experts*, 10; Wallach and Allen, "Framing Robot Arms Control," 132; ICRC, *Expert Meeting on "Autonomous Weapon Systems,"* 4; Scharre, *Autonomous Weapons and Operational Risk*, 11–17; Schmitt and Thurnher, "Out of the Loop," 239–40, 247; Johnson, Meyers, and Richards, et al., *Unmanned Effects*, 5, 10; Thurnher, "No One at the Controls," 80; and Mills, "Rosa's Dystopia," 1.

28. Sharkey, "Killing Made Easy," 120; Parkins, "Killer Robots;" Wallach, *Terminating the Terminator*; UNOG, *Informal Meeting of Experts*, 10; Wallach and Allen, "Framing Robot Arms Control,"132; ICRC, *Expert Meeting on "Autonomous Weapon Systems,"* 4; HRW and IHRC, *Shaking the Foundations*, 2, 12; and HRW and IHRC, "Advancing the Debate," 6.

29. Wallach, *Terminating the Terminator*; HRW and IHRC, "Advancing the Debate on Killer Robots," 5; HRW and IHRC, *Shaking the Foundations*, 6; Marra and McNeil, "Understanding 'The Loop,' " 60–62; Anderson and Waxman, "Law and Ethics," 5, 10; Wallach and Allen, "Framing Robot Arms Control," 127, 131; Mills, "Rosa's Dystopia," 2; and ICRC, *Expert Meeting on "Autonomous Weapon Systems,"* 8.

30. Schmitt and Thurnher, "Out of the Loop," 239–40, 247; Johnson, Meyers, and Richards, et al., *Unmanned Effects*, 5, 10; Thurnher, "No One at the Controls," 80; and Mills, "Rosa's Dystopia," 1.

31. Jeffrey S. Thurnher, *The Law That Applies to Autonomous Weapon Systems*, American Society of International Law 17, no. 4, 13 January 2013, https://www.asil.org/insights/volume/17/issue/4/law-applies-autonomous-weapon-systems; Schmitt and Thurnher, "Out of the Loop," 243–81; and Anderson and Waxman, "Law and Ethics," 8–9.

32. Sharkey, "Killing Made Easy," 116; Wallach, *Terminating the Terminator;* HRW and IHRC, "Advancing the Debate," 13; and HRW and IHRC, *Shaking the Foundations*, 19–22.

33. *Department of Defense Law of War Manual* (June 2015), 39–49, http://archive.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf.

34. Schmitt and Thurnher, "Out of the Loop," 251.

35. Kenneth Anderson, Daniel Reisner, and Matthew Waxman, "Adapting the Law of Armed Conflict to Autonomous Weapon Systems," *International Law Studies*, 90 (2014), 395, https://www.usnwc.edu/getattachment/a2ce46e7-1c81-4956-a2f3-c8190837afa4/Adapting-the-Law-of-Armed-Conflict-to-Autonomous-We.aspx.

36. Thurnher, *The Law That Applies to Autonomous Weapon Systems*; Schmitt and Thurnher, "Out of the Loop," 245; and Anderson and Waxman, "Law and Ethics," 8.

37. Guarini and Bello, "Robotic Warfare," in *Robotic Ethics*, 131; Thurnher, *The Law That Applies to Autonomous Weapon Systems*.

38. Guarini and Bello, "Robotic Warfare," in *Robotic Ethics*, 131; Schmitt and Thurnher, "Out of the Loop," 246; UNOG, *Advance Copy of the Report of the 2015 Informal Meeting of Experts on LAWS*, 7; and Thurnher, *The Law That Applies to Autonomous Weapon Systems*.

39. Schmitt and Thurnher, "Out of the Loop," 247–48; and Scharre and Horowitz, *An Introduction to Autonomy in Weapon Systems*, 10.

40. Guarini and Bello, "Robotic Warfare," 147; Thurnher, *The Law That Applies*; Schmitt and Thurnher, "Out of the Loop," 249–51; and Kanwar, "Post-Human Humanitarian Law," 8.

41. *Department of Defense Law of War Manual*, 50–66; HRW and IHRC, *Shaking the Foundations*, 15; Thurnher, *The Law That Applies*; Vik Kanwar, "Post-Human Humanitarian Law: The Law of War in the Age of Robotic Weapons," *Harvard Journal of National Security* 2 (3 June 2010), 5; Anderson and Waxman, "Law and Ethics," 8; Schmitt and Thurnher, "Out of the Loop," 250–55; Anthony and Holland, *The Governance of Autonomous Weapons*, 428; and Heyns, Report of the Special Rapporteur, para. 66.

42. With the exception of discussing whether the use of ethical autonomous weapons might be required under some circumstances, which is addressed in the "Positive Improvements in Ethical Warfare" section.

43. Thurnher, *The Law That Applies;* Schmitt and Thurnher, "Out of the Loop," 251; and Anthony and Holland, *The Governance of Autonomous Weapons*, 428.

44. Sharkey, "Killing Made Easy," 118; Wallach, *Terminating the Terminator*; HRW and IHRC, "Advancing the Debate," 5; Anderson and Waxman, "Law and Ethics," 10; Heyns, Report of the Special Rapporteur, para. 67; and HRW and IHRC, *Losing Humanity*, 31.

45. Guarini and Bello, "Robotic Warfare," 130; Sharkey, "Killing Made Easy," 118; Thurnher, *The Law That Applies*; Heyns, Report of the Special Rapporteur, para. 68; and ICRC, *Expert Meeting on "Autonomous Weapon Systems,"* 2.

46. Guarini and Bello, "Robotic Warfare,"131–32; Sharkey, "Killing Made Easy," 116–18; HRW and IHRC, "Advancing the Debate," 5, 11; HRW and IHRC, *Shaking the Foundations*, 13; and Heyns, Report of the Special Rapporteur, para. 67–68.

47. Wallach, *Ensuring Human Control*; Guarini and Bello, "Robotic Warfare," 148; Johnson, Meyers, Richards, et al., *Unmanned Effects*, 10; Schmitt and Thurnher, "Out of the Loop," 240, 262, 264–65; Thurnher, "No One at the Controls," 80–81; and Heyns, Report of the Special Rapporteur, para. 54, 69.

48. Defense Science Board, *The Role of Autonomy in DOD Systems*, 62–64.

49. Anthony and Holland, *The Governance of Autonomous Weapons*, 428; Thurnher, *The Law That Applies*; and Heyns, Report of the Special Rapporteur, para. 70.

50. Sharkey, "Killing Made Easy," 123–24; Wallach, *Terminating the Terminator;* HRW and IHRC, "Advancing the Debate," 6; HRW and IHRC, *Shaking the Foundations*, 16; Marra and McNeil, "Understanding 'The Loop,' " 60–62; Anderson and Waxman, "Law and Ethics," 10; HRW and IHRC, *Losing Humanity*, 31; and Schmitt and Thurnher, "Out of the Loop," 254, 256–57; Thurnher, *The Law That Applies*.

51. Schmitt and Thurnher, "Out of the Loop," 256; and Thurnher, "No One at the Controls," 82–83.

52. HRW and IHRC, "Advancing the Debate," 6; and Thurnher, *The Law That Applies;* Schmitt and Thurnher, "Out of the Loop," 256; and Thurnher, "No One at the Controls," 82–83.

53. Consider, for example, a cruise missile, which may take several hours to strike with no recall capability. See also Scharre and Horowitz, *An Introduction to Autonomy*, 10; and Schmitt and Thurnher, "Out of the Loop," 255.

54. Peter M. Asaro, "A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics," in *Robotic Ethics*, 171, http://www.peterasaro.org/writing/Asaro%20Body%20to%20Kick.pdf; Sharkey, "Killing Made Easy," 124; HRW and IHRC, "Advancing the Debate," 13; HRW and IHRC, *Shaking the Foundations*, 19; Heyns, Report of the Special Rapporteur, para. 78; and HRW and IHRC, *Mind the Gap*, 19–20.

55. Sharkey, "Killing Made Easy," 116–17; Wallach, *Terminating the Terminator*; HRW and IHRC, *Shaking the Foundations*, 19–22; HRW and IHRC, "Advancing the Debate," 13; UNOG, *Informal Meeting of Experts on LAWS*, 14; Heyns, Report of the Special Rapporteur, para. 76; and HRW and IHRC, *Mind the Gap*, 18–37.

56. Guarini and Bello, "Robotic Warfare," 151–52; HRW and IHRC, *Shaking the Foundations*, 19–20; Schmitt and Thurnher, "Out of the Loop," 278; Heyns, Report of the Special Rapporteur, para. 78; and Patrick Lin, George Bekey, and Keith Abney, *Autonomous Military Robotics: Risk, Ethics, and Design*, US Department of the Navy, award #N00014-09-1-1152, N00014-08-1-1209, 20 December 2008, 66, http://ethics.calpoly.edu/ONR_report.pdf (arguing responsibility adheres to the initiator of the autonomous systems' actions).

57. Sharkey, "Killing Made Easy," 117; HRW and IHRC, "Advancing the Debate," 12–13; HRW and IHRC, *Shaking the Foundations*, 19; HRW and IHRC, *Mind the Gap*, 18–37; and UNOG, *Informal Meeting of Experts on LAWS*, 14.

58. Schmitt, "Autonomous Weapon Systems," 13.

59. HRW and IHRC, *Mind the Gap*, 13; Guarini and Bello, "Robotic Warfare," 149–50; and Anderson and Waxman, "Law and Ethics," 12.
60. Asaro, "A Body to Kick," 177.
61. Anderson and Waxman, "Law and Ethics for Robot Soldiers," 17.
62. Sharkey, "Killing Made Easy," 116; Wallach, *Terminating the Terminator*; HRW and IHRC, "Advancing the Debate," 21; HRW and IHRC, *Shaking the Foundations*, 23–24; UNOG, *Informal Meeting of Experts on LAWS*, 17; Anderson and Waxman, "Law and Ethics," 11; Ray Acheson, *The Unbearable Meaninglessness of Autonomous Violence*, Campaign to Stop Killer Robots, CCW Report, 16 April 2015; and Heyns, Report of the Special Rapporteur, para. 89–97.
63. Universal Declaration of Human Rights, preamble, para. 1; HRW and IHRC, *Shaking the Foundations*, 23–24; and Heyns, Report of the Special Rapporteur, para. 89–97.
64. Rob Sparrow, "Can Machines Be People? Reflections on the Turing Triage Test," in *Robotic Ethics*, 306, http://arteca.mit.edu/book/robot-ethics.
65. Guarini and Bello, "Robotic Warfare," in *Robotic Ethics*, 152, http://arteca.mit.edu/book/robot-ethics; Defense Science Board, *The Role of Autonomy*, 48; Kanwar, "Post-Human Humanitarian Law," 5; and UNOG, *Informal Meeting of Experts on LAWS*, 9, 20.
66. *See the* "Potential Improvements in Ethical Warfare" section of this article.
67. Consider the US kinetic strike by a manned aircraft against the Doctors without Borders hospital in Kunduz, Afghanistan. *See* Eugene R. Fidell, "The Wrong Way to Handle the Kunduz Tragedy," Opinion-Editorial, *New York Times*, 1 May 2016, http://www.nytimes.com/2016/05/02/opinion/the-wrong-way-to-handle-the-kunduz-tragedy.html?ribbon-ad-idx=5&rref=opinion.

Maj Thomas B. Payne, USAF

Major Payne (BA, Guilford College; BS, Georgia Institute of Technology; and JD, Vanderbilt University) serves as an executive officer and Air Staff counsel, Administrative Law Directorate, Office of The Judge Advocate General. The Administrative Law Directorate provides legal advice and assistance to the Air Staff; elements of the Secretariat, including the Personnel Council, the Board for Correction of Military Records, and the Discharge Review Board; The Inspector General; and command and staff judge advocates on matters relating to the organization, administration, operation, personnel, and functions of the Air Force. Major Payne received his commission through the Air Force Basic Officer Training School in October 2003.

Global Command and Control for the Future Operating Concept

Implications for Structural Design and Information Flow

Maj Ian Slazinik, USAF
Maj Ben Hazen, USAF

It appears that the end of the traditional air operations center (AOC) as we know it is within sight. Lt Gen David Deptula, USAF, retired, one of the chief planners of the Operation Desert Storm air campaign, recently stated ". . . our ability to command and control (C2) air and space forces will be affected by three major interrelated trends: emerging threats, new technologies, and the velocity of information."[1] Air Force leaders actually described

this future C2 environment in their "Call to the Future" and the "Air Force Future Operating Concept (AFFOC)" describing the multidomain operations center (MDOC) of 2035, complete with new divisions, impressive resiliency, robust reach-back capabilities, and a smaller in-theater footprint, which left many asking, how can the Air Force get to that future state?[2] Rapid information flow and decision making will be critical, and modern organizational structures such as matrix and edge offer possible solutions. Furthermore, network centric operations offer information-age organizations structures tailored for rapid information processing and utilization.[3] The C2 of air mobility aircraft, a limited worldwide resource utilized yet split between multiple combatant commanders (CCDR), presents a particularly challenging problem set in light of these technological and organizational advances since the advent of the AOC. The purpose of this article, then, is to examine how the air mobility C2 enterprise might adapt its organizational structure to increase the speed of information flow between the globally minded 618th AOC and the regionally focused air mobility divisions (AMD). This research suggests that increasing the lateral ties between the 618th AOC and regional AOCs, while not a manpower savings, would increase the agility and information flow through the air mobility C2 enterprise as a whole. A theater-specific reach-back cell within the globally focused 618th AOC might be a first step on the road to the future operating concept's realities of 2035.

Background

The current AOC, a concept that is only a few decades old, is based on Air Force doctrine and rooted in a history of practices that have shown continual success in the crucible of combat. This organization takes a commander's guidance and intelligence and fuses it into a daily executable plan, more effectively utilizing airpower in support of theater objectives. However, the initial design of the AOC structure was somewhat limited by the technological capabilities of the time. For example, air tasking orders (ATO) were physically flown to aircraft operating locations instead of being sent electronically. Air Mobility Command's (AMC) mobility aircraft are centrally controlled through their worldwide-oriented Tanker Airlift Control Center unless these aircraft are transferred to a theater commander with an AOC able to assume that role locally as a result of a request for forces from that theater commander. In that case, they're controlled through that AOC's air mobility division, one of five specialized divisions spelled out in Air Force doctrine and under the command of the joint or combined forces air component commander in theater. This transfer normally happens when the aircraft perform tasks primarily in that one theater for typically more than a few weeks.

Due to increasing demands on air mobility aircraft, US Transportation Command (USTRANSCOM) has more recently advocated retaining operational control (OPCON) of aircraft it might have transferred to a requesting combatant command in the past. This recent approach mirrors that of similar-type civilian logistics operations that are centrally managed to maximize efficiencies by flowing resources to the point of need without having to navigate through time-consuming sourcing processes. Furthermore,

the acceleration of information availability has condensed decision timelines and changed how similar civilian organizations organize and perform, allowing them to react seemingly on a dime to changing market conditions anywhere.[4] While retaining OPCON might help USTRANSCOM to meet the demand from multiple theaters, it also complicates command relationships and control responsibilities. This current challenge presents an opportunity to examine not necessarily changing the relationship between these entities, but the ways they pass information to assist in moving toward the predicted realities of 2035.

As early as the 1970s, organizational theorist Jay Galbraith's research anticipated the information age and sought ways to gain organizational advantages in this new domain. He proposed that the amount of information processed between decision makers is proportional to the amount of uncertainty in a task. Uncertainty limits the ability of an organization to preplan or make decisions about activities in advance of their execution.[5] His resulting organizational information process theory (OIPT) can inform the structure of not only commercial business, but also the C2 of military aircraft. How the C2 enterprise organizes around information flow and uncertainty could play a key role in the ability of rapid global mobility to meet the nation's needs. As such, through the lens of OIPT, this research addresses the following questions related to the structure of the air mobility C2 enterprise:

1. What specific criteria determine the functions that can or should be performed at a central hub and which functions should be present in a regional entity to increase the speed and reach of information while decreasing equivocality?
2. How might the structure of the air mobility C2 personnel be leveraged more effectively in a future information-driven, integrated planning, and execution cycle to increase the organization's ability to respond to uncertainty?

Literature and Guidance on the Future of Command and Control

Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations*, describes joint command and control practices for air operations and prescribes centralized control and decentralized execution: "Centralized control is giving one commander the responsibility and authority for planning, directing, and coordinating a military operation or group/category of operations."[6] Further, decentralized execution delegates execution authority to subordinate commanders to keep up with the pace of operations and the uncertainty and fluidity of combat operations. JP 3-30 also notes that decentralization enables mission command, allowing for subordinates to take the initiative tactically based on clear instructions and commander's intent. This flexibility is critical for the air operations C2, unique in speed, range, and flexibility. Missions with a higher degree of uncertainty are subject to a greater degree of decentralized execution, while highly sensitive air strikes would be subject to a greater proportion of centralized control. The keys to success are clear centralized guidance and resistance to over controlling, which hampers operator initiative and effectiveness.[7]

JP 3-17, *Air Mobility Operations*, recommends treating the rapid global mobility mission as a global enterprise: "Although it is not necessary for a single global organization to centrally control all air mobility forces, all commanders should envision air mobility as a global system capable of simultaneously performing intertheater and intratheater missions."[8] There is a clear delineation of control regarding intra and intertheater airlift between USTRANSCOM's air C2 arm, the 618th AOC, or TACC and the theater AMDs. While these organizations differ in structure, there is a considerable overlap in function: "The AMD functions are similar to those of the 618 AOC Tanker Airlift Control Center (TACC). The AMD's theater focus is critical in teaming with the joint deployment and distribution operations center or joint movement center to coordinate and prioritize the phasing of intertheater and intratheater airlift requirements. The AMD has vast theater familiarity and is best able to assess requirements, allocate forces to meet those requirements, and when needed, seek USTRANSCOM augmentation."[9] Interoperability is considered critical between these two entities, "Effective support of the supported CCDRs mobility requirements demands theater and continental US-based forces form a mutual partnership. This partnership must operate as an integrated force with interoperable planning, tasking, scheduling, and C2 systems."[10] For this partnership to function seamlessly, there must be clear, frequent communication and interoperability between the two entities. Current and former Air Force leadership have provided an outline of what this might look like.

In September 2015, the Air Force chief of staff office published its AFFOC where "many of the mission specific functions of 2015's AOCs have merged or moved to geographically dispersed reach back cells with globally networked capabilities."[11] Furthermore, "the AOC's divisions, benefitting from new technology and use of distributed operations, have reduced their forward-deployed footprints and reorganized."[12] This ideal vision of the future consists of agility, increased proficiency, and change to keep pace with the realities of the information age while reducing physical vulnerabilities. It also points at using C2 organization that can keep up.

In a 2014 interview, General Deptula stated, "Advancing threats demand that we move beyond large, centralized, and static C2 facilities. Replacing them with a mobile, distributed C2 structure that can handle the same volume and diversity of information as today's regional CAOC will call for a reappraisal of how we deal with information flow."[13] For example, today's AOCs contain stovepiped divisions that task and execute assets using different software that often does not synchronize without manual assistance. These types of artificial roadblocks in information flow seem to be a symptom borne of the traditional AOC construct. "It is time to end the segregation inherent in the current combined air operations center organizational and process design and move to a much more integrated planning and tasking function."[14] In a constrained fiscal environment, General Deptula contends the Air Force cannot do this through the systematic AOC upgrades as originally intended by AOC creators. The Air Force must leverage its creativity to make a dramatic change in how it accomplishes C2.[15]

Where Are We Headed?

The term *net-centric warfare* (NCW) has recently permeated the realm of military jargon. Many would classify NCW as the technology or systems linking a variety of worldwide sensors to create an integrated information network. However, according to David Alberts, a former American director of research with the Office of Assistant Secretary of Defense for Networks and Information Integration, this is not NCW, but rather what enables it in the first place. NCW is about human and organizational behavior.[16] Due to the increased proliferation of information technology and sensors across the battlespace, more information confronts the C2 enterprise than ever before. The most important focus of C2 is the need to manage that information.[17] It is transparent to missions, force size, and geography. Moreover, NCW does not focus on network-centric computing and communications, but rather on information flows, the nature and characteristics of battlespace entities, and how they interact.[18] Because certain types of information flow differently, the type of information present in an organization, in this instance, should play a role in how an organization is structured to enable NCW. There is a theory that focuses directly on information flow within organizations.

Organizational Information Process Theory

In the midseventies, Galbraith published a theory regarding information flow called *organizational information process theory*. The basic proposition follows that the degree of uncertainty correlates to the amount of information that needs to be processed between decision makers to obtain a given level of performance.[19] Furthermore, if the task is well-defined before execution, then much of the task can be preplanned, much like what an operational plan attempts to accomplish. Organizational structures should be designed according to an overall strategy. In hypothetical organizations, tasks are divided into subtasks that require specialists, and integrating the subtasks around the completion of the main task is crucial. To integrate subtasks, an organization creates integrating mechanisms. These include rules and programs for more predictable tasks, a hierarchy for greater uncertainty, or targets and goals for an even higher degree of uncertainty. Each has its virtues, but the ability of an organization to successfully utilize mechanisms depends on the frequency of exceptions that must be decided by the hierarchy and the capacity of the hierarchy to handle them. As uncertainty increases, an organization can either limit or increase information processing. There are two strategies for each, with the eventual goal being a reduced requirement for hierarchy intervention, assuming that the limiting factor is organizational ability to process unanticipated, consequential information.[20]

In reducing information processing, two strategies are the inclusion of slack resources and the creation of self-contained tasks. Slack resources simply do not compliment operational agility in the employment of airpower. The second method—self-contained tasks—creates multiple suborganizations, each with its complement of specialties. The method shifts the basis of the authority structure from one based on input, resources, skill, or occupational category to one based on output or geographical categories.[21] This approach applies to the network of regional AOCs, but the cost is the loss of utilization of economies of scale. This is also why there is

tension over the control of air mobility assets between the respective regional and global AOCs.

To increase information processing, two strategies are establishing vertical information systems and creating lateral relations. Vertical information systems create a formal language that simplifies decision making. This simplification manifests itself in the Air Force through systems such as the joint operation planning and execution system. The authors posit that if the data is formalized and quantifiable, then this strategy is viable, yet ambiguous data may prove unable to clear up confusion. The lateral relationship strategy brings decision making down to where the information exists but does not reorganize around self-contained groups. As uncertainty increases, lateral relationships can develop from simple, direct contact all the way to a matrix organization. The cost of this approach is an increased amount of personnel in integrating and managerial roles. In conclusion, when confronted with increased uncertainty, the authors state that if an organization does not choose a strategy, decreased performance will be virtually automatic.[22]

Further research on Galbraith's OIPT by media richness theorists Richard L. Daft and Robert H. Lengel shows that organizations process information to eliminate uncertainty, or the lack of information and equivocality, which refers to information that is unclear or of poor quality.[23] Furthermore, researchers found that face-to-face meetings resolved equivocal data thoroughly by interpretation of nonverbal cues. With unequivocal data, an email or document was sufficient. This simple frame shows that determining the structure of an organization is more than just processing information to reduce uncertainty. Building on Galbraith's research, Daft and Lengel aimed to show that organizations can be structured to provide information with suitable richness to reduce equivocality as well as uncertainty. Information richness is defined as information with the ability to change understanding within a certain time interval. Viewed on a spectrum, group meetings provide the highest return on equivocality reduction, while offering typically only a small amount of raw information exchange. On the opposite end, rules and regulations pass large amounts of information but do little to reduce equivocality. The best blends are located in the middle of these two types of information exchange.[24]

Differentiation, meaning the different language, goals, and culture that evolve in different groups within an organization, influences equivocality. Equivocality is highest when differentiation is great, and organizational structure should allow for discussion and resolution of conflicts between interdependent departments. That said, the characteristic that most influences uncertainty is the strength of interdependence between departments, or how much two departments depend on each other.[25] Departments with low interdependence experience more autonomy and stability.

In a 2011 interview, Galbraith stated that many international organizations are going to a matrix structure to contend with added complexity, and that complex organizational structures built to keep up with the demands of the world are starting to be seen as a strength. This foreshadows the world of twenty-first-century military operations, where complex coalitions and anti-access/area denial environments become more common. Furthermore, Galbraith stated that process, along with structure, is what makes complex organizations work.[26] The more complex the structure, the more critical the process becomes. Reflecting on the AFFOC, it seems that the

ATO cycle will become much more adaptive to rapidly updated information. Galbraith's words indicate that C2 organizational design should take a more adaptive and agile approach, but to determine just what that organizational changes might be made, it is important to determine what types of information are present now and how current organizations relate to each other.

Research Method Analysis

Semistructured interviews were chosen as a research method for this project. Upon receiving Institutional Review Board approval and obtaining conformed consent from participants, 17 interviews with C2 experts were conducted. The average length of each interview was approximately one hour. The interviews included nine participants with experience as either an AMD chief or a director of mobility forces, five with C2 experience outside the AMD, and three participants with AMD experience. Participants had experience at six different AOCs. The interviews were recorded, transcribed, coded, and analyzed for answers to the specific research questions. Not all participants were asked the same questions because, for example, certain AMD questions would not pertain to non-AMD personnel. The following is a synopsis of the responses from the research regarding the research questions:

Table. Subjects related to Organizational Information Process Theory and location

Subjects	*Percentage*
Success using reach-back with all AMD positions	0 percent
Success using reach-back with some AMD positions	92 percent
Success integrating entire AMD into AOC divisions	92 percent
Success keeping some AMD entity within AOC	100 percent
Leaders overloaded with information/decision requirements	0 percent
More AMD differentiation with the 618th AOC	75 percent
More AMD interdependence with the 618th AOC	41 percent
AMD deals with more equivocality than a lack of information	75 percent
Lateral relationships highly important for success	65 percent
Face-to-face interaction needed to resolve equivocality	60 percent
Face-to-face interaction not significant to resolve equivocality	20 percent

Results Related to Air Mobility Command and Control Task Location Research Question

1. Most participants responded that using reach-back with some AMD positions would be successful.
2. Regarding physical positions in the AMD, aeromedical evacuation (AE) team members needed to be near other AMD personnel due to the typical urgency of their operations. Having air mobility expertise close to the ATO integrator

was also preferred. Also, a requirements team synchronized with the strategy division would benefit contingency operations, although this didn't necessarily mean the two would be in close physical proximity. The air refueling control team (ARCT) was often located with the combat plans division already. Furthermore, no leadership interviewed proposed that the ARCT be moved, nor airlift execution.

3. Most participants responded that they were more likely to talk face-to-face with personnel who were located physically nearby to their position. Specifically, participants would rather walk a short distance across a building than use a phone call or email to resolve equivocality, although email was a preferred method for record keeping.
4. Most participants pointed out that while C2 training was imperative, experience was much more significant in increasing information flow while minimizing equivocality. Specifically, experience in a specific location assists is reducing task equivocality and lack of information, with equivocality generally more common.
5. Regarding reach-back or distributed operations, AMD members encountered slower support or products that were different from what they had requested, which they attributed to different schedules and the lack of accountability for geographically separated organizations.

Results Related to Organizational Structure Research Questions

1. Some AMD entity within the theater AOCs is essential, and integrating the entire AMD into other AOC divisions would hurt the air mobility C2 enterprise. While leaders acknowledge the value of lateral relationships, the synergies gained from having at least some air mobility experts working alongside each other outweigh potential gains of integrating the entire AMD into the remainder of the AOC. Yet gains have been realized in AOCs where air mobility leaders made the choice to embed personnel in other divisions. Strategy embeds seemed especially valuable, as AMD members were able to positively influence planning efforts earlier in the process. Defining command relationships amid these lateral moves proved difficult. Others observed success from a more complicated matrix structure.
2. Leaders have an appropriate balance of information/decision requirements, with the caveat that when operations moved from phase zero/one into phase two, there is a high potential for overload due to manning for phase zero/one operations. Most decisions within an AMD would occur with relevant members present in a face-to-face meeting.
3. Most AMD participants responded that more differentiation existed between the AMD and the 618th AOC than between the AMD and other AOC divisions. Although much of the language between the AMD and the 618th AOC was

similar, the varied goals and timelines between the two contributed to vast differentiation. It was rare for AMD personnel to interact face-to-face with members from other divisions outside of formal planning meetings. This resulted in some unfamiliarity with the other missions being carried out in theater, but did not appear to detract from accomplishing required AMD tasks.

4. Only slightly more interdependence existed between the AMD and parent AOCs. AMD personnel were, however, especially dependent on the 618th AOC when performing hub and spoke airlift operations because intertheater aircraft set the timing for the operation, proving difficult due to competing theater requirement priorities and the somewhat inflexible nature of worldwide mobility requirements.
5. Most AMD participants responded that they usually dealt with more equivocality than the lack of information, typically from requirements and tasks from geographically separated organizations. Furthermore, most participants responded that face-to-face interaction offered media richness much higher than other forms (video teleconference, telephone, and email) when resolving equivocality.
6. Most participants responded that lateral relationships were highly critical to ensure mission success. Requirements usually appeared via computer software, but did not necessarily paint a comprehensive picture. AMD members preferred talking face-to-face to liaisons, but sometimes called units to clarify on more complex missions. The units—Deployment and Distribution Operations Center (DDOC) and AMD—were seldom collocated, creating equivocality. Members favored collaborative information sharing websites but sometimes felt that finding the desired information usually took too much time. The real difficulty became contacting the correct person. Forming relationships quickly was deemed of the utmost importance from all interview participants.
7. Many, but not all AMD members, had an understanding of how the 618th AOC functions. When acquiring information from the 618th AOC, unfamiliar members usually called a friend or a previous contact. AMD members calling the 618th AOC were often confused and handed off from person to person to get answers. AMD-specific information did not often travel far outside the division, and members repeatedly found themselves answering the exact same questions over and over. The lack of a mirror organizational structure at the 618th AOC made it difficult to interpret information flow, acquire information, or eliminate equivocality. Additionally, most participants identified slow response times from the 618th AOC to geographic AOC requests for information.
8. Many were concerned about inadequate resiliency at the 618th AOC under the threat of a cyber attack. This, combined with observed slower reaction speed from a geographically separated organization, was the chief, but not the only reason, why leaders and AMD members alike were skeptical of AMD reach-back.
9. AMD members saw no need for a traditional full AMD staff intheater. Because many AMD tasks are similar day-to-day, personnel felt that some kind of dedicated

reach-back entity in the United States might be more efficient and could serve multiple theaters if needed, as long as this reach-back entity was dedicated to the AMD it served to ensure rapid support and provided overlapping but not identical business hours for non-24-hour AMDs.

10. Non-AMD members felt AMD personnel were generally in sync with other divisions, but believed air mobility expertise in their division would be well utilized. This embedding of personnel is something that happens occasionally with members of other communities.
11. Leaders were encouraged by information sharing across different AMDs, but saw more improvement opportunities such as a weekly update or at the very least some sort of shared information exchange space.

Research Results with Respect to Models

According to the model, the need for lateral relationships is amplified at the 618th AOC due to the increased differentiation. The observed theme that the 618th AOC is generally not responsive enough to theater needs might be due to a deficiency in the amount of lateral relationships and rich media exchange between the AMDs and the 618th AOC. One might infer that, although reach-back operations to a central C2 entity might eventually yield a manpower savings, the chief motivation for such a change should be an increase in lateral relationships, such as those present at the geographic AOCs between the AMDs and their partner divisions. Such relationships could be the key to confronting increased information flow while reducing equivocality.

