ASPJ Air & Space Power Journal

Vol. 34, Issue 3 Fall 2020

ASPJ Air & Space Power Journal

Air & Space Power Journal
600 Chennault Circle
Maxwell AFB AL 36112-6010
e-mail: aspj@au.af.edu

Visit *Air & Space Power Journal* online at https://www.airuniversity.af.edu/ASPJ/.

https://www.af.mil/

https://www.aetc.af.mil/

https://www.airuniversity.af.edu/

SENIOR LEADER PERSPECTIVE

FEATURES

VIEWS

BOOK REVIEWS

Air & Space Power Journal Reviewers

Christian F. Anrig, PhD
Swiss Air Force

Filomeno Arenas, PhD
USAF Air Command and Staff College

Bruce Bechtol, PhD
Angelo State University

Kendall K. Brown, PhD
NASA Marshall Space Flight Center

Anthony C. Cain, PhD
Wetumpka, Alabama

Norman C. Capshaw, PhD
Military Sealift Command Washington Navy Yard, District of Columbia

Christopher T. Colliver, PhD
Wright-Patterson AFB, Ohio

Chad Dacus, PhD
USAF Cyber College

Maj Gen Charles J. Dunlap Jr., USAF, Retired
Duke University

Sandra L. Edwards, PhD
Thomas N. Barnes Center for Enlisted Education

Lt Col Derrill T. Goldizen, PhD, USAF, Retired
Naval War College

Col Mike Guillot, USAF, Retired
Editor, Strategic Studies Quarterly

Col Dale L. Hayden, PhD, USAF, Retired
Birmingham, Alabama

John M. Hinck, PhD
USAF Air War College

Brig Gen S. Clinton Hinote, USAF
Air Force Warfighting Integration Capability HAF/AJA, Pentagon

Thomas Hughes, PhD
USAF School of Advanced Air and Space Studies

Lt Col J. P. Hunerwadel, USAF, Retired
Curtis E. LeMay Center for Doctrine Development and Education

Tom Keaney, PhD
Senior Fellow, Merrill Center at the School of Advanced International Studies

Col Merrick E. Krause, USAF, Retired
Executive Director, Resource Management and Planning Board of Veterans' Appeals, Veteran's Affairs

Col Chris J. Krisinger, USAF, Retired
Burke, Virginia

Benjamin S. Lambeth, PhD
Center for Strategic and Budgetary Assessments

Rémy M. Mauduit
Montgomery, Alabama

Col Phillip S. Meilinger, USAF, Retired
West Chicago, Illinois

Richard R. Muller, PhD
USAF School of Advanced Air and Space Studies

Lt Col Jason M. Newcomer, DBA, USAF
USAF Air Command and Staff College

Col Robert Owen, USAF, Retired
Embry-Riddle Aeronautical University

Lt Col Brian S. Pinkston, USAF, MC, SFS
Air Force Review Board Agency

Maj Gen John E. Shaw, USAF
Headquarters Air Force Space Command A5/8/9 Peterson AFB, Colorado

Col Richard Szafranski, USAF, Retired
Isle of Palms, South Carolina

Lt Col Michael Tate, USAF, Retired
USAF Air University

Lt Col Edward B. Tomme, PhD, USAF, Retired
CyberSpace Operations Consulting

Lt Col David A. Umphress, PhD, USAFR, Retired
Auburn University

CMSgt Michael J. Young, USAF, Retired
Montgomery, Alabama

Xiaoming Zhang, PhD
USAF Air War College

Brent A. Ziarnick, PhD
USAF Air Command and Staff College

Information Warfare, Cyberspace Objectives, and the US Air Force

Brig Gen Gregory J. Gagnon, USAF

Cyberwarfare is an emerging battlefield, and we must take every measure to safeguard our national security secrets and systems. We will make it a priority to develop defensive and offensive cyber capabilities at our U.S. Cyber Command and recruit the best and brightest Americans to serve in this crucial area.

—White House, 7 January 2017

Good or bad, odd or even, night or day, from a very young age, and throughout our schooling, we are taught through dichotomous logic. It often unconsciously shapes how we perceive the world and impacts our decisions. Before we were the Department of Defense (DOD), we were the Department of War. That dichotomous logic of war or peace often extends unconsciously to America's thinking about defense and security. The *National Defense Strategy* correctly identifies this national cognitive bias. It articulates a need for the DOD and the nation to compete today below the threshold of war to defend and secure US national security objections against adversaries who are actively using all elements of their national power to achieve their desired outcome. Although we use the term *information warfare*, such activities may be most impactful in times below the threshold of war. In October 2019, the US Air Force established the Sixteenth Air Force, our Information Warfare Numbered Air Force, and in only a short nine months and three days rapidly accelerated this organization from the

initial operating capability to the Headquarters *full* operating structure by July 2020.

Information warfare is often a debated term; in fact, it currently lacks an approved joint definition. But for the Air Force, we are focusing on information warfare (IW) as activities that synchronize the elements of intelligence, surveillance, and reconnaissance, cyberspace operations, electromagnetic warfare, and information operations to achieve outcomes in times of both war *and* peace. Today, the Air Force describes *information warfare* as "the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior."[1]

As a subset of IW, military activities in cyberspace often receive an increased amount of press. Those not involved in these activities sometimes think these military and security activities are fundamentally different and unique. But when space and cyberspace are thought of as separate and different from other domains of warfare or as separate and different elements of statecraft, our ends can become myopic, disjointed, and suboptimized. The more germane question to consider is how can cyberspace and operations in, through, and from cyberspace support US national interests? Deeper thinking about this issue reveals a strategic opportunity. Unfettered, ubiquitous global access to cyberspace is a national interest for the US, meaning a strategic objective should also be "unrestricted" access to the global network *for other global citizens*. The US Air Force is preparing itself to capitalize on this opportunity.

The Executive Branch issued an executive order on 11 May 2017 "to promote an *open*, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft." The executive order also directed multiple Executive Branch directives to assess cyberspace risk management across the federal government with follow-on requirements to build plans to improve our defensive posture. From a strategy perspective, these defensive actions are intended to deny our adversaries benefits from attacking through diminishing the likelihood of a successful attack operation.

After entering office, the Trump Administration boldly pronounced in its "Making Our Military Strong Again" proclamation that "cyberwarfare is an emerging battlefield, and we must take every measure to safeguard our national security secrets and systems. We will make it a priority to develop defensive and offensive cyber capabilities at our U.S. Cyber Command."[2] Since then, many organizational changes have occurred within the DOD. Both US Cyber Command (2018) and US Space Command (2019) were elevated to full unified combatant command status to enhance and secure our need for freedom of action in both respective

domains. Additionally, services have realigned corresponding capability development organization to meet the expanded organizing, training, and equipping needs.

Adversary attack activity is incentivized by our defensive posture or the lack thereof. The criticality of the internet to our economic well-being is fully documented and widely understood. Equally clear and documented are the cyberspace dependencies laced throughout our critical resources and key infrastructure. By and large, much of our academic writing and policy thinking about cyberspace deterrence has been about deterring adversaries by our own defensive actions. Deterrence outcomes manifest inside a decision-maker's mind. It is a complicated balancing of risk and perceived gain. In this calculus, offensively threatening an adversary is important to incentivize their restraint. An aspect that is less clear to most Americans is how information and offensive cyberspace activities can be used to promote US interests abroad and cause our adversary leadership to have to factor in the threat of a US information attack.

The offensive side of the strategy debate often remains hidden from public discourse. When most think of offensive cyberspace warfare, they think of a Hollywood portrayal of a young man, fueled on energy drinks, wearing a hooded sweatshirt hacking in the midnight hours. Or they might think of today's Russian sponsored third-party internet trolls creating disinformation for others to read and believe. Either way, we inherently assume a dark, pejorative un-American way of statecraft and these dishonest activities should make us uneasy. But what if offensive cyberspace activities could be completely congruent with promoting our foundational ideals—freedom of speech, freedom to assemble, and a commitment to truth and reason?

Using tailored operations actively promoting these foundational ideals, through and from cyberspace, would be very similar to the whole of government approach we used to battle communism during the Cold War. During the Cold War, we pursued a containment strategy against the Soviets. Resident within this approach was an active information component transmitted via Voice of America into the darkest corners of the world. Voice of America news broadcasts were a key tenet in how we countered the Soviet Union's expansionary policies in Eastern Europe with a counterbalancing barrage of freedom of expression and freedom of the press. Equally important to our strategy were approaches designed to hold our adversary's military might at a disadvantage. The Strategic Defense Initiative, which was dubbed "Star Wars," was envisioned to protect the US from Soviet nuclear forces. From the Soviet perspective, their strategic forces were the key to their stabilizing strength. The DOD and 16th AF's outreach and collaboration with the Department of State's Global Engagement Center is more profound than most would consider due to the change in today's information environment.

Our ability to project truth can now be enhanced. For example, changes in the global space market such as SpaceX's desire for true global internet connectivity from micro satellites make this access environment more fertile.

Today's most vexing national security challenges are the expansionary foreign policies of Russia, China and Iran and the threats to our homeland by a nuclear-capable North Korea. At first glance, these problems seem unrelated. But upon deeper analysis they each share similarities. These nondemocratic states are closed information societies with autocratic ruling elite. In each case, the internet and ubiquitous access to information and the expression of ideas are seen as threats. What these ruling elite hold most dear, is their illegitimate right and means to rule. *We, as a nation, should directly hold this at risk.*

Expanding free, unfettered access to all global citizens is in the best interest of the United States. But the value is two-fold. First, it expands the key market and most robust portion of the US national economy. Second, it threatens and holds at risk what our adversaries hold most dear—*information control* necessary to legitimize their autocratic rule. Today, micro technology, space, and cyberspace innovation make this possible. From a whole of government perspective, such an approach might contemplate subsidizing, promoting, and utilizing free global internet access to create greater leverage against autocratic regimes. Fundamentally the concept is to open closed societies via the information domain. The military objective in this approach is develop information access.

Unfortunately, the changing nature of statecraft and warfare is already understood by Russian and Chinese leaders. Both nations are conducting aggressive information statecraft while having weaker conventional forces vis-à-vis the United States. The utility of state power, both hard and soft, is to achieve desired ends. . . both should be used in a complimentary manner. The United States' military traditionally does not successfully use IW to improve its positional advantage in peacetime. In Russian practice, doctrine, and writing, we see Russia actively pursuing activities to exploit perceived vulnerabilities of democratic societies short of armed conflict. Information confrontation or informatsionnoe protivoborstvo (IPb) is not a new strategy for the Russians (previously known as active measures). They divide IPb into two useful subsets—informational-technical (electronic warfare, cyber) and informational-psychological (influence). The key element in the information confrontation strategy is to create confusion and sow doubt in the existence of truth. In Georgia, Ukraine, Western Europe, and the United States, Russia is pursuing this approach. Russia integrates IPb at all levels of conflict and statecraft. Russia is playing an offensive game, but what if they also needed to allocate resources to the defense? Internal to Russia, the internet is monitored by the government. Recent 2019 legislation dubbed the "sovereign internet" law gives Russian

officials wide-raging powers to restrict traffic. Within Russia this is legal and now accepted. Wisely, Russian critics fear the government is trying to create an internet firewall similar to the one employed by the Chinese Communist Party in China. In both countries, the Western concept of individual rights are subordinated to the state. Exposing their risk may cause adversary leadership to recalculate their current courses of action and dis-incentivize their current behavior.

The core US interest in cyberspace remains freedom. Freedom to access information, freedom to express, and in the virtual world, freedom to assemble. We inherently believe in truth, and that through open debate, truth can be discerned. Americans do not fear facts, but our adversaries do. The larger issue to address is not the application of this idea in times of war; it is to recognize *the true value of this approach is in times of peace and state competition.* The twentieth century's broad lesson is that democratic societies prevail over autocratic states and that people long to be free. This is a founding ideal of America. This ideal remains as valid today as it did in 1776, and I suspect it will still be valid in 2076.

I see US Cyber Command and US Space Command as the key elements in expanding our nation's ability to do the informational-technical. The more important piece for us as a nation is to preemptively agree to speak the truth. The truth that freedom of speech matters, the truth that freedom to assemble matters, and the truth that government censorship and control is wrong. People in Russia and China are not afforded liberty. Short of armed conflict, we can create wonderful dilemmas for adversary leadership. They certainly are not holding back on us.

We should not cede space and cyberspace to our adversaries due to a lack of critical thinking about the advantages they can afford us from an offensive perspective. An American national security objective should enable and provide global, unfettered access to the internet, not just for the US but for the world. America leads the world in both the space and the cyberspace markets. Our nation is a nation of innovators. This is well in the realm of doable, and we are a nation of doers. If our adversaries continue to electronically steal our digital intellectual property, attempt to compromise critical US infrastructure, and further erode our military advantage, playing just defense is proving insufficient. Holding at risk their ability to censor the internet is the right leverage to rebalance the equation. ✪

Brig Gen Gregory J. Gagnon, USAF

Brigadier General Gagnon (BA, Saint Michael's College; MS, Naval Postgraduate School; MA, Air University; MA, National War College) is the director of intelligence for Headquarters Air Combat Command (ACC). In this capacity, he advises the ACC commander on organizing, training, equipping, and maintaining combat-ready intelligence forces for rapid deployment and employment in support of combatant commanders and the National Command Authority.

Notes

1. Headquarters United States Air Force, Program Guidance Letter 19-05, Establishment of the Information Warfare Component Numbered Air Force under Air Combatant Command, 6 September 2019, 5.
2. White House, "National Security & Defense," 7 January 2017, https://www.whitehouse.gov/.