Conclusions

Overall, these findings suggest that increasing the lateral ties between the 618th AOC and regional AOCs would increase the agility and reduce uncertainty through the air mobility C2 enterprise as a whole by improving the flow of rich information. This study's research questions centered on physical location for air mobility C2 tasks, as well as what adjustments to the current air mobility C2 organizational structure best improve information flow to reduce uncertainty. In regard to the first research question, the results indicate that deciding which tasks should be performed in a theater AOC and which tasks could be performed via reach-back or distributed operations depends mostly on the definition of those tasks. Easily defined tasks are ideal for accomplishment via reach-back. Furthermore, those tasks that often require clarification, rapid changes, or joint and coalition interaction are best suited for the theater AOC. Interviews revealed that AMD personnel contend with more equivocality than uncertainty, and most equivocality exists between entities that are geographically separated and different, specifically the 618th AOC. Tasks between the DDOC and AOC, another source of equivocality, are delivered by an electronic vertical information system. By moving functions such as requirements and

planning, which sometimes deal with unclear information, to a reach-back entity, their ability to clarify those requirements remains virtually unchanged since they were usually separated from their DDOC in theater. Other sources of equivocality are from both a lack of familiarity with the 618th AOC and unclear information from organizations within the theater. The increased efficiency of a theater-focused reach-back cell at the 618th AOC could help eliminate equivocality between the theater AMD personnel and those at the 618th AOC, while allowing for additional manpower in the theaters for another purpose.

Regarding the second research question, interviewees from outside the AMD frequently steered toward lateral relationships between divisions inside AOCs as a factor in their success. These included air mobility personnel, eliminating much of the lack of clarity of information and smoothing the seams between divisions during operational planning. With more differentiation between the AMDs and the 618th AOC than there is between the AMDs and the other AOC divisions, a strengthened lateral relationship between the AMDs and the 618th AOC could be advantageous. A chief cause of their differentiation is their contrasting goals.

The danger here is the possible splitting of control between two Airmen. The risk to the mission will depend on the fidelity of the process developed in place of the current AMD process, and the fidelity and resiliency of the communications between the two entities. These arrangements would need to be worked out between CCDRs and AMC to ensure a single air commander in theater over mobility forces OPCON to that command.

Recommendations for Air Mobility Command and Control

The AFFOC spends considerable time expounding on both rapid global mobility and C2, including the assumption that our information-handling capacity needs to increase. Moreover, it explains that MDOC Airmen will need to be able to integrate global assets with those already in theater.[27] This project, while seeking to optimize information flow and organizational structure, is ultimately about a path to the projected realities of 2035.

A proposed first step in developing an optimal organizational structure could be to develop a theater-focused reach-back cell at Scott AFB, Illinois in support of theater mobility operations. These Airmen, during phase zero/one operations could perform a theater airlift requirements and planning function, along with AE functions. Tanker personnel would remain in theater due to close ties with other divisions. This reach-back division of geographic AMDs, which would essentially perform the easily defined tasks with little to no equivocality and almost no face-to-face interaction with coalition or joint members, would be led by a colonel, as other divisions in an AOC to separate this intratheater mission from the general intertheater mission of the 618th AOC. It would be highly critical that the same exercise participation at the geographic AOCs continue unaffected by this change, because such exercises establish trust for the 618th AOC as a responsive partner.

This, however, would not be planned as a manpower savings change, as any savings would be used to increase the degree of lateral relationships across the global

C2 enterprise. AMD chiefs would remain in theater along with their smaller but more integrated AMD. The mobility Airmen essential to each theater would remain in place, working on harder-to-define tasks and ensuring the success of the execution of air mobility assets in theater. The amount of personnel present in theater would need to be capable of requirements, plans, and AE functions for a short time in the case of an attack on the 618th AOC, but at a phase zero/one operations tempo.

A critical piece of this proposal is the ability to rapidly deploy elements of the reach-back cell in the case of a contingency. Such a reach-back cell would be effective and efficient in phase zero or even phase one, but once beyond that, the effectiveness of such an entity would be questionable due to rapidly changing conditions in the AOR. A theater AMD needs to be responsive to the CFACC's scheme of maneuver, and this becomes increasingly difficult to accomplish from a reach-back location during a contingency. With the lateral relationships built at the steady-state reach-back location, some members could deploy forward when needed, eliminating the increased information backlog by shifting the balance of lateral relationships to the theater.

Final Remarks

The speed and reach of information across organizations is the key to meeting future C2 needs. The C2 structure must be such that leadership is not overloaded with information and decision requirements when exceptions arise. Tasks that can be preplanned should be, but as experts predict, tasks are increasingly uncertain, requiring increased information processing capability. Differentiation leads to equivocality and can be best solved through optimized organizational structure. Complex organizational structures are better poised to confront complex information requirements, but demand enhanced processes for success.

According to the majority of research subjects, at best, most AMD tasks can be performed from a central location, and at worst, at least a few can. But should they? Interviews have shown that easily-defined tasks are the best candidates for trial in the near future. AMC and USTRANSCOM aim to solve the challenge of supporting multiple COCOMs with limited resources. The 618th AOC sought to alleviate this problem by placing a liaison in theater AOCs, but complications appear to persist. The ongoing restructure of the 618th AOC may also assist in this effort. Having a theater planning element or even a staff of theater liaisons in the 618th AOC, while not reducing the overall C2 manning requirement, could perform easily defined tasks and act as an information conduit that reduces the equivocality and differentiation between the 618th AOC and theater AOCs. This element would assist in building a more agile air mobility enterprise in support of geographic COCOMs and help the enterprise take another step into the future of airpower C2. ✪

Notes

1. Lt Gen David A. Deptula, "A New Era for Command and Control of Aerospace Operations," *Air & Space Power Journal*, July/August 2014, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-28_Issue-4/SLP-Deptula.pdf.

2. US Air Force, "Air Force Future Operating Concept: A View of the Air Force in 2035," September 2015, http://www.af.mil/Portals/1/images/airpower/AFFOC.pdf.
3. David Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. (Washington, DC: Command and Control Research Project, 2003), 25.
4. Jay R. Galbraith, "Organization Design: An Information Processing View," *Interfaces*, 1 May 1974, 4, http://pubsonline.informs.org/doi/abs/10.1287/inte.4.3.28.
5. Ibid.
6. Joint Chiefs of Staff, Joint Publication 3-30, *Command and Control of Joint Air Operations*, 10 February 2014, http://www.dtic.mil/doctrine/new_pubs/jp3_30.pdf, I-3.
7. Ibid.
8. Joint Chiefs of Staff, *Joint Publication* 3-17, *Air Mobility Operations*, 30 September 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_17.pdf, viii.
9. Ibid., I-10.
10. Ibid., II-1.
11. USAF, *Future Operating Concept*, 14.
12. Ibid.
13. Deptula, "A New Era."
14. Ibid.
15. Ibid.
16. Alberts, Garstka, and Stein, *Network Centric Warfare*.
17. Ibid.
18. Ibid.
19. Galbraith, "Organization Design," 4.
20. Ibid.
21. Ibid.
22. Ibid.
23. Richard L. Daft and Robert H. Lengel, "Organizational Information Requirements, Media Richness, and Structural Design, *Management Science*, 32, no. 5, May 1986, https://www.researchgate.net/publication/227445746_Organizational_Information_Requirements_Media_Richness_and_Structural_Design.
24. Ibid.
25. Ibid.
26. Amy Kates, "Organization Design: An Interview with Jay Galbraith," *People and Strategy* 34, no. 4 (2011): 14–17, http://www.riversoftware.com/resources/HRPS_PS34.4_Perspectives.pdf.
27. USAF, *Future Operating Concept*.

Maj Ian Slazinik, USAF

Major Slazinik (BS, USAFA; MBA, Webster University; MS, Air Force Institute of Technology [AFIT]) is an aircraft strike planner for US Strategic Command, Offutt AFB, NE. He is responsible for developing strategic-level planning guidance and providing nuclear expertise to time-critical, adaptive planning efforts in support of US war plans. Major Slazinik is a KC-135 instructor pilot who has flown in both Operations Enduring Freedom and Iraqi Freedom. He is an Air Mobility Command Phoenix Mobility program graduate with experience in contingency response and has worked and trained in numerous air operations centers. Major Slazinik graduated from AFIT's Advanced Study of Air Mobility and the Department of Defense's Executive Leadership Development Program.

Maj Ben Hazen, USAF

Major Hazen (PhD, Auburn University) is an associate professor of Logistics and Supply Chain Management at AFIT and an active duty aircraft maintenance officer. He is also a deputy director of AFIT's Center for Operational Analysis and a faculty affiliate of the University of Tennessee's Department of Marketing and Supply Chain Management. He enjoys doing research in the areas of sustainability, data science, supply chain information systems, and innovation. Major Hazen has published more than 50 peer-reviewed articles across top supply chain, information systems, and analytics journals, such as the *Journal of Business Logistics*, *Journal of Supply Chain Management*, *International Journal of Physical Distribution and Logistics Management*, *International Journal of Logistics Management*, and *Journal of Cleaner Production*. He serves as a senior associate editor at the *International Journal of Physical Distribution and Logistics Management* and is a past editor-in-chief of the *International Journal of Logistics Management*. The major now serves as the editor-in-chief of the new *Journal of Defense Analytics and Logistics*.

Airpower and the Expeditionary Trinity

Emerging Threats, Emerging Locations, and Emerging Capabilities

Lt Col Kevin K. McCaskey, USAF

Answering the two questions regarding the application of airpower is essential to the modern international security environment. The twin inquiries of how airpower should be applied (doctrine) and to what purpose (strategy) defines and describes the contribution of airpower to international conflict. In light of the role that airpower continues to play in the international security system, it is necessary to articulate a clear strategy for the future of the domain and how best to employ airpower in the associated international security paradigm.

The current threat environment places airpower at an inflection point. The strategy that the Air Force and airpower advocates will become increasingly aimed at what might be termed an *Expeditionary Trinity*, wherein airpower combats emerging threats, in emerging locations, with both sides employing emerging capabilities to achieve strategic objectives. By discussing the types of engagements in which politicians choose to employ airpower, and by analyzing the character of the current international security system, not only will the Expeditionary Trinity continue to gain in strategic importance, but that airpower—and more specifically the Air Force—will, by necessity, become the preeminent tool in sustaining American national security interests.[1] Equally important, the continued demands of expeditionary operations have serious implications for military readiness and the manner in which the Air Force organizes, trains, and equips Airmen to employ combat airpower.

Interests and Interventions

According to Carl von Clausewitz, the most important task that statesmen and commanders have to accomplish is the proper identification of the "kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something alien to its nature."[2] In strategic terms, one must correctly identify the nature of the conflict to develop and employ a strategy that can logically connect the available means to the appropriate military ways that achieve the desired political outcomes.[3] Failure from the outset to properly identify the nature of a conflict ensures mission failure, as the devised ways will be designed incorrectly.[4] What are sometimes considered second- and third-order effects might rightly be considered failures in strategic planning owing to incorrectly assessing the nature of conflict. A military built for—and employing combined arms—warfare will likely prove ineffective waging irregular combat against unconventional forces.

While the military views the nature of wars according to a spectrum of conflict (see figure) which reflects the level of exertion required to achieve political output-based objectives, an alternate method of viewing conflict is based on the magnitude of a threat aimed at input-based levels of interest. Proposed shortly after the Cold War, political author Donald Nuechterlein's conception of national interests included survival, vital, major, and periphery interests, where survival interests are existential threats that—if they cannot be overcome—are likely to result in the end of a state.[5] Only the War of 1812 and the Cold War represent this type of threat in US history. Below survival are vital threats, those which are so important to political leaders that compromise is unacceptable such as unconditional surrender in World War II or the Civil War.[6] Each of these interests resides clearly in the orange/red major theater war and greater area on the spectrum of conflict and thus represent security threats for which the DOD must always be prepared to address. Below vital are major interests, something that a country considers "important but not crucial to its well-being."[7] Major interests could range from stability in foreign countries to freedom of the seas. Least important to national security are periphery interests, those that do not impact the security of the United States but may be important to private interests.[8] Major and periphery interests lie in the green and yellow area of

the spectrum of conflict, issues that could result in military action, but by and large are not issues directly related to the national security of the United States.

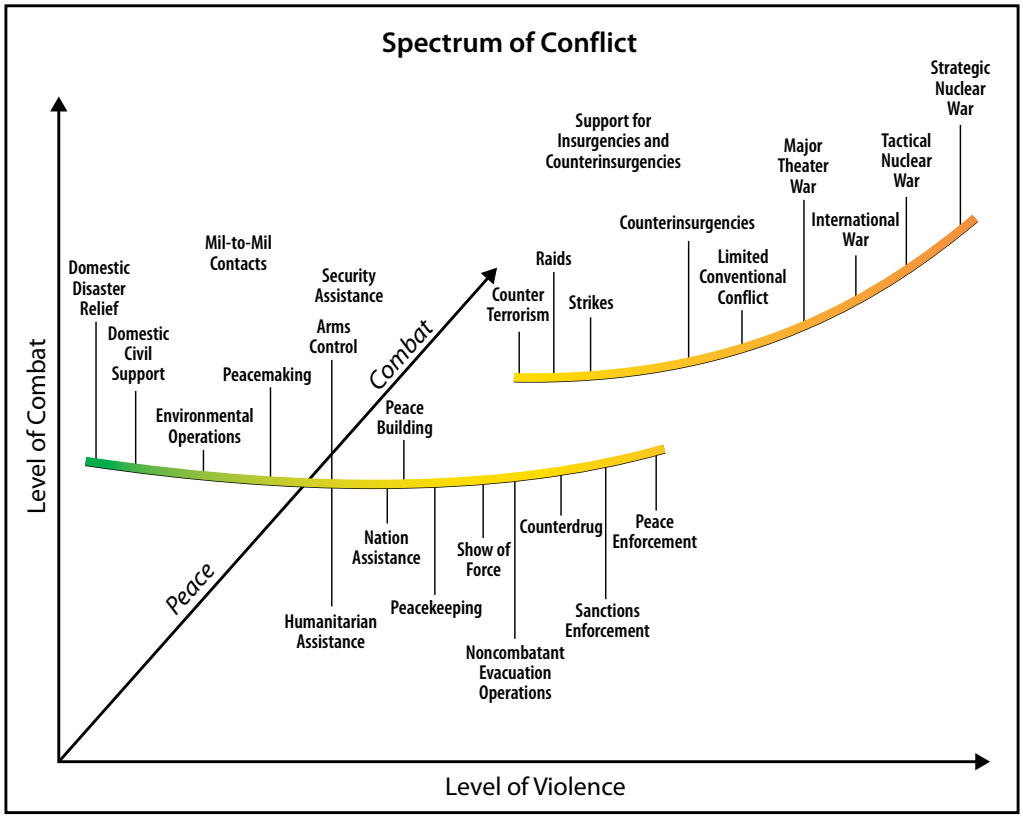


Figure. Spectrum of conflict. (Figure adapted from *Army Vision 2010* (Washington, DC: Headquarters, Department of the Army, n.d.), 5, https://rdl.train.army.mil/catalog-ws/view/100.ATSC/CE5F5937-49EC-44EF-83F3-FC25CBOCB942-1274110898250/aledc_ref/army_vision_2010.pdf)

Since 9/11, the most common use of the US military is of the low-threat nature, and this represents a perpetuation of military employment rather than a deviation from historical norms. According to the Congressional Research Service, since 11 September 2001, there have been 73 instances of the employment of US armed forces overseas.[9] By generously including each successive use of force authorization for Iraq and Afghanistan (as opposed to counting the entire 16-plus years in Afghanistan as a singular use of force), 50 uses are for low-threat to national security engagements from the left side of the spectrum of conflict, and 23 uses for Iraq and Afghanistan. This two-to-one ratio for low-threat engagements only increases if one chooses any alternate date in US history as far back as 1798.[10] The regular pattern of employment of US armed forces is for intermittent periods of vital interstate war-

fare (World War I and II, Korea, Vietnam, and the Gulf War) surrounded by low-threat conflict at the level of major national interests. The fact that American politicians have chosen to employ the military element of national power most frequently on major interest issues at the low end of the spectrum of conflict does not imply that conventional warfare between near-peer states and the vital or survival level of interests should be discounted, but rather that a military that is both effective and efficient requires honest appraisal of both the most dangerous and the most likely uses of force in conflict. Short of invasion, which hasn't occurred in the United States since 1812, states choose when to engage in war, and American politicians choose to engage primarily in low-spectrum conflict.

In the context of defining the operational environment, low-threat conflict should be considered permissive. For the sake of this article, a permissive operating environment is considered one in which US forces have freedom of action to conduct missions across domains. A permissive environment does not mean that forces are entirely secure, only that employed components (air, land, or maritime) can conduct operations at a time and place of their choosing. Permissive operating environments are a defining factor of what expeditionary operations have become.

The evolution of the expeditionary Airman could not have been foreseen when the original air expeditionary force (AEF) concept was being developed and implemented in the 1990s. The AEF was a construct designed in a unipolar international security setting, with early contingency response groups designed to transition from the battlefield to the airfield rather than a dirt patch to expeditionary operations.[11] As envisioned, an AEF would represent prepackaged airpower capabilities of 30–40 aircraft from units that had trained and deployed together previously, ready to provide regional combatant commanders, then known as regional commanders-in-chief, "rapid, responsive, and reliable airpower" tailored Air Forces.[12]

In operations such as Northern and Southern Watch, squadrons would deploy according to predefined schedules, conduct operations, redeploy, and reconstitute as a unit to air bases manned by either individually deployed or permanent party members such as Inçirlik Air Base, Turkey. By 2016, the only remaining vestige from the 1990's conceptual model is that flying squadrons deploy together (but not with other units with whom they have trained) on cycles, sometimes. For most of the expeditionary Airmen engaged in operations around the globe, however, deployments are single endeavors by single Airmen, so much so that by 2016, the incoming Air Force chief of staff, Gen David Goldfein, criticized the habit of individually deploying Airmen as inhibiting unit cohesion and mission effectiveness.[13] Although the officers that crafted the AEF model recognized in advance that the construct would represent a "journey, not a destination," the direction that expeditionary airpower evolved was not, and likely could not have been, anticipated in the relatively stable unipolar world in which the AEF was created.[14] In contrast to known threats in recognized locations with a traditional force structure (for example, the Iraq and Middle East traditionally combined an arms warfare approach in the Gulf War), expeditionary operations have evolved emergently, neither solely responsive nor continually proactive, but often a combination of both simultaneously.

The Expeditionary Trinity's Who and Where: Emerging Threats and Locations

From the counterinsurgency in Iraq through the surge in Afghanistan, to the Arab Uprising, al-Qaeda in the Arabian Peninsula or the Islamic State, airpower remains the first and often enduring response to emerging threats and, as the recent examples of Sirte and Mosul demonstrate, can prove effective when combined with ground-based special operations forces. The fact that airpower is the politically preferred military means to combating emerging threats is not in and of itself surprising; airpower has always enjoyed a shorter response time over land and maritime powers as well as a reduced risk of US casualties. What is surprising is how emerging threats and emerging locations have worked in concert to demand airpower persistence where previously only airpower projection was required.

In the last decade, expeditionary airpower operations have typically focused on nonstate actors or weak states. Organizations such as the Taliban, various al-Qaeda affiliates across three continents—the Islamic State, Boko Haram and others—have been the predominant target of airpower operations, with occasional efforts against weak states such as Libya adding variety. Because weak states can collapse quite suddenly, frequently creating the vacuum necessary for nonstate actors to arise, the use of force against nonstate and weak state actors is a characteristic of emerging locations. The Arab uprisings of 2011 illustrate this point precisely, where a revolution in Tunisia rapidly expanded to encompass all of North Africa and the Sahel. Everywhere in the region that weak states collapsed, including Libya, Mali, Mauritania, and others, emerging threats have flourished, with al-Qaeda in the Islamic Magreb (AQIM) and the Islamic State spreading as far as Western and sub-Saharan Africa following the trail of collapsing states.[15] By the fall of 2016, only in Tunisia did a stable government rule, and even the Tunisians are under assault from AQIM, Islamic State in Iraq and Syria, and homegrown terrorists, with dozens of attacks grabbing international attention.[16]

As weak or collapsed states are often without large foreign support, in geographically isolated areas where the government is unable to effectively control contested regions, in many cases violent extremist organizations (VEO) represent threats to major (important, but not crucial) interests rather than vital, and assuredly not survival, to US national security and are therefore perfect targets for expeditionary airpower. Furthermore, where VEOs are concerned, one of the chief difficulties in defeating threats in the expeditionary environment is the fleeting nature of success. An organization defeated in one location can quickly reconstitute in another location, or even as another organization, demanding yet more American effort to suppress the VEO. The ability of VEOs to rapidly reconstitute using modern multimedia recruiting methods from virtually any ungoverned location requires an ever-increasing demand for building partner capacity (a core military mission) in new locations with the hope that weak states can eventually secure their territory without American military assistance.

While VEOs pose the most recognizable emerging threats, they are certainly not alone. In the last several years, emerging threats have included disease outbreaks, cyberattacks, natural disasters, and humanitarian crises, with some of these other types of emerging threats leading directly to increased threats from VEOs. The West

African Ebola outbreak of 2014 was quickly assessed as a rapidly emerging threat to US security interests, and necessitated an expeditionary military intervention delivered with airpower to austere locations to mitigate the threat.[17] Refugee crises from natural disasters and war represent threats to regional security and global security when VEOs can operate in uncontrolled areas and export violence. The inherent flexibility of VEOs, combined with modern methods of mass communication, means that any strife can swiftly go from localized violence to global violence. Whereas in the post–Cold War security environment, failing states such as Somalia or Rwanda remained largely confined to the single or immediately surrounding states, in the post-9/11 security environment, the collapse of Libya becomes an immediate and unanticipated security threat to the entirety of North Africa and Europe.

Precisely because emerging locations arise rapidly and in unexpected areas, a chief advantage of airpower in preparing for conflict in emerging locations is the margin of error in selecting operating base locations. Whereas an early incorrect basing decision can have strategic consequences down the road, the range of airpower increases the likelihood that basing locations will remain relevant longer, allowing planners to create airbases in strategic locations and knowing that future emerging threats will likely occur within airpower strike range.[18] In the African theater, one can witness real-time the importance of basing decisions as US Air Forces Africa (AFRICOM) continues to expand according to the emerging threats moving swiftly across the continent. While the primary AFRICOM mission of building partner capacity remains paramount, the command is also steadily increasing airpower available to combat emerging threats.

If the pattern of regional combatant commands establishing expeditionary operating locations continues to follow emerging threats, then it is extremely possible that the next frontier for expeditionary airpower will be Southeast Asia, where the Islamic State is making inroads from Thailand south through the Philippines, and every state in between.[19] Because the nation states of Southeast Asia enjoy more stable governments than those of Africa, western airpower might not be necessary to meet the emerging threats, but whether western states or Southeast Asian states meet the threat, emerging capabilities will play a critical role.

The How: Remotely Piloted Aircraft's Emerging Capabilities

In the post 9/11 security environment, VEOs purposefully employ a strategy of irregular warfare to mitigate the advantages of American technological superiority and render many modern weapon systems and doctrine that the Air Force had spent decades developing largely irrelevant. Emerging threats and locations demand innovative approaches that focus on capabilities designed to meet threats as they emerge.[20] Emerging threats that can hide among populations remain hidden—until they decide to act—and often gain control of limited amounts of territory. Later these threats must relocate to avoid American airpower which presents new challenges for their own airpower application—all of which the world has seen play out as the Islamic State moves from Iraq and Syria across Africa and Southeast Asia. These factors have demanded persistence in a way airpower was previously incapable of maintaining,

and it is the ascendance of the remotely piloted aircraft (RPA) technology that has enabled this persistence.

While the first video-capable RPA operated in the Vietnam War, it is the nature of the Expeditionary Trinity that required the RPA become the critical component of American (and increasingly foreign) airpower. The ability of various RPA platforms to engage across the three levels of warfare—strategic, operational, and tactical—increases flexibility by combining previously separate roles into fewer airframes. In the American inventory, strategic assets such as the RQ-4, can transit continents and oceans before loitering over targets for almost a calendar day. Meanwhile, the operational flexibility that characterizes the MQ-1 or MQ-9 (each of which can be configured for a variety of tasks and would make previous multirole aircraft, such as the F-16 jealous) allows the assets to conduct purely intelligence, surveillance, and reconnaissance (ISR) missions, strike missions, over watch, or any combination thereof. Even down to the purely tactical, single-role, RQ-11 used in airbase defense, the RPA has become the go-to technology of necessity for airpower employment for a multitude of reasons. Persistence, rapid reaction, minimal host nation support (compared to traditional air assets), reduced production timelines, and an inherent flexibility that is unmatched by manned aircraft are critical aspects of the fragmented and empty battlefield characteristic to expeditionary operations.[21] Combined, these characteristics have made the RPA the most enduring image of expeditionary operations in the last decade, and likely the most critical in the decade to come.

Additional benefits of RPA technology include reduced human risk and less flight limitations based on human physiology.[22] The simple act of removing the pilot can dramatically improve aeronautical performance by removing requirements for pressurization and life support systems, both of which represent critical weaknesses in aircraft. The notorious case of the F-22 grounding because of life support system failures illustrates this point precisely.[23] Range and loiter can also be reduced by designing RPAs from the ground up to operate under specific conditions. Weapons systems designed to operate in permissive environments can focus on fuel efficiency and range in a way other platforms cannot. Thus, even the persistence of the RPA is directly related to the nature of expeditionary operations. The ability to have an RQ-4 on station in less than 24 hours at any spot in the world, with loiter time long enough to conduct persistent ISR gathering, and without any additional air refueling is unprecedented and a uniquely American version of airpower. The time to package and ship the MQ-1 or MQ-9 worldwide on-air mobility assets can be measured in mere days if not hours. When deployed, these same systems can represent the entire kill chain (find, fix, track, target, engage, and assess) with a minimal footprint or basing requirements in a way no manned asset can. For the price of shared ramp space, a couple of hangars, and some living area for less than a hundred people, these RPAs can deliver ISR and kinetic strike capability in a manner which previously required entire forward deployed groups or wings of hundreds or thousands of Airmen.

Equally important to the operational benefits of RPA in emerging locations and against emerging threats is the concept to the combat operations timeline that RPAs have been able to reinvent. While the MQ-1B Predator was employed as early as the Balkan conflict in the late 1990s, the Predator was declared initial operating capability

(IOC) ready as a USAF weapons system in March 2005, and the MQ-9 was declared IOC-ready and shortly after that combat-deployed in October 2007. While the Reaper represents a herculean leap forward in capabilities from the Predator B, a mere two and a half years separated their production, procurement, and employment timeline. Especially compared to the decades it typically takes the Air Force to acquire weapons systems through the normal acquisition process, the RPA concept-to-combat timeline puts greater capabilities in commanders' hands in response to and during existing conflicts rather than in the successive peace. When this timeline is further combined with the plug-and-play nature of RPAs, the capabilities generated are even greater. From improved avionics to engines operating at greater torque to yet more advanced sensor capabilities such as Gorgon Stare, RPA combat capability can be improved as fast as Big Safari can acquire new systems.[24] In the case of Gorgon Stare, the capability went from concept to able-to-tag-and-track vehicles in Afghanistan using new sensor technology in just a few years.[25] In addition to all of the advantages that RPAs possess, the permissive character of the expeditionary operating environment means that even these systems' inherent weaknesses are mitigated by operating in austere locations.

With limited to zero evasive capabilities, signature reduction technology, or air package support, current RPA technology requires an almost completely permissive environment to operate. As emerging VEO threats move to occupy and operate in ungoverned areas, they can employ integrated or even minimally advanced air defenses. Even legacy radar assisted antiaircraft technology can be mitigated with the Hellfire missiles adapted to fly on the MQ-1 or MQ-9. Other threats such as shoulder-fired man portable air defense systems typically require close proximity to launching or recovering aircraft and can be defeated merely by avoiding the weapon engagement zone of these systems, easily accomplished by positioning RPA assets in safer states or locations with semistable governments and airfield security, then later operating near VEO activity thousands of miles away. Africa again provides an excellent case study of this very dynamic. VEOs such as the Islamic State's Boko Haram in Nigeria, AQIM, Al-Mourabitoun, and others operating in Africa do so specifically because of the inability of stable governments to prevent them from doing so, but the lack of development that is a hallmark of weak or failing states is equally a hallmark of the type of operating environment in which RPAs can flourish. While current RPAs can effectively dominate the lower spectrum of conflict in permissive environments, it is not clear that future conflicts or weapon systems will enjoy this same freedom of action.

The efficacy of RPAs in a vital-level interstate conflict defined by contested airspace is worth considering. The current platforms of the MQ-1, MQ-9, and RQ-4 are utterly dominant in permissive environments, creating asymmetrical advantages by enabling kill chains and friendly ground forces a superior operating picture. If, however, this asymmetrical advantage is that beneficial, how will RPAs function in a contested environment? Let us for a moment consider hypothetical conflict in Southeast Asia. Given the Chinese drive toward an antiaccess area denial strategy and a USAF highly reliant in recent years on RPA employment, how would these weapon systems fare? While the capabilities of the Predator-C Avenger are yet to be determined, current RPAs would likely be unable to operate in the contested air-

space of a Southeast Asia conflict. Chinese offensive counterair, defensive counterair, and air defense networks could track and engage current US RPAs. Simultaneously, Chinese RPAs would enjoy the benefit of operating in uncontested airspace, having the ability to operate over mainland China inside defense zones. If RPAs do in fact generate an asymmetrical advantage, then their employment might favor adversaries in a near-peer conflict. This possibility must be accounted for in future operations. While RPAs have a demonstrated advantage over manned assets in uncontested and permissive environments, they may well represent a disadvantage in contested and nonpermissive environments. In the Expeditionary Trinity, RPAs are ascendant, but further research and analysis are warranted regarding the efficacy of these systems in contested airspace.

Further enabling RPAs as the emerging capabilities in the space and cyber domains not only make operations possible, but it also facilitates interservice and interagency cooperation and decision making in ways impossible just a decade ago. The ability to provide varying customers with tailored ISR products creates efficiencies and reduces knowledge gaps by delivering information in parallel rather than sequential fashion. Since current RPAs are regressive in the traditional critical aviation concerns of engines, avionics, radar cross section, and maneuverability, the true emergent capabilities are those space and cyber advances that do enable entire kill chains.

Fighting the Expeditionary Trinity: The Expeditionary Airman

The expeditionary operating environment has forced massive cultural changes on an Air Force designed since inception for an interstate war fought in traditional combined arms fashion. Assumptions following the Gulf War that airpower could eventually act as a silver bullet for some conflicts did not change this fundamental characteristic; nor did the original Air Expeditionary Force concept. What changed it was the experiences of officers and noncommissioned officers whom, having spent entire careers waging irregular warfare and various subsets thereof, will represent the most significant change to airpower theory and employment. Indeed, the increasingly divergent experience of expeditionary Airmen from previous generations is what is changing the manner of airpower employment.

The expeditionary Airman represents an almost complete inversion of what the Air Force had come to view as operators (typified by the name operations group) and support personnel (mission support group) during the last several decades. In the expeditionary operational environment, the traditional support Air Force Specialty Codes (AFSC) are the actual forward deployed Airmen, and if pilots are even found at forward operating locations, they are RPA pilots operating launch and recovery elements while most of the mission time is logged from stateside ground control stations. For many of these austere locations, the expeditionary air base squadron (EABS) represents the current construct for forward deployed basing. The EABS purpose is to fulfill a mission of base operations support integration. Each of these squadrons exists to enable expeditionary operations (often with RPAs, but not solely), in many cases, including support for joint and coalition operations. As the

name makes clear, these squadrons are at their core support units. The Airmen who man them, however, are beyond a doubt more closely engaged in operations than previous generations of Airmen, as evidenced by the very training newly created to address the specific issues of current expeditionary deployments.

The expeditionary Airman receives Code of Conduct training, the like of which was previously reserved for aircrew and field craft training from the air expeditionary center that prepares them to conduct operations in uncertain, if not outright, hostile environments while simultaneously building host nation relationships and capacity.[26] The expeditionary Airmen who go off base for contracting, host nation support, intelligence gathering, or base defense do so with armed escorts, Office of Special Investigation support, gunned up, or perhaps all of the above. In all cases, expeditionary Airmen know that, regardless of their AFSCs, they are at all times operating in uncertain environments, with innumerable potential threats to their person, their base, and their mission, forward deployed so that expeditionary airpower can be brought to bear in low-spectrum conflicts.

For many Airmen in the expeditionary operational environment, the first deployment comes with the first tour. At the end of a career, many expeditionary Airmen will have half a dozen or more deployments. For all of these Airmen, the defining characteristic is that they have real-world combat, hostile, and expeditionary experience. The days when deployed Airmen were assigned to massive bases safely ensconced away from enemy lines are as remote as the days when combat flying experience was predominantly the realm of the fighter or bomber pilot. In some expeditionary bases, the only flying operations are conducted by security forces Airmen flying RQ-11 Raven unmanned aerial systems for base defense. These Airmen can log more sorties in a month than many pilots will in a year and more flight hours in a six-month deployment than some Air Forces give their most elite pilots.[27]

Alongside the operational experience that expeditionary Airmen get is an additional and perhaps even more critical skill set. The expeditionary trinity of emerging threats, emerging capabilities, and emerging locations means that combatting VEOs and engaging in low-spectrum conflict is, by its very nature, a coalition and joint endeavor. The expeditionary Airman lives in the joint and coalition environment and often both simultaneously. The Airmen in an Air Force expeditionary reconnaissance squadron located on a US Naval installation in Europe are at all times working through joint planning and regulations, as well as coalition concerns, all in the interest of employing airpower. At some emerging locations, Army forces stage from USAF squadrons colocated with one or more joint allies all working with host nations to execute airpower. In both examples and others around the world, expeditionary Airmen are working operational issues with host nation governments, state department officials, and nongovernmental organizations. The net result is that more Airmen than ever before are learning with and from sister services, coalition partners, and civilian experts on different approaches to airpower and how to wield airpower in defense of national interests. The ability to actually deploy these Airmen will be essential to combat emerging threats.

While the Air Force has made improvements at the operational levels of warfare, such as the creation of expeditionary wings, groups, squadrons, combat communications squadrons, and others to account for the unique demands of the Expeditionary

Trinity without the ability to fully man these organizations with seasoned expeditionary Airmen, the USAF risks placing the proverbial cart before the horse. Expeditionary units that lack critical capabilities because the Air Force cannot provide the necessary Airmen in a timely fashion and are a hindrance to the mission and agency for which the units are designed to support. Recognizing that the role of the Air Force is to organize, train, and equip Airmen for combatant commanders, the character of the Expeditionary Trinity requires fundamentally reevaluating how the Air Force accomplishes these tasks to facilitate expeditionary operations.

By definition, the Expeditionary Trinity demands forces who maintain near constant readiness to respond to threats as they emerge, and wherever they emerge. Readiness implies that any necessary skill set or AFSC is available to deploy on short notice and to any required destination, and providing this capability consistently will demand reconsideration of how the Air Force thinks about readiness.[28] The reality is that the legacy air expeditionary force construct—which was designed in the 1990s to operate in the post-Cold War international security environment rather than the post—9/11 security environment—does not maintain a constant and measurable supply of readily deployable expeditionary Airmen. Instead, the legacy AEF construct is relying on just-in-time training as Airmen head out the door while attempting to pair the appropriate equipment to the appropriate Airmen based on deployment destination.

To have a steady supply of experienced, mobility-qualified Airmen ready to deploy on short notice, this article recommends changes to how readiness status can be achieved and assessed, when and how Airmen receive expeditionary training, and when they are equipped. First, the current model of just-in-time training (which is often not in time and drives both late deployment reporting and involuntary extensions for Airmen already deployed) should be replaced with initial qualification training and recurring training where appropriate. Second, Airmen should be, to the maximum extent possible, equipped to deploy whenever their air expeditionary force cycle window is open, rather than after receiving a tasking. Most importantly, to maximize time spent in readiness status, pay, promotion, and assignments should all be directly tied to readiness as well as performance in the line of duty. After all, in the expeditionary operating environment, an Airman who is nondeployable for any reason has far less utility than an Airman who is deployable.

Training and equipping Airmen before deployment would clearly demand more staff work on the front side, but the return on investment might well warrant the effort. Simply by incorporating expeditionary combat after capture and fieldcraft training into USAF basic training requirements would immediately reduce a month of predeployment hassle every Airman experiences. More importantly, grounding every new Airman in an expeditionary and deployable mindset would help instill readiness status as part of the airpower identity. Similarly, many late deployments could be avoided by providing every Airman an official passport upon graduating from basic military training. Yes, the State Department would initially balk at such a requirement, but the reduction or elimination of rush passport applications should provide sufficient leverage to allow the change. Providing all Airmen mobility gear before their deployment window would likely demand excessive inventory and be a waste of precious resources, but having all Airmen qualify on the pistol

and rifle, attend active shooter training, and complete deployment uniform sheets before AEF windows open are all simple and value-added measures that would dramatically improve expeditionary readiness.

The characteristics of the Expeditionary Trinity predict an ever-increasing demand for deployable Airmen. Each year, several new expeditionary air bases are stood up, each of which requires a full complement of experienced Airmen ready to employ airpower. At the same time, the USAF faces critical manning issues and budgetary considerations. To combat these issues and ensure that the Air Force can meet the demands of the Expeditionary Trinity, serious consideration should be given to a dramatic makeover of the way in which the USAF incentivizes Airmen. Pay should be directly tied to deployable status, with consecutive years on deployable status receiving increasing pay scales. Similarly, rather than reenlistment or retention bonuses, which can never represent a measurable increase in deployable Airmen, bonuses should be tied to deployments. The more Airmen are called away from home station, the more they should be paid, precisely because they are providing more airpower application than those unable to maintain deployable status. Succinctly, the mission is expeditionary airpower employment, not home station training. The notion that two Airmen of similar experience, AFSC, and time in grade should receive the same compensation is nonsensical if one of those Airmen is deployable, and the other is not. There is no real neutral ground; if the Air Force does not incentivize deployable status, then the service has automatically disincentivized maintaining deployable status. When there are neither consequences to losing deployment status nor benefits to achieving and maintaining it, the Air Force is sending the message that deployable status is of passing importance rather than the defining characteristic of being mission qualified.

Conclusion: Expeditionary Trinity and the Character of Airpower

Near-peer conflict at the level of vital or survival interests will necessarily drive how the DOD addresses the ground, maritime, and air domains, and rightly so. However, the DOD cannot ignore the character of the conflicts which politicians have chosen to employ the military element of national power since the inception of the state. Rather than the Cold War security structure where known states (communists) in known locations (Asia and Eurasia) employ known capabilities (conventional forces and possibly nuclear weapons employed in a combined arms fashion) against US interests, the post—9/11 security environment is largely defined by unknown threats (ISIS) acting in unexpected locations (Libya/northern Africa) with emerging capabilities. Airpower must simultaneously be organized, trained, and equipped to engage in continuous expeditionary operations to support major interests while remaining ready for the defense of vital or survival interests against state actors.

National security interests drive military intervention, and for almost three decades after the conclusion of the Cold War, interventions have targeted the low-intensity side of the spectrum of conflict. The Expeditionary Trinity is not going away anytime soon. Pressures that the Expeditionary Trinity place on Airmen, the Air Force, and airpower demand innovative approaches to meeting the challenge. As

the only service truly capable of providing sustained airpower during near indefinite periods of time on very short notice, the USAF cannot expect that other services will step in to meet the demands of the Expeditionary Trinity. More importantly, why would the Air Force want such an outcome? Airpower maintains an inherent comparative advantage in meeting emergent threats in emergent locations with emerging capabilities; the USAF should seek to embrace that role and build toward a culture where every Airman aims to achieve and maintain the ability to deploy on a moment's notice. Creating that culture will be critical to the ability of the Air Force to meet national security objectives and continue to wage war on the low-intensity end of the spectrum of conflict. ✪

Notes

1. While the argument in this article is that the most likely employment of airpower in the coming decades will be in emerging locations against emerging threats, the possibility of near-peer conflict in a conventional combined-arms war remains an important consideration. Conventional conflict will be addressed in the emerging capabilities section and the relationship between permissive operating environments and the emerging capabilities of remotely piloted aircraft.
2. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 88.
3. Colin S. Gray, *The Future of Strategy* (Cambridge, UK: Polity Press, 2015), 10.
4. Hy Rothstein, "Civil-Military Relations and Assessments," in *Assessing War: The Challenges of Measuring Success and Failure*, ed. Leo Blanken et al. (Georgetown University Press, 2015), 18.
5. Donald E. Nuechterlein, *America Recommitted: A Superpower Assesses Its Role in a Turbulent World* (Lexington, KY: The University of Kentucky Press, 1991), 15–20.
6. Ibid.
7. Ibid.
8. Ibid.
9. Barbara Salazar Torreon, *Instances of Use of United States Armed Forces Abroad, 1798–2015*, CRS Report R42738 (Washington, DC: Congressional Research Service, 2015), 1–33.
10. Ibid., 1–33.
11. Lt Col James Spaulding, "Airbase Opening in Force Generation," *Journal of the JAPCC* 4 (2006): 26–29, http://www.japcc.org/wp-content/uploads/japcc_journal_Edition_4.pdf.
12. William R. Looney III, "The Air Expeditionary Force: Taking the Air Force into the Twenty-first Century," *Airpower Journal* 10, no. 4 (Winter 1996): 6, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-10_Issue-1-Se/1996_Vol10_No4.pdf.
13. Stephen Losey, "Goldfein's Grand Plan: His Priorities Are Right, Former Service Chiefs Say, but Success Could Be Elusive," *Air Force Times* 77, no. 27, 11–13.
14. Donald Cook et al., "Strategic Implications of the Expeditionary Aerospace Force," *Aerospace Power Journal* 14, no. 4 (Winter 2000): 6, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-14_Issue-1-4/2000_Vol14_No4.pdf.
15. Anour Boukhars, "How West Africa Became Fertile Ground for AQIM and ISIS," *World Politics Review*, 29 November 2016, http://www.worldpoliticsreview.com/articles/20556/how-west-africa-became-fertile-ground-for-aqim-and-isis.
16. Dalia Ghanem-Yazbeck, *Why is AQIM Still a Threat?*, *Carnegie Middle East Center*, 23 March 2016, http://carnegie-mec.org/2016/03/23/why-is-aqim-still-regional-threat-pub-63121.
17. Amaani Lyle, "Ebola Remains National Security Issue, Official Says," *DoD News, Defense Media Activity*, 24 October 2014, http://www.defense.gov/News-Article-View/Article/603517.
18. Lt Col Denis Stengel, French Air Force, "From Airfield to Airport: Airbase Laydown," *Journal of the* [*Joint Air Power Competence Centre*] *JAPCC* 10 (2009): 30–33, http://www.japcc.org/wp-content/uploads/JAPCC_Journal_Edition_10.pdf.

19. Rohan Gunaratna, "New Threat Landscape in Southeast Asia," *Cipher Brief,* 9 February 2017, https://www.thecipherbrief.com/article/exclusive/asia/new-threat-landscape-southeast-asia-1089.

20. Kevin McCaskey, "Constructive Effects: Focus on Capabilities," *Military Review*, August–September 2016, 119–27, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20161031_art018.pdf.

21. Lt Gen Hans-Joachim Schubert, "How Airpower Can Overcome the Phenomenon of the Empty Battlefield," *Journal of the JAPCC* 5 (2007): 20–22, http://www.japcc.org/wp-content/uploads/JAPCC_Jounal_Edition_5.pdf.

22. Col Hans Wolf, German Army, "Do We Still Need 'the Man' in the Cockpit?," *Journal of the JAPCC* 2 (2005): 42, http://www.japcc.org/wp-content/uploads/japcc_journal_edition2.pdf.

23. Elisabeth Bumiller, "Oxygen Problems on F-22 Elude the Air Force's Fixes," *New York Times*, 2 July 2012, http://www.nytimes.com/2012/07/03/us/politics/for-f-22-oxygen-problems-elude-air-forces-fixes.html.

24. Gareth Jennings, "DoD Confirms Gorgon Stare to be Operational in Afghanistan," *Jane's Defence*, accessed 17 December 2105, http://www.janes.com/article/56720/dod-confirms-gorgon-stare-to-be-operational-in-afghanistan (site discontinued).

25. Leon Thompson, "Air Force's Secret 'Gorgon Stare' Program Leaves Terrorists Nowhere to Hide," *Forbes*, 10 April 2015, http://www.forbes.com/sites/lorenthompson/2015/04/10/air-forces-secret-gorgon-stare-program-leaves-terrorists-nowhere-to-hide/.

26. Lorrie A. Arellano, "Air Advisor Academy Consolidates Expertise and Training under the Expeditionary Center," *USAF Expeditionary Center Public Affairs*, 13 July 2015, http://www.expeditionarycenter.af.mil/News/Article-Display/Article/787938/air-advisor-academy-consolidates-expertise-and-training-under-the-expeditionary/.

27. Author interviews with USAF security forces RQ-11 Raven operators forward deployed to US Africa Command revealed Airmen logging more than 50 sorties a month and 300 hours or more in a single deployment. As recently as 2013, the *Wall Street Journal* reported Air Force pilots logging fewer hours than their Chinese or Indian counterparts, and sometimes as few as 120 a year.

28. Todd Harrison, "Rethinking Readiness," *Strategic Studies Quarterly* 8, no. 3 (Fall 2014): 38, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-08_Issue-3/Fall_2014.pdf.

Lt Col Kevin K. McCaskey, USAF

Lieutenant Colonel McCaskey (BA, USAFA; MA, American Military University; and PhD, Naval Postgraduate School) is the USAFA Department of Military and Strategic Studies' deputy department head for academics. He is responsible for the development and instruction of 17 classes informing the chairman of the Joint Chief of Staff's commissioning requirements and compliance with Higher Learning Commission rules on faculty expertise. A command C-17 instructor pilot with more than 1,000 combat hours, Lieutenant Colonel McCaskey previously served as the commander of the 722nd Expeditionary Air Base Squadron. He researches and publishes in the fields of strategy, airpower, security studies, and civil-military relations.

Operationalizing Air Force Critical Thinking

Lt Col James M. Davitch, USAF*
Lt Col Robert D. Folker Jr., USAF

The Requirement for Critical Thinkers

Air Force senior leaders have stressed the importance of developing and maintaining critical thinking capability. The service has approached the requirement as an academic shortfall, failing to accord this important skill its place as a core combat capability. The 2015 Air Force Future Operating Concept (AFFOC) plainly states that the Air Force must "recruit [and] assess individuals with [the] demonstrated potential for critical thinking" to successfully fight and win in contested environments.[1] Although the Air Force articulated an ambitious end state to build and utilize Airmen of the future who can think critically about vexing issues, it is not properly identifying personnel who possess the necessary skills. The USAF has habitually relied on intuitive assessments regarding high-stakes outcomes in uncertain conditions. Individual judgment is typically plagued by overconfidence, cognitive biases, and other psychological factors that lead to poor decision making. The Air Force needs a more deliberate approach if it wants to improve critical thinking so that it can make better decisions across a range of areas including strategic planning, budgeting, human capital management, intelligence, medicine, and acquisition.

Implementing a forecasting program is one low-cost method which would allow the Air Force to measure critical thinking, provide accountability, and identify Airmen with the ability to demonstrate and improve critical thinking by mitigating cognitive errors. To start this process, critical thinking is defined as a mode of reasoning in which one improves the quality of their thought by skillfully analyzing, assessing, and reconstructing their thought processes. A forecasting program, as will be discussed in this article, will provide the best means to measure progress.

Before discussing a practical implementation plan, it is useful to identify why, given multiple requests to improve critical thinking, it has not yet occurred. This problem requires a different resourcing strategy than the typical Air Force acquisition response to meet requirements. Critical thinking is essential to waging modern warfare today, but its intangible nature complicates the service's ability to resource it

*In the Summer 2017 edition, *Air & Space Power Journal* published an article by Col Adam J. Stone, USAF, entitled, "Critical Thinking Skills in USAF Developmental Education." The authors believe that the proposal within could be one way to quantitatively measure and develop critical thinkers within the Air Force to meet Colonel Stone's objectives.

as compared to how it resources most other combat capabilities. For instance, to adequately meet operational plan requirements for defensive counterair, the Air Force understands it must purchase a certain amount of jets, radars, and air-to-air missiles.

Thus, the Air Force is able to measure this traditional combat capability by the number of aircraft, weapons, and qualified aircrew. The Air Force approach to develop critical thinking has primarily consisted of formal training classes, such as the Critical Thinking and Structured Analysis course at Goodfellow AFB, Texas. While such attempts may be helpful, no process exists to routinely measure the critical thinking capability within the Air Force. Accurately measuring critical thinking cannot be done by counting graduates from a course. Rather, the individual critical thinking skills of each Airman should be developed and measured throughout their careers.

Critical thinking skills should be measured over time in a way similar to how instructor pilots conduct periodic check rides for their students. In a cognitive check ride, the evaluator can host a sort of forecasting debriefing or a survey, from which data can be used to improve thought processes. Until we hold ourselves accountable for our assessments derived from critically analyzing problems, it is impossible to judge whether one's subjective opinion is worth anything.

The Illusion of Expert Judgment

In the absence of a systematic effort to collect critical thinking metrics, the Air Force turns to those with experience. Considering experienced individuals have seen and often been instrumental in key decision-making events, this seems to make perfect sense. It is not unreasonable to assume that these individuals would be best suited to recommend future solutions simply by their experiences. Unless decisions are captured in a policy memorandum, most experienced individuals rarely have any documented history of making the best decisions. Indeed, multiple scientific studies have shown that individual judgment is habitually plagued by overconfidence, cognitive biases, and other psychological factors.[2] Oftentimes, those affected by decision makers' judgments do not know whether critical thought was applied to a problem, or if the best decision to solve it was made. In many cases, the thought processes behind decisions simply are not documented using a standard rubric.

In the absence of these things, the Air Force by and large resorts to considering qualifying details such as one's time in service or some outward signifier of experience, such as a weapons school graduate patch on the uniform that signifies some specialized training or experience, rather than solid evidence of critical thought and good decision making. Certainly, extensive experience carries a quality all its own, but experience by itself does not equate to skill in critical thinking. Individuals with unexamined records of success should not answer complex predictive questions based solely on their intuition. At the very least, these same individuals, when asked to provide critical thought, should first be held to an objective standard that measures the secondary and tertiary effects of a proposed course of action.

Some Inconvenient Results

Col Adam "Mez" Stone was one of the first Air Force officers to measure critical thinking ability. He used a standardized exam called the Watson-Glaser Critical

Thinking Appraisal (WGCTA). The test consisted of 40 questions, measured five critical thinking skills, and provided a means for identifying critical thinking ability in comparison to a similar reference population.[3] He knew senior leaders were asking for better critical thinkers, but his first task was to establish a baseline of behavior and to answer the question, "Where do we stand, right now?" His results, which were published in the fall of 2008, became an indictment of the Air Force's critical thinking skills at the time.[4] The group of 180 junior Air Force officers who were the test subjects scored well below average when compared to the graduate degree norm group.

While studying at the Air War College (AWC) in 2015, Colonel Stone used the WGCTA again for a similar study of officers' critical thinking skills at Air Command and Staff College (ACSC), AWC, and the School of Advanced Air and Space Studies (SAASS). In his study, SAASS students scored in the 61st percentile. The ACSC and AWC students scored in the 36th percentile, which was below average in comparison to similar master's level programs.[5] The 2015 study concluded with a condemnation of the Air Force's failure to appropriately educate and train its personnel to develop critical thinking skills through professional military education programs. His assertion is coincident with demands at the highest levels of our leadership for better critical thinking skills.

Despite Colonel Stone's efforts to measure the Air Force's critical thinking capability, there are still no sustained, long-term measurements collected within it. Although measuring critical thinking will not in and of itself provide a complete picture, the mere fact of having individuals make verifiable assessments will improve their critical thinking skills. In short, performance will improve through measurement, feedback, and repetition. The Air Force should capitalize on Colonel Stone's findings and begin to methodically gather data to measure and improve the critical thinking skills of Airmen.

Ways and Means: Practicing and Measuring Critical Thinking

Participants who learn to overcome cognitive traps by measuring their performance and adjusting their approach based on reliable feedback will demonstrate a quantifiable ability to think critically, consistent with the definition proposed earlier in this article. Fortunately, there is evidence that one's subjective judgment can be aided in several ways to avoid mental pitfalls. In so doing, we may identify critical thinkers like Colonel Stone did, build critical thinking capability, and adequately respond to our senior leaders' stated request for critical thinkers.

Few areas are as fraught with cognitive pitfalls as forecasting. While we do not dispute there are many avenues to improve one's critical thinking skills, attempting to anticipate future events provides unique opportunities for individuals to get unambiguous feedback, identify cognitive errors, and improve skills. Therefore, due to the proven success demonstrated by the Good Judgment Project, an Intelligence Advanced Research Projects Activity (IARPA)-funded geopolitical forecasting tournament and research study in which "thousands of people around the world predict global events," this article recommends a long-term critical thinking program which uses forecasting as one measure of critical thinking ability.[6] The program should include a modest amount of training to deal with typical errors in reasoning, such as

overconfidence, bias, and base-rate neglect.[7] The program's participants would make predictive estimates based on numeric probabilities (that is, 40 or 60 percent), rather than possible or probable estimative language. Finally, the program should track performance over time.

Multiyear-long research studies funded by IARPA have shown impressive results with this approach. The first IARPA tournament began in 2011 and explored the potential of crowd-sourced forecasting. Participants made predictions about real-world events, which were then judged by their forecasts' precision. Perhaps the most important aspect of the IARPA forecasting events was that it measured participants' performance longitudinally. These measurements identified individuals who consistently improved and performed well over time. Dubbed super forecasters, they demonstrated the same critical thinking skills, such as bias mitigation and open-mindedness, the Air Force desires in its personnel.

Thus, the primary method to develop critical thinking is submitting regular forecasts in areas of specific interest to the Air Force. For example, since the DOD programming, budgeting, and acquisitions cycle takes years to produce a new weapons system, it is necessary to make the right decisions as to which weapon systems the Air Force should invest to counter a future adversary threat. When making these forecasts, individuals should characterize uncertainty and express that characterization in probabilistic terms through predictive analysis that drives good decision making. Social scientists have published empirical data showing the ability to improve one's forecasting accuracy can be cultivated.[8] They have identified characteristics that differentiate between those who are better and worse at accurately predicting the results of a course of action over a period. Those elements are not indicative of natural-born intelligence or aptitude, but rather a mental determination to exercise critical thought and learn from mistakes. Critical thinkers will take the feedback obtained by measuring their performance, critique the process they used to make a forecast, and improve their decision making.

The process of evaluating an individual's forecast might appear to generate subjective results, which is the reason that the forecasting questions and scoring should be done by an independent central authority, such as the Air Force Research Laboratory. Moreover, proper academic preparation can help minimize the influence of natural heuristics and biases yielding forecasts with remarkable precision.[9] Several studies in the field of decision theory show that a modest amount of preparation can radically improve cognitive performance compared to those who do not receive training.[10] Training is needed that helps identify certain cognitive errors including overconfidence, confirmation bias, and base rate neglect. Daniel Kahneman, Amos Tversky, and Philip Tetlock all explored critical thinking in great detail as it relates to forecasting and cognitive dissonance.[11]

What's Your Brier Score? Operationalizing Critical Thinking

The results of repeated assessments should be graded using a Brier Score, which is a useful way to verify the accuracy of a probability forecast. Brier Scores provide a quantitative means to compare and improve critical thinking while also holding individuals accountable for their estimates. For instance, consider the following question,

"Will the ruler of Country X conduct a nuclear test by the end of 2017?" The outcome is binary, the leader will (100 percent) or will not (0 percent) test a nuclear device. Assume a predictive analyst forecasts a 60 percent chance the test occurs and a 40 percent chance that it does not. If Country X conducts the test, then the score for the assessment would be 0.16. If it does not, the score would be 0.36. Since the Brier Score measures error, the lower the number is, the better, like a golf score.[12]

If the Air Force commits to improving its personnel's critical thinking skills through a forecasting program, it could prove both inexpensive and lucrative. This program would require an administrator function to manage enrollment, generate forecast questions, and score the results. But how might the program attract participants? One option is through monetary incentives. The Air Force already incentivizes individuals to gain and maintain foreign language capabilities. If they attain a high enough reading, writing, and speaking proficiency level on the Defense Language Proficiency Test, they then receive additional compensation. If the Air Force judges that critical thinking skill is as valuable as, or more so than, foreign language capability, then there is a precedent for such incentive pay.

Alternatively, individuals could opt into the program purely to better their cognitive capabilities and compete with peers. It may be possible that the pursuit of a better Brier Score might be incentive enough to improve cognition. Studies show that job satisfaction routinely eclipses financial incentives as primary drivers of personal fulfillment.[13] Since a Brier Score is an objective method to determine the accuracy of a forecast, it levels the playing field. This approach could spotlight a young, inexperienced Airman seeking a reputation for being a person whose thinking is objective and uncluttered by bias. It could also repel those who have established a reputation for fear that their lack of CT skill will be exposed. In short, because it provides accountability, some may avoid establishing a Brier Score if given a choice.

Just as the Air Force requires physical training (PT) culminating in regular tests, so should it mandate participation in a "cognitive PT" program. While coercive, this approach could maximize participation at the lowest cost. Over time, the Brier Score could become a part of the Air Force culture, and the benefits would become obvious to all. Results from multiple large-scale forecasting tournaments revealed, "Prediction accuracy is possible when people participate in a setup that rewards only accuracy—and not the novelty of the explanation, or loyalty to the party line."[14] In other words, competition like this fosters critical thinking while sharpening skills on an individual level. Furthermore, a mandatory competitive program may lend itself to developing and asking questions that can be answered, measured, and scored.

Competitive events are not new for the military. For decades, fighter pilots have trained against rival squadrons during "turkey shoot" events. Winners receive accolades and the recognition of their peers. The Air Force would be well-served by a cognitive turkey shoot, challenging participants to form their conclusions based on openly available information, thereby granting agency to the individual and allowing motivated professionals to best demonstrate their analytic prowess. Ideally, to check a peer's decision-making process, individuals might routinely ask each other, "So, what's your Brier Score?"

Furthermore, the prediction tournament proposed in this article would be one way to quantitatively measure and develop critical thinkers within the Air Force to

meet Colonel Stone's objectives. For instance, the top forecasters in the prediction tournament should be measured for critical thinking skills according to Colonel Stone's method to test for a correlation between forecasters with above average Brier's scores and higher than average critical thinking skills. If a positive correlation exists, then the forecasting tournament may prove to be one of the most effective ways to measure and develop stronger critical thinking skills within the Air Force.

Summary

In short, we must value critical thinking as a core combat capability and measure it. It requires the same degree of training, monitoring, and validation that flying qualification demands. The Air Force would never allow a nonqualified aviator to pilot an aircraft. The risk to individual life and equipment is too great. Similarly, we must ask, why would we be less stringent about larger situations of uncertainty that could introduce risk to thousands? In areas that demand verified critical thinking skill, why would we turn to one's intuitive judgment that may be susceptible to unmitigated cognitive error?

President John F. Kennedy once said, "Too often we. . . enjoy the comfort of opinion without the discomfort of thought."[15] As scientific studies have shown, intuitive judgment is flawed. Institutionalizing a culture of critical thinking will complement expert intuition by mitigating cognitive error and bias. In doing so, the Air Force will step toward a process that rewards true skill through measurement, accountability, feedback, and improvement. ✪

Notes

1. USAF, *Air Force Future Operating Concept*, http://www.af.mil/Portals/1/images/airpower/AFFOC.pdf, 30 September 2015, 43.

2. Welton Chang, Eva Chen, Barbara Mellers, and Philip Tetlock, "Developing Expert Political Judgment: The Impact of Training and Practice on Judgmental Accuracy in Geopolitical Forecasting Tournaments," *Judgment and Decision Making 11*, no. 5, 509–26, September 2016, http://journal.sjdm.org/16/16511/jdm16511.pdf.

3. Goodwin Watson and Edwin Glaser delineated the five skills of critical thinking: inference, recognition of assumptions, deduction, interpretation, and evaluation of arguments.

4. Col Adam J. Stone, "Critical Thinking Skills of Air Force Intelligence Officers: Are We Developing Better Critical Thinkers?" (master's thesis, National Defense Intelligence College, 2008).

5. Col Adam J. Stone, *Critical Thinking Skills of US Air Force Senior and Intermediate Developmental Education Students* (Maxwell AFB, AL: Air War College, 2016).

6 . Office of the Director of National Intelligence, Intelligence Advanced Research Projects Activity (IARPA), "The Good Judgment Project," accessed 26 July 2017, https://www.iarpa.gov/index.php/newsroom/iarpa-in-the-news/2015/439-the-good-judgment-project.

7. Base rate neglect, or base rate bias, is a formal fallacy. If presented with related general information, such as 85 percent of small businesses fail within the first 5 years, the base rate, and specific information, such as this particular business owner has special training or skill, the mind tends to ignore the former and focus on the latter.

8. Chang, Chen, Mellers, and Tetlock, "Developing Expert Political Judgment," 509–26.

9. Based on the research report generated after one large-scale predictive tournament, this training can be executed in 45 minutes.

10. Barbara Mellers et al., "Psychological Strategies for Winning Geopolitical Forecasting Tournaments," *Psychological Science* 25, no. 5, 2014, http://journals.sagepub.com/doi/abs/10.1177/0956797614524255.

11. Daniel Kahneman and Amos Tversky, two eminent psychologists, have written extensively on each.

12. A Brier Score measures the mean squared error of one's assessment. If Country X's leader is deposed, the Brier Score is calculated as [(1.00 – 0.60)2 + (0.00 - 0.40)2 / 2 = 0.16. If Country X conducts a nuclear test, the Brier Score is calculated as [(0.00 – 0.60)2 + (1.00 - 0.40)2 / 2 = 0.36.

13. Daniel J. Benjamin, Ori Heffetz, Miles S. Kimball, and Alex Rees-Jones, "What Do You Think Would Make You Happier? What Do You Think You Would Choose?," *American Economic Review* 102, no. 5 (2012): 2083–110, https://www.aeaweb.org/articles?id=10.1257/aer.102.5.2083.

14. Angela Chen, "Philip Tetlock's Tomorrows," *The Chronicle of Higher Education*, 5 October 2015, http://www.chronicle.com/article/Philip-Tetlock-s-Tomorrows/233507.