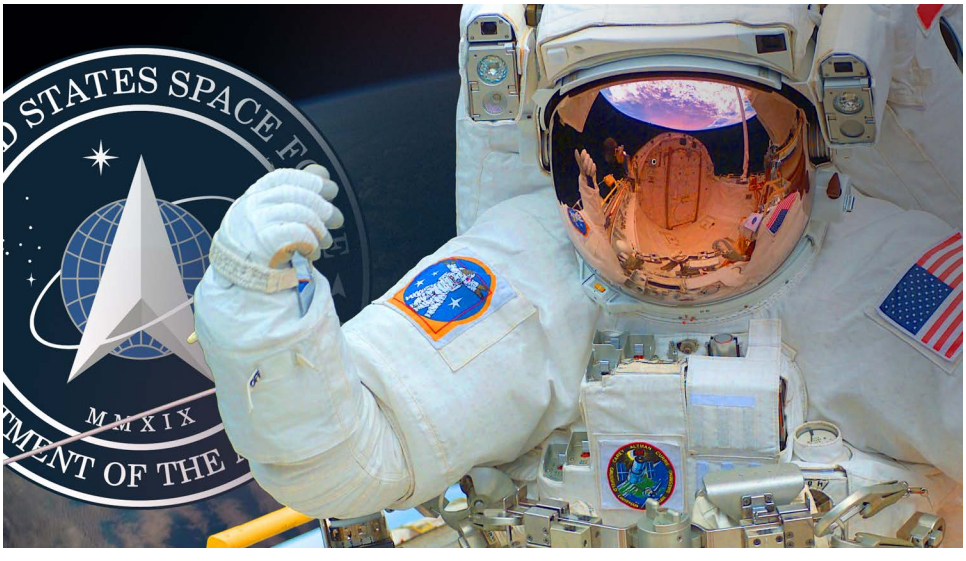
FEATURE

Establishing a Space Profession within the US Space Force

Lt Col Bryan M. Titus, USAF

We're not a profession simply because we say we're a profession.

Gen Martin E. Dempsey, Chairman of the Joint Chiefs of Staff
"General Dempsey's Letter to the Joint Force," 1 October 2011



Introduction

In 2019, the United States demonstrated its strategic commitment to the space domain by reestablishing US Space Command and creating the US Space Force. For the last two decades, the US, and particularly the Air Force, wrestled with the imperative to develop a cadre of military space professionals. The emergent Space Force provides an opportunity to revisit the topic of space professionalism and consider its importance within the space service. The Air Force made important strides in space professional development, but its focus centered on the individual space professional rather than the institutional space profession.

"How can I be a professional if there is no profession?"[1] This provocative statement came from an Army major in 1999 as her service assessed the health of Army professionalism, implying that professional development relies on a well-established profession. The Army developed an extensive body of work on the topic and showed that establishing and maintaining a profession goes beyond education and training. Professions require a focus not only on competence, but

on other factors such as character, commitment, trust, and stewardship at the institutional and individual level. Army scholars observed that a military service, as a profession and a large government bureaucracy, is dual-natured, and military leaders must ensure that service behavior leans more toward profession than bureaucracy.[2] Army experiences and insights into promoting its profession are instructive toward solidifying a space profession within the Space Force.

During the last 20 years, the US government issued a myriad of policies and assessments emphasizing the development of a space professional cadre to maintain space dominance. The 2001 Space Commission recognized the importance of developing a space-minded workforce and recommended that the government "create and sustain. . . a trained cadre of military and civilian space professionals."[3] Congress subsequently added a provision to US Code, Title 10, for the Air Force to create a career field for space system development, which the service chose not to implement.[4] The Air Force instituted a formal program to build a professional cadre from the space operations and acquisition career fields, primarily through space-focused training and education opportunities and professional certification.[5] Despite Air Force efforts to implement Space Commission recommendations, space programs continued to experience significant cost and schedule overruns and multiple congressional oversight reports identified shortfalls in space workforce expertise, particularly in space acquisitions. The successful development of space professionals at the individual level requires the firm establishment of a space profession at the institutional level and an institutional commitment to develop the profession properly. When space was simply another mission in the Air Force portfolio, it was reasonable to assume that providing space-focused training and education to Air Force professionals was sufficient. However, the space domain's elevated strategic importance justifies a separate military space service and should also warrant a distinct military space profession.

The Space Force should be built on the foundation of a space profession of arms because:

1. Effective professions instill service, expertise, ethics, identity, and stewardship in their members.
2. Military services that do not identify as a profession will tend to behave more like a bureaucracy.
3. National-level policies and assessments of the space workforce consistently emphasize the need for space professionals and indicate that Air Force efforts have not met expectations.
4. The emerging strategic environment demands an effective space workforce.

5. The creation of the Space Force provides an unprecedented opportunity to formally establish the space profession as its basis.

To this end, this article first introduces the defining characteristics of professions and identifies the unique aspects and challenges of military professions. Second, the article discusses the recommendations and policies of the US toward developing the military's space workforce and evaluates the Air Force's efforts. Third, it analyzes the strengths, weaknesses, opportunities, and threats that will help shape the military space profession. Finally, this article recommends four specific actions for instituting a military space profession within the Space Force.

Characteristics of Professions

Medicine, theology, law, and military service are traditionally considered professionalized occupations.[6] The following factors generally characterize professions:

Service: Professions provide a useful and vital *service* that society cannot provide for themselves.[7]

Expertise: Professions possess and apply *expertise*, specialized knowledge, and unique skills in their practice.[8]

Ethics: Professions are guided by a *professional ethic* that is determined by their values, beliefs, laws, and moral standards.[9]

Identity: Professions are united by a *professional identity* that creates a shared purpose and is influenced by culture, ethos, expected behaviors, customs, traditions, titles, and attire.[10]

Self-regulation: Professions *self-regulate*; they have a collective responsibility to self-police and certify educated, proficient, and ethical professionals.[11]

Professions earn the *trust* of society through effective and ethical application of their expertise, and, in exchange, society grants them a high level of *autonomy* and *discretion* to apply their expert knowledge and necessary skills in service of society.[12] If a profession does not maintain society's trust, it will gradually begin to lose the autonomy and discretion needed to practice its profession. While the factors outlined above apply to professions in general, military professions have unique characteristics and challenges.

Unlike other professions, military professions are responsible for the coordinated management of violence, and they are required to operate as a profession within a large government bureaucracy. There are currently three distinct warfighting professions in the US, corresponding with the departments of the Army, Navy, and Air Force.[13] Each service provides expertise for its respective warfighting domain—land, sea, or air and space.[14] Gen Martin E. Dempsey, former

chairman of the Joint Chiefs of Staff, emphasized that the military profession is unique because of its "expertise in the justified application of lethal military force and the willingness of those who serve to die" for the nation.[15] Because of the national defense mission's lethal nature, it is necessary for the services and the Department of Defense to preserve the key characteristics of the military profession and ensure service members understand their roles, responsibilities, and obligations as military professionals. It is also important to recognize the dual nature of a military service. Each military service is a profession and a bureaucracy at once, creating a challenge because professions and bureaucracies often have competing perspectives for problem solving. Professions are primarily concerned with effectiveness, while bureaucracies focus more on efficiency.[16] The notion that military services are both a profession and a bureaucracy is not necessarily a negative concept. Military bureaucracies must co-exist and operate accordingly to compete for resources in the greater bureaucracy. However, military leaders should remain vigilant to ensure the bureaucratic tendencies do not dominate the military profession.[17] Bureaucratic decision-making is sometimes colored by parochialism, infighting, bargaining, compromise, and resistance-to-change.[18] Military professions are better postured for success in this paradigm when the characteristics of a profession are understood and reinforced at each echelon.

Army scholars have published a wealth of information on their profession, and the Army codified many of these findings in service doctrine. The Army War College offered a concise description of attributes that professions should strive for at the institutional and individual levels (see the table).

Table. Attributes of professions and professionals

Profession	*Professional*	*Description*
Expertise	Skill	Professions require expertise, demonstrated as unique skills in the professional.
Trust	Trust	Trust is the currency of professions, both externally and internally.
Development	Leadership	Professions require continuous development of individuals, manifested as leadership by professionals.
Values	Character	Professions require a value-based ethic, demonstrated in the character of individual professionals.
Service	Duty	Professions provide a vital service, manifested in the duty of the individual professional.

Source: Don M. Snider, Once Again, The Challenge to the U.S. Army During a Defense Reduction: To Remain a Military Profession *(Carlisle Barracks, PA: Army War College, February 2012), 19–20.*

Army doctrine instituted these concepts into the essential characteristics of the Army profession (trust, honorable service, military expertise, stewardship, and esprit de corps) and the certification criteria for Army professionals (competence, character, and commitment).[19] The Army War College's recommendations, the

characteristics of the Army profession, and the certification criteria of the Army professional, directly correlate with the characteristics of professions described earlier in this section. The Army's model could be tailored to meet the military professions' unique requirements in other war-fighting domains.

The decision to establish the Space Force provides an opportunity for the new service to solidify a profession of arms for the space war-fighting domain, like the war-fighting professions of the air, land, and sea. Though aspects of a space profession are evident in the Air Force, there is still room for growth. The lack of a clearly defined space profession and the Air Force's reluctance to create a space acquisition career field limited space professional development. They impacted the Air Force space programs' execution, which arguably contributed to the need for an independent space service. The nature of the military space mission puts the space service several steps removed from the "fighting and dying" aspect of the profession of arms. While physical courage may not be as relevant, moral courage and character remain essential to mission success. This unique nature of the space mission creates an even greater imperative to institute a military space profession. It provides the service with an overarching construct for establishing its own military culture, values, and system for developing and certifying professionals. Like the Army, space professional certification should go beyond competence and incorporate the elements of character and commitment.

The 2001 Space Commission

The Fiscal Year 2000 National Defense Authorization Act formally established the Space Commission to assess the management and organization of National Security Space (NSS).[20] The resulting Rumsfeld Commission report provided five key recommendations: to leverage space to modernize US forces, enhance intelligence collection from space, shape the space regulatory environment, promote technology investment, and create a trained cadre of military and civilian space professionals.[21] The commission recognized that to fully exploit the complex technology and operational concepts of future space, the government would need a deep pool of expertise in science, engineering, and systems operations and leaders with extensive space experience.[22] Additionally, the commission emphasized developing space professionals with a depth of experience in their field and a breadth of understanding across the range of space mission areas.[23] Congress reinforced the commission's recommendations by establishing a law for the Air Force to create an officer career field with the technical competence to develop and operate space systems. Although a space operations career field was already well established, the Air Force did not create a career field focused on space sys-

tems development. Space Command did, however, move quickly to address the Rumsfeld Commission recommendations.

Space Professional Development Program

In response to the Rumsfeld Commission, Air Force Space Command (AFSPC) pursued the Space Professional Development Program (SPDP) to identify and develop a cadre of space experts from the operations and acquisition career fields. AFSPC defined *space professionals* as "skilled and knowledgeable in the development, application and integration of space concepts, doctrine, and capabilities to achieve national security objectives."[24] The SPDP provided continuous learning opportunities toward professional certification and documented individual space experience to inform future assignments in military space. Space Command made SPDP its priority and accomplished several significant milestones toward achieving its vision.[25] It stood up the Space Professional Management Office, gained Secretary of the Air Force approval for the SPDP strategy, established the National Security Space Institute to provide basic, intermediate, and advanced space courses. It also formalized a professional certification program, redesigned the space operations badge as "space wings," and codified the SPDP in Air Force policy.[26] By the end of 2004, more than 7,000 Air Force members were identified as space professionals.[27] Though widely embraced by the workforce, SPDP was somewhat limited in its ability to formally establish a space profession within the Air Force institution.

Despite the SPDP's efforts, two key elements are missing from the Air Force's approach—the formal establishment of a space profession and the creation of a space acquisition career field. First, the characteristics and attributes of a space war-fighting profession are not defined in Air Force policy or guidance. A central assumption is that the effective development of professionals requires the formal establishment of a well-defined profession. Professionals should understand their profession's concepts of service, ethics, identity, and self-regulation so they can fulfill their role in meeting the profession's obligation to society. For example, the five characteristics of the Army profession and the three components that are used to certify Army professionals are codified in Army doctrine. Air Force policy outlines training and education criteria for certifying space professionals but does not define the space profession's distinct characteristics.[28] Specific recommendations for space profession characteristics will follow. Space professionals will find it difficult to self-regulate if these characteristics are not codified and effectively communicated.

Second, the Air Force did not establish a separate space acquisition career field to develop a depth and breadth of expertise in space system development. As dis-

cussed, professions possess and apply expertise, specialized knowledge, and unique skills in their practice. Assuming that operations *and* acquisition expertise are necessary for the end-to-end success of a military space program, establishing a distinct space acquisition career field would strengthen the acquisition expertise within the space profession. While the space operations career field is well-established and provides operators with multiple avenues for honing their expertise, the lack of a space acquisition career field limits the development of space acquisition expertise. Space acquisition life cycles and operating environments are inherently different than the acquisition lifecycles and operating environments for nonspace weapon systems. Building space acquisition experts warrants successive assignments delivering space systems, rather than rotating between space and nonspace programs. The 2001 Space Commission recommended building a cadre of space professionals with the necessary depth and breadth to effectively develop and deliver space capabilities. Still, the Air Force did not commit to a space acquisition career field, and multiple space programs have experienced significant cost and schedule overruns. Acquisition career field managers have argued that "the acquisition skills needed for an acquisition program—such as those for program management, engineering, and contracting—are largely the same regardless of the product type."[29] This dynamic illustrates the struggle between bureaucratic efficiency and professional effectiveness. From the bureaucracy's perspective, identifying a subset of members as space acquisition officers limits the flexibility of the Air Force to assign acquirers to nonspace programs and is therefore inefficient. From the profession's standpoint, establishing a space acquisition career field enables the service to develop and manage the careers of its space-experienced scientists, engineers, and program managers, increasing expertise and the effectiveness of its major space acquisition programs. The Air Force wants to develop acquisition officers with breadth in multiple weapon systems, while the space profession needs acquirers with depth in space weapon systems. Ultimately, the Air Force decided to manage its acquisition workforce at the corporate level with a secondary consideration for tracking space-experienced acquirers to space assignments. While the Air Force resisted external calls to create a separate acquisition career field, military space programs and the space workforce remained under heavy scrutiny.

Subsequent Assessments of the Space Workforce

In addition to the 2001 Space Commission, the White House, Congress, and the Government Accountability Office (GAO), the "congressional watchdog," generated numerous policies and reports on space programs and the space workforce. The following list provides a snapshot of major developments over the last two decades, highlighting cost and schedule challenges associated with the Space-Based Infrared

System (SBIRS) and the Global Positioning System (GPS). However, several other space acquisition programs experienced significant challenges, as well.

- 2001: Congress established a law mandating an Air Force career field for space development.
- 2005: The SBIRS was $6 billion over cost and delayed six years against its program baseline.[30]
- 2006: *National Space Policy* emphasized space professional development and expertise in space-based science, engineering, acquisitions, and operations.[31]
- 2007: The GAO warned of expertise shortages in the space acquisition workforce.[32] Congress created the Allard Commission and highlighted the need for a space acquisition career field.[33]
- 2008: The Allard Commission recommended the Air Force modify its personnel policies to promote technical competence, experience, and continuity for space acquirers.[34]
- 2009: The SBIRS was $7.5 billion over cost and delayed seven years against its program baseline.[35] The GAO noted significant expertise shortages in major space programs.[36]
- 2010: *National Space Policy* directed the development and retention of space professionals.[37]
- 2011: The first SBIRS satellite launched, but the program was almost $14 billion over cost and nine years behind schedule.[38] The *National Security Space Strategy* emphasized space cadre development.[39]
- 2012: The GAO turned its attention toward cost and schedule growth on the GPS program.[40]
- 2013: The GAO identified disconnects between synchronizing satellite, ground control systems, and user equipment for multiple space programs, including GPS.[41]
- 2015: The GPS ground segment schedule slipped four years.[42] The SBIRS ground segment schedule delayed the usability of on-orbit sensor data for five years.[43]
- 2017: The GPS program was $3.4 billion over cost and delayed five years against the baseline.[44] The GAO highlighted concerns with synchronizing GPS space, ground, and user segments.[45]
- 2019: The GAO questioned whether the Air Force had sufficient space expertise to manage its space programs and noted that the space acquisition workforce was not routinely monitored.[46] President Trump directed the establishment of the Space Force.

Despite strong support from congressional and national leadership for the development of a space professional cadre, space program execution indicates that Air Force efforts did not meet expectations. Concern for the management of the space acquisition workforce is a recurring theme, related to the cost and schedule challenges experienced by several major space programs. Since 2001, Air Force programs that provide missile warning, satellite communications, and satellite navigation breached Nunn-McCurdy acquisition thresholds multiple times, and yet, the Air Force never created a space acquisition career field. Dr. John Stopher, a former space policy advisor to the Secretary of the Air Force, noted that the Air Force's space acquisition challenges were used as justification for creating the Space Force.[47] These cost and schedule challenges are multifaceted and complex. A separate space acquisition career field would not solve the Air Force's acquisition challenges. Still, the GAO consistently identified the lack of depth in space expertise as a key contributing factor. It illustrates an institutional reluctance to dedicate a portion of Air Force acquirers to focus on space. The intent to staff the Space Force with its acquisition officers creates a new opportunity to develop the expertise of space-focused acquirers alongside their operator counterparts.[48] Assessing the strengths and challenges facing the profession is appropriate for the Space Force to establish a strong team of acquisitions and operations professionals effectively.

The Space Profession—Strengths, Weaknesses, Opportunities, and Threats

As the Space Force begins its journey, it is prudent to conduct a strengths, weaknesses, opportunities, and threats analysis to identify key influencing factors and determine how they may shape the establishment of a military space profession.

Internal Strengths

The decision to establish an independent Space Force provides a strong forcing function toward developing a space profession. First and foremost, independence from the Air Force enables the space service to solidify the Space Force profession of arms. The Air Force profession of arms is defined as: "A vocation comprised of experts in the design, generation, support and application of global vigilance, global reach and global power serving under civilian authority, entrusted to defend the Constitution and accountable to the American people."[49] Now there is an opportunity to define the Space Force profession independent from the Air Force and establish a unique identity. Second, it permits the Space Force to manage and develop its members independently from the Air Force. This independence provides

space professionals, space acquirers in particular, with the opportunity to focus on the space mission rather than rotating between space and nonspace assignments, enhancing expertise and identity within the force. Finally, the space profession can borrow heavily from the professional ethic of the Air Force. The Space Force will most likely mirror the Air Force in its core values, and it will not be difficult for space service members to embrace the new service's values-based ethics. These internal factors, along with others, will help the Space Force define the space profession, but the Space Force has internal challenges to address.

Internal Weaknesses

The potential for "tribalism" among space professionals may weaken the Space Force's ability to develop a cohesive space profession. There are two "tribes" within the space cadre—operators and acquirers. A natural and healthy tension exists between system acquirers and system operators, and this is not unique to the space domain. Ideally, space operators and acquirers work seamlessly to provide an operational mindset and technical understanding of space systems. The Rumsfeld Commission recognized that space systems are unique, requiring a close relationship between acquirers and operators.[50] The Space Force should examine this dynamic and consider how to leverage the combined expertise of operators and acquirers to develop, deliver, and employ space capabilities effectively. First, the highly technical nature of space war fighting requires space operators with the technical background to understand the foundational concepts of space systems and the space operating environment. The Rumsfeld Commission recommended the NSS community develop technically-oriented officers who understand the "functions and underlying technologies of their systems that enable them to use the systems more efficiently in combat."[51] A 2014 RAND study of science, technology, engineering, and mathematics (STEM) degrees in the Air Force found that, while the institutional goal was 60 percent, less than 30 percent of space and missile operators held STEM degrees.[52] In 2018, the goal for STEM-degreed space operations officers was increased to 80 percent.[53] This goal is a shift in the right direction, but it will take time to achieve that goal across the career field. In contested domain operations, space operators will be more effective at dynamically employing space capabilities by leveraging a deep technical understanding of space systems rather than relying on standard operating procedures or checklists.

Second, space acquirers are more effective at developing and delivering space capabilities when they have space operations experience. The Rumsfeld Commission advocated for leveraging space acquirers with operational experience to influence satellite design directly.[54] The National Reconnaissance Office utilized an effective model at its satellite ground stations by certifying new officers, regardless

of the career field, as space operations crew commanders before transitioning them into program management or engineering positions. Acquisition officers who spend time on a space operations crew gain valuable insight, enhancing their ability to acquire space capabilities effectively. It may be beneficial to consider the "Every Marine a rifleman" model to provide new space officers with a strong foundation in operations before transitioning to acquisition duties. It is commonly discussed within the Air Force acquisition community that sending newly commissioned lieutenants to a product or logistics center for their first assignment is not ideal for leadership development. For comparison purposes, there are no Army acquisition lieutenants. The Army does not accept officers into its Acquisition Corps until they are midgrade captains, giving them operational leadership experience before managing an acquisition program.[55] The Navy has a similar model. A 2019 GAO report found that the Air Force's space acquisition hub, the Space and Missile Systems Center, had a significant number of excess lieutenants assigned.[56] If the additional capacity exists, the Space Force will benefit by creating a pipeline of technically-oriented officers who spend the first few years of their careers leading space operations, increasing the number of STEM-degreed officers conducting space operations, and producing more space acquisition officers with operational expertise. Indeed, applying technical expertise in space operations and leveraging operational experience in space acquisitions enhances the the space profession's effectiveness. Providing a common experiential baseline in space operations creates a shared identity, common understanding of the space domain, and establishes operational credibility among young space professionals, increasing overall cohesiveness. Space acquirers and operators need to function as a cohesive team to meet the strategic challenges that lie ahead.

External Opportunities

US national strategy, the identification of a pacing threat, and presidential emphasis on space all create an enormous opportunity for the Space Force and its associated space profession. The *National Security Strategy* acknowledges the great-power competition with China and Russia and warns that adversaries will attempt to limit US access in all domains.[57] The *National Defense Strategy* identifies long-term strategic competition with China and Russia as a principal priority requiring investment.[58] With the pacing threat identified, the Joint Staff and Services are developing visions of how the Joint Force will compete in an antiaccess, area-denial (A2/AD) environment through the employment of joint, all-domain, sensor-to-shooter capabilities. Both the Air Force and the Army produced operational concepts that recognize the reliance of air and ground forces on space capabilities in an A2/AD conflict. Moreover, the president is placing extraordinary emphasis on the

space domain. Since taking office, President Trump reestablished the National Space Council, called for the reinvigoration of human space exploration, published the "America First" *National Space Strategy*, stood up a space-focused combatant command, and established a new space service. The administration's efforts are clearly aimed at maintaining US space dominance, and the Space Force has an opportunity to lead government efforts toward achieving the president's goals.

China is challenging US dominance in space by aggressively pursuing a broad spectrum of space capabilities. While this is a potential threat to US national security, it presents an opportunity for the space profession. China demonstrated a direct-ascent antisatellite capability in 2007 and expressed a willingness to target reconnaissance, communication, navigation, and early warning satellites.[59] China is making significant progress in lunar exploration, as evidenced by landing a probe on the far side of the Moon and deploying a relay satellite in lunar orbit.[60] Additionally, China plans to establish a lunar research station in the next 10 years and a lunar base by 2050.[61] The current strategic environment requires the NSS community to rapidly field space capabilities that support great-power rivalry, deter potential adversaries, and, if deterrence fails, seamlessly integrate into the all-domain operational concepts of the air, land, and sea forces. The current strategic context requires the Space Force to expand its role beyond the traditional missile warning, communications, navigation, intelligence, and counterspace mission sets by integrating into all-domain operational concepts.

In the emerging strategic context, there are at least two mission areas that should be considered in the Space Force's strategic mission and vision. First, space-based capabilities must be integrated into an all-domain, sensor-to-shooter, Joint Force kill chain to compete in the A2/AD threat environment. Consider an A2/AD conflict where the Joint Force is denied the ability to establish domain superiority in air, land, or sea. The Joint Force commander relies on space-based sensors to find, fix, and track the enemy and share data with an all-domain command and control (C2) node. The C2 node fuses space-based sensor data to target the enemy and directs fires from unmanned aircraft and Army and Navy long-range munitions. In parallel, space assets continually assess the battlespace and defend friendly space assets from terrestrial and on-orbit enemy threats. It is difficult to envision how the Joint Force succeeds in an A2/AD conflict without the integration of space capabilities.

Second, the Space Force must ensure that the US maintains its global advantage in the space domain. China's antisatellite capability threatens NSS assets, and its plans to establish a major presence on the Moon expands China's cislunar presence, further threatening NSS systems. In the context of great power rivalry, it is prudent for the US to seriously consider lunar basing options and focus on

getting there faster than China. Although international law prohibits the establishment of military bases on the Moon, the Outer Space Treaty permits military personnel to conduct scientific research and utilize lunar-based equipment and facilities for peaceful purposes.[62] Appointing the Space Force to lead efforts in establishing a lunar base enables military space to support US civil and commercial interests in space. It provides an opportunity to project an American military presence across cislunar space. While the civil and commercial space sectors will reap significant benefits from the decision to establish a lunar base, they can rely on military space to build and operate a base in the austere conditions of the lunar surface. One of the primary advantages of a lunar base is the potential opportunity for in-situ fuel production. Given the Chinese threat, NSS satellites will need agility, and hence fuel, to maneuver. Fuel is potentially a limiting factor, but a lunar base with fuel production capabilities enables the Space Force to refuel US satellites without launching from the earth's surface. Although ambitious, establishing a multipurpose lunar base would help enable the US to protect its assets in a conflict that extends into space.

Moreover, a lunar-base initiative supports the president's goal to reinvigorate human space exploration to the Moon and beyond. Professions are defined by the unique service they provide to society. Given the emerging mission needs, the Space Force profession of arms is well-positioned to help the US achieve its national objectives. To succeed fully, the new service must articulate to society how it will protect national security.

External Threats

The potential inability of society to understand the distinct mission of the Space Force threatens the establishment of a credible space profession. As discussed earlier, a profession earns the trust of society by effectively and ethically providing a unique and vital service. In exchange, society grants the profession significant autonomy and discretion to conduct its practice. It will be difficult for the space profession to thrive if the service provided is not well understood by society. Following the post-World War II military drawdown, Samuel Huntington discussed the importance of a military service's *strategic concept*. The strategic concept of a military service describes its role in implementing national policy and protecting national security.[63] Without a well-defined strategic concept, society will not understand the role or need for the service. Consequently, the service will not receive the resources needed to conduct its mission.[64] There are strong indications that society does not understand the strategic concept of the Space Force. The health of the space profession relies on the perceived legitimacy of the Space Force mission, both externally and internally. Externally, the space profes-

sion needs to overcome the "giggle factor" by clearly articulating to the public how the Space Force contributes to the protection of national security. Internally, the commitment of space professionals to their profession and the service it provides relies on a common and shared understanding of the Space Force's strategic concept. With a well-defined and communicated strategic concept, space professionals are positioned and motivated to advocate for the space mission, rather than to feed into the "giggle factor," which marginalizes the legitimacy of their profession. The current strategic environment provides a tremendous opportunity for the Space Force profession of arms to articulate a compelling strategic concept that society understands and endorses.

Recommendations

The Space Force should be built on the foundation of a space profession. The legitimacy of the space profession relies on a clearly articulated strategic concept that communicates how the Space Force will protect national security. To implement the strategic concept, the Space Force needs proficient, ethical, and service-oriented space professionals that embody the space profession's defining characteristics. Because of the unique nature of the military space mission, professionals should develop a common technical and operational understanding of the physically distinct space domain to develop, deliver, and employ war-fighting capabilities effectively. This understanding leads to four recommendations for instituting the Space Force profession of arms.