15. John F. Kennedy Presidential Library and Museum, "Kennedy Library and Museum Rededication Film (1993): Source of Quotation, 'We Enjoy the Comfort of Opinion. . .,' Address by President Kennedy, 11 June 1962, Yale University Commencement," https://www.jfklibrary.org/Research/Research-Aids/Ready-Reference/Kennedy-Library-Fast-Facts/Yale-University-Commencement-Address.aspx.

Lt Col James M. Davitch, USAF

Lieutenant Colonel Davitch (BA, Penn State University; MA, University of Oklahoma; MS, Blue Horizons Fellowship) is the division chief of intelligence operations at Air Force Global Strike Command, Barksdale AFB, LA. He is the command lead for all intelligence unit support, formal training, and analytical functions. Previously, he completed the Blue Horizons Fellowship at Air University where he analyzed new methods to identify indicators and warning of conflict. Lieutenant Colonel Davitch is a career intelligence officer and has held intelligence assignments at the tactical level in the combat air forces, operational level at the air operations center, and strategic level at Headquarters, US Air Force. He is a 2007 graduate of the Air Force Weapons School, where he was also an instructor.

Lt Col Robert D. Folker Jr., USAF

Lieutenant Colonel Folker (BS, Excelsior College; MS, National Intelligence University) is an airpower strategist in the Checkmate Directorate, Headquarters US Air Force, Washington, DC. He leads concept and strategy development to integrate emerging USAF capabilities into combatant command operational planning; directly supports the deputy chief of staff (DCS) for air, space, and cyber operations; and provides best military advice to the chief of staff of the Air Force. Previously, he supported the DCS for intelligence, surveillance, and reconnaissance (ISR) as the program element monitor for the Air Force Distributed Common Ground System and intelligence training programs and oversaw the programming, budgeting, and execution of more than $5B. Before his assignment at the Pentagon, he served as the director of operations for the 19th Weapons Squadron, US Air Force Weapons School (USAFWS). As an intelligence weapons instructor, Lieutenant Colonel Folker conducted sensitive reconnaissance operations across the globe and combat ISR operations in Operations Enduring Freedom and Iraqi Freedom.

Innovation in a Bipolar Air Force

Lt Col John S. Sellers, USAF, Retired

If it's not broke, don't fix it. This seemingly sound policy is a double-edged sword. A 2016 RAND Corporation study observed that USAF innovation hinges largely upon problem recognition, finding Airmen to be remarkably innovative once they have identified a problem.[1] But the USAF sometimes fails to identify problems, declaring them not broke when in fact they are. In these cases, the Air Force will, with the best of intentions, vigorously do whatever is necessary to "not fix" the problem that it failed to recognize. This bipolar love/hate relationship with innovation leaves Air Force innovators unsure if they'll be promoted or shown the door.

We're going to look at innovation with the same type of approach used in a fighter debrief. Fighter pilots dislike the word *maybe*, as in maybe we'll be better innovators if we implement Quality Air Force, Six Sigma, Lean Air Force, or Air Force Smart Operations of the 21st Century (AFSO21). No, fighter pilots focus upon mission objectives. If they meet their objectives, then it's "well done, beers are on me." But if they don't meet their objectives, then it's time for a long debrief. They determine *exactly* where the problem occurred, and they look at the tapes and ask questions until they determine *exactly* what went wrong. Once the problem is identified, they focus on specific corrective action.

USAF leaders are not providing the type of clarity found in a mission debrief. In his 2013 *Vision for the United States Air Force*, Gen Mark A. Welsh, the previous USAF chief of staff (CSAF), commends the Air Force for a long history of innovative thinking. So maybe it's mission accomplished and beers on the CSAF, but the same document tells all Airmen to "look for smarter ways of doing business" and cautions leaders to "empower Airmen to think creatively, find new solutions, and make decisions."[2] So maybe these are things we aren't currently doing, and it's time to settle in for a long debrief. Leaders need to clarify whether we are meeting the standards of innovation or not. If we aren't, then they need to identify the problem. We're going to examine a case study on aircraft deconfliction to show that the Air Force does indeed have an innovation problem. Spoiler alert: the problem is problem recognition, so we'll look at that first to provide a proper lens through which to view the case study.

Innovation and Problem Recognition

We like to think of ourselves as rational beings, capable of reliably identifying problems and developing good solutions. However, cognitive scientists have amassed an unassailable body of knowledge that demonstrates humans are not always as rational as we would like to believe. Their explanation is surprising, fascinating, and valuable to our quest for innovation.

> Reasoning is generally seen as a means to improve knowledge and make better decisions. However, much evidence shows that reasoning often leads to epistemic distortions and poor decisions. This suggests that the function of reasoning should be rethought. Our hypothesis is that the function of reasoning is argumentative. It is to devise and evaluate arguments intended to persuade. Reasoning so conceived is adaptive given the exceptional dependence of humans on communication and their vulnerability to misinformation. A wide range of evidence in the psychology of reasoning and decision making can be reinterpreted and better explained in the light of this hypothesis. Poor performance in standard reasoning tasks is explained by the lack of argumentative context. When the same problems are placed in a proper argumentative setting, people turn out to be skilled arguers. Skilled arguers, however, are not after the truth but after arguments supporting their views. This explains the notorious confirmation bias. This bias is apparent not only when people are actually arguing, but also when they are reasoning proactively from the perspective of having to defend their opinions. Reasoning so motivated can distort evaluations and attitudes and allow erroneous beliefs to persist. Proactively used reasoning also favors decisions that are easy to justify but not necessarily better. In all these instances traditionally described as failures or flaws, reasoning does exactly what can be expected of an argumentative device: Look for arguments that support a given conclusion, and, ceteris paribus, favor conclusions for which arguments can be found.[3]

In other words, people have a genetic blind spot for problem recognition. The word *adaptive*, used in the biological sense, means that evolution favors argumentation and persuasion. An individual who can persuade others has a survival edge over individuals who cannot. A society that can be persuaded into unified action has a survival edge over societies that cannot. Evolution has designed confirmation bias to serve as a built-in mental filter that helps us argue—we subconsciously capture the data that supports our beliefs and discard the data that might disprove them. But the same bias that helps us persuade others to adopt our beliefs also makes it difficult to see when our beliefs are wrong.

Cognitive science supports RAND Corporation's observation that the USAF often has difficulty seeing problems. But we can train ourselves to smell what we can't see. Bad ideas will often exhibit a strong odor of argument because irrationality and confirmation bias are the genetic result of a brain designed to argue. It's easy to differentiate argument from invention because they are opposite mental processes. An inventor starts with a broad survey of data, then sorts through many solutions to pick the best. When presented with a new idea, an inventor will become excited, ask questions, and investigate. An arguer starts with the solution, then sorts through the data, discarding anything that doesn't support the conclusion. When presented with a new idea, an arguer will become uncomfortable or angry and will immediately try to scuttle it without investigation. Arguers are so certain of their answer that they won't reopen the question.

When we come across an idea or doctrine that is characterized by the omission of relevant data, twisted and contorted logic, and a refusal to consider alternatives, then that odor should alert us to the potential presence of bias and irrationality. We might

be arguing our way to a suboptimal solution, rather than rationally inventing our way to an optimal one. We'll now examine a flight safety issue that reeks of argument.

The Deconfliction Problem

The Air Force has some good rules on deconfliction. *General Flight Rules* 3.17 and 3.18 require all pilots to "detect and avoid" other aircraft, and USAF Training Rules require pilots to knock off any engagement if safety is in question; if a dangerous situation is developing; or when situational awareness is lost. But these mandatory rules are bent and broken in subordinate training publications.[4]

For instance, the requirement to detect and avoid other aircraft has somehow morphed into the requirement for pilots to clear their flight paths, fundamentally changing the visual cross-check in ways that are not good. Rather than looking for the presence of nearby aircraft wherever they might be, they instead look for the absence of aircraft along their own flight path. An article from *Weapons Review Magazine* explains: "while both fighters should clear their own flight path, the engaged fighter has the option to completely disregard the other."[5] Substituting the specious notion of clearing the flight path in place of the requirement to detect and avoid other aircraft is a safety rule violation that has killed many pilots. The following example will illustrate.

Maverick is flying east at 300 knots. He has 12 seconds until he reaches the place he will die, just 1 mile ahead. He looks east along his intended flight path and sees the exact spot of his demise, but he doesn't see a jet there or any other indication of hazard. That's because Iceman is flying at 450 knots and is still 1.5 miles from the collision site. So where might Iceman be? The locus of points representing Iceman's possible locations forms a circle with a 1.5-mile radius from the crash site. If we drop a pencil anywhere on this circle and draw a line toward the center, then that is one of an infinite number of Iceman's potential collision vectors. We can also do this in the vertical plane, so Iceman could really be at any point on a sphere with a 1.5-mile radius from the impending fireball. From Maverick's perspective, Iceman could be at virtually any position on the horizontal or vertical clock. The only way Maverick can be sure to detect and avoid the hazard is to keep track of Iceman, but that's precisely what the *Weapons Review* article says we don't have to do.

Perhaps the requirement to clear the flight path is not to be taken literally. Maybe the guidance is intended to warn pilots to take whatever action is necessary to prevent another jet from ever becoming a flight path conflict. But that's circular reasoning—collision avoidance requires clearing the flight path, and clearing the flight path requires doing the things to avoid a collision. The question remains: exactly what are these things that pilots must do to prevent a collision?

For all other subjects related to flight safety, the USAF has logical and detailed written guidance. The guidance is refined during mishap investigation: the school of hard knocks. It's a beautiful example of the scientific method in action. For each hazard, the USAF provides what amounts to its best hypothesis on how to avoid or survive it. The hypothesis is tested on each flight. Data is gathered from each mishap to improve the hypothesis, and the cycle repeats, but somehow deconfliction has escaped this process of optimization.

The innovation we'll examine next is simply the application of the above process to the subject of deconfliction, or more specifically, element deconfliction. The flight lead and wingman pose the greatest mutual collision threat by constant exposure to one another under every conceivable variation of formation and combat maneuvering situations. We'll focus on formation deconfliction because that's where most of our collisions occur. We'll cover the proposed plan and then evaluate it with respect to logic and the school of hard knocks.

✳ ✳ ✳ ✳ ✳

Proposed Element Deconfliction Plan

Safety is the first priority for all pilots at all times. In accordance with General Flight Rules 3.17 and 3.18, all pilots must "detect and avoid" other aircraft regardless of flight position or maneuvering role. Element members should adhere to the deconfliction contract depicted in the table below.

Table. Element deconfliction contract

Yielding pilot	*Pilot with right-of-way*
Cross-check element mate	Cross-check element mate
Detect collision geometry	Ensure mate yields
Alter course for safe separation	Take corrective action

Cross-check

The visual cross-check should be proportional to the hazard. In formation, the wingman's cross-check frequency is a function of distance. The flight lead should cross-check flight members before, during, and after initiating any action requiring a deconfliction response: rejoins, turns, formation changes, and so forth. In larger formations, all pilots should use these same cross-check techniques to maintain situational awareness on all aircraft in the flight.

During air combat maneuvering (ACM), each pilot must maintain situational awareness on the other and must again base the visual crosscheck on the hazard (distance and closure). Pilots should use the air-to-air tactical air navigation system and radio to aid in deconfliction. Clearing the flight path **does not** ensure safety and cannot substitute for an effective visual cross-check on nearby aircraft.

Collision Geometry

Collision geometry is indicated by an airplane with zero line-of-sight, frozen on the canopy, and growing larger. The yielding pilot should immediately alter course

to ensure safe separation. It is not acceptable to remain on a collision vector, intending to correct the situation later (after taking a shot, for example).

Safe Separation

In cruise formation, safe separation is specified by the formation parameters. During tactical formation and ACM, safe separation is specified by major command regulations (usually 500 feet). If safe separation is in question, then the yielding pilot has failed, and pilot with right-of-way must immediately correct the dangerous situation (verbal direction, "knock it off," and/or evasive maneuvers).

Formation Integrity and Wingman Consideration

Flight leads should use "wingman consideration" techniques to avoid creating task overload during critical phases of flight. Flight leads must also correct poor formation before a dangerous situation develops. Inadequate spacing reduces reaction time, while excessive spacing and poor fore/aft positioning can lead to confusion or loss of visual. If the flight lead fails to correct such situations, it is appropriate for any flight member to make a "check formation" call.

✳ ✳ ✳ ✳ ✳

Deconfliction Logic

We'll examine the proposed deconfliction plan above by logically dissecting its component parts, beginning with the easily misconstrued concept of priority. Pilots often speak of priority as a time apportionment tool, but this isn't the case. Something can be a high priority and take very little time to accomplish. The definition of priority is: "something given or meriting attention before competing alternatives," so safety only interferes with tactics when these two things become mutually exclusive. That's why we try to teach pilots to be safe and tactically effective at the same time.

Pilots have a wide playing field on which to accomplish the mission. At the edges of this field are the boundaries formed by our regulations and safety rules. All pilots must know where these boundaries are and never cross them. A pilot who stays in the wide part of the playing field can be as mission-oriented as he likes. This enables pilots to spend the majority of time and brain cells on mission-related tasks while periodically asking, "Am I getting ready to lose control, or run out of gas, or hit the ground, or hit another airplane?" Usually the answer is no, and the pilot is free to continue focusing on the mission. Occasionally the answer is yes, and the pilot is faced with a situation where mission and safety have become competing alternatives. In these situations, the pilot must immediately address the safety hazard.

Both pilots should be involved in the deconfliction plan. Although it only takes one pilot to avoid a collision, resting the entire plan on the yielding pilot's shoulders

is a bad idea. While it is true that USAF pilots are almost perfect, the word *almost* becomes important when we fly millions of sorties. As a general rule, any safety cross-check should be proportional to the hazard. Our ground avoidance techniques provide a good example. At high altitude, the ground hazard is nil, so the ground cross-check is nil. At low altitude, the hazard increases, so the cross-check increases. If the cross-check is too slow, the pilot can easily "die relaxed" and impact the ground before realizing the hazard. If the cross-check is too rapid, the pilot is wasting time that can be put to good use for tactical employment. For element deconfliction, the hazard level increases whenever the flight lead initiates an action requiring a response from the wingman.

The yielding pilot's cross-check is based upon the worst-case assumption that the flight lead could initiate action at any time. In the closest formation (fingertip), a collision could occur almost instantly, so the wingman must stare almost continuously at the flight lead. In the loosest formation (tactical) it might take 10 seconds for a collision to develop, so the wingman can relax the cross-check to that time interval. By contrast, the flight lead does not have to assume worst case because he knows when he will do something that will increase the hazard. A flight lead should cross-check his wingman (all of them) before initiating a turn, rejoin, or any other action requiring a deconfliction response.

With a good cross-check established, pilots must be able to recognize collision vectors. Because collision geometry is identical to rejoin geometry, the visual indications are exactly what the USAF teaches during rejoin training: a jet with zero line-of-sight rate, frozen on the canopy, and getting bigger. Once collision vectors are recognized, wingmen must know the safe separation standards that guide their actions. The proper criteria for safe separation also provides a margin of safety that gives the flight lead adequate time to realize that the wingman has fumbled, then to take whatever action is needed to prevent the collision.

Finally, pilots should avoid situations that unnecessarily aggravate the collision hazard, like poor formation and bad wingman consideration. In other words, they shouldn't poke the bear and create a predicament from which they will subsequently have to extract themselves.

Deconfliction School of Hard Knocks

We'll look at five randomly selected collisions to see what patterns emerge.

1. Misawa AB, Japan: G-awareness turn (fatal)[6]
2. Hill AFB, Utah: 30-degree check turn during a tactical intercept (fatal)[7]
3. Nellis AFB, Nevada: Rejoin (fatal)[8]
4. Hulman Field, Indiana: Tactical 180-degree turn (fatal)[9]
5. Kadena AB, Japan: Slight check turn during a tanker intercept[10]

All five collisions resulted from a chain of events that, if broken at any link would have prevented the crash. The proposed deconfliction plan provides detailed instruction for the wingman: the most obvious link in the collision chain. But we

also address the two adjacent links: we teach all pilots to avoid situations that unnecessarily increase the potential for conflict, and we teach flight leads to verify that the wingman is properly yielding during critical times. These other two links are easy to address and effective at preventing collisions.

In all five mishaps, the flight paths of all ten aircraft were clear until the instant of impact. For example, at Kadena (fig. 1), the flight paths were clear to the west, but the collision axis was north/south. At Misawa (fig. 2), the jets were turning to a south heading. The flight paths of both jets were clear to the south, but the collision axis was east/west. The jets were turning hard in a 90-degree bank, so the flight lead was actually below the wingman's feet, obscured by the floor of the aircraft. The wingman was directly above the flight lead's head, or slightly behind. In these two crashes and the other three, clearing the flight path could not have prevented collision.

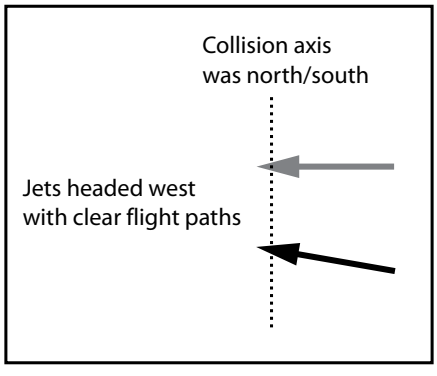


Figure 1. North/south collision axis

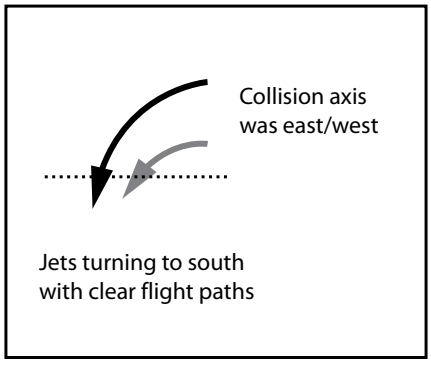


Figure 2. East/west collision axis

In three of five accidents, the jets were grossly out of position. At Misawa and Hill, the pilots were flying at less than half the proper spacing. This increased the potential for conflict and reduced reaction time. At Hulman, the 4-ship was spread

out over 10 miles—more than twice the proper spacing. This certainly contributed to the number two wingman's loss of situational awareness. Making matters worse, the flight lead called for an operations check in the middle of a turn, causing all pilots to go heads-down into the cockpit instead of heads-up to monitor the formation. After rolling out of the turn, number two began flying formation off of the wrong jet and collided with his flight lead. There were eight pilots in these three flights, and they all silently accepted situations that greatly aggravated the collision hazard. The proposed deconfliction plan teaches pilots the dangers of bad formation and poor wingman consideration and empowers anyone in the flight to say something about it. This single measure would have prevented all three of these accidents and saved three pilots.

In four of five accidents, the wingmen showed poor cross-check techniques. At Kadena and Hill, the cross-check was too slow in relation to the distance between the aircraft. The flight leads changed direction and covered the intervening distance before the wingman noticed. At Nellis and Hulman, the wingmen were not visual on all three other jets in their four-ship; nor did they think that this lack of awareness merited a radio call. They both began flying formation off the wrong jet and collided with their flight leads. We should also note that a proper cross-check by the noninvolved members of these four-ships would have given them the opportunity to see and prevent the impending collision between their element mates. The proposed deconfliction plan teaches proper cross-check techniques for wingmen. This single measure surely would have prevented the mishaps at Nellis and Hulman, saving two pilots. It would have lessened the likelihood of the Kadena and Hill mishaps, but it's impossible to eliminate momentary lapses of attention. This is why we must teach flight leads to cross-check the wingmen during predictable times of increased collision hazard.

In all five accidents, the flight leads exhibited no effective cross-check whatsoever. Each initiated an action without glancing over to notice that the wingman was either distracted, confused, or not in a position to safety react to the event. The proposed plan teaches flight leads to cross-check when they initiate action that requires a deconfliction response from the wingman. This single, low-effort measure would have easily prevented all five of these crashes, saving the lives of four pilots.

We've seen that properly addressing any one of the three links in a typical accident chain is very effective in reducing collisions. Teaching all pilots to address all three links is exponentially more effective. Almost any of the 14 pilots in these 5 mishap flights could have prevented the collision at multiple links. Good deconfliction training would have prevented all five accidents with near certainty.

Improving our element deconfliction guidance also improves our mission effectiveness. A collision is a highly negative mission outcome: we've not only failed to accomplish that particular mission, but we've also lost the use of those aircrews and aircraft for all future missions. The safety techniques pilots must learn to keep track of their wingmen can be put to tactical use in keeping track of enemy aircraft in complex situations. Any pilot who demonstrates the inability to maintain awareness of his wingman is not only unsafe, but also unready for large force employment like Red Flag Exercises or actual combat.

Before we conclude this section, we'll note one final pattern: collisions are expensive. These five midair collisions cost four highly trained pilots and eight combat aircraft worth $144.6 million. That dollar figure does not include the value of human life, the cost to train the pilots or the cost of the accident investigation and aircraft salvage operations. The jets from our examples were older fourth-generation fighters valued at about $20 million. But now that fifth-generation fighters cost upwards of $100 million per copy, we're starting to talk about real money.

Innovation and Problem Identification

So why hasn't the USAF recognized the deconfliction problem? There has been ample opportunity. Midair collision is historically one of the leading causes of airborne Class A mishaps. Our five example accidents were drawn from a 10-year period (1997–2007) when Air Combat Command alone experienced 18 Class A element collisions involving 4 A-10s, 10 F-15s, and 22 F-16s. If we include Class B and C mishaps, the number grows to 26 collisions involving 52 aircraft.[11]

The accident reports from our five collisions are notable for two reasons. Firstly, three of the boards reached conclusions that were simply wrong. The reports from Kadena, Hill, and Misawa mention a failure to clear or deconflict flight paths even though the jets involved were displaced from each other's flight paths by 90, 60, and 90 degrees respectively. Lastly, all of the boards made some great observations that should have been captured in our element deconfliction guidance but were not. To consistently find these two failures in a series of accident reports is rare, troubling, and indicative of confirmation bias. The boards subconsciously selected and interpreted the data to fit to their preexisting belief that we have good deconfliction guidance.

The author has tried to alert the Air Force to its deconfliction problem. He has written two articles published in *Combat Edge* magazine, contacted the Air Force Safety Center, AFSO21, and attempted to engage leadership. The answer at every level was "we don't see the problem, so we aren't looking into it." The Catch-22 is that they won't see the problem *unless* they look into it. Given the high quality of Air Force officers, the deconfliction problem is inexplicable until we view it through the lens of confirmation bias. USAF education does address bias but tends to approach it from a historical perspective. Airmen study examples of biased decision making, along with the familiar warning that those who are ignorant of history are condemned to repeat it. The implication is that those who are familiar with history can avoid the mistakes of the past, so we think we have a good handle on bias, but cognitive science tells a different story.

Science tells us that history is a rich source of data, but that enlightenment only occurs after we synthesize the data to find patterns and causes. For example, in the early days of aviation pilots caught in clouds were taught to fly by the seat of their pants. We racked up a history of mishaps, each seeming to show how important it was for pilots to rely very carefully upon their senses to maintain attitude. Finally, we synthesized the data and discovered that our senses were easily duped by the peculiar motions of flight. Thus enlightened, we developed gyroscopic instruments. Now we teach pilots to rely upon their gauges because our senses lie to us.

Cognitive scientists tell us that our brains often lie to us. When we believe something, the bias resulting from our genetic proclivity for argument and persuasion naturally leads us to collect only the evidence that our belief is correct. Innovation requires us to search for evidence that our beliefs might be wrong. In short, an innovative Air Force doesn't argue with its innovators. Instead, the USAF must engage with its innovators to look for patterns and root causes that reveal new ideas and beliefs. This article provides the opportunity to do exactly that.

Here are the patterns to look for in our element collision records. These are simple yes/no questions that can be answered in a half-hour per collision. Every "yes" answer provides evidence that we need a new deconfliction plan. The 5 collisions we've examined have already produced 22 yes answers out of a possible 25, and studying additional formation mishaps will further confirm these patterns.

1. Were the flight paths clear before the collision?
2. Was bad formation or poor wingman consideration involved?
3. Did the flight lead just initiate an action requiring a deconfliction response?
4. Did the flight lead perform this action without cross-checking the wingman?
5. Did the wingman exhibit a slow cross-check, or fail to account for all jets in the flight?

Approaching the deconfliction problem with the mentality of a fighter debrief will produce two desirable outcomes. First, we will have solved an unrecognized safety problem that has the potential to save a squadron of aircraft worth more than a billion dollars during the next 10 years. That's not far-fetched: If we prevent only 1 collision per year, then that's 20 jets. As more fifth-generation fighters enter the fleet, we'll start to see single collisions that cost hundreds of millions.

The second outcome is harder to quantify but far more valuable. The deconfliction problem is not just a safety failure—it's also an innovation failure. If we are to learn from this, we must determine *exactly* what went wrong. The authors of *Air Force Tactics, Techniques, and Procedures* should have produced effective and compliant deconfliction doctrine but did not. The USAF Safety Center should have corrected the problem, but did not. Leadership should have stepped in, but did not. Applying a fighter debrief mentality to these issues will produce quantum improvements concerning tactics, doctrine, safety, professional military education, and our main subject: innovation.

Conclusion

We began with the axiom if it's not broke, don't fix it, and we'll end with the related axiom that necessity is the mother of invention. Although the USAF claims to value innovation, it has done little to address its blind spot for problem recognition. Time will tell whether it has a senior officer with the vision and leadership to recognize and fix the deconfliction problem before events make it necessary. Otherwise, the day might come when a *60 Minutes* news team knocks on the CSAF's door with a copy of this article, asking why we just had a $300 million F-22 collision that scattered flaming, toxic wreckage onto the community below.

A truly innovative Air Force is eager to exchange a good idea with a better one. The deconfliction example shows that today's Air Force is unwilling to exchange a terrible idea for an excellent one. Our current deconfliction guidance is ineffective, irrational, violates flight rules, lacks detail, and fails to incorporate lessons learned from collision reports. The proposed deconfliction plan corrects all of those issues while simultaneously improving mission effectiveness. But the USAF considers this to be a solution for a problem that doesn't exist, despite losing scores of aircraft to collisions.

RAND observed that the Air Force fails to innovate when it fails to see problems. Cognitive science supports and explains this observation as a byproduct of a brain that evolved to argue and persuade. Instead of seeing innovative solutions that better fit the facts, arguers see only the facts that fit their favored solution. But we can smell what we can't see, because argument always produces an odor. If we catch a whiff of contorted logic, omitted data, and refusal to consider alternatives, then that should alert us to an unseen problem and trigger the innovation process. The Air Force must train its nose. ✪

Notes

1. Adam R. Grissom, Caitlin Lee, and Karl P. Mueller, Innovation in the United States Air Force: Evidence from Six Cases, RAND Report RR-1207-AF (Santa Monica, CA: RAND, 2016): vii, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1207/RAND_RR1207.pdf.

2. Department of the Air Force, *The World's Greatest Air Force, Powered by Airmen, Fueled by Innovation: A Vision for the United States Air Force* (Washington, DC: Department of the Air Force, 11 January 2013), http://www.airuniversity.af.mil/Portals/10/CMSA/documents/Required_Reading/The%20World%27s%20Greatest%20Air%20Force_A%20Vision%20for%20the%20USAF.pdf.

3. Hugo Mercier and Dan Sperber, "Why Do Humans Reason? Arguments for an Argumentative Theory," *Behavioral and Brain Sciences* 34, no. 2 (2011): 57–111, http://www.dan.sperber.fr/wp-content/uploads/2009/10/MercierSperberWhydohumansreason.pdf.

4. Air Force Instruction (AFI) 11-202, Vol. 3, *General Flight Rules*, 10 August 2016, 22–23, http://static.e-publishing.af.mil/production/1/af_a3/publication/afi11-202v3/afi11-202v3.pdf; and AFI 11-214, *Air Operations Rules and Procedures*, 14 August 2012, 12, http://static.e-publishing.af.mil/production/1/af_a3/publication/afi11-214/afi11-214.pdf.

5. Maj Kevin J. Robbins, "Element Deconfliction in the Multibogey Arena," *Weapons Review Magazine* (Winter 1999): 4.

6. Executive Summary: *F-16CJ/90-0811 and F-16CJ/90-0801 Aircraft Accident Investigation*. Misawa AB, Japan: Pacific Air Forces, 13 November 2000, https://drive.google.com/file/d/0B9HnS7GIIWBxNzlmZU9tRW5UX1E/edit.

7. Executive Summary: *F-16CG/89-2006 and F-16CG/89-2001 Aircraft Accident Investigation.* Hill AFB, UT: Air Combat Command, 25 October 2002, https://drive.google.com/file/d/0B9HnS7GIIWBxV0xQQmQxNFFoaXM/edit.

8. Executive Summary: *A-10A/79-0191 and A-10A/80-0225 Aircraft Accident Investigation*. Nellis Air Force Base, NV: Air Combat Command, 4 December 2002, https://drive.google.com/file/d/0B9HnS7GIIWBxd01WeE8xaUFLN1U/edit.

9. Executive Summary: *F-16C/85-1555 and F-16C/86-0260 Aircraft Accident Investigation.* Hulman Field, IN: Indiana Air National Guard, 17 May 2004, https://drive.google.com/file/d/0B9HnS7GIIWBxNkJfTmhlQnpuRzg/edit.

10. Executive Summary: *F-15C/85-00093 and F-15C/85-0098 Aircraft Accident Investigation*. Kadena Air Base, Japan, 4 October 2004, https://drive.google.com/file/d/0B9HnS7GIIWBxeTVScGc0ZnlULXM/edit.

11. John Sellers, "Element Deconfliction Redux," *Combat Edge* 15, no. 8 (January/February 2007) 23.

Lt Col John S. Sellers, USAF, Retired

Lieutenant Colonel Sellers (BS, Yale University, MA, School of Advanced Air and Space Studies), a combat instructor pilot with 2,500 hours in the F-15C, also served in the Joint Doctrine Division at the Air Force Center for Doctrine and was director of the Qatar Combined Air Operations Center Combat Operations Division from 2003–2004.

The Air Force's Misconception of Integrated Air and Missile Defense

Col Craig R. Corey, USAF, Retired

Counterair has been the bedrock of theater air operations and is a critical enabler to the continued success of the joint force for decades. According to DOD Joint Publication (JP) 3-01, *Countering Air and Missile Threats*, counterair integrates offensive and defensive operations to attain and maintain the desired degree of control of the air and protection by neutralizing or destroying enemy aircraft and missiles, both before and after launch.[1] However, in the last few years, "IAMD," or integrated air and missile defense, has crept into the lexicon of combatant command operation plans, theater area air defense plans, Air Force instructions, and even USAF doctrine, gradually replacing long established terms such as *air and missile defense* (AMD) and *defensive counterair* (DCA), and inventing new terms such as *IAMD operations* and *IAMD forces*. This terminology is incorrect, and conflating IAMD with or supplanting DCA and AMD could have negative consequences for not only the Air Force, but joint operations writ large.

The Counterair Framework

While often perceived as Air Force-centric, counterair is a joint mission using air and surface assets from all of the services. Counterair is unique because it holds the enemy at risk by dominating the airspace while protecting friendly forces from the effects of enemy air and missile threats. The purpose of offensive counterair (OCA) is to destroy, disrupt, or otherwise neutralize the adversary's air assets (including cruise missiles), ballistic missiles, missile launch platforms, and supporting command and control (C2) networks and structures that enable them—before or after launch—as close to the source as possible. The OCA mission consists of attack operations, the suppression of enemy air defenses (SEAD), fighter sweep, and fighter escort, with the aim of controlling the air and preventing enemy launches of air and missile capabilities. DCA is a protection mission with the objective of destroying or neutralizing the adversary's air and missile assets and their effects when attempting to penetrate friendly airspace. AMD is all active and passive defensive actions

taken against hostile air and ballistic missiles threats.[2] Fundamentally, the USAF conducts DCA with AMD assets.