First, codify the Space Force profession of arms in service policy. This step should include the key characteristics of the space profession and its professional ethic. Policy and guidance should emphasize the collective responsibility of space professionals for stewardship of the profession. The space war-fighting profession should include the following characteristics:

Competence: Professions require expertise, specialized knowledge, and unique skills.

Character: Professions are guided by a professional ethic, determined by their values, beliefs, laws, and moral standards.

Commitment: Professions provide a vital and unique service to society.

Leadership: Professions require leadership at each echelon to establish and self-regulate the profession, develop and certify professionals, and cultivate the professional identity.

Trust: Professions rely on external trust to practice their profession with autonomy and discretion, and they rely on internal trust to operate effectively and cohesively.

Second, define the strategic concept for the Space Force to ensure that space professionals and society understand precisely how the service protects national security. A compelling and clear strategic concept strengthens the commitment of space professionals to the service's unique mission. The Space Force should define its strategic concept along three lines: traditional, emerging, and long-term. Traditional missions include missile warning, satellite communications, space-based navigation, intelligence, and counterspace. The emerging mission focuses on integrating traditional and innovative space capabilities into all-domain operations, delivering joint lethality to achieve dominance in an A2/AD conflict. In the long-term, lunar basing supports civil and commercial space endeavors and enables the US to protect and defend its on-orbit assets while projecting US space power. Recognition of these three mission areas offers the Space Force a compelling narrative that describes tangible ways the new service will protect national security by cooperating with partners, competing with other space-faring nations, deterring adversaries, and providing critical all-domain capabilities in an armed conflict. A compelling narrative helps mitigate the "giggle factor" that potentially threatens the perceived legitimacy of the space profession. Failure to establish a strategic concept puts the notion of a space war-fighting profession at risk.

Third, establish a professional certification program that assesses an individual's competence, character, and commitment. The profession has a collective responsibility to ensure members are proficient in their practice, ethical in their decision-making, and resolute in their service to society. Certifying professional competence is fairly objective and should leverage existing certification programs for assessing expertise in space operations and acquisitions. Certifying an individual's character and commitment is more subjective, although not unprecedented. Air Force annual performance reports rely on supervisors to assess such subjective factors as loyalty, dedication, integrity, and judgment. Similar factors should be applied and emphasized for space professional certification. Individual character is assessed through personal observation and interaction, certifying the member's judgment and ability to apply the professional ethic in decision-making. The certification of individual commitment assesses whether the member demonstrates honorable and resolute service in the Space Force and to the nation. Utilizing a whole-person concept for professional certification ensures members are qualified to self-regulate and uphold the characteristics of the profession.

Fourth, create a common experiential baseline to ensure new space professionals have a shared understanding of the space war-fighting domain. Newly accessed military members should gain operational experience and professional certification in satellite command and control, space launch, space control, or space surveillance in their first assignment. Following their first assignment, members

should then be tracked to either space operations or space acquisitions, depending on their background, job performance, and personal preferences. This tracking helps establish a common identity, a shared sense of purpose, and operational credibility among space professionals. Learning the operational side of space as lieutenants enables young officers to gain valuable experience and build a network of colleagues that will benefit them in the future, whether they ultimately serve as operators or acquirers in the Space Force.

Conclusion

The Air Force made significant progress in developing a cadre of space professionals since the release of the Space Commission report in 2001. The creation of the Space Force provides a further, unprecedented opportunity to revisit the concept of space professionalism by determining the characteristics of a space profession and taking a holistic approach to develop and certify space professionals. If the strategic importance of the space domain necessitates a separate military space service, it should also warrant the establishment of a distinct military space profession. The Space Force should codify the characteristics of the space profession of arms in service policy, define the Space Force's strategic concept, establish a comprehensive professional certification process, and ensure new members of the space profession obtain a common baseline of operational experience early in their careers. The Space Force has a tremendous opportunity to build its service upon the indelible foundation of a military space profession, ensuring the United States remains the predominant global space power. ✪

Lt Col Bryan M. Titus, USAF

Lieutenant Colonel Titus (BSEE, University of Florida; MSEE, California State University) is the deputy commander of the 30th Operations Group, Vandenberg AFB, California. He is an engineer who has served as a space launch squadron director of operations, space operations squadron commander, and space program element monitor at the Pentagon.

Notes

1. Don M. Snider, "American Military Professions and Their Ethics," in *Routledge Handbook of Military Ethics,* ed. George Lucas (London: Routledge, 2015), 15.
2. Snider, "American Military Professions and Their Ethics," 18.
3. Rumsfeld Commission, *Commission to Assess United States National Security Space Management and Organization,* report to Congress (Washington, DC: 11 January 2001), viii, https://fas.org/.
4. *National Defense Authorization Act for Fiscal Year 2002*, Public Law 107-107, 107th Cong., 28 December 2001, 186, https://www.govinfo.gov/.
5. Air Force Space Command, "Space Professional Development, Frequently Asked Questions," *High Frontier Journal* 1, no. 1 (Summer 2004): 12, https://ufdc.ufl.edu/.

6. Snider, "American Military Professions and Their Ethics," 17.
7. Snider, "American Military Professions and Their Ethics," 16.
8. Richard M. Swain and Albert C. Pierce, *The Armed Forces Officer* (Washington, DC: National Defense University Press, 2017), 19–20, https://ndupress.ndu.edu/.
9. Snider, "American Military Professions and Their Ethics," 17.
10. Swain and Pierce, *The Armed Forces Officer*, 24–26.
11. Snider, "American Military Professions and Their Ethics," 16.
12. Snider, "American Military Professions and Their Ethics," 18.
13. Snider, "American Military Professions and Their Ethics," 15.
14. Snider, "American Military Professions and Their Ethics," 18.
15. Gen Martin E. Dempsey, "America's Military—A Profession of Arms," white paper (Washington, DC: Chairman of the Joint Chiefs of Staff, February 2012), 4, https://archive.defense.gov/news/.
16. Snider, "American Military Professions and Their Ethics," 18.
17. Snider, "American Military Professions and Their Ethics," 19.
18. David Patrick Houghton, *The Decision Point* (New York: Oxford University Press, 2013), 35.
19. Army Doctrine References Publication 1, *The Army Profession*, June 2015, v, https://fas.org.
20. *National Defense Authorization Act for Fiscal Year 2000,* Public Law 106-65, 106th Cong., 5 October 1999, 303, https://www.congress.gov/.
21. Rumsfeld Commission, *Commission to Assess United States National Security,* vii–viii.
22. Rumsfeld Commission, *Commission to Assess United States National Security*, 42–46.
23. Rumsfeld Commission, *Commission to Assess United States National Security*, 44–45.
24. Air Force Space Command, "Space Professional Development, Frequently Asked Questions."
25. Gen Lance W. Lord, "Welcome to High Frontier!," *High Frontier Journal* 1, no. 1 (Summer 2004): 4, https://ufdc.ufl.edu/.
26. Air Force Policy Directive (AFPD) 36-37, *Space Professional Development*, 23 March 2006, 1–5, https://static.e-publishing.af.mil/.
27. Tamar A. Mehuron, "Building the Space Cadre," *Air Force Magazine*, March 2005, 23, https://www.airforcemag.com/.
28. AFPD 36-37, *Space Professional Development*.
29. Government Accountability Office (GAO), *Defense Space Systems: DOD Should Collect and Maintain Data on Its Space Acquisition Workforce* (Washington, DC: GAO, March 2019), 9, https://www.gao.gov/.
30. GAO, *Space Acquisitions: Stronger Development Practices and Investment Planning Needed to Address Continuing Problems* (Washington, DC: GAO, July 2005), 6.
31. *U.S. National Space Policy* (Washington, DC: White House, 31 August 2006), 3, https://history.nasa.gov/.
32. GAO, *Space Acquisitions: Actions Needed to Expand,* 16–17.
33. *National Defense Authorization Act for Fiscal Year 2007*, Public Law 109-364, 109th Cong., 17 October 2006, 279, https://www.congress.gov/.
34. Allard Commission, *Leadership, Management, and Organization for National Security Space*, report to Congress (Alexandria, VA: Institute for Defense Analysis, July 2008), 24, https://spacepolicyonline.com/.
35. GAO, *Space Acquisitions: Government and Industry Partners Face Substantial Challenges in Developing New DOD Space Systems* (Washington, DC: GAO, April 2009), 8, https://www.gao.gov/.

36. GAO, *Space Acquisitions: Government and Industry Partners*, 16.

37. White House, *U.S. National Space Policy*.

38. GAO, *Space Acquisitions: DOD Delivering New Generations of Satellites, but Space System Acquisition Challenges Remain* (Washington, DC: GAO, May 2011), 6–8, https://www.defense-aerospace.com/.

39. *National Security Space Strategy* (Washington, DC: White House, January 2011), 8, https://archive.defense.gov/.

40. GAO, *Space Acquisitions: DOD Faces Challenges in Fully Realizing Benefits of Satellite Acquisition Improvements* (Washington, DC: GAO, March 2012), 4.

41. GAO, *Space Acquisitions: DOD is Overcoming Long-Standing Problems, but Faces Challenges to Ensuring Its Investments Are Optimized* (Washington, DC: GAO, April 2013), 10, https://www.gao.gov/.

42. GAO, *Space Acquisitions: Some Programs Have Overcome Past Problems, but Challenges and Uncertainty Remain for the Future* (Washington, DC: GAO, April 2015), 7, https://www.gao.gov/products/.

43. GAO, *Space Acquisitions: Some Programs Have Overcome Past Problems, but Challenges and Uncertainty Remain for the Future* (Washington, DC: GAO, April 2015), 11–12, https://www.gao.gov/products/.

44. GAO, *Space* Acquisitions, 11-12.

45. GAO, *Space Acquisitions: DOD Continues to Face Challenges of Delayed Delivery of Critical Space Capabilities and Fragmented Leadership* (Washington, DC: GAO, 17 May 2017), 9, https://www.gao.gov/.

46. GAO, *Space Acquisitions: DOD Continues to Face Challenges*, 15.

47. Sandra Erwin, "U.S. Space Force Has Lifted Off, Now the Journey Begins," *United States Space Force*, 24 January 2020, https://spacenews.com/.

48. "How Will the Space Force Impact Me," *United States Space Force*, accessed 23 December 2019, https://www.spaceforce.mil/.

49. USAF, *Strategic Roadmap: United States Air Force Profession of Arms* (Washington, DC: USAF, May 2015), 4, https://www.airman.af.mil/.

50. Rumsfeld Commission, *Commission to Assess United States National Security*, 68.

51. Rumsfeld Commission, *Commission to Assess United States National Security*, 45.

52. Lisa M. Harrington et al., *Air Force—Wide Needs for Science, Technology, Engineering, and Mathematics (STEM) Academic Degrees* (Santa Monica, CA: RAND Corporation, 2014), 20, https://www.rand.org/.

53. United States Air Force, *Air Force Officer Classification Directory* (San Antonio, TX: Air Force Personnel Center, 30 April 2018), 246, https://afrotc.unm.edu/.

54. Rumsfeld Commission, *Commission to Assess United States National Security Space Management and Organization*, 68.

55. "AC Officer Career Timeline," *army.mil*, accessed 21 January 2020, https://asc.army.mil/.

56. Government Accountability Office (GAO), *Defense Space Systems: DOD Should Collect and Maintain Data on Its Space Acquisition Workforce*, GAO-19-240 (Washington, DC: GAO, March 2019), 23, https://www.gao.gov/.

57. *National Security Strategy of the United States of America* (Washington, DC: White House, December 2017), 27, 29, https://www.whitehouse.gov/.

58. Department of Defense (DOD), *Summary of the 2018 National Defense Strategy* (Washington, DC: DOD, 2018), 4, https://dod.defense.gov/.

59. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: Office of the Secretary of Defense, 2019), 51, https://media.defense.gov/.

60. *Annual Report to Congress*, 50.

61. *Annual Report to Congress*, 50.

62. United Nations, *Treaties and Principles on Outer Space* (New York: United Nations, 2002), 4.

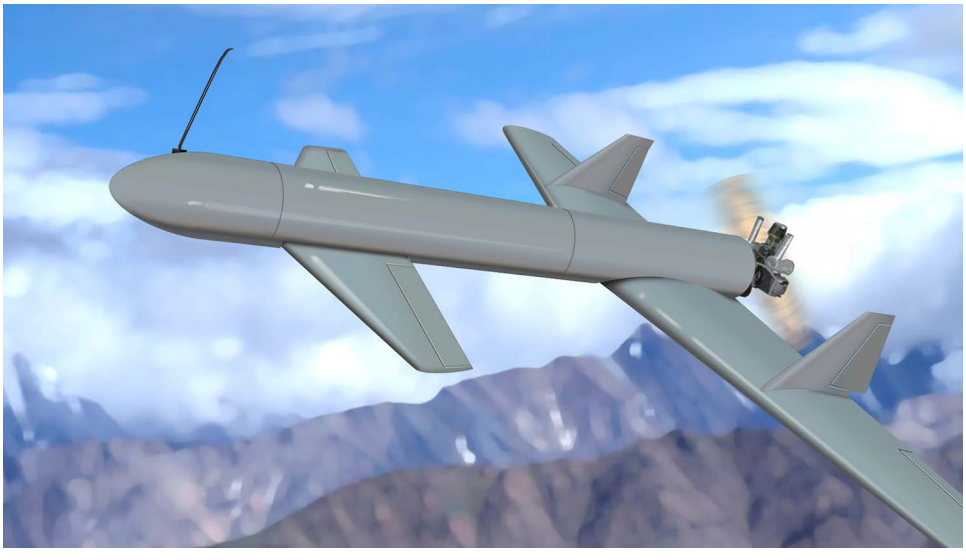
63. Samuel P. Huntington, "National Policy and the Transoceanic Navy," *United States Naval Institute Proceedings* 80, no. 5 (May 1954): 483, https://blog.usni.org/.