The integration of OCA and DCA occurs within the air operations center (AOC) and is the responsibility of the joint force air component commander (JFACC), with the JFACC commanding OCA and the area air defense commander (AADC) commanding DCA.[3] Normally, the individual who is designated as the JFACC by the joint force commander will also be designated as the AADC and the airspace control authority, although doctrinally the JFAAC and AADC could be two separate individuals given certain conditions. The AADC's responsibilities are extensive, and the two most important are to establish the integrated air defense system (IADS) and develop the theater area air defense plan (AADP). The IADS is comprised of active and passive AMD capabilities—the two key pieces of DCA of all the services' capabilities available in the theater—and consists of sensors, weapons, intelligence systems, associated personnel, and the C2 systems that integrate them together. The AADP prescribes the integration of active and passive AMD measures and the required C2 to implement the IADS and puts the comprehensive approach to defend against enemy air and missile threats into an executable format. While OCA and DCA are the two elements that comprise counterair, they are not autonomous from each other. This simultaneous offensive and defensive capability provides a credible deterrent to any adversary.

What IAMD Is and What It Is Not

At the joint level, IAMD is an "approach" that is supposed to "synchronize" DCA and OCA attack operations with other missions outside of the counterair framework, specifically homeland defense, global missile defense (cross-geographic combatant command boundaries), global strike when the target is associated with an air or missile threat; and counter-rocket, artillery, and mortar (C-RAM).[4] IAMD is *not* synonymous with counterair, nor is it a mission or an operation. Both the 2012 and 2017 versions of JP 3-01, *Countering Air and Missile Threats*, clarified the separation, and the 2017 version included a diagram attempting to show the relationship between the counterair mission and the IAMD approach. (See figure)[5]

Joint IAMD (separate from Army and Navy IAMD efforts primarily focusing on netting together integrated fire control networks and elevated sensors to counter tactical indirect fires, low and slow unmanned aerial vehicles, and cruise and antiship missiles at the service-level) began as a joint integrating concept (JIC) published in 2004. The JIC envisioned a holistic approach to countering air and missile threats across six broad mission areas: common battlespace awareness and understanding, C2 and battle management, OCA attack operations, active air defense, passive air defense, and joint logistics. It was a concept to support an acquisition strategy to develop new technology and processes and integrate them together to "defend the Homeland and US national interests, protect the Joint force, and enable freedom of action by negating an adversary's ability to achieve adverse effects from their air and missile capabilities" in the 2015 timeframe.[6] Since the JIC was published, these have been narrowed down to OCA attack operations, active air defense, passive air defense, and command, control, communications, computers,

intelligence, and reconnaissance (C4ISR). Coincidentally, these four mission areas were also the operational elements of Joint Theater Missile Defense (JTMD) and included in the 1996 edition of JP 3-01.5, Doctrine for Joint Theater Missile Defense. JP 3-01.5 was retired as a standalone joint publication many years ago, but the four legacy operational elements of JTMD are sometimes referred to today as the "four pillars" of IAMD, although that term has never been included in joint doctrine.[7]

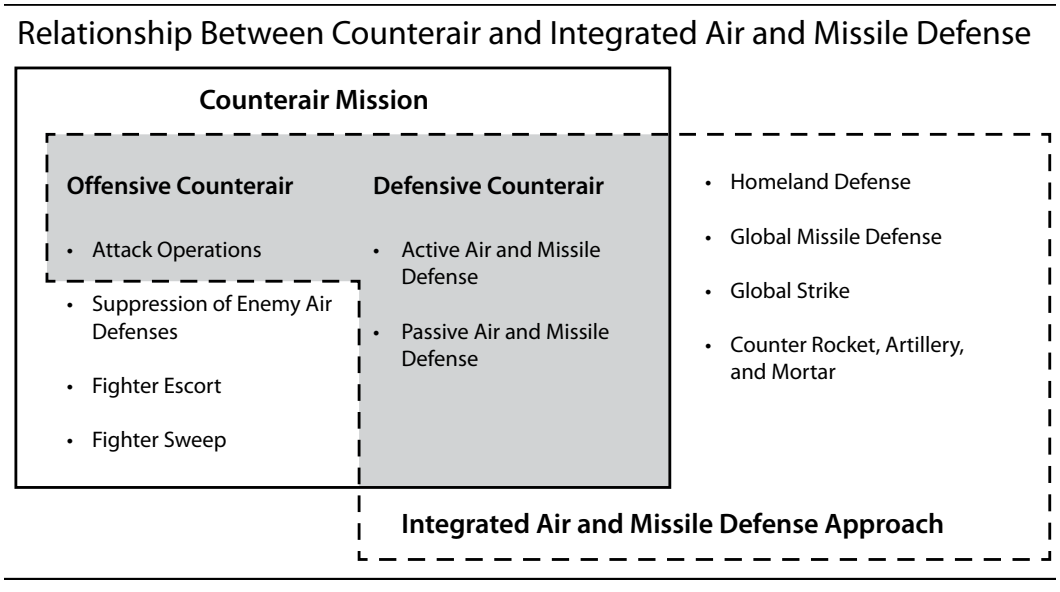


Figure. The relationship between counterair and Integrated Air and Missile Defense. JP 3-01, *Countering Air and Missile Threats*, 21 April 2017, I-3, http://www.dtic.mil/doctrine/new_pubs/jp3_01_20172104.pdf

In the following years, various concept and capabilities documents were developed outlining material requirements to bring joint IAMD to reality. Some of these solutions were a single integrated air picture (SIAP) that allowed battle managers to maintain high situational awareness and direct operations as needed; elevated sensors to overcome line-of-sight limitations, improve surveillance capabilities, and provide cued engagements; integrated fire control (IFC) so weapon systems can develop fire control solutions from nonorganic sensor sources and engage adversary assets remotely; and automated decision aids so commanders could make decisions at a faster rate and gain the advantage over the enemy by controlling the pace of the battle. Most of these were considered "critical" and "necessary" to achieve IAMD in the concept papers. However, none have come to fruition to the level envisioned, if at all.

SIAP has been a holy grail of visualization tools since the Tactical Air Control System/Tactical Air Defense system was launched in 1969.[8] Thirty years later, SIAP was a primary requirement in the joint theater air and missile defense vision—the forerunner to IAMD—to provide commanders with a view of the battlespace to improve coordination and decision making, as well as to permit everyone to understand the situation the same way.[9] However, SIAP proved too costly and technically challenging

and was cancelled by the secretary of defense in 2009. A lesser capability named the Joint Track Management Capability (JTMC) was pursued which greatly relied on the Army's Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS) and the Navy's Cooperative Engagement Capability (CEC). However, like SIAP, JTMC never materialized, in part, due to the bleak future of JLENS after one of the aerostats broke free in 2016 and drifted over several states before deflating and falling to the ground.[10] IFC systems and automated decision aids are in development by the Army, as well as the Navy's development of IFC systems that are part of CEC, but are years away from fielding.[11]

The oft-cited 2014 chairman of the Joint Chiefs of Staff's *Joint Integrated Air and Missile Defense: Vision 2020* lays out even more "imperatives," such as incorporating, fusing, exploiting, and leveraging "every bit of information available regardless of source or classification;" and targeting the development, modernization, and fielding of IAMD capabilities to fill gaps while "stressing affordability and interoperability."[12] The problem with these broad strategic vision statements is the vagaries are never translated into action. Like many "vision" documents, IAMD *Vision 2020* contained no resourcing solutions, no direction as to whom is responsible for achieving the broad platitudes, or any strategy to accomplish the objectives. *Vision 2020* articulates the need to invest in new technology, develop the technology into integrated weapons systems, and field these systems that are "melded into a comprehensive joint and combined force capable of preventing an adversary from effectively employing any of its offensive air and missile weapons."[13] However, using the old acquisition adage of you can have it good, cheap, or fast, but not all three, this just can't be done without sacrificing other programs and impacting readiness. Finally, *Vision 2020* stresses IAMD is beyond solely DOD activities, and must include other government agencies, thus making IAMD a national-level approach but lacking a national-level strategy.[14]

Another problem confronting IAMD is the lack of ownership. The Joint Integrated Air and Missile Organization (JIAMDO) plans, coordinates, and oversees joint AMD requirements, operational concepts, and operational "architectures."[15] However, JIAMDO, which is under the Joint Staff Force Structure, Resources, and Assessment (J-8) directorate, is a coordinating authority at best and is not empowered to compel the services or other offices to agree on issues. United States Joint Forces Command (USJFCOM) was the executive agent for joint IAMD; however, this responsibility was not officially passed to another organization when USJFCOM was disestablished in 2011. United States Strategic Command requested and was granted the role as Air and Missile Defense Integrating Authority in 2008, but a few years later asked to be relieved of this responsibility, which was approved in 2015. Finally, technical authority for joint IAMD was passed from JIAMDO to the Missile Defense Agency (MDA) in 2013, but unfortunately the resources to do it were not. The MDA, whose funding has been reduced significantly in the past few years, has little capability to focus on threats other than ballistic missiles, which is only part of IAMD.

In the end, IAMD isn't really very integrated. There is no operational C2 structure for IAMD from C-RAM at the tactical level, through counterair at the theater level, and cross-area of responsibility (AOR) operations and defense of the homeland at the strategic level. Joint IAMD is not a whole—it's merely the sum of its disparate

parts and provides no basis for terms such as *IAMD forces* or *IAMD operations*. With no dedicated IAMD material solutions for integration on the immediate horizon, no singular agency acting as the integrator or executive agent, and no C2 structure that integrates the disparate missions, joint IAMD is rudderless and remains largely a collection of operational concepts, requirements documents, and planning guides. So why is IAMD in joint and Air Force doctrine?

Confusion between Counterair and Integrated Air and Missile Defense

In 2010, the secretary of the Air Force and the chief of staff of the Air Force (CSAF) endorsed a white paper on the relationship between counterair and IAMD.[16] The paper established IAMD as a subset of counterair, using as justification the statement "IAMD is a Joint Requirements Oversight Council (JROC) – approved subset of the counterair mission." The white paper was primarily focused on the need for better cross-combatant command AOR integration, development of better missile warning systems, and development of air-launched ballistic missile interceptor technology. It also instructed the Curtis E. LeMay Center for Doctrine Development and Education to incorporate IAMD into its service doctrine.

IAMD was subsequently incorporated into Air Force Doctrine Annex 3-01, *Counterair Operations*. It states that the IAMD approach is a subset of counterair and cautions that IAMD has the potential to split offensive and defensive activities and fracture unity of command and unity of effort. It therefore instructs "Airmen should always advocate the counterair framework vice IAMD when discussing countering air and missile threats, even in a joint context."[17] It clearly specifies that OCA attack operations are commanded by the JFACC and DCA operations are commanded by the AADC, with the JFACC responsible for the integration of offensive and defensive components of IAMD. However, it also goes further and explains OCA attack operations will be planned and executed within the larger offensive campaign against the adversary targets and conducted simultaneously with suppression of enemy air defenses (SEAD), fighter sweep, and fighter escort operations.

However, the original statement above implying that the JROC approved IAMD as a subset of the counterair mission is elusive and, so far, unverifiable whether it was specifically contained in a JROC memorandum or another JROC-approved document. Joint doctrine does not recognize IAMD as a subset of counterair, nor does any other service's doctrine, and the Air Force's position may be a loose interpretation of the 2008 *IAMD Operational Concept*. This concept was approved by the JROC and was heavily focused on OCA attack operations and DCA, and less on the tactical level and missions beyond the AOR. There are three reasons why it is not in the best interest of the Air Force to consider IAMD as a subset of counterair.

First, IAMD serves no operational purpose within the theater-level counterair construct. As mentioned earlier, OCA attack operations will be conducted and integrated simultaneously with the other elements of OCA as part of the JFACC's counterair campaign. Viewing IAMD apart from counterair misses the broader operational approach envisioned by the JFC, and the JFACC's staff will need to plan for that. Even though the AOC is the C2 center for theater counterair operations, it will

still be the JFACC's C2 center for certain missions beyond the theater such as global strike or cross-AOR operations. If there is an air or missile threat emanating from another AOR, the theater commander at risk will be designated the supported commander and that AOC will coordinate with the supporting AOCs to synchronize operations. If the cross-AOR threat is deemed significant, persistent, or more than just air and missile defense, a joint operations area crossing AOR boundaries may be established with clear C2 structure and supported/supporting relationships specified in the establishing directive. The IAMD approach does nothing at the theater level that isn't already being accomplished through the counterair framework.

Second, by putting a fence around IAMD at the theater level and saying IAMD is a subset of counterair, the Air Force has confused planners, operators, and those assigned to AOCs, and has led to doctrinally incorrect instructions within its own service. Air Force Instruction 13-01AOC (Volume 3), *Operational Procedures–Air Operations Center*, states IAMD is the responsibility of the defensive operations team, which has "oversight of the overall coordination of global, IAMD for the theater, and execution of theater operations."[18] Since the IAMD approach includes OCA attack operations, this gives the impression the defensive operations team, and the AADC, are responsible for OCA attack operations. This is incorrect. Doctrinally, the defensive operations team is responsible for AMD within the theater, not IAMD, and the AADC, through the defensive operations team, makes targeting recommendations to the JFACC for OCA attack. Courseware within the 505th Command and Control Wing, teaching AOC operations to personnel assigned to AOCs, teaches "(t)he IAMD Cell is responsible for the execution of IAMD within the Counterair framework."[19] This also implies the IAMD cell executes OCA attack operations. Finally, Air Force Tactics, Techniques, and Procedures (TTP) 3-1.AOC erroneously quotes JP 3-01 as stating "IAMD is the application of the counterair framework at the theater level." It is incorrect since IAMD does not include SEAD, fighter sweep, and fighter escort—the other parts of the counterair framework and not part of IAMD. The application of the counterair framework at the theater level is simply counterair.

In 2015, *Air & Space Power Journal* published an article suggesting, among other things, the "I" in IAMD is made possible by C2, and described how the Air Force major command commander, as the JFACC, relied on the AOCs in the theater for "IAMD operations."[20] That's technically correct, but it's factually wrong. The AOC does exercise C2 over the theater-level missions that are enveloped under the IAMD approach, but it's because they are counterair missions, not because they are part of the IAMD approach. AOCs were developed before the inception of IAMD to plan and execute the C2 of counterair operations within the theater and oversee AMD in the theater.[21] The "I" is implied within the Air Force and joint definition of AMD.

The 2012 version of JP 3-01 stated the geographic combatant commander is responsible for IAMD within the theater. This may have been misinterpreted or assumed to be a mission that the JFACC would have responsibility for, but no mention was made in the publication that this could be operationally delegated to any component commander. The 2017 edition of JP 3-01, just as Air Force doctrine, is very clear that the JFACC commands OCA, the AADC commands DCA, and the JFACC is responsible for the integration of the two. Since IAMD is not a mission or operation, JP 3-01 does not address the command or authority of IAMD, only that the integration

of the offensive and defensive counterair components of IAMD is the responsibility of the JFACC.[22]

Third, IAMD is too broad to plan for in the joint planning and execution community. Current CCMD operation plans (OPLANS) consistently use opaque and inaccurate terms such as *IAMD operations* and *IAMD forces*, usually in an IAMD appendix to the operations annex. However, the focus of these appendices is always on theater-level AMD. If OCA attack operations are discussed, it's for the purpose of pointing out the coordination required with the offensive operations team. C4ISR systems are also discussed, but these are systems that were developed for support of overall counterair operations, not IAMD. Due to the multiple missions that are under the broad concept of IAMD, the logistics planners who develop the time-phased force and deployment data, the TPFDD, will need more granularity on what types of forces should be planned for to support an OPLAN. *IAMD forces* and *IAMD operations* would encompass C-RAM, air defense artillery batteries, multiple launch rocket systems, squadrons of fighter aircraft, ships, and on and on—many of them multimission platforms. These are vague and obfuscated terms of reference and serve no purpose in an environment where specificity of types of capabilities and gaps are needed to develop plans that execute operations. This propagates inaccurate and confusing planning and execution documents with statements, such as "IAMD of the DAL," when discussing how assets on the defended asset list will be protected, "conduct IAMD with DCA in support of the JFC" when describing a line of effort to support the JFC's operational approach, and identify the theater AADC as the "supported component commander" when describing the air component's authority level.[23] Merely telling the JFC the joint force will conduct or is conducting IAMD operations does not convey a picture useful in supporting the JFC's operational approach.

The bottom line is AMD is already integrated at the theater level through the AOC. Putting an "I" in front of AMD serves no purpose in Air Force doctrine. More importantly, it has the potential to split offensive and defensive activities and fracture unity of command and unity of effort. AOC directors, deputy directors, and IAMD cell members will dutifully say IAMD is a subset of counterair in Air Force doctrine, but seldom if ever follow up with "but Airmen should always advocate the counterair framework vice IAMD when discussing countering air and missile threats."[24]

Moving Forward

IAMD is a valuable term for developing acquisition strategies for air and missile defense systems. "Integrated air and missile defense" is a clear, albeit bumper sticker, umbrella phrase that easily points out to even those unfamiliar with military operations what our objectives are when procuring weapons and C2 systems. But integration is a continuous process and one that we have been doing for many years and will continue to do as more and better technology and processes evolve. IAMD is not a condition that can be achieved in the sense that we achieve air superiority; nor can it be conducted like DCA or OCA are conducted.

It's in the best interest of the Air Force to stress the primacy of counterair. This needs to come from the top of the Air Force leadership. The following are some suggested actions the Air Force could take:

- Delete "theater-level IAMD" from Air Force doctrine since it's redundant to the current discussion of counterair contained in the Air Force Doctrine Annex 3-01 and confuses the separation of counterair and IAMD. Air Force doctrine should instead focus on how C2 of theater-level air and missile defense operations should be integrated with missions beyond the theater that impact the JFC and/or JFACC operations.
- Review Air Force instructions and TTP to ensure terminology is consistent with Air Force and joint doctrine. It is clear there is confusion in Air Force instructions between IAMD and AMD in the theater—that without the "I" in front, AMD somehow is not integrated—but AMD is much more accurate since it is specifically defined as all active and passive defensive actions taken against hostile air and ballistic missiles threats, instead of the broad definition of IAMD.[25]
- Review current Air Force training curriculum to ensure that personnel understand the integration of the two halves of counterair, the responsibilities of the JFACC and AADC, and how DCA is commanded and controlled. There are too many invented definitions and a consistent misunderstanding of what IAMD is, and its relationship to counterair.
- Develop TTPs for split operations when the JFAAC and AADC are not collocated. Hawaii's emergency management agency is developing preparedness plans for their islands in case of a North Korea missile attack due to the concern that so much key military infrastructure is based in their state that it could make them a target for hostilities.[26] A key component of passive AMD is the dispersal of assets. This dispersal could include CCMD and component leadership and headquarters, but we seldom exercise this level of continuity of operations if C2 centers have to transfer responsibilities to other commands and locations. It's a common assumption the JFAAC will always be dual-hatted as the AADC and operate at the theater AOC. However, with the range and proliferation of ballistic and cruise missiles, theater AOCs are vulnerable to attack which could negatively impact the ability to conduct JFAAC and AADC responsibilities at the same location. With the expanding missile capabilities of adversaries in the Pacific and Europe, JFACC responsibilities could relocate to the continental United States if the AOC cannot be defended, while the Army air and missile defense command commander or the Navy component commander could assume the duties of the AADC, and remain in theater.
- Finally, the CSAF should consider sending a "personal for" message to AOC directors and deputy directors emphasizing the primacy of the counterair framework as opposed to the IAMD approach. This message should emphasize to them that, in their course of duties at the AOC, they should always advocate the counterair framework versus IAMD when discussing countering air and

missile threats, or otherwise risk splitting offensive and defensive activities and fracture the unity of command and unity of effort.

If the Air Force believes that IAMD has the potential to fracture the unity of command of counterair, then it's a problem largely of its own making. Counterair is at the core of the USAF's existence, yet it has incrementally allowed IAMD to take the place of counterair in both lexicon and practice. *IAMD* is a good term to use for acquisition programs of systems that will provide the commander greater visualization tools and battle management aids to allow quicker decisions and quicker action, but the integration of air and missile defense has been a continual process and the reason that the Air Force developed AOCs. The USAF needs to be at the forefront of the intellectual discussion of counterair and IAMD, but it is not. At least it is not now. ✪

Notes

1. Joint Publication (JP) 3-01, *Countering Air and Missile Threats*, 21 April 2017, I-3, http://www.dtic.mil/doctrine/new_pubs/jp3_01_20172104.pdf.
2. Ibid. Pages I-4 through I-7 include the definitions for offensive counterair (OCA), defensive counterair (DCA), and air and missile defense (AMD).
3. Ibid., II–9.
4. Ibid., I–1.
5. Ibid., I–12.
6. Jason Cutshaw, "SMDC Leads the Way for Integrated Air, Missile Defense, 1 July 2015, http://www.theredstonerocket.com/military_scene/article_90d09a80-1ffa-11e5-bc78-1336e3b535cd.html.
7. JP 3-01.5, *Doctrine for Joint Theater Missile Defense*, 22 February 1996, I-4, https://www.hsdl.org/?abstract&did=3748.
8. Committee to Review DOD C4I Plans and Programs, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, DC: National Academies Press, 1999), 40, https://www.nap.edu/catalog/6457/realizing-the-potential-of-c4i-fundamental-challenges.
9. Herbert C. Kaler, Robert Riche, and Timothy B. Hassell, "A Vision for Joint Theater Air and Missile Defense," *Joint Force Quarterly* 23 (Autumn/Winter 1999–2000): 65–70, http://www.dtic.mil/dtic/tr/fulltext/u2/a525453.pdf.
10. "JLENS: Coordinating Cruise Missile Defense—And More," *Defense Industry*, 13 February 2017, http://www.defenseindustrydaily.com/jlens-coordinating-cruise-missile-defense-and-more-02921/.
11. Jen Judson, "Army Anti-Missile Command System's IOC Delayed Four Years," *Real Clear Defense*, 25 May 2017, http://www.realcleardefense.com/2017/05/25/army_anti-missile_command_system039s_ioc_delayed_four_years_293397.html; and Sydney J. Freedberg Jr., "We CAN Tie Army, Navy Missile Defense Networks: Navy Experts," *BreakingDefense*, 24 February 2017, http://breakingdefense.com/2017/02/we-can-tie-army-navy-missile-defense-networks-navy-experts/.
12. Chairman of the Joint Chiefs of Staff, "Joint Integrated Air and Missile Defense: Vision 2020," 27 January 2014, 4, http://www.jcs.mil/Portals/36/Documents/Publications/JointIAMDVision2020.pdf, 4.
13. Ibid.
14. Ibid., 1, 3.
15. The Joint Staff, "Department of Defense Fiscal Year (FY) 2017 Request for Additional Appropriations," March 2017, 13, http://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2017/budget_justification/pdfs/2017MarchAmended/03_RDT_and_E/TJS_FY17_RDTE_ABS.pdf.
16. The Office of the Secretary of the Air Force, and Chief of Staff, United States Air Force (USAF), "Integrating Air and Missile Defense: Incorporating Ballistic Missile Defense within the Counterair Framework," 3 June 2010.

17. USAF, *Annex 3-01 Counterair Operations: Counterair Framework* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education), 27 October 2015, https://doctrine.af.mil/download.jsp?filename=3-01-D08-AIR-Framework.pdf.

18. Air Force Instruction 13-1 AOC 3, *Operational Procedures—Air Operations Center (AOC),* 2 November 2011 (incorporating change 1, 18 May 2012), http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi13-1aocv3/afi13-1aocv3.pdf.

19. "AOC Initial Qualification Training Student Guide," 505th Training Squadron, Hurlburt Field, FL, 16.

20. Kenneth R. Dorner, Maj William B. Harman, and Maj Jason M. Teague, "Back to the Future," *Air & Space Power Journal* (*ASPJ*) 29, no. 1 (January–February 2015): 61, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-29_Issue-1/ASPJ-Jan-Feb-2015.pdf. This article attempts to explain the Pacific Air Forces "IAMD strategy," building on three vignettes from World War II, the Cold War, and post–Cold War, and focusing on DCA and OCA attack operations. However, what the authors posit as "IAMD"—whether in the historical examples or PACAF's current strategy—are merely the normal plans and operations that combatant commands and their components have been conducting for a long time, such as working with allies and partners, hardening bases, dispersing assets when needed, preparing defense plans, and integrating new service capabilities such as the AOC, Aegis ships, and Patriot defense system; into the overall command and control structure of their theater plans. In the Spring 2017 issue of *ASPJ*, an article was published stating "counter-AMD" is a construct "broken into two primary areas: OCA and DCA" (Maj Dillon R. Patterson, "Defeating the Threat of Small Unmanned Aerial Systems"). This is also incorrect since neither the Air Force or joint doctrine uses "counter-AMD," and OCA and DCA are obviously the missions of counterair. "Counter-AMD" would likely be considered suppression of enemy air defenses.

21. Maj J. Taylor Sink, *Rethinking the Air Operations Center: Air Force Command and Control in Conventional War*, (Maxwell Air Force Base, AL: the School of Advanced Airpower Studies, academic year 1992–1993), 2.

22. JP 3-01, *Countering Air and Missile Threats*, II-9.

23. Personal observations from Chairman of the Joint Chiefs of Staff exercises.

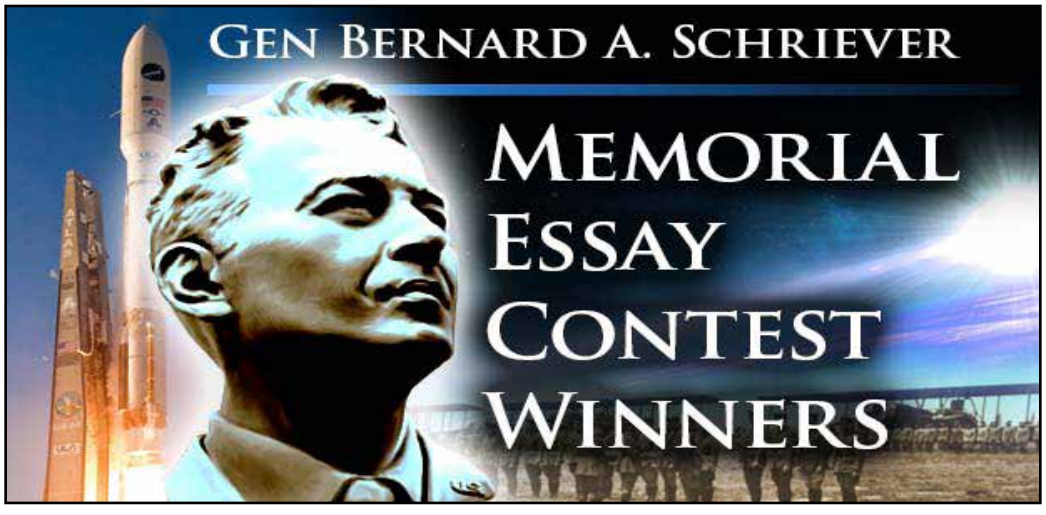
24. USAF, *Annex 3-01 Counterair Operations.*

25. Ibid.

26. "Hawaii Rolling Out Preparedness Plan for North Korean Missile Attack," 21 July 2017, https://www.washingtonpost.com/news/morning-mix/wp/2017/07/21/hawaii-rolling-out-civil-defense-plan-for-north-korean-missile-attack/?utm_term=.5adb8f0e05bf.

Col Craig R. Corey, USAF, Retired

Colonel Corey (BA, MPA, Memphis State University) retired from the US Air Force in 2011 after 26 years of service. During his career, he flew C-130s in Europe, Southwest Asia, and in the Asia-Pacific. He was also an associate professor of Military Art and Science at the US Air Force Academy, a country desk officer in the office of the Deputy Undersecretary of the Air Force for International Relations, a deployable training team chief for US Joint Forces Command, and an action officer and speech writer on two four-star commander's action groups. Colonel Corey served in Operations Desert Shield and Desert Storm, Allied Force, and Iraqi Freedom. He is currently a civilian in the Joint Force Development Directorate of the Joint Staff.



In the name and memory of a great Air Force pioneer, the Lance P. Sijan Chapter of the Air Force Association, in partnership with the *Air & Space Power Journal*, is pleased to announce the winners of the Gen Bernard A. Schriever Memorial Essay Contest. The purpose of the contest is to stimulate thought, discussion, and debate on matters relating to how the Air Force and Air Force Space Command provide space and cyberspace capabilities for the joint force and the nation.

First Place: Capt Michael Nayak, USAF, PhD

"Deterring Aggressive Space Actions with Cube Satellite Proximity Operations: A New Frontier in Defensive Space Control"

Runner-up: Lt Col Mark Reith, USAF, PhD

"Brandishing our Air, Space and Cyber Swords: Recommendations for Deterrence and Beyond"

Honorable Mention

Roberta Ewart, **PhD**, "Persistent Space Situation Awareness for the Guardians of the High Frontier"

Capt Keith Nordquist, **USAF**, "The New Matrix of War: Digital Dependence in Contested Environments"

Capt Isaac Nacita, **USAF**, "Cyber War and Deterrence—Applying a General Theoretical Framework"

Deterring Aggressive Space Actions with Cube Satellite Proximity Operations

A New Frontier in Defensive Space Control

Capt Michael Nayak, USAF, PhD*

Today, America's strategic advantage and military superiority are critically codependent on its space superiority.[1] Space-based systems provide critical information, intelligence, warning, and communication capabilities to commanders and warfighters across the spectrum of global conflict. As the reliance of the military enterprise on the effective use of space power grows, top leaders are consistently sounding the warning bell about a growing vulnerability to hostile action.[2] Calling the US dependence on space its "soft ribs," one Chinese analyst writes, "for countries that can never win a war with the United States by using [. . .] tanks and planes, attacking the U.S. space system may be an irresistible and most tempting choice. Part of the reason is that the Pentagon is greatly dependent on space for [. . .] its military action."[3] It is, therefore, no surprise that countries such as China, Russia, and India have chosen to aggressively invest in counterspace capabilities.[4]

Within this operating picture, it is vital to note the considerable recent progress of nanosatellites called *Cube Satellite* or *CubeSat*-sized spacecraft. A standard 1-unit (U) CubeSat form factor is 10 cm x 10 cm x 10 cm in dimensions, 1 liter in volume, and weighs approximately 1 kg in mass.[5] The number of CubeSat segments designates system size; a 10 x 10 x 30 cm system is a 3U, and a 10 x 20 x 30 cm system is a "6U" CubeSat, roughly 3 and 6 liters in volume respectively. Developed in the 1990s to train students in real-world satellite integration and testing, government and private entities have launched more than a thousand CubeSats.[6] Science requirements for sophisticated instruments, communications, propulsion, and three-axis

*This work is adapted from two other works by the author, "Cube-Satellite Proximity Operations: The Natural Evolution of Defensive Space Control into a Deterrence Initiative," published in *The Space Review* 18 January 2016; and "Fighting a War in Space: An Unusually Careful Selection of Staff," (in journal review as of October 2017) in *Astropolitics*.

stabilization have been demonstrated.[7] The commercial utility of CubeSats are increasing exponentially; the firm Planet Labs has launched more than seventy 3U CubeSats for responsive earth imaging.[8]

Extrapolating the explosive growth of satellite system miniaturization to a national security context, CubeSat systems are easier for adversarial nations with less sophisticated space programs to design, build, and launch. In considering the question of what the United States should do to better prepare to deter aggressive action in space, an active deterrence strategy to effectively combat small satellite-enabled hostile actions is of vital importance. In parallel with the development of new deterrence strategies that consider small satellites,[9] taking immediate steps to direct integration of CubeSat technologies into the US military space enterprise can help the United States respond proportionally and prevail should deterrence fail.

The Threat from Nations with Less Advanced Space Programs

In less than a decade, space miniaturization technology has come so far that students at a high-school level of education are now capable of designing, integrating, launching, and operating CubeSat systems.[10] Some university-designed systems boast sophisticated maneuvering and navigation capabilities and are capable of advanced military-relevant mission sets.[11] From a doctrinal and policy point of view, it is important to consider that CubeSat systems are far easier for nations with less sophisticated space programs to design, build, and launch. The price of failure in the small-satellite industry is less, making incremental growth more practicable. With the elimination of a need for heavy space lift and triple-redundant systems, it is almost certain that adversarial nations with smaller space programs can soon assemble and field capabilities they are today incapable of. It is feasible that within the next decade, we will see North Korea fielding a surveillance capability via a crude optical sensor on a CubeSat, in competition with South Korea, which is today developing a CubeSat-based telescope system.[12] Equally probable is Iran fielding a rudimentary missile warning system onboard a vehicle similar to the "Promise of Science and Industry" national satellite, recently built by Iranian university students and launched atop a modified long-range missile.[13]

Although systems centered on smaller spacecraft may not be as reliable, these development efforts prove that the technology is both mature and accessible. Today's clumsy student satellite feeds tomorrow's "wisdom of experience." Today's school-bus sized communication spacecraft (for example, the MUOS, the Mobile User Objective System) will tomorrow be the size of a shoebox (for example, lasercom on LADEE, the Lunar Atmosphere and Dust Environment Explorer).[14] Combining easy fabrication with access to space via ride-shares, small satellites are becoming a force to be reckoned with. At the rate of current development, the United States might find some of its actions or objectives deterred by the capabilities of its adversaries in the near future.

As it stands today, an adversary with basic space lift capability may be able to deny, disrupt, or degrade the US military enterprise by striking a few centers of gravity (COG) of space power that fulfill a critical defense or military enabling function.

This can be accomplished either through a direct-ascent antisatellite (ASAT) weapon, or a co-orbital ASAT weapon, where a satellite is placed into a similar or intercepting orbit as its target, and then maneuvered into a collision course with it. This threat dates back to the Cold War and the USSR's *Istrebitel Sputnikov* program.[15] Translated as *satellite killer*, the program focused on satellites capable of large maneuvers to rendezvous with their targets, prepositioned to execute a "kamikaze-style" takedown of US space systems if and when commanded.[16]

One immediate deterrent to hostile space action is therefore to distribute the US concentration of space power, lessening the reward for hostile action. Fielding duplicate, redundant systems to those in existence is unrealistic in a fiscally constrained environment. Distributed or disaggregated systems, on the other hand, are intrinsically less vulnerable. Since the capability is exerted through a larger number of redundant component parts, multiple component satellites can be lost before total system failure. The exploding growth of CubeSats, which have a reputation for being low-cost and easily reproducible, has a natural place in this discussion.[17]

While there are definite cost and size advantages to CubeSats, they are also significantly less capable than larger spacecraft, particularly in military applications. Larger spacecraft can lose multiple components and still have backup functionality. They host larger instruments better capable of fulfilling primary military functions. CubeSats are largely "single-string," not robust to single-point failure, and are size- and volume-limited in the instrumentation they can host. They are simply not a factor in signals intelligence, hyperspectral collection, or protected survivable secure communications. While they can fill a complementary role in ground-based imaging and imagery intelligence collection, larger optics, wider wavelength bands, and the need for cryocooling will always point in the direction of larger spacecraft.

The forte of CubeSats appears to be in the "numbers game." Even in the absence of direct conflict, a disaggregated system allows for cost and efficiency benefits in acquisition and operations. Such systems are resilient by nature. A distributed systems architecture serves to eliminate the US dependence on finite COGs of space power; with multiple systems in play, the payoff for an attack lessens. Therefore, in an environment where any small satellite in a similar orbit to a national security asset could be a potential ASAT threat, American space policies must ensure that capabilities in this arena are not left behind.

However, military space acquisition policy and business practices are both behind the times. Although policy papers by recent space acquisition leaders lean in favor of disaggregation, there has yet to be a push to implement this through enterprise leverage of small-satellite technology.[18] The only US government organizations actively involved in CubeSat development are either doing so for research and development (R&D) or because of cost constraints; the resolve to make small satellites a part of our national space architecture is simply not present. However, these systems are set to become an integral part of every other space-faring nation's military capability, likely within the next generation.

Therefore, there is an immediate need for decisive leadership action to focus US space acquisitions and operations into smaller, more agile systems, and more importantly, transition these capabilities into the mainstream "operational" space industry directly benefiting the warfighter. This will drive a strategic investment

that will reduce the risk to space COGs. It will also support direct integration of small satellite technology into the national space enterprise, both military and civilian. Deploying mature technologies in parallel with ongoing R&D efforts for further development can help the United States widen the conversation on possible proportional and reciprocal dissuasion of enemy counterspace action, and preserve the "ultimate high ground" of space.

Applications of Cube Satellite Technology to Space Control

Any hostile action against a US spacecraft is considered tantamount to a declaration of war.[19] However, in reality, the distance of and limited access to space provides anonymity to offensive space actions, similar to cyber attacks. It is more likely that to maintain regional superiority, adversarial nations would seek to develop a denial of service counterspace capability against the United States. A satellite malfunction could be caused by space environment conditions, faulty, or inadequate satellite design, or even orbital debris factors.[20] Culpability, attribution, and retaliation are complicated by the lack of borders or sovereign regions in space and the infeasibility of total space situational awareness (SSA). This adversary may, therefore, be able to deny, disrupt, or degrade the US military space enterprise while maintaining plausible deniability. The uncertainty involved increases exponentially if hostile CubeSats are deployed as co-orbital ASAT devices. A low-velocity impact can be engineered to have just enough speed to shatter the impactor, causing disabling damage to the target, and leaving relatively little debris.

However, this is the crudest use of CubeSat technology as a counterspace tool. Rendezvous and proximity operations (RPO) are the ultimate tools for space surveillance, advanced space-based SSA, and even offensive action. In 2005 and 2007, respectively, the United States proved an experimental RPO capability with missions such as the Air Force Research Laboratory's XSS-11 and the Defense Advanced Research Projects Agency's Orbital Express.[21] While Orbital Express was more than 1,000 kg in mass and fielded two spacecraft that were aware of each another, XSS-11 was 150 kg and demonstrated advanced maneuvering around its own spent upper stage. It demonstrated the capability to safely approach an "uncooperative" object, image it, and retreat to a safe distance.

Small satellites in space control are not a near-future scenario; rather, they are today's emergency. China has developed a small satellite reputedly able to capture another satellite with a robotic arm.[22] Published work by US academic authors discusses the concept and ongoing design of a CubeSat-sized RPO mission, with precise attitude determination and control, pointing accuracy, real-time maneuver commanding, and even optimal trajectory design for docking applications from a future CubeSat platform.[23] A 10–25 kg (12U) CubeSat with optical sensors and agile maneuvering capability is a configuration that is easily achievable with today's technology; such vehicles have a negligible radar cross-sectional area. In geostationary orbit, they would be invisible from the ground.

Further, the delivery system for CubeSat is easily configurable. CubeSats can be released from stowed configurations designed to ride along with any launch vehicle.

Launch options include hosted payload services, a quickly growing industry that government payloads have utilized as secondary missions on commercial communications satellites. These payload services provide numerous launch opportunities per year to any desired orbit regime. This has even expanded to the commercial sector; international telecommunication satellites, as well as national security satellites, have demonstrated the capability to host CubeSats.[24]

As this technology becomes smaller and easier to launch, the detectability factor significantly decreases, which would allow adversaries to take autarchic actions against the US space enterprise with a lessened fear of retribution or discovery. One example is the Russian object 2014-28E. Initially thought to be drifting space junk associated with the launch of three Russian telecommunication satellites, it has since been observed to be maneuverable, and made a close approach to the rocket stage that boosted it into orbit as recently as November 2014.[25]

Apart from *satellite killer*, another translation of *istrebitel sputnikov* is *satellite fighter* (*istrebitel* translates as *fighter aircraft*). The big push in next-generation fighter aircraft is stealth, and it is not unreasonable to refer to small satellites as the stealth aircraft of space. The existence of 2014-28E was not announced, and the smaller the spacecraft, the less the probability of ground-based detection. If sensor avoidance techniques are employed during an approach, the target object may not ever detect another satellite in its local space.[26] Cumulatively, this reduces the culpability for space control actions, emboldening adversaries to move past proximity surveillance to offensive actions. . . all from a CubeSat platform.

RPO-capable CubeSats have the potential to be of critical importance to space-borne intelligence gathering. They are capable of close approaches, surveillance, functionality, and material characterization, and battle damage assessment, all with a minimal fear of discovery. Even if discovered, close approaches are legal if they do not endanger the operation of the target body. Sociopolitical ramifications are likely inside a certain approach distance, but this is a gray area without much legal precedent or policy backing.[27]

This expanded reach of space-borne space control is the true jump in capability presented by burgeoning CubeSat technology. Never before has there been the capability for a force so large to be wielded from a body so small. CubeSats are poised to become the stealth aircraft of space technology. A nation capable of wielding a CubeSat-based offensive space control capability creates a real and present threat to US space superiority. This article will next address what the United States can do to deter aggressive action in space concerning this threat, and prevail should deterrence fail.

Combating the Threat of Hostile Cube Satellite Actions

One of the key factors for successful deterrence is the criterion of "proportionality, reciprocity, and coercive credibility." The more superior a nation's available instruments to inflict harm, the larger costs for non-compliance it may credibly impose.[28] The dissuasion of enemy escalation is accomplished by the threat of progressive retaliation, discouraging the enemy from an initial action.[29] The political will to exert this response is never in doubt.[30] The concept of proportionality drives the US's re-

taliatory action, but in the arena of space deterrence, each unique attack requires a unique response.

Three steps of escalating response and consequence are detailed below, derived from principles of force protection conditions (FPCON).[31] The proposed staged strategy ensures that the US response is proportional to the existing threat while maintaining both strategic advantage and technological superiority.

The base of the CubeSat threat pyramid may be considered to be FPCON Alpha, where there exists "a general threat of possible terrorist activity, the nature and extent of which is unpredictable."[32] This translates to no known deployment of RPO capability by an adversarial nation or RPO missions in a first-time R&D regime only. Given this threat level, a security posture of deterrence through ground detection and observation is proportional and must be capable of being maintained indefinitely. Methods currently utilized today, such as the Space Fence, the Space Surveillance Network, and the Space-Based Space Situational Awareness system are able tools for maintaining this ability to attribute.[33]

The next level on the CubeSat threat pyramid is FPCON Bravo, when "an increased and more predictable terrorist threat activity exists."[34] The threat increases when specific intelligence suggests the capability for possible aggression by a particular nation and is realized when there is a known, operational RPO capability beyond the first-time R&D phase. If an adversary is aware that their technology is sufficiently advanced that it may be able to attack and escape undetected, this can create an incentive to act. Dissuading an adversary nation from exercising mature RPO capabilities requires an escalation in the US's ability to detect and respond to such an action. Amputating the veil of invisibility around co-orbital RPO CubeSats can have a sizable impact on the political will to act. The small size and detectability of inbound CubeSats imply that ground-based SSA is likely inadequate to accomplish the objective of dissuasion by detection. The onus for deterrence falls on the shoulders of space-based SSA mission sets.

The implementation of a similar policy can be inferred with regard to recent news reports concerning the GEO Space Situational Awareness Program (GSSAP).[35] GSSAP mission sets were announced to the world by then-USAF Space Command head Gen William L. Shelton.[36] "GSSAP will bolster our ability to discern when adversaries attempt to avoid detection," General Shelton said at the 2014 Air Warfare Symposium, "and to discover capabilities they may have which might be harmful to our critical assets."[37]

The protection of space assets in the event of more direct threats is the final level on the threat pyramid and has larger geopolitical consequences, including impacts to warfighters in harm's way. Nations with less accomplished space programs are capable of developing CubeSat technology; these nations are also less likely to adhere to the classic psychology of deterrence. The threats become more diverse and immediate as well: for example, command of a co-orbital satellite could be assumed by cyber-offense, at which point it becomes an unintended ASAT weapon.[38] Alternately, a known CubeSat could have an alternate purpose and later exploit holes in US detection capabilities to maneuver into a new orbit. By the time this satellite is reacquired, it could have caused harm to a high-value asset. To assign attribution, respond proportionally, and deter this kind of threat, the United States must be able

to characterize the motion, intent, and capability of inbound CubeSats, assign attribution, and avoid imminent harm to space COGs, all in a responsive manner.

Enabling the full awareness of local space in the vicinity of a high-value asset can ensure that any object, even CubeSat-sized, will be detected and characterized. The United States must, therefore, make a concerted effort to develop CubeSat RPO technology for utility in the operational realm, exert deterrence by possession of such space control capabilities, and employ these RPO-capable CubeSats in a defensive posture to perform proximity operations around high-value assets and monitor their local space. If justified and directed, interception attacks by the RPO "guardian" CubeSat may even be needed to ensure the safety of the asset.

Guardian CubeSats designed for RPO can ensure the safety and sanctity of local space, while simultaneously performing as a contributing sensor yielding information to global SSA systems. Designed for passive, autonomous proximity operations, such CubeSats would not interfere with the primary asset's mission. The presence of a responsive communication link between the Guardian and its high-value asset gives the COG sufficient time to maneuver out of the way of an interception. The Guardian would also be able to image the interceptor, perform orbital tracking, deliver responsive intelligence regarding the source of the attack, and provide a post-event battle damage assessment. This is apart from the deterrence aspect: the protective security function of the Guardian, the high likelihood of failure for hostile actions and subsequent negative consequences combine to dissuade the adversary from ever attempting the action. Critically, they also provide the United States the ability to respond to such an attack in a timely and proportional manner.

Conclusion

The natural evolution of a guardian paradigm becomes a truly revolutionary change to the status quo. Once the capability is established, and policy favors their continuous and rapid employment, deterrence becomes a function of uncertainty. In this scenario, Guardians are not deployed as continuous orbiters, but rather, "on demand." Designs exist for ride-along CubeSats within the spare storage space aboard commercial telecommunications satellites;[39] high-value assets could be similarly adapted to fit not one, but multiple RPO-capable CubeSats within their volume. In response to an increased threat or intelligence hinting at an impending attack, the high-value COG can deploy its Guardians to assess local space, determine threats, ensure safety, and provide responsive battlespace awareness. Deterrence by uncertainty can be achieved when adversarial nations are unable to determine if a particular target may (or may not) be hosting protector CubeSats within its volume. With the knowledge that these Guardians are RPO-capable, autonomous, and responsive to threats, the risk to invade the local space of a high-value asset will become too high to justify action, thus preparing the nation to deter aggressive action, while maintaining readiness to deflect an attack should deterrence fail. ✪

Notes

1. Michael Nayak, "CubeSat Proximity Operations: The Natural Evolution of Defensive Space Control into a Deterrence Initiative," *Space Review*, 18 January 2016, http://www.thespacereview.com/article/2902/1, 1–2.

2. *SPACENews* Editor, "Intelligence Director Cites Threats to U.S. Satellites," *SPACENews*, 10 February 2014, http://spacenews.com/39437intelligence-director-cites-threats-to-us-satellites/; Douglas Loverro, "Commentary: Space Resilience, Deterrence, Fast Ships, and Harm's Way," *SpaceNews*, 26 May 2014; and Mike Gruss, "U.S. Space Assets Face Growing Threat From Adversaries, STRATCOM Chief Warns," *SpaceNews,* 26 February 2014, http://spacenews.com/39669us-space-assets-face-growing-threat-from-adversaries-stratcom-chief/.

3. Wang Huacheng, "The US Military's 'Soft Ribs' and Strategic Weaknesses," *Liaowang* 27, reprinted in *Xinhua Hong Kong Service*, 5 July 2000, in FBIA—CHI—2000—0705.

4. Ashley J. Tellis, "China's Military Space Strategy," *Survival* 49, no. 3 (1 September 2007): 41–72, http://dx.doi.org/10.1080/00396330701564752; Jana Honkova, "The Russian Federation's Approach to Military Space and Its Military Space Capabilities," *George C. Marshall Institute Policy Outlook* 2013, http://marshall.org/wp-content/uploads/2013/11/Russian-Space-Nov-13.pdf; and Peter J. Brown, "India Targets China's Satellites," *South Asia Times*, 22 January 2010, http://www.atimes.com/atimes/South_Asia/LA22Df01.html.

5. Armen Toorian, Ken Diaz, and Simon Lee, "The CubeSat Approach to Space Access" (paper presented at the 2008 Institute of Electrical and Electronics Engineers (IEEE) Aerospace Conference), 20 May 2008, 1–14, http://ieeexplore.ieee.org/document/4526293/.

6. Josh Berk, Jeremy Straub, and David Whalen, "The Open Prototype for Educational NanoSats: Fixing the Other Side of the Small Satellite Cost Equation" (paper presented at the 2013 IEEE *Aerospace Conference*, 13 March 2013), 1–16, http://ieeexplore.ieee.org/document/6497393/; and Michael Swartwout, "Twenty (Plus) Years of University-class Spacecraft: a Review of What Was, an Understanding of What is, and a Look at What Should be Next," (paper presented at the 20th Annual American Institute of Aeronautics and Astronautics [AIAA]/Utah State University [USU] Conference on Small Satellites, North Logan, UT), 2006, https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1532&context=smallsat.

7. Giovanni Minelli, Antonio Ricco, Christopher Beasley, et al., "O/OREOS Nanosatellite: A Multi-payload Technology Demonstration," (paper presented at the 2010 Small Satellite Conference, Moffett Field, CA); Milan Diaz-Aguado, Shakib Ghassemieh, Van Outryve et al., "Small Class-D Spacecraft Thermal Design, Test and Analysis-PharmaSat Biological Experiment," (paper presented at the IEEE Aerospace Conference, Big Sky, MT, 2009), 1–9, https://www.researchgate.net/publication/251884791_Small_Class-D_spacecraft_thermal_design_test_and_analysis_-_PharmaSat_biological_experiment; and Christopher Kitts, John Hines, Elwood Agasid et al., "The GeneSat-1 Microsatellite Mission: A Challenge in Small Satellite Design," (paper presented at the 2006 Small Satellite Conference, Moffett Field, CA), https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1558&context=smallsat.

8. Christopher R. Boshuizen, James Mason, Pete Klupar et al., "Results from the Planet Labs Flock Constellation," Staff Selection Commission (SSC) Paper 14-I-1, 2014, https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=3016&context=smallsat.

9. Nayak, "CubeSat Proximity Operations", 1–2.

10. Carlos G. Niederstrasser, Alishan Hassan, Jake Hermle et al., "TJ3Sat–The First Satellite Developed and Operated by High School Students," SSC Paper 09-XII-5, 2009, https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1342&context=smallsat.

11. Stewart Davis, "Construction of a CubeSat Using Additive Manufacturing," *SAE* International Technical Paper 2011-01-2568, http://papers.sae.org/2011-01-2568/; Benjamin W. Longmier, Frans H. Ebersohn, J. P. Sheehan, and Timothy A. Collard, "The CubeSat Ambipolar Thruster: Earth Escape in a 3U CubeSat," (paper presented at the Joint Conference of the 30th Symposium on Space Technology and Science, 34th International Electric Propulsion Conference and 6th Nano-satellite Symposium), Hyogo–Kobe, Japan, 10 July 2015, http://pepl.engin.umich.edu/pdf/IEPC-2015-243.pdf; Gilbert Moore, Walter Holemans, Adam Huang et al., "3D Printing and MEMS Propulsion for the RAMPART 2U CubeSat," (paper presented at the AIAA/USU Conference on Small Satellites, North Logan, UT), https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1205&context=smallsat; Kristia Harris,

Michael McGarvey, Ha Youn Chang et al., "Application for RSO Automated Proximity Analysis and IMAging (ARAPAIMA): Development of a Nanosat-based Space Situational Awareness Mission," (paper presented at the AIAA/USU Conference on Small Satellites, North Logan, UT), 2013, 1–19, http://www.dtic.mil/dtic/tr/fulltext/u2/1034457.pdf; Bogdan Udrea, Michael V. Nayak, Adam Huang et al., "Mission Design and Concept of Operations of a 6U CubeSat Mission for Proximity Operations and RSO Imaging," (paper presented at the Fifth International Conference on Spacecraft Formation Flying Missions and Technologies, Munich, Germany, 2013), 1–15, https://www.researchgate.net/publication/280133315_Mission_Design_and_Concept_of_Operations_of_a_6U_CubeSat_Mission_for_Proximity_Operations_and_RSO_Imaging; and Michael Nayak, Jaclyn Beck, and Bogdan Udrea, "Real-time Attitude Commanding to Detect Coverage Gaps and Generate High Resolution Point Clouds for RSO Shape Characterization with a Laser Rangefinder," (paper presented at the IEEE Aerospace Conference, Big Sky, MT, 2013), 1–14, http://ieeexplore.ieee.org/document/6496861/.

12. Ho Jin, Youngju Kim, and Sanghyuk Kim, "Optical Design of a Reflecting Telescope for CubeSat," *Journal of the Optical Society of Korea* 17, no. 6, 2013, 533–37, https://www.osapublishing.org/josk/abstract.cfm?URI=josk-17-6-533.

13. Tarik Malik, "Iran Launches Small Earth-Watching Satellite Into Orbit," *Space.com*, 3 February 2012, https://www.space.com/14464-iran-launches-small-satellite-orbit.html.

14. J. Nicholson and B. T. Gerstein, "The Department of Defense's Next Generation Narrowband Satellite Communications System, the Mobile User Objective System (MUOS)," (paper presented at the MILCOM 2000: 21st Century Military Communications Conference, IEEE [Vol. 2], 2000), 805–09; and B.S. Robinson, D. M. Boroson DM, D. A. Burianek et al., "Overview of the Lunar Laser Communications Demonstration" (paper presented at *SPIE LASE*, International Society for Optics and Photonics, 2011, 792302). MUOS, or the Mobile User Objective System, is a narrowband tactical satellite communications system. LADEE, or the Lunar Atmosphere and Dust Environment Explorer, demonstrated high-bandwidth laser communications from lunar orbit using a receptor the size of two postage stamps.

15. Daniel A. Gallton, "The Challenge of Small Satellite Systems to the Space Security Environment" (master's thesis, Naval Postgraduate School, 2012), https://calhoun.nps.edu/handle/10945/6797. Examples include missile warning, protected communications, space-based position-navigation-timing, and China's Fengyun-1C Anti-Satellite Test, 2007.

16. Sergei N. Khrushchev, *Nikita Khrushchev and the Creation of a Superpower* (University Park, PA: Penn State Press, 2010), 351–60.

17. Disaggregated system is defined as "the dispersion of space-based missions, functions or sensors across multiple systems spanning one or more orbital plane, platform, host or domain."

18. Lt Col Ellen Pawlikowski, USAF, Doug Loverro, Defense Intelligence Senior Executive Service, and Col Tom Cristler, USAF, Retired, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly* 6, no. 1, 2012, 27–54, http://www.au.af.mil/au/ssq/2012/spring/pawlikowski.pdf; and Air Force Space Command (AFSC), *Resiliency and Disaggregated Space Architectures*, US government white paper (Peterson AFB, CO: AFSPC, 2013), https://fas.org/spp/military/resiliency.pdf.

19. Adam E. Frey, "Defense of US Space Assets: A Legal Perspective," *Air & Space Power Journal* 22, no. 4, 75–84, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-22_Issue-1-4/2008_Vol22_No4.pdf.

20. Michael Nayak, "Impact of National Space Policy on Orbital Debris Mitigation and US Air Force End of Life Satellite Operations," (paper presented at the SpaceOps 2012 Conference, Stockholm, Sweden, 2012), 1–9, https://arc.aiaa.org/doi/abs/10.2514/6.2012-1284611.

21. "XSS-11 Micro Satellite," *Kirtland.af.mil*, accessed 18 October 2017, http://www.kirtland.af.mil/Portals/52/documents/AFD-111103-035.pdf?ver=2016-06-28-110256-797; I. T. Mitchell, T. B. Gorton, K. Taskov et al., "GN&C Development of the XSS-11 Micro-satellite for Autonomous Rendezvous and Proximity Operations," (paper presented at the *29th Annual AAS Guidance and Control Conference*, Breckenridge, CO, 2006); David A. Whelan, E. Allen Adler, Samuel B. Wilson et al., "DARPA Orbital Express Program: Effecting a Revolution in Space-based Systems," (paper presented at the International Symposium on Optical Science and Technology, 2000), 48–56, https://www.spiedigitallibrary.org/conference-proceedings-of-spie/4136/1/DARPA-Orbital-Express-program--effecting-a-revolution-in-space/10.1117/12.406656.short?SSO=1; Andrew Ogilvie, Justin Allport, Michael Hannah et al., "Autonomous Satellite Servicing Using the Orbital Express Demonstration Manipulator System," (paper presented at the Ninth International Symposium on Artificial Intelligence, Robotics, and Automation in Space, Beijing,

China, 2008), 25–29, http://robotics.estec.esa.int/i-SAIRAS/isairas2008/Proceedings/SESSION%2014/m113-Ogilvie.pdf; and Robert B. Friend, "Orbital Express Program Summary and Mission Overview," (paper presented at the Society of Photographic Instrumentation Engineers *Defense and Security Symposium*, Orlando, FL, 15 April 2008), https://www.spiedigitallibrary.org/conference-proceedings-of-spie/6958/1/Orbital-Express-program-summary-and-mission-overview/10.1117/12.783792.short.

22. Bill Gertz, "China Launches Three ASAT Satellites," *Washington Free Beacon*, 26 August *2013*, http://freebeacon.com/national-security/china-launches-three-asat-satellites/.

23. Kristia Harris, Michael McGarvey, Michael Nayak, Bogdan Udrea et al., "Application for RSO Automated Proximity Analysis and IMAging (ARAPAIMA): Development of a Nanosat-based Space Situational Awareness Mission", SSC Paper 13-VI, 2009, http://digitalcommons.usu.edu/smallsat/2013/all2013/40/, 1–19; Bogdan Udrea, Michael Nayak, Michaella Ryle et al., "Mission Design and Concept of Operations of a 6U CubeSat Mission for Proximity Operations and RSO Imaging" (paper presented at the Fifth International Conference on Spacecraft Formation Flying Missions and Technologies, Munich, Germany, 2013), 1–15; Francisco J. Franquiz, Peter Edwards, Bogdan Udrea et al., "Attitude Determination and Control System Design for a 6U CubeSat for Proximity Operations and Rendezvous," (paper presented at the AIAA/American Astronautical Society Astrodynamics Specialist Conference, San Diego, CA, 2014), 1–18; Bogdan Udrea, Michael Nayak, and Finn Ankersen, "Analysis of the Pointing Accuracy of a 6U CubeSat Mission for Proximity Operations and Resident Space Object Imaging" (paper presented at the Fifth International Conference on Spacecraft Formation Flying Missions and Technologies, Munich, Germany, 2013), http://www.sffmt2013.org/PPAbstract/4139p.pdf; and Parv Patel, Bogdan Udrea, and Michael Nayak, "Optimal Guidance Trajectories for a Nanosat Docking with a Noncooperative Resident Space Object," (paper presented at the 2015 IEEE Aerospace Conference, Big Sky, MT, 2015), 1–11.

24. Linda M. Herrell, "Access to Space for Technology Validation Missions: a Practical Guide" (paper presented at the 2007 IEEE Aerospace Conference, Big Sky, MT, 2015), 1–8, http://ieeexplore.ieee.org/document/4161322/; and Phillip C. Kalmanson, Bryan Benedict, Michael Do et al., "Micro & Nanosatellite Launch Capabilities from the Star Bus GEO Commercial Communications Platform" (paper presented at the 22nd Annual AIAA/USU Conference on Small Satellites, Logan, UT, 2008), https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1408&context=smallsat. Example: Space Systems Loral hosted payloads on Intelsat and SES Astra space vehicles and has an established business model in place for government collaborations.

25. Mike Wall, "Is Russian Mystery Object a Space Weapon?" *Space.com,* 19 November 2014, https://www.space.com/27806-russia-mystery-object-space-weapon.html.

26. Michael Nayak, Jaclyn Beck, and Bogdan Udrea, "Design of Relative Motion and Attitude Profiles for Three-dimensional Resident Space Object Imaging with a Laser Rangefinger" (paper presented at the 2013 IEEE Aerospace Conference, 2013), 1–16, http://ieeexplore.ieee.org/document/6496837/; and Parv Patel, Bogdan Udrea, and Michael Nayak, "Optimal Guidance Trajectories for a Nanosat Docking with a Noncooperative Resident Space Object" (paper presented at the 2015 IEEE Aerospace Conference, 2015), 1–11. *Istrebitel* is the Russian word for "fighter aircraft."

27. Frey, "Defense of US Space Assets," 75–84.

28. Bruce W. Jentleson and Christopher A. Whytock, "Who Won Libya," *International Security* 30, no. 3, 47–86, https://lse.rl.talis.com/items/21C96C88-07BC-6BCB-EE7D-6BA3C5A73222.html.

29. Thomas T. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 202–33.

30. Shawn C. Fairhurst, "Realities of Deterrence and Retaliatory Options to Attacks in Space and Cyberspace," Technical Report (Maxwell AFB, AL: Air War College, 2012), 2–29.

31. Civil Air Patrol, "FPCON (Force Protection Condition) Categories," 22 August 2003, http://capnhq.custhelp.com/app/answers/detail/a_id/1023/-/fpcon%-%28force-protection-condition%29-categories.

32. Ibid.

33. Jayant Sharma, Grant H. Stokes, Curt von Braun et al., "Toward Operational Space-based Space Surveillance" *Lincoln Laboratory* 13, 2002, 309–34.

34. USAF, *AFD-110501-004*.

35. SpaceFlight 101, "GSSAP Satellite Overview," 25 July 2014, accessed 17 October 2017, http://spaceflight101.com/spacecraft/gssap/.

36. Stephen Clark, "Air Force General Reveals New Space Surveillance Program," *Space.com*, 3 March 2014, https://www.space.com/24897-air-force-space-surveillance-program.html.

37. Ibid.
38. Fairhurst, "Deterrence and Retailiatory Options."
39. Ian Garrick-Bethell, Robert P. Lin, Hugo Sanchez et al., "Lunar Magnetic Field Measurements with a Cubesat," in *Systems and Sensors for Space Applications VI*, ed. Khanh D. Pham, Joseph L. Cox, Richard T. Howard RT, et al., (Bellingham, WA: International Society for Optical Engineering, 2013).