64. Huntington, "National Policy and the Transoceanic Navy."

FEATURE

Off the Shelf: The Violent Nonstate Actor Drone Threat

Kerry Chávez
Dr. Ori Swed



In a recent *Air & Space Power Journal*, Maj Jules "Jay" Hurst explains how small unmanned aerial vehicles (UAV) enable less capital-rich nations to enter the air domain.[1] Though airpower has historically been scarce for its costs and complexities, commercial UAVs can affordably replace or supplement military-grade models for certain tasks. As a result, the range of actors leveraging airpower's unique attributes is growing in number and variety, making tactical air control more challenging.[2] We contend that it is not only resource-constrained states taking to the air with commercial platforms but also violent nonstate actors (VNSA). For instance, the Islamic State in Iraq and the Levant (ISIL) has flown hundreds of UAV sorties against Western and Middle Eastern troops.[3] Sending up swarms of drones costing a few hundred dollars each, the US admitted a lapse in tactical superiority of the airspace during the battle of Mosul.[4] Thus, with the advance of small UAVs, the range of airborne actors is even broader, and their capabilities are even more diverse. Our objective in this study is to highlight and describe the scope and potential impact of the VNSA drone threat.

Violent nonstate actor drone use is more widespread, diverse, sophisticated, and rapidly advancing than depicted in the nascent literature. The reason is that

until recently, scholars have neglected or conflated commercial drones with military-grade platforms. Looking only at the latter, proliferation is restricted to three Iranian state-sponsored terror groups in the Middle East—Hezbollah, Hamas, and Houthi rebels. Including commercial technologies, our original dataset on VNSA drone incidents features 40 separate groups covering every continent except Antarctica.[5] Terrorist-operated drones constitute a security concern for two reasons: 1) they grant VNSAs a new offensive edge in conflict, and 2) they increase defensive challenges for security providers. In the next section, we describe where commercial drones sit on the spectrum of UAV technologies and why they are attractive to VNSAs. We then discuss how drones offensively benefit terrorist groups and defensively challenge state actors. Finally, we trace several successful VNSA drone use cases in three broad theaters—international, domestic, and aviation security.

Definitions and Scope

UAVs, or drones, span a broad spectrum of capabilities and types.[6] On the low-end, they include hobbyist drones that many individual consumers can afford and operate with little instruction, including children. On the high-end, the spectrum features exquisite platforms such as the RQ-170 Sentinel, the stealthy "Beast of Kandahar." The Department of Defense classifies UAVs according to gross weight, speed, and altitude.[7] As UAV technologies advance, however, technical specifications might blur across boundaries as commercial drones attain higher performance and military-grade models miniaturize or specialize with proprietary subcomponents.[8] Consequently, we employ Kelley Sayler's taxonomy of drones, based on accessibility and technical and infrastructural requirements to operate.[9] She sets forth four categories: hobbyist, commercial and mid-sized military, large military-specific, and stealth combat. The higher the category, the less accessible, and the more intensive the requisites become to operate and maintain the UAV.

VNSAs predominantly use hobbyist and commercial UAVs (civilian drones), and a select few use Iranian mid-sized military drones. This use puts them squarely along the lower end of the UAV spectrum. The reason is that civilian drones are affordable, accessible, and user-friendly. Hobbyist drones have the lowest entry barriers, being low-cost (i.e., a few hundred dollars), unregulated, and with minimal technical or infrastructural requirements.[10] For instance, ISIL's drone of choice was the DJI Phantom, a popular hobbyist model manufactured in China.[11] Commercial drones are more expensive (ranging from thousands to tens of thousands of dollars), might entail regulation in some cases, and have higher capacity requirements. However, these drones are still attainable by many VNSAs. Mid-sized military drones have similar capacities but are more costly and heavily regu-

lated, requiring state-sponsorship for VNSAs to attain.[12] Like less endowed states, VNSAs cannot attain large military-specific and stealth combat drones for their costs, legal restrictions, and complexity.[13] Even constrained to civilian drones, however, VNSAs can leverage airpower's unique attributes to advance their agendas. As private-sector technologies progress, they will increasingly benefit from these simpler platforms.

There are also potential dangers of VNSAs scavenging, reverse-engineering, and deploying downed military-operated drones. In May 2012, an allied raid on a Taliban base in Helmand Province yielded a small drone, thought to be a North Atlantic Treaty Organization (NATO) model.[14] Turkish security forces found a US RQ-20 Puma during a search of a Kurdistan Worker's Party (PKK) cell in Silopi in early 2016.[15] Later that year, Jabhat Fatah al-Sham published a Telegram post featuring photos of a downed Russian surveillance drone in the Jabal al-Akrad, the "Mountain of the Kurds," expressing intentions to reverse-engineer it.[16] In 2016 alone, ISIL seized 18 military-grade drones (2 US RQ-7 Shadows, a US MQ-9 Reaper, an unspecified US reconnaissance drone, 13 Iraqi UAVs, and a Kurdish reconnaissance model).[17] With most of these seizures, the group merely boasted and threatened on social media. However, some outlets reported that a Shahed-129, a fairly advanced Iranian UAV, was fielded by an insurgent group against US forces in 2017. While the operator has not been positively identified, some sources suggest that ISIL obtained the machine following a crash and recovery.[18] Although our focus remains on more accessible civilian drones, we foresee that VNSAs assimilating commercialized airpower will become adept across an increasing bandwidth of UAV technologies, further problematizing security in a drone-dense future.

The Threat

Gaining access to cheap civilian drone technology has granted VNSAs a new offensive edge. Though VNSAs have had limited aerial capabilities for some time—balloons, missiles, rockets, even hijacking commercial planes—civilian UAVs are more affordable and versatile. They are more agile and inconspicuous than balloons. They are more multiuse and reusable than missiles and rockets. They are lower risk and less costly than sending operatives aboard a commercial plane to disrupt its flight. Consequently, civilian drones provide VNSAs a new, efficient platform to advance their agendas. Though Hurst emphasizes the challenges of tactical air control as more states deploy small UAVs,[19] we submit that civilian models benefit VNSAs at all levels. At the strategic level, they are using drones for propaganda generation, both to advertise their newfound aerial capabilities and their effects and to publish striking cinematography of other opera-

tional successes.[20] At the operational level, they use UAVs for intelligence, surveillance, and reconnaissance (ISR) and to enhance command and control (C2) in real-time. At the tactical level, civilian drones open access to otherwise unreachable targets, such as rear headquarters and transit routes, extending the range of VNSAs' lethality. By offering mobility, flexibility, and covertness in the launch location relative to an attack site, they lower risks for violent groups that might enable protracted campaigns.[21]

In addition to boosting VNSAs' offensive edge, civilian drones increase defensive challenges for security providers. Many have been aware of, preparing for, and succeeding against malicious aerial threats for decades. However, civilian drone technology is rapidly advancing and proliferating. Thus, the sophistication and volume of the threat require greater attention and resources that must be diverted and redistributed from other concerns. Focusing on the United States, where regulatory limitations on using commercial UAVs were recently relaxed, Maj Bryan A. Card expects that the malicious use of drones will expand. In offering active defense recommendations, he discusses the difficulties and tradeoffs of intercepting small UAVs. The drones' small size and low altitude make them harder to detect on radar, the principal air traffic monitoring technology. Indeed, proper detection and disruption would require widely distributed and proactive measures. In an urban environment, Card argues that a dynamic defense model would require multiple trained operators staged throughout multiples avenues of approach.[22] These would be high cost to both install and maintain. At the same time that VNSAs are benefiting from improved intelligence, mobility, and operational reach with drones, their targets are taxed with a higher volume and density of aerial threats. The combination of these characteristics elevates the threat of VNSA drones relative to many other platforms.

The Theaters

International Security

The most distant but obvious venues in which VNSAs exploit civilian drones are active war zones. Their versatility is apparent: individual actors using UAVs for propaganda, ISR, C2, target acquisition, and weaponized attacks. In 2011, in an early instance of reconnaissance with a drone, Libyan rebels obtained a commercial minidrone after being denied access to NATO aerial telemetry. Purchased from Aeryon Labs in Ottawa, a Canadian veteran tucked it into a backpack, flew to Malta, then boarded a tuna boat bound for the Libyan coast. The combatants quickly mastered the user-friendly platform, using it to identify and observe enemy positions during their rapid march from Misrata to Tripoli. With night-

vision camera technology, they were able to continue and adapt under the cover of darkness. An Aeryon stakeholder remarked that "the rebels needed barely a day of training to use a technology that many national armies would love to acquire."[23]

ISIL began using drones in 2013. Entirely grassroots, the group's drone program depended on off-the-shelf technologies and do-it-yourself modifications. Yet it had the most robust drone infrastructure and intensive use of perhaps any VNSA.[24] ISIL initially used UAVs solely for ISR. Though aerial imagery is available, much for free and some of higher accuracy for purchase, drone telemetry provides context-specific and time-sensitive intelligence on-demand. In March 2016, a drone drifted over a series of American and Iraqi bases in northern Iraq shortly before militants launched a Katyusha rocket into a populated zone of a US Marine base, killing a Soldier. The strike's accuracy, called a golden shot, led some military officials to speculate that drone surveillance enabled it.[25] Two months later, ISIL used drones for C2 (and propaganda) in a large-scale assault on Pershmerga positions north of Mosul, during which US Navy Seal Charles Keating IV was killed.[26] Scholars also believe that UAVs facilitated the takeover of Raqqa, which would serve as the group's headquarters and main stronghold, and the operation that led to the capture of a major oil refinery in Baiji, Iraq.[27]

Used for passive purposes for two years before weaponization, ISIL first booby-trapped drones before successfully deploying aerial munitions. Two notable instances occurred at the end of 2016. The first involved three quadcopters rigged with explosives that killed two Kurdish fighters and seriously injured two French special forces soldiers upon detonation.[28] In the second attack, a drone strapped with an explosive gained aerial access to a checkpoint, destroying some buildings.[29] ISIL launched its first weaponized drone over Mosul in January 2017, when it dropped a bomb over an Iraqi outpost wounding and possibly killing a small group of soldiers.[30] This bombing was followed by a flurry of similar attacks. The group's propaganda channels became sated with imagery of combat drones, including models hovering over Western landmarks alongside calls for attacks abroad.[31] ISIL drones had a high degree of accuracy and were often used in swarms, compelling allied forces to reposition, reorient, and sometimes retreat.[32] Occasionally, rebels would wait for government forces to send up their drones so they would confuse ISIL drones with friendly materiel. According to a scholar at the Combating Terrorism Center at West Point, at the peak of its scale of operations in the spring of 2017, ISIL was conducting between 60–100 weaponized attacks per month. These attacks led to significant injuries that a surgeon in Mosul estimated to reach at least 10 per day.[33] Such success absent state-sponsorship is a stark product of civilian drone advancement and accessibility.[34]

The Syria civil war is another war zone rife with VNSA drone use. Alongside US Reapers, the Israeli Skylark, Chinese stealth tech, the Turkish Bayraktar, Russian Forposts, and multiple Iranian models flown by the Syrian regime, rebels are flying commercial, hobbyist, and even homemade drones. This number made the war the most drone-dense conflict to date.[35] The state actors have a clear preponderance of airpower, yet rebels give them a run for their money with their recreational platforms. After a drone carrying explosives was downed in Idlib in August 2018, Russia admitted the frequency and success of VNSA weaponized drone attacks.[36] A spokesperson from Russia's Ministry of Defense insists that the drones, though improvised in appearance, are sophisticated and accurate.[37] Earlier that year, Russia blamed the US for coordinating a drone swarm attack on its Hmeimim airbase after 13 primitive-looking drones coordinated their flight patterns to penetrate aerial defenses.[38] This attack followed a successful weaponized attack at the same location, in which two soldiers were killed, and (allegedly, per Russia's *Kommersant* newspaper) seven Russian aircraft were destroyed.[39] Russian Federal Security Service chief Alexander Bortnikov remarked, "We believe that one of the pressing problems now is the growing danger of terrorists using unmanned aerial vehicles, both homespun and, even more dangerous, those manufactured professionally."[40]

Rebel-operated drones are just as prolific in conflicts outside the boundaries of hot wars. Indeed, UAVs extend those boundaries, increasing VNSAs' logistical and lethal reach. While military forces on the front lines anticipate a certain tempo and timber of conflict, support units positioned in rear headquarters, logistical facilities, and routes in between are less prepared. In a striking example, Russian-backed Ukrainian separatists used drones to drop a thermite grenade on an arms depot, exploding approximately 70,000 tons of munitions estimated at $1B in damage.[41] Houthi rebels have also reached softer, yet high-value targets with UAVs. In January 2019, fighters deployed drones in three salient attacks. At a military parade, a drone killed at least six soldiers (among them Yemen's chief of military intelligence). It also injured several senior officials of the Arab coalition forces, including Yemen's chief of staff, deputy chief of staff, and the provincial governor.[42] A day later, Houthi rebels sent a kamikaze drone in pursuit of more Arab coalition officials in the Asir region, claiming that they attained more casualties. Then, an armed drone targeted a major general participating in UN peace talks. While it was intercepted en route, it did disrupt the meeting.[43] The September 2019 drone attack on the Saudi Aramco oil facilities in Khurais and Abqaiq demonstrates that this newfound reach puts critical infrastructure in danger as well.[44] Analysts estimate that the attack stunted 5 percent of the daily global oil supply and took several days to repair.[45]

Violent nonstate actors are leveraging drones in conflicts, not only beyond war boundaries but churning below the threshold of war in insurgencies and low-intensity conflicts. As early as 2002, the Colombian Army seized nine drones from the Fuerzas Armadas Revolucionarias de Colombia during a camp raid.[46] Like cartels around the globe, they now use these "narco-drones" to scout routes and exchanges, observe security measures, transport and deliver contraband, and for weaponization.[47] Maute rebels and other Islamic State-affiliated insurgents in the Philippines use commercial drones to track and evade military forces.[48] Boko Haram has begun using drones for surveillance, though authorities fear they will rapidly progress to weaponized platforms.[49] The PKK began dabbling in armed drones in 2017.[50] In their first attack in August of that year, the group used an off-the-shelf drone modified with an explosive to attack a Turkish army outpost, wounding two Turkish soldiers.[51] The PKK has increased its UAV use over time. In a two-week period in March 2019, the group attempted a dozen drone attacks on Turkish forces, claiming some casualties. Spanning four continents, this shortlist well exhibits the versatility and impact of civilian drones for resource-constrained rebels.