Capt Michael Nayak, USAF, PhD

Captain Nayak (PhD, MS, University of California at Santa Cruz; BS, Embry-Riddle Aeronautical University) is a research scientist with the Directed Energy Directorate, Air Force Research Laboratory. Captain Nayak has published more than 35 journal and conference papers on interdisciplinary research ranging across aerospace engineering, planetary science, astrophysics, space mission design, guidance navigation and control, geophysics, and space policy. His experience outside the USAF spans work at three National Aeronautics and Space Administration centers, including as a certified space shuttle engineer, coprincipal investigator of a cube satellite program and a National Defense Science and Engineering Graduate Fellow at the University of California. He is also a commercial pilot and skydiving instructor.

Brandishing Our Air, Space, and Cyber Swords

Recommendations for Deterrence and Beyond

Lt Col Mark Reith, USAF, PhD*

Courtesy Stacy Burns

The United States has arrived at a historic crossroads for space and cyber. For decades, space and cyber have been treated as neutral territory or part of a global commons, but the rise of competitors and the commoditizing of technology within these domains have drastically changed the calculus of strategic deterrence. One road takes the United States down the path of massive and time-intensive investments into hardened and resilient systems with no guarantee that next-generation technology will be any more resistant to crafty attackers than the last.

Another road takes the United States down the path of multidomain offensive capabilities to create multiple dilemmas that overwhelm and hold the adversary at

*Special thanks to Col Brad Pyburn, Col David Snoddy, Col Heather Blackwell, Lt Col Eric Trias, Lt Col Joy Kaczor, and Capt Carlos Rodriguez for their insightful contributions.

risk, but the efficacy of this approach across a range of actors is unknown. Yet just beyond the technical horizon, we face the implications of science fiction in motion as new technologies such as artificial intelligence, robotics, and weaponized lasers are developed and fielded against a disturbing backdrop of world events.[1] Consider the Russian–Ukrainian cyber conflict playing out across the fabric of society, including utilities, mass media, and finance, and all while the international community fails to establish intervention redlines as malware spills beyond the borders of the conflict.[2]

> *Strategic deterrence in the 21st century is much bigger than nuclear deterrence was in the 20th century. The US military is still "catching up" to this new deterrence reality and having a robust discussion on what deterrence means in today's global threat landscape.*
>
> —Gen John Hyten, USAF
> Commander, US Strategic Command

> *Conflict may occur along the spectrum at any point, in varying degrees of intensity, with more than one adversary, and in multiple domains. At all phases. . . our planning and operations are designed to deter and develop "off ramps" to de-escalate the conflict. . . while dissuading our adversaries from considering the use of cyber attacks, counterspace activities, or nuclear weapons.*
>
> —Adm Cecil D. Haney, USN
> Former Commander, US Strategic Command

Furthermore, ponder North Korea's offset strategy to hold conventional American forces at risk with nuclear weapons while employing asymmetrical tools with a clear intent and resolve to challenge US hegemony.[3] As we grapple with this dynamic environment, we find ourselves at the precipice of the next revolution in military affairs, and our next investments will heavily influence our future options.

This article examines how the nation could better prepare to deter aggressive action in space and cyberspace, and if necessary, prevail should deterrence fail. The key themes throughout this article include a strong need for space and cyber situational awareness, the need for an international attribution and escalation framework, and a national investment in space and cyber education, along with an updated national strategy and military doctrine. Although related, this article focuses on deterrence and avoids the topic of cyber coercion.

Problematic Assumptions in the Strategic Deterrence Framework

> *Deterrence prevents adversary action through the presentation of a credible threat of counteraction. In both peace and war, the Armed Forces of the United States help to deter adversaries from using violence to reach their aims. Deterrence stems from an adversary's belief that a credible threat of retaliation exists, the contemplated action cannot succeed, or the costs outweigh the perceived benefits of acting. Thus, a potential aggressor chooses not to act for fear of failure, cost, or consequences.*
>
> —Joint Publication 3-0, *Joint Operations*

The concept of deterrence has a long history in warfare and military doctrine reflects a deep understanding of its most salient elements. From the Joint Publication's description of deterrence, the most important element involves the adversary's belief in retaliation, failure, or unacceptable costs. The description makes several assumptions that are problematic when considering space and cyberspace. The first assumption asserts that the United States can quickly and reliably attribute behavior to an adversary. The second assumption is that the adversary can observe success or failure of their actions, let alone the actions of others. Finally, the third assumption states that costs and benefits can be measured and rationalized. Challenging these assumptions may reveal opportunities to exploit situations.

For deterrence to be effective, several conditions should be met:

1. *The threat must be communicated accurately to the target.*
2. *The target must clearly understand the threat.*
3. *The target must believe that the anticipated cost of its undertaking the action outweighs potential benefits.*
4. *The target must believe that the "deterrer" will take the threatened action(s).*

—USAF Doctrine Annex 3-0
Operations and Planning

The US Air Force elaborates on the conditions of deterrence as part of USAF doctrine. Here, too, we observe assumptions that are problematic in the modern age. First, cyber and space activities are often hidden due to the highly classified nature before and after they have occurred, and often under the guise of anonymity. Unlike nuclear tests and operations that are generally observable to all adversaries, cyber and space activities may or may not be detectable by the target, and typically not by third parties. Second, the description assumes that all adversaries are paying attention and understand the threat. Within the space and cyber domains, this may require specialized tools that detect disturbances in these domains, and more importantly, interpret correctly for their situation. Finally, the description assumes that the prep work supporting threatening actions has already been accomplished. For example, the United States has strong relations with the international community and generally adheres to an ethical and legal framework to maintain the legitimacy of its world leadership role. An adversary, suspecting that no legal framework for retaliating across the global commons exists, might not believe the United States is willing to take threatening actions. Additionally, the same adversary might not believe that the United States has prepositioned space and cyber weapons available to retaliate. Although not addressed in Joint or USAF Doctrine, the timing of retaliatory action must also be considered. Space and cyber attacks have the potential to rapidly scale and affect large populations, then disappear into the complexity of cyberspace. This highlights the need for agile options, to include real time action, lest aggressors become emboldened with guerrilla style tactics.

Challenges in Deterring Cyber Attacks

Summary of Challenges to Cyber Deterrence

- *Difficulty of attributing cyber attacks to their perpetrators*
- *Ease of acquiring cyber weapons and conducting cyber attacks*
- *Broad scope of state and nonstate actors who engage in cyber attacks for a multitude of reasons and against both state and nonstate targets*
- *Short shelf life of many cyber weapons*
- *Difficulty of establishing thresholds and red lines for cyber aggression*
- *Difficulty of setting and enforcing international norms regarding cyber behavior*
- *Challenges associated with avoiding escalation*

—Dorothy E. Denning
Emeritus Distinguished Professor
Navy Postgraduate School

Some scholars have identified a collection of challenges associated with cyber deterrence.[4] Information security researcher Dorothy E. Denning summarizes many of these challenges and compares, as many others have, the nature of cyber deterrence to that of nuclear deterrence. Key differences might include the degree of difficulty in acquiring weapons, the shelf life of these weapons, and the motivations and attribution of firing these weapons, to name a few. One might infer from the community of researchers that instead of comparing cyber deterrence to nuclear deterrence, strategists and policymakers need to instead reflect on the strategic deterrence framework and either shape space and cyber to allow the traditional deterrence model to work or reset expectations about the effectiveness of deterrence in these domains. The next section provides some perspectives on how to accomplish both.

Applying the Deterrence Framework to Cyber

Deterrence is all about capability and intent, and in cyber we've shown a little of either publicly. I think of the nuclear "tests" we conducted in the '50s/'60s to demonstrate not just capability, but resolve. . . we should showcase the broad spectrum of capabilities we can bring to bear through our powerful "engine" of offensive cyber. We show "demonstrations" of how cyber can impact kinetic systems—this will also help decision makers properly prioritize cyber security/hygiene/defense through the proper risk-informed investment strategies.

—Col Brad Pyburn, USAF
Commander, 67th Cyberspace Wing

As previously discussed, applying the deterrence framework to the cyber domain can be challenging and complicated. This article expands upon Geist's recommendation for a "Strategy of Technology" to implement a cyber deterrence framework.[5] Geist outlines three components of his strategy: denial, resilience, and offensive capabilities. The article examines each component, maps it back to DOD Joint Operations

doctrine, outlines shortfalls, and makes recommendations for building a robust deterrence framework.

Deterrence by Denial (Fear of Failure)

The first, and generally considered the most effective, component is deterrence by denial. This type of deterrence is characterized by rendering cyber weapons ineffective such that an adversary is discouraged to even attempt an attack. From DOD Joint Operations, this exploits a fear of failure and opens the possibility of potential attribution. The classic example involves a strong vulnerability patching approach that leaves exploit weapons inert. Denial works because exploits tend to be fragile in that some technical and situational conditions need to be satisfied before the exploit is effective. The fact that some conditions exist gives great hope as a form of deterrence because the defender can often influence many of these conditions. The typical problem involves a numbers game: multiply the number of potential vulnerabilities (order of thousands) with the number of enterprise systems (order of hundreds of thousands) and the number of exploit attempts (that is, the Air Force blocked 1.3 billion connection attempts in 2016), and you get an upper bound on the number of possible exploits in a given time frame.[6] Granted that actual risk exposure is dependent on linkages between systems, vulnerabilities, and exploit attempts, but the key theme involves a scale of problem that is difficult to manage. Another typical problem involves some legacy systems from developers who never imagined these systems would be exposed to exploit attempts. Utility infrastructure, vehicles, and embedded systems are good examples of such exposure.

The United States can enhance its deterrence by denial strategy in several ways. First, the most obvious solution involves implementing cyber security best practices such as defense in-depth, patching, configuration management, strong authentication, deep inspection of communications traffic, and so on. Chinese research into quantum cryptography using satellites is a great example of strategic investment into their denial deterrence.[7] Second, workforce education and training are paramount, along with exercises, drills, and accountability for online behavior. Third, the United States needs to change expectations regarding technology. Specifically, strategists and policymakers need to stop viewing information technology as a utility, and instead expect a perpetually contested environment. In doing so, they can segment forces into groups with extremely limited exposure to cyber threats, accepting the potential for a reduced capability for the short period in which the cyber terrain is contested.

Deterrence by Resiliency (Cost)

The second component is deterrence by resiliency. This type of deterrence is characterized by increasingly expensive efforts such that an adversary is discouraged, although not necessarily prevented, from attacking. From DOD Joint Operations, this exploits a resource cost in multiple ways. First, this strategy may consume the adversary's exploit tools and zero-day opportunities. Exploit owners cannot guarantee sole ownership, and over time such tools and opportunities often become stale. Once an exploit is understood, and a patch is deployed, the tool may have reduced

value. This is particularly a problem if the exploit tool was expensive to develop or acquire. Loss of anonymity is a related cost because as the exploit tool or technique is repeatedly used, the defender may piece together enough information for reasonable attribution. Second, as the defender's capacity increases, the adversary may require a larger force to find and exploit vulnerabilities *that meet their specific objectives*. Consider how redundancies may dampen the effect of denial of service attacks while increasing the adversary's required resources. Third, over time previously understood networks may change, reducing the value of reconnaissance info and prompting rework. Finally, even upon successful exploit, active defenders might detect and force an adversary out, thus inducing the cost of finding another way back into the system.

The United States can enhance its deterrence by resiliency strategy in several ways. First, the most straightforward approach involves investment into active defense capabilities. Additional manpower and research into automated detection and investigation capabilities help find, fix, track, engage, and assess adversaries on contested US networks. Investments into mission mapping technology help defenders identify key cyber terrain and fight adversary activity to assure missions.[8] Second, leverage the natural advantage of the home game. Since cyberspace is malleable and mutable, shaping the environment to give defenders the advantage makes sense. Deploy software-defined networks to unpredictably change the environment and render previous adversary reconnaissance useless. Harness the workforce by defining meaningful cyber conditions based on mission set rather than by geography, and exercise such conditions routinely. Third, leverage the natural complexity inherent in cyberspace. Deploy thousands of decoy systems, and let adversaries run around the mirror maze while defenders observe and learn from their tactics. Deploy distributed file systems that store fragments of files across thousands of systems. Owners will be able to find and reassemble, whereas adversaries will grow frustrated and make mistakes, ultimately leading to attribution. Planting malware in these decoys and file systems may ultimately increase the adversary's cost considerably. Furthermore, revealing evidence of a cyber attack to the international community, particularly in the context of standing treaties, may also increase an adversary's cost.

Deterrence by Punishment (Consequences)

Finally, the third component is deterrence by punishment. This type of deterrence is characterized by attacking, or threatening to attack, the adversary directly such that they are too intimidated to fight back. From DOD Joint Operations, this exploits a fear of consequences but requires strong attribution to be effective. Punishment deterrence can be a complex topic for several reasons previously outlined by Denning. Critical among them is the question of whether cyber deterrence is limited to cyber types of punishment, or are other instruments of power available? Questions of redlines, escalation, proportionality, and survivability are germane to this discussion and should be framed before considering this dimension of deterrence.

The United States could work toward a deterrence by punishment strategy in several ways. First, a framework of international and domestic law should be established in at least two areas. One area involves guidelines associating cyber punish-

ments with cyber violations. The other area involves integrating and relating strategic domain actions (space and cyber) with traditional domain actions (air, land, and sea).[9] Here Manzo suggests establishing equivalent classes that are agreed upon by the international community, may be used to interpret the significance of actions across domains, and may avoid unintended escalation. Typically, this occurs through tradition and custom, but conflict in space and cyber are still normalizing. For example, should the United States decide to leverage its new naval laser technology as a potential space weapon, it should establish a framework that clearly establishes redlines and employment criteria.[10] Second, the United States could promote a cyber arms race complete with a showcase of exploit tools and a significantly large industrial base able to craft new exploit tools over time. Note that the deterrent isn't any particular exploit tool, but rather the industrial base that builds them. While this may lead to a space and cyber arms race, the counter argument might be that this is an eventuality, and the United States might as well seize the initiative. The key to developing a viable build-and-discard cyber weapon capability includes significant reforms or new authorities in the federal acquisition regulations. Third, the United States could take the initiative to preplace malware on their adversaries' critical infrastructure as a means of holding cyber terrain at risk. While demonstrating evidence of such preplaced capabilities might sacrifice the asset, planting the seed of doubt in the trustworthiness of their systems may pay dividends for years. If the United States were to highlight this exposure to other potential adversaries, the impact might reverberate across state-sponsored actors. Care would need to be taken to distinguish malware intended to create cyber effects versus malware intended to facilitate intelligence collection.

Fourth, the United States could entangle government and military systems with global civilian systems to change the calculus of deterrence. This approach assumes that an attack on the US government would be sufficiently egregious to the civilian population and world economy, and thus garner political support for full-spectrum options. The Global Positioning System (GPS) shares this characteristic in so far as an attack on it to degrade military operations would also impact civilian populations across the globe and help justify kinetic countermeasures.

Deterrence across a Range of Actors

Investments into deterrence strategies must account for potential attacks across a range of adversary actors. Whereas a nation-state might be more receptive to deterrence by punishment, nonstate actors may have little to hold at risk and therefore deterrence by denial or resiliency might be more appropriate. Historically, the US military has put disproportionately more effort towards denial strategies, with some growing efforts toward resiliency, because it requires little external coordination. However, nation-states are not deterred by these internal efforts because within their strategic calculus, the potential payout has historically far exceeded the risk of attribution and US action. The key to deterrence by punishment is to position something the adversary values at risk. For nation-states, perhaps this aligns with Col John A. Warden's centers of gravity theory.[11] For nonstate actors, the impact of

offensive cyber operations remains unclear.[12] Current theory suggests focusing on key leadership individuals and their immediate objectives.[13]

Recommendations

Increase Global Space and Cyber Situational Awareness

> *I think all warfare today requires interdependencies, coalitions, and partners. But in cyber, I think there is a more profound requirement to have partnerships in ways that are different than other military warfighting domains.*
>
> —Lt Gen J. Kevin McLaughlin, USAF
> Deputy Commander, US Cyber Command

Among the many concerns regarding space and cyber deterrence, attribution and transparency must be addressed if meaningful deterrence is desired. Each factor should include at least two components. First, the adversary needs to know that they have been caught red-handed and thus subject to justice. Second, potential adversaries need to observe that bad actors are held accountable for their actions to deter further undesirable behavior. In an age of encryption and spoofing, holding the offenders accountable may seem like an insurmountable problem, but one merely has to remember that cyberspace is, by definition, a man-made environment and thus malleable and mutable.[14] Instead of defaulting to an environment that allows end-to-end encrypted traffic to pass obfuscated through systems owned by nation-states; instead require traffic to be inspectable based on the laws of the hosting government.[15] This is not to say that all traffic will be inspected, only that governments retain the right to inspect any good or service (in this case, information) that passes through their borders, even transient traffic. While some countries may not adopt this model; neither is the recipient of such traffic under any obligation to accept it, nor does the model impede public traffic. However, this model does provide collaborating governments with a means of detecting and tracing bad behavior, and more importantly, collecting evidence for closer inspection by the international community. Additionally, collaborating governments can assist each other to facilitate cyber attacks in a manner similar to allowing flight paths through friendly airspace, creating a more natural framework for coalition vice unilateral engagement. With evidence in hand, all instruments of national power across all domains become plausible.

Establish a National and International Framework

> *One thing the exercises have highlighted is the difficulty at times of determining the appropriate response due to a lack of rules of engagement in space. If we're going to act decisively in real time, we have to address these issues legally and operationally.*
>
> —Vice Adm Charles A. Richard, USN
> Deputy Commander, US Strategic Command

Closely related to the aforementioned investments into global space and cyber situational awareness, the need for a national and international framework for managing behavior in the global commons is paramount. Key among these needs is a requirement for governments to be accountable for space and cyber activities that are either sanctioned by or originate from their jurisdiction. While it may seem foolish on the surface to enact a law that is difficult to enforce, the true goal is to force a decision on state actors. Either the originator acknowledges that they are a space/cyber combatant and thus deals with the aftermath, or they claim the part of victim or bystander. In the latter cases, this opens an opportunity for the injured parties to shape the outcome by requiring additional laws, cyber security education, limitations on outbound traffic, or in extreme cases network isolation. The premise behind this strategy involves an expectation that states allowing technology to be used must first demonstrate the ability to govern it because of the potential for global impact.

Consider the idea of consolidating management of cyberspace and assigning the United States as the international steward for the benefit of humanity. While this may seem outlandish at first, reflect on the way that the United States already plays a similar role for space (GPS) and world currencies (US dollar as the world's reserve currency). The United States already influences much of the infrastructure (that is, domain name services) through research and development, and US companies (Google, Intel, Microsoft, and so forth) are directly involved in crafting cyberspace, so perhaps the US government might take a larger role in the employment of such technologies. Perhaps part of this role might involve the registry of devices and people allowed to use the Internet, thus striking a balance between privacy and security.

Strategically Develop Space/Cyber Military Operators and Citizen Militias

> *Cyber Airmen may attend professional developmental opportunities such as Air Force Institute of Technology, Computer Network Operations Development Program, or the Air Force Weapons School, all of which will positively impact the operationalization of the cyberspace domain within the Air Force and in turn, the future of the Cyber Mission forces.*
>
> —Maj Gen Chris P. Weggeman, USAF
> Commander, 24th Air Force and Air Forces Cyber

One of the key strengths of the United States and many western democracies is the freedom of innovation and industry. Investments into such programs as Cyber Patriot, National Collegiate Cyber Defense, and Advanced Cyber Education yield generations of citizens with cyber acumen (shown in figure).[16]

Showcasing the investment and resulting abilities becomes a strategic tool for deterrence since not only government agencies but also private corporations have a deep understanding of cyber security. However, deeper investments of computer science, engineering, and cyber operations into K-12 is needed to demonstrate a national commitment to our security and safety. This is much more than formal education, but rather a cultural change where cyber role models, children's television programming, and successful careers shape the attitudes of our youth. By building a national reserve of ethical talent, the United States not only enhances the cyber

resiliency within domestic companies and products, but may also draw upon this reserve in times of crisis. Whereas totalitarian regimes might limit the development of such talent in fear of regime overthrow, the United States might embrace ethical hacking in a manner similar to universal gun rights and ownership, thus giving the United States a strategic advantage. In a similar manner, the forecasted ubiquity of space travel through companies like Space X may create a similar deterrence effect where any attack on travelers may yield a conventional response, particularly if attribution and transparency are addressed.[17]

Courtesy Stacy Burns

Figure. Hannah Kirst (Texas A&M University), David Home (University of Colorado), Matthew Holt (Lock Haven University, Anh Bui (University of North Carolina at Charlotte) and Albert Bierley (University of California) are among the students benefitting from Advanced Cyber Education at the Air Force Institute of Technology in July 2017.

Update National Security Strategy and Joint and Air Force Space/Cyber Doctrine

> *I would argue that we should view cyber as one element of a broader deterrence campaign.*
>
> —Adm Mike Rogers, USN
> Commander, US Cyber Command

As previously mentioned in joint and Air Force doctrine, deterrence requires clearly communicated and credible threats along with a believable intent to exercise those threats. Current space doctrine emphasizes responsible behavior, partnerships that encourage restraint, collaboration toward quick attribution, and appropriate responses when deterrence fails.[18] However, current cyber doctrine specifies very little toward a deterrence strategy.[19] One might be tempted to adopt the same deterrence strategy across space and cyber, however, this may not work for several reasons. First, the cyber landscape changes more rapidly than space. Second, the United States has more deterrence options and actors in cyberspace. However, given the increasingly contested nature of both domains, the United States should be more explicit about taking action both within and across domains. Furthermore, enhancements

to the National Security Strategy might include the full spectrum of national instruments of power to realize this article's recommendations. A consistent strategy and doctrine will be key to safeguarding the nation.

Conclusion

> *It is unfortunate when men cannot, or will not, see danger at a distance; or seeing it, are restrained in the means which are necessary to avert, or keep it afar off. . . Not less difficult is it to make them believe, that offensive operations, often times, is the surest, if not the only (in some cases) means of defence.*
>
> —President George Washington
> 25 June 1799

In summary, the United States has reached an important crossroad as it contemplates the future of space and cyber deterrence. Historically strategic deterrence has worked, but applying such constructs to space and cyber domains remains challenging without better attribution, international laws, human capital investment, and updated national strategies and doctrine. Without these changes, space and cyber will remain niche and nuanced domains, susceptible to attack and exploitation, and in the worst case, our nation's Achilles' heel. As leaders entrusted to make sound investment decisions, we have the ability to shape not only space and cyber, but possibly our national destiny as well. ✪

Notes

1. Defense Science Board, "Task Force on Cyber Deterrence," Technical Report (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics), 1 February 2017, http://www.dtic.mil/docs/citations/AD1028516.

2. Andy Greenberg, "How an Entire Nation became Russia's Test Lab for Cyber War," *Wired*, 20 June 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

3. Lt Gen In-Bum Chun, ROKA (Ret.), "North Korea's Offset Strategy," in *Breakthrough on the Peninsula: Third Offset Strategies and the Future Defense of Korea*, ed. Dr. Patrick M. Cronin (Washington, DC: Center for New American Security, November 2016), 39–48, https://www.cnas.org/publications/reports/breakthrough-on-the-peninsula.

4. Martin C. Libicki, Edward Geist, Dorothy E. Denning, Stephen J. Cimbala, Frank J. Cilluffo, and others have identified challenges associated with cyber deterrence.

5. Edward Geist, "Deterrence: Stability in the Cyber Age," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015), 44–62, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-09_Issue-4/Geist.pdf.

6. Data compiled from the National Vulnerability Database, https://nvd.nist.gov; and Air Force Public Affairs Alumni Association, *Air Force Communication Waypoints 2017*, http://www.afpaaa.org/PDF/Waypoints0817.pdf, 20.

7. Sophia Chen, "Chinese Satellite Relays a Quantum Signal between Cities," *Wired*, 15 June 2017, https://www.wired.com/story/chinese-satellite-relays-a-quantum-signal-between-cities/.

8. Jeff Guion and Mark Reith, "Dynamic Cyber Mission Mapping," Institute of Industrial and Systems Engineers Annual Conference, 2017.

9. Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?" *Strategic Forum* 272, National Defense University Institute for National Strategic Studies, December 2011, http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf.

10. Michael Fabey and Kris Osborn, "Navy to Fire 150Kw Ship Laser Weapon," *Scout*, 23 January 2017, https://scout.com/military/warrior/Article/Navy-to-Fire-150Kw-Ship-Laser-Weapon-From-Destroyers-Carriers-101455353.

11. Maj Gary M. Jackson, USAF, "Warden's Five-Ring System Theory: Legitimate Wartime Military Targeting or An Increased Potential to Violate the Law and Norms of Expected Behavior?," Research Report (Maxwell AFB, AL: Air University Press, April 2000), www.dtic.mil/get-tr-doc/pdf?AD=AD A425331.

12. Jeff Seldin, "Cyber War Versus Islamic State 'Work in Progress,' " *Voice of America News*, 18 May 2016, https://www.voanews.com/a/cyber-war-versus-islamic-state-work-in-progress/3336773.html.

13. Statement of Dr. Craig Fields, chairman, Defense Science Board, and Dr. Jim Miller, former undersecretary of defense (policy) and member, Defense Science Board, in "Cyber Deterrence," unclassified testimony before the US Senate Armed Services Committee, 115th Congress (Washington, DC: 2 March 2017), https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller_03-02-17.pdf.

14. Mark Reith, Seeley Pentecost, Daniel Celebucki, and Robert Kaufman, "Operationalizing Cyberspace: Recommendations for Future Research," International Conference on Cyber Warfare and Security, March 2017, https://search.proquest.com/openview/0c3e05994e4a362d80ad6374fb1b10e9/1?pq-origsite=gscholar&cbl=396500.

15. This is accomplished by decrypting and reencrypting traffic at each segment of the traffic's journey using public key infrastructure technology. This would clearly create multiple privacy concerns; however, history reveals that societies are continually reshaping expectations of privacy against the need for security, and the concept of privacy has grown in proportion to technology, self-sufficiency, and wealth. Ergo, the concept of privacy is not an absolute right, but rather a privilege determined by the community.

16. The Air Force Institute of Technology hosts Advanced Cyber Education, https://www.afit.edu/ace/news.cfm.

17. Don Lincoln, "Elon Musk is Changing the Rules of Space Travel," *CNN*, 1 April 2017, http://www.cnn.com/2017/04/01/opinions/elon-musk-change-rules-of-space-travel-lincoln/index.html.

18. Joint Publication (JP) 3-14, *Space Operations*, 29 May 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

19. JP 3-12, *Cyberspace Operations*, 5 February 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Lt Col Mark Reith, USAF, PhD

Lieutenant Colonel Reith (PhD, University of Texas at San Antonio) previously served as deputy commander of the 26th Cyberspace Operations Group and commander of the 690th Network Support Squadron, leading enterprise cyber defense and Department of Defense Information Network forces respectively. He currently serves as director of the Center for Cyberspace Research and assistant professor of Computer Science at the Air Force Institute of Technology.

Baptism of Fire: The First Combat Experiences of the Royal Hungarian Air Force and Slovak Air Force, March 1939 by Csaba B. Stenge. Helion & Company (https://www.helion.co.uk/), 26 Willow Road, Solihul B91 1UE, England, 2014, 136 pages, $24.96 (softcover), ISBN 978-1-906033-93-4.

During 23–24 March 1939, Hungary and Slovakia fought a very short conflict over Sub-Carpathia, a small section of eastern Slovakia that had been part of the Kingdom of Hungary before 1918 but awarded to Czechoslovakia, established by the post–World War I peace settlement. In early October 1938, Hitler annexed the German-inhabited Sudetenland and then annexed the Czech provinces of Bohemia and Moravia on 14 March 1939 and established an "independent" Slovakia. The Hungarian government now sought to annex Sub-Carpathia from a weak Slovakia. The "air campaign" of this short conflict pitted the Royal Hungarian Air Force, which had existed only since 1920, and the newly formed Slovak Air Force, which had existed for only about two weeks. *Baptism of Fire* provides the history of this very short and little-known air campaign—one that is obscure even in the nations that fought it, virtually unknown outside these two Central European countries in the turbulent interwar period, and completely lost among the greater air campaigns of the much larger European war, which began on 1 September 1939.

Author Csaba B. Stenge is a Hungarian architect and military historian. Born in Pécs, Hungary, in 1975, he received his master's degree and doctorate in history from the University of Pécs, writing his doctoral dissertation on the Royal Hungarian Air Force during World War II. He has worked in the archives at Tatabánya, Hungary, since 2003 and became its director in 2011. His research interests are in air warfare during World War II, particularly the history of the Hungarian Air Force. *Baptism of Fire* is Dr. Stenge's seventh book (his second in English), and he has published 70 articles in four languages.

Despite the relative obscurity of this air campaign, the book does have several merits. First, the governments of the belligerent countries believed that the conflict was important to them. Hungary sought to recover a historic region of the pre-1918 kingdom, arbitrarily taken from it in the postwar peace settlement and, at the same time, to establish a common border with its historic ally Poland. Slovakia, on the other hand, saw the annexation as a sufficient affront to its sovereignty to justify fighting for it. After a two-day conflict, the Hungarian military forces prevailed, and Hungary annexed the area. However, the annexation was short-lived because in August 1944, the Soviet Army occupied Hungary, and, after the war, Stalin forced the restored Czechoslovakia to cede this territory to the Soviet Union. It is now a part of Ukraine.

Second, the book documents the two-day air campaign between these two relatively new air forces. The Royal Hungarian Air Force, formed in 1920, consisted originally of Hungarian pilots and ground crews of the former Austro–Hungarian Air Force of World War I. The Slovakian Air Force was even newer and less experienced, consisting of Slovakian pilots and ground crews of the former Czechoslovakian Air Force before the dissolution of "rump" Czechoslovakia, the German annexation of Bohemia and Moravia, and the establishment of an independent Slovakia two weeks before this air campaign. The actual offensive consisted of mainly tactical air operations: Slovakian attacks against Hungarian ground forces, Hungarian air strikes against Slovakian airfields, and air-to-air confrontations between aircraft of both

air forces. These air arms flew a mixture of Italian and German biplanes and monoplanes of the 1930s. This two-day air campaign was the only combat experience of both air forces before Operation Barbarossa, the German invasion of the Soviet Union in June 1941, two years and two months later. Perhaps the most interesting facet of this campaign was not about the campaign itself. During Barbarossa, the two air forces—now German allies—participated in the initial air action, and one Slovakian pilot, Ján Režňák, fired on a Hungarian pilot, once his enemy but now his "ally." By the end of the war, Režňák had become the most successful Slovak pilot of the war.

Finally, *Baptism of Fire* offers a wealth of information and data about both air forces. Since the majority of Hungarian primary materials was destroyed during World War II, the author made a tremendous effort to find the documentation needed to prepare this book. It contains a full and detailed account of the origins and conduct of the conflict, appendices of Slovakian and Hungarian air force ranks, air victories claimed by the Hungarian Air Force fighter squadron, technical details of the major aircraft that fought in the conflict, Hungarian soldiers who received decorations, and short biographies of the Hungarian pilots who fought in the war. Finally, the book includes numerous photographs, many provided by the author, of the pilots and operations of both sides, as well as color prints of the aircraft that fought in this campaign. For readers interested in the history of Central European air forces or European military aviation in the interwar years, *Baptism of Fire* would be useful and interesting.

Robert B. Kane, PhD
Maxwell AFB, Alabama

Strategy in the Second Nuclear Age: Power, Ambition, and the Ultimate Weapon
edited by Toshi Yoshihara and James R. Holmes. Georgetown University Press (http://www.press.georgetown.edu), 3240 Prospect Street, NW, Suite 250, Washington, DC 20007, 2012, 256 pages, $32.95 (softcover), ISBN 978-1-58901-928-7.