National Security

The aerial threat is not limited to nations contending with war, insurgency, or low-intensity conflict. It presents a formidable national security problem, especially for nations normalized to civilian drones in the airspace like the US. Despite the US's extensive investment to safeguard domestic assets and infrastructure after 9/11, many are easily bypassed by overflight.[52] From our survey of intended, attempted, and successful drone attacks in multiple nations, it is clear that VNSAs have long been aware of and interested in this platform. As early as 1973, the Jewish Defense League deliberated the use of a "drone airplane" to bomb the Soviet Mission to the United Nations in New York.[53] The first known attempt to weaponize a drone was in 1994 when Aum Shinrikyo ran failed trials to release sarin from a minicopter designed for aerosol crop spraying.[54] A 2002 *Security Management* piece indicated that Osama bin Laden actively discussed using a drone rigged with an improvised explosive device to attack world leaders at the 2001 G8 Summit in Italy. However, the group opted for a more familiar technology platform in the end.[55] In 2002, al-Qaeda aimed to deploy a drone filled with anthrax against the English House of Commons. The operator, Mozzam Begg, was intercepted before the plan unfolded and sent to Guantanamo.[56]

Perhaps the most renowned case connected to al-Qaeda is that of Rezwan Ferdaus. In 2008, he revealed precise plans for rigging and exploding three drones in the US Capitol and Pentagon to Federal Bureau of Investigation (FBI) agents posing as al-Qaeda members, leading to his arrest and conviction.[57] Don Rassler

points out the technical hurdles he faced, including a long runway, payload limitations, and flight stability. An aeronautics expert remarked in a televised interview that "the idea of pushing a button and this thing diving into the Pentagon is kind of a joke, actually."[58] The commercial drone industry decimated all of these hurdles. Automatic vertical take-off and landing, autonomous stabilization, obstacle avoidance, dramatically higher payloads, moving target tracking, and Global Positioning System-guided pre-programmable autonomous flight are just a few features embedded in current-generation models. As for the last hurdle of detonation, there is ample evidence that VNSAs have overcome it. In one curious case, Venezuelan military defectors loaded two commercial drones with a kilogram of C-4 explosives each and detonated them near President Nicolás Maduro in a 2018 assassination attempt.[59]

Israel, surrounded by terrorist groups seeking its destruction, has more experience than most nations with violent nonstate aerial threats. To its north is Hezbollah, sponsored, supplied, and funded by Iran. Hezbollah took a slow, steady pace in developing its UAV program, benefiting mostly from ISR. In 2012, the group sent an Ayub drone into Israeli territory via the Gaza Strip, making it 35 miles west into the Negev. Some reports suggested that the group conducted reconnaissance of a joint military exercise with the US, main airfields, ballistic missile sites, and the Dimona nuclear reactor.[60] To Israel's west in the Gaza Strip, Hamas has long had UAVs (also benefiting from Iran's state sponsorship) and is avidly pursuing the development of its drone program because of the low cost and multiuse value.[61] Israeli forces reinforced walls at the Iron Dome battery barracks in 2018 after several Hamas incursions into their airspace. This reinforcement was to guard against the possibility of a civilian drone explosive reaching the cluster of armed missiles that would generate a larger blast.[62] Palestinian Islamic Jihad has also deployed drones, pulling off the first successful terrorist UAV bombing of the Israeli military, though the armored tanks targeted suffered minimal damage.[63] Israel has also contended with drones straying from the Syria civil war, such as the one it shot down with a Patriot missile.[64]

Iron Dome, Israel's primary aerial defense system, is ineffective against small UAVs because it eliminates slow-moving targets from its acquisition algorithms to avoid becoming overtaxed.[65] Adding their small size, lack of heat signature, the similarity of radar signature to stealth aircraft, low flight paths, and minimal noise, civilian drones present distinct detection and defense challenges.[66] Once through defense measures, the military must mitigate the threat of enemy drones upon detection to avoid the potential of ISR gathering or violence. This mitigation stands whether the craft is an advanced stealth model or a jury-rigged child's toy. Thus, despite Israel's experience and qualitative military edge, it illustrates the

challenge of tactical air control as drone use expands. As commercial drone technology proliferates, more VNSAs are joining the airspace, Israeli and otherwise, for affordable ISR, antagonism, and violent attack. This situation requires security providers to divert resources to mitigate the growing threat.

On a more focused scale, law enforcement agencies contend with similar challenges. Individuals, gangs, and cartels use civilian UAVs to augment crimes and disrupt police efforts. Some use drones for reconnaissance on potential burglary and robbery targets, to surveil law enforcement, or for witness intimidation.[67] Smuggling efforts abound, even in prison. The most common items smuggled include drugs, tobacco, and weapons, although there is no lack of unusual contraband payloads from super glue to hacksaw blades.[68] In a more creative use, one gang used drones to swarm, buzz, and flush out an FBI hostage rescue team attempting a raid at an undisclosed location in Colorado.[69] The increasingly broad and diverse range of airborne actors led the International Criminal Police Organization to initiate a new unit solely to monitor criminal drone activity in 2018.[70] Though not new in concept, the scale and variety of VNSA commercial drone use will increasingly tax the resources of local, national, and international security providers.

Aviation Security

Another theater threatened by malicious drone use is civilian aviation. Hobbyist drones can potentially disrupt commercial aircraft, either by an attack on airfields, impact in flight, or catalyzing engine failure.[71] Certainly, commercial planes are at risk from a number of sources—pilot error, equipment malfunctions, fellow planes, birds, not to mention the ground. VNSA drones are distinct from these, though, in that they actively aim to undermine flight safety. Terrorists recognized the opportunity to disrupt aviation using commercial UAVs early in their development. According to German intelligence, al-Qaeda discussed plans to attack a passenger plane with a model airplane as early as 2002.[72] As commercial technologies have improved, similar plans have become more frequent. In a single month in 2016, social media featured numerous jihadist calls to use drones to carry explosives to attack passenger planes parked on airfields, suggestions on the mass production of weaponized drones, and varied discussions on how to carry out terror attacks on airplanes with UAVs.[73] In this same year, Spain's Centre against Terrorism and Organised Crime cited drones as the biggest malicious threat to civil aviation.[74]

Knowing the magnitude of potential damage and casualties, aviation security specialists, pilots, and air traffic control personnel are quick to react to drone sightings. They frequently cause flight diversions, delays, and cancellations, and

at times the shutdown of entire airports. A Michigan news station reports 36 instances of drone interference with airplanes.[75] In Ohio, drones nearly collided with planes 117 times over a five-year observation period.[76] The UK Airprox Board reports a monthly average of 15 "airprox incidents" in 2017, 11 in 2018, and 12 in 2019.[77] In 2018, the nation reported the closest near-miss incident in their history, a drone avoiding impact with the engine of a commercial plane carrying 264 passengers by 10 feet.[78] Similarly, in 2019, a drone came within 20 feet of smashing into a jet carrying 300 passengers in Abu Dhabi.[79] In-flight over Mexico, a drone reportedly did collide with the nose of a Boeing 737 passenger plane, causing it to perform an emergency landing in Tijuana and causing "considerable damage."[80] Given the imminence, liability, and profit loss involved, the aviation industry has long been aware of this threat. As civilian drones advance and proliferate, however, the threat could become more difficult to mitigate.

Conclusion

In response to VNSAs increasingly joining the range of actors leveraging airpower's attributes, we offer three considerations. First, resorting to antidrone technologies is commonsense. Any such programs, however, must consider cost proportionality and sustainability. Shooting down hobbyist drones with Patriot missiles and other traditional firepower addresses neither. Jamming signals to disrupt a potentially threatening drone, which could also jam other civil functions, such as industrial, medical, Bluetooth, mobile, and wireless internet bands, might not be proportionate in many contexts.[81] Constant, extensive, or intensive systems might not be sustainable. Since commercial drones are affordable, reusable, and replaceable, their countermeasures must be similarly feasible.

Second, in some cases, it might be more valuable for state powers to shift the focus from combating battle-ready drones in the skies to disrupting logistical supply chains and degrading terrorist drone workshops before the drones become operational. Granted, one reason that commercial UAVs are attractive to VNSAs is that they are accessible and unregulated, making supply chain disruption difficult. However, prolific users of weaponized drones tend to have streamlined drone programs, including manufacturing and modification centers. For example, when allied troops recaptured Ramadi from ISIL in 2015, they found a drone manufacturing and modification workshop.[82] In another instance, following several attacks over many months, Russian forces operating out of Hmeimim airbase in Syria discovered a drone workshop in a cave system nearby.[83]

Finally, given the variety of theaters in which VNSAs are using drones, we encourage contextual responses. Law enforcement solutions might be more embedded in the local landscape, while military solutions will need to be more mo-

bile. Protective measures in hot war zones might look different than those in low-intensity conflicts or counterinsurgencies. Successful antidrone systems will vary across urban, forested, desert, mountainous, or littoral terrains. Some defense apparatuses must be broadly distributed, while some can isolate strategic corridors or zones of flight. Some antidrone programs should remain exclusive to a single security provider, while others might operate best shared jointly across allies. The only universal response we promote is critical attention to the phenomenon of increasing VNSA drone use. It is likely here to stay. ✪

Kerry Chávez

Ms. Chávez (BA, Biola University; MLitt, University of St. Andrews; MA, Texas Tech University) is a PhD candidate in Political Science at Texas Tech University. Her research focuses on the determinants, strategies, and technologies of conflict. Previously, she served as a terrorism liaison officer for the Los Angeles Joint Regional Intelligence Center while employed in law enforcement and also worked for the US Department of Defense in International Security Affairs, Middle East Policy.

Ori Swed, PhD

Dr. Swed (BA, Hebrew University; MA, Hebrew University; PhD, University of Texas) is an assistant professor in the Department of Sociology, Anthropology, and Social Work at Texas Tech University. He is also the director of the Peace, War, and Social Conflict Laboratory at Texas Tech. Dr. Swed is a former special forces and reserve captain in the Israeli Defense Forces as well as a former private security contractor.

Notes

1. Though a variety of terms are used for unmanned aerial technologies, we interchangeably use the terms *UAV* and *drone* in this article.

2. Maj Jules "Jay" Hurst, "Small Unmanned Aerial Systems and Tactical Air Control," *Air & Space Power Journal* (*ASPJ*) 33, no. 1 (2019): 19–33, https://www.airuniversity.af.edu/ASPJ/.

3. Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (West Point, NY: US Military Academy Combating Terrorism Center, 2018), https://ctc.usma.edu/.

4. David B. Larter, "SOCOM Commander: Armed ISIS Drones Were 2016's 'Most Daunting Problem,'" *Defense News*, 16 May 2017, https://www.defensenews.com/.

5. The dataset is based on extensive surveys of open-source media, policy reports, and the Global Terrorism Database from 1994 (the first known instance of a VNSA drone attempt when Aum Shinrikyo attempted to disperse sarin gas from an agricultural quadcopter) to 2019.

6. Though cruise missiles are technically unmanned aerial vehicles, we do not include these in our definition scope. The platforms popularized under the term *UAV*, or *drone*, are more akin to an aircraft than a missile, having recoverable airframes, loitering capacities, ISR functions, and recall/return to base capabilities. For a fuller treatment of the distinctions, see Michael C. Horowitz, "Drones Aren't Missiles, So Don't Regulate Them Like They Are," *Bulletin of the Atomic Scientists*, 26 June 2017, https://thebulletin.org/.

7. *United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047* (Washington, DC: USAF, 2009), http://fas.org/irp/program/.

8. Derya Ozdemir, "U.S. Army Awards Pocket-Sized Drones $20.6 Million Contract," *Interesting Engineering,* 23 June 2020, https://interestingengineering.com/.

9. Kelley Sayler, *A World of Proliferated Drones: A Technology Primer* (Washington, DC: Center for a New American Security, 2015), https://drones.cnas.org/.

10. We conceptually lump homemade drones with hobbyist drones since they bear similar costs, accessibility, and technical specifications.

11. Chris Abbott et al., *Hostile Drones: The Hostile Use of Drones by Non-state Actors Against British Targets* (London: Remote Control Project, 2016); Larry Friese, N.R. Jenzen-Jones, and Michael Smallwood, *Emerging Unmanned Threats: The Use of Commercially Available UAVs by Armed Non-state Actors* (Perth: Armament Research Services, 2016); Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology* (West Point, NY: USMA Combating Terrorism Center, 2016); and Ryan Jokl Ball, *The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications* (Livermore, CA: Lawrence Livermore National Laboratory, 2017).

12. For instance, Hezbollah and Hamas have been known to fly the Ababil-2, and Hezbollah has also used the Mohajer-2 and Mohajer-4, all regulated Iranian military-grade models.

13. Hurst, "Small UASs and Tactical Air Control"; Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, "Separating Fact from Fiction in the Debate over Drone Proliferation," *International Security* 41, no. 2 (2016): 7-42, https://www.mitpressjournals.org/; and Andrea Gilli and Mauro Gilli, "The Diffusion of Drone Warfare? Industrial, Organizational, and Infrastructural Constraints," *Security Studies* 25, no. 1 (2016): 50–84, https://www.tandfonline.com/.

14. Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2015).

15. Hürriyet Staff, "Drone Used by PKK Found in Southeast Turkey," *Hürriyet Daily News*, 21 January 2016, http://www.hurriyetdailynews.com/.

16. Steven Stalinsky and R. Sosnow, "A Decade Of Jihadi Organizations' Use Of Drones—From Early Experiments By Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones," *MEMRI*, 21 February 2017, https://www.memri.org/.

17. This count comes from our original dataset on VNSA drone incidents from 1994–2019.

18. K. E. Truitte, "Drones over Syria: Proliferation of Drone Use in the Syrian Civil War," *Medium*, 3 January 2015, https://medium.com/; and Thomas Gibbons-Neff, "ISIS Drones are Attacking U.S. Troops and Disrupting Airstrikes in Raqqa, Officials Say," *Washington Post*, 14 June 2017, https://www.washingtonpost.com/.

19. Hurst, "Small UASs and Tactical Air Control."

20. Isabel Kershner, "Israel Shoots Down Drone Possibly Sent by Hezbollah," *New York Times*, 25 April 2013, https://www.nytimes.com/; Ash Rossiter, "Drone Usage by Militant Groups: Exploring Variation in Adoption," *Defense & Security Analysis* 34, no. 2 (2018): 113–126; and Joshua Tallis, Ryan Bauer, and Lauren Frey, "ISIL's Battlefield Tactics and the Implications for Homeland Security and Preparedness," *Contemporary Voices: St. Andrews Journal of International Relations* 8, no. 3 (2017): 31, https://cvir.st-andrews.ac.uk/.

21. Eugene Miasnikov, "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects," *Center for Arms Control, Energy and Environmental Studies*, 2005, http://www.armscontrol.ru/; Rossiter, "Drone Usage by Militant Groups"; Tallis, Bauer, and Frey, "ISIL's Battlefield Tactics"; and Maj Bryan A. Card, "Terror from Above: How the Commercial Unmanned Aerial

Vehicle Revolution Threatens the US Threshold," *ASPJ* 32, no. 1 (2018): 80–95, https://www.airuniversity.af.edu/ASPJ/.

22. Card, "Terror from Above."

23. Stephen Ackerman, "Libyan Rebels are Flying Their Own Minidrone," *Wired*, 23 August 2011, https://www.wired.com/.

24. Truls Hallberg Tønnessen, "Islamic State and Technology—A Literature Review," *Perspectives on Terrorism* 11, no. 6 (2017): 101-111.

25. Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones," *New York Times*, 11 October 2016, https://www.nytimes.com/.

26. Asaad Almohammad and Anne Speckhard, *ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics* (Washington, DC: International Center for the Study of Violent Extremism, 2017), https://www.academia.edu/.

27. Ball, "The Proliferation of UAVs," 19; Tallis, Bauer, and Frey, "ISIL's Battlefield Tactics"; and Gibbons-Neff, "ISIS Drones are Attacking U.S. Troops."

28. Peter Bergen et al., "Non-State Actors with Drone Capabilities," *New America Foundation*, 2019, https://www.newamerica.org/.

29. Schmidt and Schmitt, "Pentagon Confronts a New Threat."

30. Almohammad and Speckhard, *ISIS Drones*; and Joby Warrick, "Use of Weaponized Drones by ISIS Spurs Terrorism Fears," *Washington Post*, 21 February 2017, https://www.washingtonpost.com/.

31. Almohammad and Speckhard, *ISIS Drones*; and Ball, *Proliferation of UAVs.*

32. Gibbons-Neff, "ISIS Drones are Attacking U.S. Troops."

33. Rassler, *The Islamic State and Drones*, 5.

34. Tønnessen, "Islamic State and Technology."

35. Truitte, "Drones over Syria"; and Dan Gettinger, "Drones Operating in Syria and Iraq," *Center for the Study of the Drone*, 2016, http://dronecenter.bard.edu/.

36. FARS News Agency, "Russia Downs 4th Armed Drone in 3 Days Targeting Humeimim Airbase in Syria," *FARS News Agency*, 12 August 2018, https://www.tasnimnews.com/.

37. Interfax Editorial Staff, "Forty-five Drones Downed on Approach to Russia's Hmeimim Airbase in Syria over Past Month—Russian Defense Ministry," *Interfax News Agency*, 16 August 2018; and Rasha Raslan, "Russian MoD: Technologically Advanced Parties Provide Terrorists with Technology to Assemble UAVs Packed with Explosives," *Syrian Arab News Agency*, 17 August 2018, https://sana.sy/en/.

38. Kyle Rempfer, "Did US Drones Swarm a Russian Base? Probably Not, but That Capability isn't Far off," *Military Times*, 28 October 2018, https://www.militarytimes.com/.

39. Joseph Trevithick and Tyler Rogoway, "Russia Confirms Syria Attack but Denies Seven Aircraft Got Destroyed as Photos Emerge," *The Drive*, 4 January 2018, https://www.thedrive.com/.

40. ITAR-TASS, "Unrestrained Drone Use Increases Threat of Terrorist Attacks, FSB Chief Warns," *TASS*, 7 November 2018, http://tass.com/.

41. Rossiter, "Drone Usage by Militant Groups."

42. Ahmed Al-haj, "Bomb-Laden Rebel Drone Kills 6 at Yemen Military Parade," *Associated Press,* 10 January 2019, https://apnews.com/.

43. Lt Col Michael Segall, "Houthi Drones Attack Senior Officials in Yemenite and Saudi Armies," *Jerusalem Center for Public Affairs,* 14 January 2019, https://jcpa.org/.

44. Associated Press, "Major Saudi Arabia Oil Facilities Hit by Houthi Drone Strikes," *Guardian,* 14 September 2019, https://www.theguardian.com/.

45. Nada Altaher, Jennifer Hauser and Ivana Kottasová, "Yemen's Houthi Rebels Claim a 'Large-Scale' Drone Attack on Saudi Oil Facilities," *CNN*, 14 September 2019, https://www.cnn.com/.

46. Rassler, *Remotely Piloted Innovation*.

47. Brenda Fiegel, "Narco-Drones: A New Way to Transport Drugs," *Small Wars Journal,* 5 July 2017, https://smallwarsjournal.com/; Adriaan Alsema, "Colombia's 21st Century Drug War: Police Drones vs Narco Drones," *Colombia Reports*, 19 September 2019, https://colombiareports.com/; and Maria Alejandra Navarrete, "Drones Pose New Threat on Colombia's Pacific Coast," *InSight Crime,* 25 September 2019, https://www.insightcrime.org/.

48. Joseph Tristan Roxas, "Maute-ISIS bandits Use Drones in Marawi to Evade Pursuing Soldiers," *GMA News*, 19 June 2017, https://www.gmanetwork.com/.

49. Cara Anna, "Nigerian Leader: Islamic Extremists are Now Using Drones," *Associated Press*, 30 November 2018, https://apnews.com/.

50. Haye Kesteloo, "DJI Mavic Pro Rigged with Bomb Seized in Turkey," *Drone DJ,* 13 November 2017, https://dronedj.com/; and Bergen et al., "Non-state Actors with Drone Capabilities."

51. Metin Gurcan, "Turkey-PKK 'Drone Wars' Escalate," *AL-Monitor,* 18 September 2017, https://www.al-monitor.com/.

52. Stephen Maddox and David Stuckenberg, "Drones in the U.S. National Airspace System: A Safety and Security Assessment," *Harvard National Security Journal*, 24 February 2015, https://harvardnsj.org/.

53. Anti-Defamation League, "The Jewish Defense League," *ADL.com*, n.d., https://www.adl.org/.

54. Rassler, *Remotely Piloted Innovation*.

55. Michael A. Gips, "A Remote Threat," *Security Management* 46, no. 10 (2002): 14; and Bunker, "Insurgent UAVs."

56. Bunker, "Insurgent UAVs"; and Rassler, *Remotely Piloted Innovation*.

57. Bunker, "Insurgent UAVs"; and Maddox and Stuckenberg, "Drones in the U.S."; and Rassler, *Remotely Piloted Innovation*.

58. Rassler, *Remotely Piloted Innovation*, 21.

59. Rassler, *Remotely Piloted Innovation*, 21.

60. Milton Hoenig, "Hezbollah and the Use of Drones as a Weapon of Terrorism," *Public Interest Report* 67, no. 2 (2014), https://fas.org/; and Mariam Karouny, "Hezbollah Confirms It Sent Drone Downed over Israel," *Reuters*, 11 October 2012, https://www.reuters.com/.

61. Anna Mulrine, "Drones in the Hands of Hamas: How Worrisome is That?" *Christian Science Monitor*, 18 July 2014, https://www.csmonitor.com/; and David Zucchino and Ralph Vartabedian, "Hamas Drone Injects New Element into Arab-Israeli Conflict," *Los Angeles Times*, 15 July 2014, http://www.latimes.com/.

62. Alex Fishman, "The New Explosive Drone Threat from Gaza," *Ynetnews,* 29 July 2018, https://www.ynetnews.com/.

63. Zak Doffman, "Iran-Backed Terrorists Release Video Claiming First Drone Strike on Israeli Forces," *Forbes*, 31 May 2019, https://www.forbes.com/.

64. Sputnik News Service, "Israel Launches Patriot Missile at Drone from Syria—IDF," *Sputnik News Service*, 13 July 2018.

65. Dennis Gormley, "Addressing the Spread of Cruise Missiles and Unmanned Air Vehicles (UAVs)," *Nuclear Threat Initiative,* 2004, https://www.nti.org/.

66. Fishman, "The New Drone Threat"; and Karouny, "Hezbollah Confirms Drone Downed."

67. Michael Hicks, "Criminal Intent: FBI Details How Drones are Being Used for Crime," *Tech Radar*, 4 May 2018, https://www.techradar.com/; *Dedrone*, "Worldwide Drone Incidents," *Dedrone*, 2019, https://www.dedrone.com/; and Vanessa Swales, "Drones Used in Crime Fly under the Law's Radar," *New York Times*, 3 November 2019, https://www.nytimes.com/.

68. Heide Brandes, "Drone Carrying Drugs, Hacksaw Blades Crashes at Oklahoma Prison," *Reuters*, 27 October 2015, https://www.reuters.com/; Alejandro Sanchez and Cameron McKibben, "Worst Case Scenario: The Criminal Use of Drones," *Council on Hemispheric Affairs*, 2 February 2015, www.coha.org/; and *Dedrone*, "Worldwide Drone Incidents."

69. Patrick Tucker, "A Criminal Gang Used a Drone Swarm to Obstruct an FBI Hostage Raid," *Defense One,* 3 May 2018, https://www.defenseone.com/.

70. International Criminal Police Organization, "International Experts Meet on Potential Threat Posed by New Technologies," *Targeted News Service,* 6 December 2018, https://continuitycentral.com/.

71. *Verge* Staff, "Idiots with Drones Shut Down the UK's Second Largest Airport—Again," *Verge*, 21 December 2018, https://www.theverge.com/.

72. Gips, "A Remote Threat."

73. Eitan Azani et al., "Trends in Aviation Terrorism," *International Institute for Counter-terrorism,* 8 October 2016, https://www.ict.org.il/; and Pierluigi Paganini, "A Small Drone Hit a British Airways Plane over the Heathrow Airport," *Security Affairs,* 18 April 2016, http://securityaffairs.co/.

74. Rebecca Flood, "ISIS Using GOOGLE MAPS to Plot Airport and Plane Terror Attacks, Report Warns," *Express*, 27 September 2016, https://www.express.co.uk/.

75. Dave Bondy, "Close Calls between Drones and Aircraft in Mid-Michigan," *NBC News*, 8 April 2019, https://nbc25news.com/.

76. Max Filby, "Drones Nearly Hit Planes 117 Times in Ohio in Five Years," *Government Technology*, 26 August 2019, https://www.govtech.com/.

77. According to this reporting entity, an *airprox* is "a situation in which, in the opinion of a pilot or air traffic services personnel, the distance between aircraft as well as their relative positions and speed have been such that the safety of the aircraft involved may have been compromised." Since it is based on the subjective perspective of aviation professionals actively in the cockpit or tower, it does not involve quantitative distances to assess. UK Airprox Board, "Monthly Airprox Reviews," *Airproxboard.org*, 2019, https://www.airproxboard.org.uk/.

78. *Skynews* Staff, "Virgin Atlantic Jet in 'Closest Ever' Near-Miss with Drone on Approach to Heathrow," *Skynews*, 23 October 2018, https://news.sky.com/.

79. Dedrone, "Worldwide Drone Incidents."

80. Andrea Navarro and Alan Levin, "Boeing 737 Passenger Jet Damaged by Possible Midair Drone Hit," *Bloomberg,* 13 December 2018, https://www.bloomberg.com/.

81. Card, "Terror from Above."

82. Warrick, "Use of Weaponized Drones."

83. Maxime Popov, "In Syria, a Vast Underground Hideout Housed Rebel Base," *Yahoo News,* 26 September 2019, https://news.yahoo.com/.