The editors of *Strategy in the Second Nuclear Age* offer a collection of essays that challenge the reader to examine strategies and options in light of the breakout of new nuclear nation-states. Toshi Yoshihara and James Holmes precede and follow these pieces with a thought-provoking introduction and conclusion. The former takes issue with the limited scope of Carl von Clausewitz's *On War* by stating that strategy is much more than the operational strategy of battles and engagements. Nuclear strategy involves the fielding of high-end "engines of war" technologies in peacetime that nation-states do not want to use in the conduct of war. The conclusion is based upon analysis of the essays, highlighting that "proliferation is now a fact and nuclear rollback is a remote prospect at best" (p. 225).

Each essay independently contributes to the two recurring themes of rationality and interaction. Rationality can be thought of as a nation's intellectual approach to its policy-making process, particularly the use of its nuclear strategy to achieve a favorable political end state. Interaction pits that rationality against other nation-states and introduces questions of stability versus predictability. On the one hand, for example, if opposing conventional forces pitch weak against strong, then nuclear states with weak conventional forces may well consider nuclear escalation a viable option. On the other hand, nations with comparable nuclear capabilities may seek advantage through conventional means.

One of the most fascinating early chapters in the book (chap. 2) discusses deterrence theory and its application by emerging nuclear states. This (deterrence theory) is the foundation that formalizes strategy, and it quickly becomes apparent to the reader that a myriad of subjects need to be analyzed. Having challenged Clausewitz, the editors substantiate their

claims that "more is better" with a broadening discussion on several factors that affect the resultant strategy and political status quo. No reader is left doubting that nuclear strategy is a complicated, devious, and fully expansive subject. Those of us who thought we had a good understanding of it will find additional gems of knowledge to admire.

These factors include the size of a nation's nuclear arsenal, concerns over the transfer of technology and know-how to states and nonstate proxies, and use of the program as cover for conventional aggression (p. 23). Perhaps the most important factor is the level of a nation's desire to use nuclear weapons in war. This, the most dangerous part of any strategy, is in turn supported by a subset of related considerations. The contributor offers sound arguments about how a state on the verge of defeat could gamble by introducing nuclear weapons to the fight, hoping that the psychological shock of their use could turn defeat into victory. The point is well made and gives the reader a good example of the themes already mentioned—rationality and interaction.

Nine of twelve chapters focus on individual nation-states, and because each is a standalone essay, they can be read in any order. Nevertheless, their selection for inclusion is interesting in itself. China is one of the official nuclear states, having detonated a device in 1964 and thus meeting the conditions laid out in Article IX of the Nuclear Non-Proliferation Treaty. At the other end of the spectrum, Japan also warrants an essay even though it is not a nuclear state. Yoshihara and Holmes include Japan because it does have a robust deterrence policy, linked closely to its relationship with the United States. Developing a nuclear weapon capability, however, is not on Japan's near-political horizon. South Africa is featured as well, having developed a covert nuclear program that it subsequently relinquished. The nuclear and conventional impasse between India and Pakistan ensures that these two nuclear nations receive similar yet contradictory essays. The ambiguity of Iran is discussed. The motivations, policies, and strategies of North Korea come under the microscope. Since the book was published, North Korea has continued to develop and improve its nuclear technology. In hindsight, the essay offers fascinating insight into how the rationality of new nuclear states is difficult to predict with any degree of certainty. The contributors offer many surprises, and I have deliberately not expanded on the details. All I will say is that to gain full benefit, readers should question—really question—the balance of argument.

Each piece not only tells the story of nuclear technological achievement but also adds to our vocabulary of the building blocks of a nation's nuclear strategy. Terms like *credibility*, *nuclear umbrella*, and *extended deterrence* join more familiar verbiage like *first- and second-strike capabilities* or *nuclear security*.

Readers benefit from the layout of *Strategy in the Second Nuclear Age*. No one chapter is overwhelming or contains too much information to absorb. Each one can be read as a standalone entity yet can still contribute to our understanding of what makes nuclear strategy. The editors' analysis in the final chapter requires much more concentration, but at least by this stage our knowledge has prepared us for a more difficult read. Surprisingly, the generic title of the book does not really prepare readers for the level of information included within the covers.

Wing Cdr John M. Shackell, RAF, Retired
Air Force Installation and Mission Support Center
San Antonio, Texas

The Battle of Britain on Screen: "The Few" in British Film and Television Drama, 2nd ed. by S. P. MacKenzie. Bloomsbury Academic (http://www.bloomsbury.com/us/academic/), 1385 Broadway, 5th Floor, New York, New York 10018, 2016, 192 pages, $79.80 (hardcover), ISBN 9781474228459; $20.96 (softcover), ISBN 9781474228466.

In this second edition, S. P. MacKenzie updates his earlier study of the British Film and Television Drama treatment of the *Battle of Britain on Screen*. In modern British history, World War II's Battle of Britain holds a key spot in the collective memory. Facing Adolf Hitler's war machine alone after the fall of France, England knew that its fate rested in the flying skills of a "few" British Royal Air Force (RAF) fighter pilots. The RAF prevented a German invasion by defending England from the Luftwaffe's aerial assault. Since the battle played such a pivotal role in the homeland's survival, it is only logical that a portrayal of that struggle would make its way to both film and television.

The Battle of Britain on Screen does more than merely describe the plot of six movies and television dramas. Rather, it offers a full history of the productions, addressing how each film's concept was developed, how the cast was selected, and how both flying and static aircraft were sourced. Following a brief account of the making of the projects are a synopsis of the plot and technical details about the films. Because movies and television shows are not created in a vacuum, the author also examines the social environment during their production and how it affected the treatment of the Battle of Britain. Finally, the book covers both the critics' and public's reception of these dramas.

Actually produced before the battle, *The Lion Has Wings* (1939) is the first movie that MacKenzie discusses. Filmed in record time as Britain was on the cusp of the war, *The Lion Has Wings* is best described as a teaming with propaganda to bolster British morale, portraying the RAF and British air defenses as nearly invincible. As one might expect, access to British aircraft for air-to-air filming was limited and nonexistent for German planes.

In 1942, fewer than four years after the release of *The Lion Has Wings*, the wartime film *The First of the Few* appeared on the silver screen with its telling of the story of R. J. Mitchell and the development of the legendary Supermarine Spitfire. Although the movie was well received, the producers "took liberties with the facts" (p. 30) to put forward their desired story line.

Angels One Five was the first British post–World War II film (1952) about the Battle of Britain. As with all such movies, securing period aircraft proved difficult; consequently, the film's focus shifted from the machines to the people involved in the battle. Furthermore, the title changed from *The Battle of Britain* to *Angels One Five*, which portrays life at a British fighter station by following Pilot Officer T. B. "Septic" Baird from his arrival on station until his death in combat.

Four years later (1956), *Reach for the Sky* premiered, telling the story of British ace Sir Douglas Bader, who lost his legs in a flying accident prior to the war but fought his way back into the RAF and became of Britain's top aces before he was shot down and captured. Bader actually consulted on the making of the film.

More than 25 years (in 1969) after the Battle of Britain came to an end, a movie of the same name presents both the British and German sides of the battle. Doing so required the production team to walk a tightrope to accommodate both the British and German veterans who served as technical advisers. In this genre of movies, *Battle of Britain* is known for having assembled the largest collection of British and German (actually Spanish-made under license) aircraft. The filmmakers shot a considerable amount of air-to-air footage (primarily in Spain)—so much that the outtakes and excess footage have been used in other more recent Battle of Britain movies (both British and international).

Reflecting a shift away from portraying the "few" (British fighter pilots) as gallant heroes, the television series *Piece of Cake* (1988) portrays the mythical RAF "Hornet" fighter squadron

in what was described as a "revisionist interpretation" (p. 84) of the "few." *Piece of Cake* follows the squadron during the early days of the war with the British expeditionary force in France and ends with the Battle of Britain. Some of the aerial footage is beautiful, but MacKenzie points out that the series is riddled with inaccuracies, including the use of Spitfires in pre-Battle of Britain France (Hawker Hurricanes were too difficult to secure for filming).

In what the author calls "a reaction against *Piece of Cake*" (p. 86), the 1991 television drama *A Perfect Hero* features British Spitfire pilot Hugh Fleming, whose face becomes disfigured when his airplane catches fire after being shot by a German fighter. The story covers Fleming's trials and tribulations in war-torn England during his recovery and attempt to adjust to his disfigurement. Ultimately, he discovers that he feels comfortable only when he flies a Spitfire.

Finally, *First Light* (2010) is based on teenage Spitfire pilot Geoffrey Wellum's autobiography, which he wrote as a form of personal therapy to help him with "survivor's guilt" (p. 114). *First Light* "foregrounded the cumulative psychological stress of aerial combat in a way rarely touched on in earlier screen dramas" (p. 115).

Although the subject of this text is British film and television, MacKenzie does take the occasional detour to briefly discuss non-British productions such as the Czech film *A Dark Blue World* and the American films *Pearl Harbor* and *Yank in the RAF*. Throughout the book, the author highlights the British distain for American movies about the Battle of Britain that depict Americans as heroes who came over to England and saved the day.

Even though *The Battle of Britain on Screen* might appear to be a "niche" book concerned only with a small group of movies and television shows, this account supplies a well-delivered understanding of how the social memory of events affects their portrayal on screen. Aficionados of war movies will certainly enjoy this book, as will students of the Battle of Britain. A quick Internet search confirmed that all of the movies and television shows are still available for purchase. Warbird fans will also enjoy the text because it relates how the various production efforts were able (or not able) to secure the aircraft necessary to bring the movies and television shows to life. Hopefully, S. P. MacKenzie will expand his study of the Battle of Britain by writing a book on the American movie industry's treatment of the European air war.

Lt Col Dan Simonsen, USAF, Retired
Barksdale AFB, Louisiana

Nuclear Nightmares: Securing the World Before It Is Too Late by Joseph Cirincione. Columbia University Press (https://cup.columbia.edu), 61 West 62nd Street, New York, New York 10023, 2013, 280 pages, $26.95 (hardcover), ISBN 978-0-231-16404-7; 2015, $18.95 (softcover), ISBN 978-0-231-16405-4.

Joseph Cirincione's latest work, *Nuclear Nightmares*, offers a thoughtful and balanced look at the issue of nuclear proliferation and arms control. Echoing a recent theme by the Obama administration, Cirincione labels nuclear weapons as one of two threats that could lead to global catastrophe, the other being global warming (p. 1). The author serves as president of the Ploughshares Fund, an organization that finances and supports initiatives to prevent the proliferation of weapons of mass destruction—a fact that helps explain the subject of this work and the title of the publication. Although he desires to focus solely on nuclear proliferation, a concurrent theme running throughout the book is the debate surrounding the nuclear policy of the Obama administration (p. 2).

Cirincione presents arguments from both sides of the particular issues he addresses, including counterproliferation, force structure, modernization, and the nuclear defense budget. While he provides competing views on various matters concerning America's nuclear policy and force structure, the reader can clearly determine which side of the debate the author

aligns with based upon his writing. Cirincione's approach expands beyond current debates about diplomacy and budgets as he adds chapters covering topics like nuclear effects and nuclear accidents. Perhaps the most controversial part of *Nuclear Nightmares* is the declaration that Pakistan is the most dangerous country on the earth. It is not that the nation possesses a nuclear capability, the author argues; rather, it is the "confluence of several disturbing trends[:] . . . an unstable government, a fragile economy, strong extremist influences in its military and intelligence agencies, and enough nuclear material for 200 bombs" (p. 119).

Cirincione acknowledges the realism associated with pursuing nuclear weapons but offers a cooperative diplomatic strategy for confronting proliferation. As he notes, "The main reasons that states acquire nuclear weapons are security, prestige, domestic policies, and, to a lesser degree, technology, and economics" (p. 153). Although realism drives the desire to acquire nuclear weapons, the author states that international regimes can put the genie back in the bottle: "The reason that more states do not have nuclear weapons is because many nations working together have implemented policies to steadily reduce the role and numbers and desirability of nuclear weapons in the world" (p. 154). There appears to be some inconsistency in Cirincione's analysis since most of those nations banning together already possess nuclear weapons. Is this really an international regime at work or just national realism in action as the haves try to keep the have-nots from joining the nuclear club?

Anyone without a firm foundation in nuclear weapons policy, force structures, or even weapons effects will find *Nuclear Nightmares* a solid primer on these issues. Although Cirincione attempts to deal with such matters evenhandedly, his last chapter delves into promotion, which outlines the work of the Ploughshares Fund and other organizations devoted to nonproliferation. Despite such self-aggrandizement, readers will discover in that chapter a treasure of information about grant money available for further research into these topics. *Nuclear Nightmares* takes a compelling look at a national security issue that will continue to grow in importance.

Col Mel Deaile, PhD, USAF, Retired
Montgomery, Alabama

Spies and Shuttles: NASA's Secret Relationship with the DoD and CIA by James E. David. University Press of Florida (http://www.upf.com/), 15 NW 15th Street, Gainesville, Florida 32603, 2015, 370 pages, $49.95 (hardcover), ISBN 978-0-8130-4999-1.

In response to the surprising and successful launch of the Soviet Union's first satellites, *Sputnik I* and *Sputnik II*, a year earlier, the US Congress passed legislation establishing the National Aeronautics and Space Administration (NASA) in 1958. Although this legislation mandated that NASA's space program carry out research in a peaceful, scientific, and open manner—separate from the US national security and intelligence agencies—according to James David's *Spies and Shuttles*, NASA "could not and did not always follow" (p. 3) its own guiding principles. Instead, the lines of separation between NASA and the covert and military operations of the Department of Defense (DOD) and intelligence community were blurred from the beginning despite NASA's well-managed public appearance as an exclusively civilian space-exploration agency.

With clarity and detail, *Spies and Shuttles* lays out the Cold War dynamics that challenged NASA's status as a separate civilian agency, arguing that to accomplish their missions, both sides needed each other's hardware and personnel and heavily depended on each other for data and expertise on foreign spacefaring nations' programs. Organized in

chronological order, the book traces the evolution of the strategic partnership among these strange bedfellows—one that has forced NASA to both veer from its guiding principles and at times operate under severe restrictions imposed by the defense and intelligence agencies. While much of the previous literature on NASA has covered the open, unclassified relationship between civilian and national security space agencies, David's book represents the most careful and comprehensive attempt to demonstrate that their interactions were far more complex, hidden, and classified than previously thought. Despite what its title suggests, this book is not exclusively about their cooperation on the space shuttle program. Rather, by reviewing newly declassified records, David offers a remarkable overview of NASA's history as well as its consumption and criticism of CIA intelligence reports on the USSR's space programs—particularly the national intelligence estimates. The estimates concluded that the Soviets were not engaging in a manned lunar landing program that could compete with Apollo—a determination that did not prove useful during efforts to convince the White House that budgets needed increasing. Over the years, NASA also participated actively in classified and covert activities, including providing the U-2 cover story until the capture of Gary Powers and testing the CIA's A-12 reconnaissance aircraft. David brings to light the contentious discussions and strained interactions regarding limitations imposed on NASA (due to national security concerns), from the first restrictions on Tiros—NASA's first low-Earth-orbital weather satellite and space-based Earth-imaging program—to its systematic land remote-sensing programs. *Spies and Shuttles* also documents the growth and dramatic expansion of NASA during the Apollo era (1961–72) and its continued role as a consumer and critic of the CIA's reports. David maintains that the space shuttle program was the culmination of the partnership and further "sacrificed its guiding principles" (p. 189). Despite the slow start, outrageous price tag, and the absence of flights until April 1981, the shuttle program contributed tremendously to growth of the interaction among civilian and national security agencies until STS-53—the last dedicated DOD mission in late 1992.

Although the subject might be interesting to the wider air and space community, this book is highly recommended to readers seeking to understand the evolution of the US space strategy and integration of space power into global military and intelligence operations. Missing, however, are some critical reflections on how the international security environment affects and challenges NASA's guiding principles. As a curator in the Division of Space History at the Smithsonian National Air and Space Museum, David is fully committed to writing a comprehensive history of the common interests and activities of NASA and national security space programs, but his study includes little interpretation and analysis of that relationship. The account entirely relies on unclassified documents to tell a story since it offers no firsthand individual accounts and interviews that potentially would have added, or perhaps even demanded, a closer critical engagement with the data presented. Moreover, *Spies and Shuttles* neither raises questions for the future nor elicits a debate about the future of NASA's support of the DOD's operations. Perhaps the most significant contribution of this book is that it might generate new research such as studying threat perceptions, the effects of adversary decision makers on American policy makers and agencies, and even wider government deterrence efforts to learn why these agencies engaged in the way they did. None of these shortcomings detracts from the book's exhaustive, insightful, and admirable contribution to our better understanding of the extent and terms of engagement between NASA and national security agencies. We just need a bit more analytical and critical engagement to fully explore the unknown.

Lana Obradovic, PhD
University of Nebraska–Omaha

Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond by Erik J. Dahl. Georgetown University Press (http://press.georgetown.edu), 3240 Prospect Street, NW, Suite 250, Washington, DC 20007, 2013, 288 pages, $29.95 (softcover), ISBN 978-1-58901-998-0.

In *Intelligence and Surprise Attack*, Erik J. Dahl, a retired Navy intelligence officer, examines how and why major surprise attacks—whether by conventional military forces or terrorists—succeed and fail based on intelligence specialists' and policy makers' understanding of strategic and tactical intelligence. He challenges the commonly held belief that intelligence analysis alone can prevent such attacks, asking specifically about the degree of tactical intelligence necessary to do so and the level at which policy makers must be receptive to warnings from intelligence analysts. As he explores these questions, the author compares well-known intelligence failures with well-known successes to determine how and why surprise attacks fail and succeed. Dahl's core thesis is that these strikes are prevented by a combination of precise tactical warning from the American intelligence community and the receptivity of decision makers to the data provided. He argues convincingly that the intelligence community should develop tactical-level capabilities while simultaneously cultivating relationships between intelligence professionals and decision makers who can respond appropriately to specific threats.

Dahl examines several case studies that support his thesis. In chapter 2, he concludes that a lack of tactical intelligence and decision makers' poor reaction toward intelligence allowed the Japanese to carry out the surprise attack on Pearl Harbor. Thus, he takes issue with the conventional notion that sufficient intelligence was available but simply misunderstood or ignored. That said, the author allows both the intelligence community and decision makers to share responsibility for the Pearl Harbor debacle.

Dahl then compares the failures of Pearl Harbor with later American intelligence successes, finding that—in stark contrast to Pearl Harbor—the Battle of Midway benefited from specific tactical-level information on Japanese plans supplied by the American intelligence community and from decision makers' acceptance of such information following Pearl Harbor. This comparison of the two attacks offers the most convincing evidence of Dahl's primary thesis. The following chapter tests his argument on nine case studies of surprise attacks, ranging from the outbreak of the Korean War to Iraq's invasion of Kuwait. Dahl's examination of these cases suffers from cursory analysis that fails to contribute significantly to his overall argument. Additionally, he limits his case studies to an American analyst's point of view. Although the brief treatment of the 1973 Yom Kippur War recognizes the failure of both Israeli and American intelligence, the analysis examines only the Americans' inability to foresee the attack on Israel. At least some consideration of Israeli decision makers' receptivity to the intelligence available to them could have provided additional evidence strengthening Dahl's overall contention.

Although the case studies of Pearl Harbor and the Battle of Midway, as well as Korea and Vietnam, lend support to the author's position, the other studies pertaining to conflicts that did not involve direct US military involvement could have been set aside in favor of more relevant ones (that is, the Cuban missile crisis). Furthermore, even though Dahl's objective is to analyze the use of tactical-level intelligence to prevent surprise attack, he doesn't explain what US policy makers could or should have done to prevent the Soviet invasions of Czechoslovakia and Afghanistan even had they been more willing to consider intelligence indicating imminent invasions. Given the United States' issues in Vietnam in 1968, it is unclear what steps America might have taken to prevent the invasion of Czechoslovakia had President Lyndon B. Johnson's administration been more attune to intelligence warnings. Consequently, Dahl's core argument is most convincing when he addresses attacks on American interests in the second half of the book.

Part 2 examines surprise attacks by terrorists, including the East Africa embassy bombings in Kenya and Tanzania, a failed 1993 strike on New York City, and the 9/11 attacks. The author's analysis of these events offers convincing support for his chief argument by finding that unsuccessful terrorist attacks are not foiled by a sharp intelligence analyst who pieces clues together for a decision maker who in turn reacts promptly to avert the catastrophe. Instead, such attempts fail because government officials pay attention to specific tactical-level intelligence of an attack provided by intelligence professionals. Dahl asserts that although an enemy's hostile intent is often well known and understood by intelligence officials—as it was at the time of the embassy bombings—prevention depends upon whether or not the intelligence community and law enforcement give decision makers sufficiently specific warnings that convince them to take action. His case study of the 1993 attack on New York demonstrates that the attempt failed thanks to specific actionable intelligence and policy makers' acknowledgment of the threat following the 1993 World Trade Center bombing.

Dahl's rather limited selection of choices and his US-centric analysis leave much room for further investigation, a point he himself admits (p. 175). Further, the two chapters in which he tests his argument against a broader range of cases would benefit from more thorough examination and additional case studies. However, this criticism is relatively minor considering the strength of the author's more extensive case studies.

Ultimately, by challenging conventional notions and stressing the importance of relationships between intelligence professionals and decision makers, Dahl sets the stage for further discussion and debate on how the two communities should work together to prevent future surprise attacks. Both military intelligence professionals and individuals involved in policy making would do well to consider his arguments.

1st Lt Herman B. Reinhold, USAF
Department of History
United States Air Force Academy, Colorado

Global Responses to Maritime Violence: Cooperation and Collective Action edited by Paul Shemella. Stanford University Press (http://www.sup.org/), 500 Broadway Street, Redwood City, California 94063-3199, 2016, 344 pages, $27.95 (softcover), ISBN 9780804798419.

Global Responses to Maritime Violence, a collection of essays written by a wide range of subject-matter experts, describes the issues and opportunities associated with violent activities in the maritime environment, as well as their effect on a variety of stakeholders, including those not located on the high seas. The book is well organized and logically presented in three parts. The first part, "Examining Maritime Violence," introduces and describes the problem. In part 2, "Riding the Storm," the contributors provide a detailed review of historical and current operations addressing the issue of violence in the maritime environment. Part 3 offers a series of case studies chosen to reinforce and validate the theories and recommendations of Captain Shemella and his contributors.

Part 1 introduces and identifies the type and scope of violence in the maritime environment. Establishing a baseline, Shemella defines the subject environment as one that includes oceans, seas, and their littoral regions as well as navigable rivers and lakes and the infrastructure that supports them all (that is, ports, locks, and canals). The editor completes the baseline by describing the significant socioeconomic impact of the maritime domain on the world's population.

Contributors then dissect the difference between maritime terrorism and armed criminal activity. Terrorism strikes a strong chord with most readers. Acts of terror, whether for political, religious, or financial reasons, command society's attention. The senseless and remorseless destruction and death associated with the event often outweigh the actual damage it causes. As a result, the fear of terrorism leads one to believe it is far more prevalent than reality suggests.

Despite the fact that terrorism captures the public's attention, armed criminal activity is identified by the contributors as by far the most common form of violence on the seas. The contributors offer an excellent description of the issues and effects arising from criminal activity that targets stakeholders. They also examine the socioeconomic and sociopolitical dangers and effects related to criminal activities against maritime targets.

Part 2 delves more deeply into the cooperative efforts and options available to interdict and mitigate violent activities in this environment. Contributors address the strategy and tools employed by national and international government, nongovernmental, and commercial organizations to detect, monitor, and—when possible—counter terrorist and criminal activities.

Part 3 provides a selection of case studies detailing incidents of terrorism and violent crime on the world's oceans. The case examples include a review of maritime terrorist activities of the Sri Lankan Tamil Tigers insurgency, together with examples of piracy and violent crime on the Horn of Africa, in the Straits of Malacca, and off the coast of Guinea-Bissau. Lessons learned from these cases supply significant validity and credibility for the editor's and contributors' suppositions.

Throughout the book, a number of common themes emerge. For example, the contributors note the lack of consistent governance, especially when vessels operate far from national borders. In some cases, governance is virtually nonexistent, a fact especially true for the littoral and maritime areas located in or near unstable states wracked by political and economic conflict.

Another common theme is that violence on the high seas is a direct extension of sociopolitical and socioeconomic crises and challenges on land. For example, poverty-stricken fishermen in the Horn of Africa may turn to piracy when their primary fishing grounds are depleted due to overfishing or when they are spoiled by industrial pollution. The consistent emergence of common themes across a literary work is an indication of saturation with regard to the subject matter. In research, significant levels of saturation provide a commensurately high level of credibility for the subject matter.

In many ways, *Global Responses to Maritime Violence* is similar to a textbook. The essays are well written, describing their subjects in coherent, easy-to-understand concepts. Under the editorial control of Captain Shemella, the contributors first develop the reader's base of knowledge regarding issues faced by stakeholders operating within or depending upon the maritime environment. The second part then builds on the first by informing the reader's knowledge of the concepts and options available to government, nongovernmental, and commercial organizations tasked with maintaining governance on the seas. Part 3 knits the first two sections together through real-life examples of terrorism and violent crime in the maritime environment. By the end of the book, the reader has acquired a broad knowledge of the issues, complexities, and options associated with this diverse and complex area of the world.

The book's academic style reflects Shemella's pedigree as a lecturer and subject-matter expert at the Naval Postgraduate School in Monterey, California. He possesses the requisite knowledge to discuss the issue and has gathered together a distinguished group of experts to delve more deeply into specific concepts and issues related to the topic. *Global Responses to Maritime Violence* could easily be used as a primary text for a course in either maritime or homeland security.

Unlike most textbooks, however, this study is an easy and informative read. The editor's presentation of concepts, coupled with examples, keeps the reader's attention without coming across as preaching or lecturing. Instead, Captain Shemella and his contributors teach by telling a story that happens to be true. Consequently, the book is not only informative but also enjoyable. I recommend *Global Responses to Maritime Violence* to any individual—academic or otherwise—interested in the subject of terrorism or violent crime in the maritime environment.

John L. Mahaffey, PhD
NATO Communications and Information Agency
The Hague, Netherlands

Operation Overflight: A Memoir of the U-2 Incident by Francis Gary Powers with Curt Gentry. Potomac Books (http://www.nebraskapress.unl.edu/pages/PotomacBooks.aspx), University of Nebraska Press, 1111 Lincoln Mall, Lincoln, Nebraska 68588-0630, 2003, 344 pages, $27.95 (softcover), ISBN 978-1-57488-422-7.

When I was stationed at Osan Air Base, Republic of Korea, from 1996 to 1998, I often heard the roar of U-2s launching. I recall a memorable protocol visit, standing on the Osan flight line with a World War II fighter ace and his spouse, a Korean War fighter ace and his WASP (Women's Airforce Service Pilot) spouse, and base leaders. We were filled with anticipation, and our excitement increased as we observed the U-2 taxi onto the runway, launch, and vanish from sight. The exhilaration that we felt that day equates to the intellectual and emotional stimulation that people will experience when they read *Operation Overflight: A Memoir of the U-2 Incident*.

I spent several days rereading this thought-provoking and inspiring memoir. Kudos to the authors for their personable writing style and foreshadowing reflected in such passages as "one question was never asked, one subject never discussed" (p. 21) and "maximum altitude" (p. 78), which occur throughout the book. These and other literary hooks kept me wondering if or when the authors would reveal the answers.

The tantalizing bread crumbs that they strategically shared made it difficult to select a topic for this review. For example, should I focus on the U-2's mechanical and utilization evolution, good and bad? Questionable decisions about centralized control and decentralized execution that were made without consulting the experts? Pulitzer Prize–worthy spin-doctored material that yielded the perfect scapegoat-making platform? The captivating historical interconnectedness of the Korean conflict, *President Kennedy* (emphasis added), and the 1968 North Korean capture of a US spy ship? Conspiracy theories, including one about a US Marine Corps private who in 1959 defected to Russia and was mentioned in the National Archives "Commission Document No. 931 [that] is still classified and withheld from research [as of 13 October 1969]. . . . The title . . . is '[*Lee Harvey* (emphasis added)] Oswald's Access to Information About the U-2'." (p. 305)

Exploring these and other topics, this review focuses on Francis Gary Powers the leader. Given the opportunity, I would have jumped at the chance to serve under him—a statement I would make to and about only a few leaders. His courage to ask the tough questions, do what's right in the best interest in our nation, and strengthen his resilience when it appeared that several US government leaders, reporters, and citizens called or considered him a traitor is praiseworthy.

Glimpses into his character-building begin in chapter 1. Sharing insight into his youth, the authors highlight how after his first airplane ride, Mr. Powers was hooked. His patriotism grew to such an extent that although he missed World War II, he would find a way to

serve and, hopefully, fly. During this time, Mr. Powers's rebellious streak and search for exciting adventures sprouted when he enlisted in the Air Force. In 1951 he became an officer and joined the Air Cadets.

Enter the "Agency" (Central Intelligence Agency [CIA]) in 1956. The remainder of chapter 1 and all of chapter 2 elaborate on how Mr. Powers and others became CIA civilian pilots, the training they received, and the eagerness to collect information from behind the Iron Curtain. At this point (circa March 1960), the rebellious Mr. Powers posed the unasked question and topic never mentioned by the Agency: " 'What if something happens and one of us goes down over Russia? . . . What story does he use? Exactly how much should he tell?' His [Agency intelligence officer's] exact words were, 'You may as well tell them everything, because they're going to get it out of you anyway' " (p. 52).

Chapter 3 includes details of Mr. Powers's 1 May 1960 capture, incarceration, interrogation and trial, and treatment. Notable actions include his ignoring CIA guidance and abiding by the code of conduct created after the Korean conflict and learned while he served in the Air Force. The fact that he had to play by the rules of a foreign judicial process and was unable to defend himself or make an appeal seems unreal. I wonder how many people could have prevailed in similar circumstances.

Chapter 4 describes the deplorable behavior of the press and senior US government officials who maligned Mr. Powers when he could not defend himself publicly and honestly. Only after openly testifying before Congress was he praised for demonstrating loyalty to his country. As the truth was revealed, the American public started expressing its skepticism of the media and the government, wondering what other deceptions lurked about.

Along with Mr. Powers's strength of conviction to set the story straight by writing a book, his loyalty continues to shine in chapter 5. Here, the authors justify criticism of certain agencies and individuals but, in fairness, thank them for their beneficial efforts and support. Despite the fact that many individuals in the United States initially considered Mr. Powers a traitor (perhaps some still do), he remains protective of his nation: "I have omitted some matters which I feel could affect present national security" (p. 307). Mr. Powers never revealed the "maximum altitude" at which a U-2 could fly.

Anyone who wishes to explore Mr. Powers's admirable behavior, to learn from history, to examine espionage and groupthink, to use the power of deception for the greater good, and to encounter themes relevant to our current volatile environment should read this book. I believe that Mr. Powers was on target when he said, "There was much that could—no *should*—be known if for no other reason than to avoid repeating the same mistakes in the future" (p. 283). Hopefully, more people will read *Operation Overflight: A Memoir of the U-2 Incident* and, like Mr. Powers, think critically, ask tough questions, take action, admit mistakes, protect our nation, and catalyze positive change by doing the right thing.

Lt Col Katherine Strus, PhD, USAF, Retired
San Antonio, Texas