Air, Space, and Cyberspace: Reinvigorating Defense of US Critical Infrastructure

Maj Lou Nguyen, USAF
Lt Col Jeremy L. Sparks, USAF

"We have proven that by doing evil deeds, retribution does not come."
—Unidentified GandCrab ransomware proprietor

In June 2019, the purported masterminds behind the ransomware known as GandCrab announced their retirement from running a global computer malware distribution operation.[1] In the relatively short span of 15 months, GandCrab managed to rake in a record-breaking $2 billion in ransom payments.[2] The commercialization of cybercrime services by the likes of GandCrab, akin to the types of Infrastructure-as-a-Service and Software-as-a-Service commodities offered by more legitimate commercial cloud vendors, demonstrate that cybercriminal organizations are increasing in sophistication and ability. GandCrab's ransomware scheme's size and scope, and the temerity and impunity in which they operated, indicate the daring yet mercurial nature of modern malicious cyber actors, particularly advanced persistent threat (APT) groups.[3] If governments and law enforcement agencies were unable to stop, much less identify and prosecute, an overtly criminal entity like the gang behind GandCrab, what hope is there to prevent more serious threat actors from targeting critical infrastructure networks and systems? Malicious cyber actors continue to operate with such audacity for two primary reasons. First, the internet offers malicious cyber actors a level of anonymity that is difficult to counter without sufficient resources and determination.[4] Second, even if the identities of threat actors behind the malicious cyber activity are established, they typically encounter limited or no consequences, such as financial penalties, criminal prosecution, a military response, and so on.[5] We argue that through a combination of policy changes, organizational improvements, revamping of existing models, and increased threat actor identification efforts, air, space, and cyber forces can help meet and mitigate the threat malicious cyber actors pose to the national security of America.[6]

Fortunately, the US is already well on its way in addressing the various policy gaps that allow APTs to thrive. First and foremost, the *2011 Department of Defense (DOD) Strategy for Operating in Cyberspace* set the tone for organizing cyber forces,

charging US Cyber Command (USCYBERCOM) with responsibilities hitherto, and establishing partnerships for collective cyber operations. Additionally, the 2011 DOD cyber strategy explicitly states that the DOD reserves the right to respond to cyber threats appropriately.[7] The most recent iteration of this strategy, the *2018 Department of Defense Cyber Strategy*, articulates a more mature and vigorous approach. The DOD, principally through USCYBERCOM, will persistently confront malicious cyber activity and defend US critical infrastructure.[8]

To that end, senior US officials have recently credited USCYBERCOM with conducting operations against Russian state-sponsored hackers. For example, USCYBERCOM is reported to have disrupted Russian information operation campaigns aimed at interfering with the 2016 US midterm elections.[9] While the Pentagon deemed the operations a success, some cybersecurity experts weren't as convinced that they successfully countered foreign interference. These operations, and the skeptical responses from cybersecurity pundits, highlight a paradox in how the US is addressing APTs.[10] Since 2011, the US has reserved the right to use military force in retaliation against cyber attacks. Still, despite repeatedly stating that it is willing to engage adversaries targeting the homeland in the cyber domain kinetically, the US has, in very few instances, acted against said adversaries in meaningful ways.[11] This disconnect between what the US states as strategy and the actions the government is willing to take to back up those assertions, is well understood by APT actors. One country taking a different approach to protecting its sovereignty in cyberspace is Israel.

In May 2019, the Israeli Defense Forces (IDF), amid an escalating conflict with Hamas, launched an airstrike targeting a Hamas cyber unit that was attributed to conducting cyber operations against Israel.[12] The IDF reported that its cyber forces identified the geographical location of a Hamas cyber unit and coordinated with the Israeli Air Force for kinetic actions. Soon after the coordination, Israeli air assets employed precision munitions against the Hamas cyber actors and equipment, destroying the specific rooms of the building where Hamas was conducting its cyber operations.[13] The ability to attribute, geolocate, and quickly target menacing cyber actors via kinetic means, represents an evolution of multidomain operations. The US can develop and employ similar synchronization of air, space, and cyberspace to ensure that "evil deeds" do not go unpunished. Being able to impose costs, mainly through kinetic means, will be a keystone effort in promulgating an aggressive "Defend Forward" posture in cyberspace.[14]

However, there are a few key points to consider as it relates to Israel's precedent. Hamas and Israel were already engaged kinetically, so an additional airstrike is not overly escalatory in nature. Additionally, further research still should be done to determine how effective Israel's actions were in deterring future Hamas cyber op-

erations. Those points aside, the Israeli example may offer insights for future US actions. First, the US should have the mechanisms to conduct such a mission, practice it, and then publicize the results of the rehearsals. Second, the US should continue to advertise and execute its right to exercise sovereign options in cyberspace and update its various strategy and doctrine to reflect this position. The intent is to remove any ambiguity in where and how a cyberspace attack might warrant a response, lethal or nonlethal, much like in the traditional air, sea, or even land domains. In so doing, the US seeks to impose a new decision calculus to foreign actors.[15] Malicious cyber actors need to understand that cyber attacks, such as damaging or degrading US critical infrastructures (e.g., electrical control systems or bulk telecommunication networks), will be evaluated for equivalency to an attack on the US homeland. The evaluation could merit a violent, forceful response.

How could multidomain responses to a cyber attack work? There is a two-fold requirement that needs refinement and development in US government and DOD operating procedures and doctrine. First, by executing and publicizing its sovereign options in cyberspace, the US will continue setting norms on what types of assets, personnel, and other protected resources will trigger a response (e.g., the declaration of a national emergency up to and including a declaration of war) if attacked in cyberspace. Secondly, the US must resolve the attribution problem, namely the incontrovertible and unambiguous identification of cyber threat actors, including the infrastructure and information systems used by adversary cyber and APT forces. While attribution is no small feat, the US must invest and deploy resources to discover, to an acceptable degree of certainty, who is responsible for cyber attacks, including the geolocation of the attackers.

Additionally, the DOD, in coordination with interagency partners and the National Security Council, should incorporate kinetic response options to cyber attacks into existing strategies, plans, and rules of engagement (ROE) for all combatant commands in which threat actors reside. Engaging in "cyber diplomacy" is one immediate and potentially dividend-yielding activity that the DOD can employ. The DOD has well-developed expertise in cyber and network defense. Consequently, sharing this knowledge will help partner nations build out their defensive capabilities and enhance the US's alliances. Sharing cyber expertise will enable partners to detect and defend their networks, report and share adversary identifications, markers, and tactics, techniques, and procedures (TTP). It will also reduce the network surface through which an adversary can launch cyber attacks against US critical infrastructure.[16]

Specifying the type of malicious cyber activity that could trigger a forceful response is the first step in presenting a new value proposition to competitors in cyberspace. A starting point for the discussion could be the list of critical infra-

structure identified in Presidential Policy Directive (PPD) 21, which lists 16 categories of interests that underpin US safety and national security.[17] This list leads to the second condition, for which there is no simple solution: how to accurately identify these APTs and threat actors and attribute their hostile activities to them.

How would the US go about identifying cyber threats and also resolve the nonrepudiation problem? As stated earlier, identifying the responsible party of a cyber attack presents an asymmetric challenge—attribution is often much more complicated than the effort required to obfuscate the source of the attack. The difficulties of attributing an attack are not just an issue in cyberspace. The attribution problem is common to several national security threats, namely transnational criminal networks (TCN) and terrorist networks. In fact, there are many similarities between APTs and terrorists and TCNs as evidenced by the table below.

Common properties	*Cyber threats and APTs*	*TCNs and terrorist networks*
Can be motivated by financial gain	GandCrab campaign generated $2 billion in revenue.[18]	Upon seizing Mosul, the value and assets Islamic State in Iraq and Levant ISIL seized was worth $2 billion.[19]
Disregard for rule of law and human suffering	For two years hackers/APTs targeted Ukrainian electrical infrastructure disabling power to thousands of customers.[20]	Cartel members overwhelming Government of Mexico forces and threatening violence to thousands of civilians in a bid to free cartel leader[21]
Operate in hostile countries, often tolerated	Russia is tolerating the participation of "Patriotic Hackers" during conflicts with its neighbors.[22]	The government of Sudan and the Taliban in Afghanistan allowing al-Qaeda to operate unchecked within their respective countries
Targets critical infrastructure/US military/allies	Consistently targeting US cities, federal agencies, and defense contractors	2019 attack on Saudi Arabian oil infrastructure[23]

Table. Common properties of cyber threats and APTs vs TCNs and terrorist networks

The likenesses between cyber threat actors and terrorist or criminal threats may be advantageous in that the doctrinal principals of counterterrorism may apply well to counter-APT efforts. Using Joint Publication (JP) 3-25, *Countering Threat Networks*, as a model, the identification of cyber threats and APTs would begin by conducting network analysis. This analysis will characterize the capabilities of a particular cyber threat or APT.[24] The next step is to conduct critical factors analysis, leading to the identification of adversary centers of gravity (COG), critical capabilities (CC), critical requirements (CRs), and critical vulnerabilities (CV).[25] As a notional example, a COG might be the command and control (C2) element or individuals associated with a threat, critical capabilities might be the attack and exploitation mechanisms a cyber-threat or APT might possess, a CR might be the network connectivity needed for a cyber threat or APT to initiate attacks, and a CV might be vulnerabilities within the TTPs that such a group might employ.

Just as the US does not tolerate the existence of threatening terrorist networks, neither should it tolerate the existence of cyber threat networks. From the *2018 Cyber Strategy*, persistent engagement means the US government (USG) and DOD should collaborate and coordinate the full spectrum of the intelligence community to employ human intelligence, signals intelligence, electronic intelligence, communications intelligence, and every other capability in between to discover and enumerate these networks. If a particular APT has a tactic or procedure to use virtual private networks, the onion routing network, or other mechanisms to hide their sources, it is imperative the intelligence community discover and monitor these sources and build up the technical capabilities to do so. If there is a particular school, website, or learning service that an adversary prefers to employ to train their cyber forces, the US must employ collection methods into these areas, not unlike having sources and insights into terrorist training camps and facilities.

Assuming the USG establishes and attribute the identities and actions of cyber threats or APTs, a next step is to employ the targeting cycle with deference to the desired effects on networks metrics of neutralize, degrade, disrupt, destroy, defeat, deny, or divert. Ultimately, this tactic could lead to outcomes of violent military force, such as bombing a building (e.g., the IDF airstrike on the Hamas cyber unit) or employing US Special Operations Command forces to capture or kill foreign cyber threat actors targeting US critical infrastructure.[26] Lastly, in order to fully exploit Total Force Integration, the expansion of Guard and Reserve intelligence and cybersecurity organizations and programs, such as the Joint Reserve Intelligence Centers (JRIC) or National Guard Cyber Protection Teams (CPT), should be explored as both could be a significant force and capability multiplier, especially if said Guard and Reserve members are placed in civilian cybersecurity roles within US critical infrastructure when on civilian status.[27] Suppose an incident response or security operations center analyst at an electrical utility was a Guard or Reserve member. He/she/they may then be trained to become familiar, or even expert, with some of the utility's control systems. This analyst may even be able to install and monitor CPT sensors on their utility's control network, assuming the technical, financial, and legal considerations can be overcome. In the event of compromise, the analyst could then start direct reporting information to the Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA), possibly having direct classified discussions, assuming the infrastructure is in place to do so. Subsequently, the analyst could immediately then get on voice orders, go to a JRIC, Guard CPT, or even an air operations center component like the Intelligence, Surveillance, Reconnaissance Division, and start adding expertise with an unprecedented level of insight into cyber or

even kinetic targeting cycles. The analyst could aid in weaponeering and help in identifying the right affect against a particular target, given their intimate knowledge of the adversary TTPs being employed. Or the analyst could go to a Joint Targeting Board to articulate the type of effect a cyber threat or APT is having on their employer's control system network in order to increase targeting priorities. It is worth noting that the DHS already leverages programs like the Cyber Information Sharing and Collaboration Program and the EINSTEIN Project. These programs aid in information sharing, but figuring out and overcoming the necessary legal, jurisdictional, operational, and civil-military obstacles are also easier said than done to enable these cohesive, rapid, and full-range responses.[28] All of these steps would be essential for appropriate mission analysis in the Joint Operating Planning Process for Air.[29]

Using the above information as a backdrop, consider the following scenarios, steps of action, and responses. Cyber espionage against US election systems or cleared defense contractors (CDC) might warrant responses by legal means, including indictments by the Department of Justice. Still, cyber espionage to conduct the equivalent of Joint Intelligence Preparation of the Operating Environment (JIPOE) against US electrical, water, gas, telecommunication, and other critical infrastructure may need joint law enforcement or military response. In this case, if a utility detected and verified the Indications of Compromise (IOC) or TTPs from known APTs, the DHS and CISA could notionally be notified with the evidence of these IOCs and TTPs. These include relevant Internet Protocol or Media Access Control addresses, network traffic, email artifacts, system and event logs, login account audits, malware samples, and any other supporting information.[30] If the threat is determined to be sourced outside the jurisdiction of the US, then DHS and CISA should then liaise with DOD entities, such as the Defense Intelligence Agency and/or National Security Agency, to assist in determining the attribution of the cyber threat group. Again, this notification cycle might be shortened if there are Guard or Reserve members on civilian status employed as civilians within the cyber security organization of an affected utility. If the cyber threat group is based overseas, the combatant command responsible for the area in which the threat resides would perform standard targeting and planning processes, using established targeting guidance and JP 3-25 procedures. If the foreign threat/APT furthers their compromise of a utility by moving beyond the JIPOE phase into manipulating or disrupting a utility's Human Machine Interfaces, Distributed Control System, or Supervisory Control and Data Acquisition system, forceful response actions, having been enriched by the intelligence generated by the aforementioned processes, could then be considered.

Given such a notional scenario, suppose that mission analysis concludes that malicious cyber actors, operating out of a multistory building (such as the facility mentioned that the IDF targeted), are determined to be responsible. Further, suppose that the building is within an area of responsibility of a combatant command where ROEs, for both kinetic and nonkinetic effects, already exist. If the building meets targeting guidance for the AOR, the facility is subject to target nomination. If the target is validated and vetted, the target may be added to the Joint Integrated Priority Target List, and, if consistent with the joint force commander's guidance, added to the air tasking order.[31] Mobile targets or targets that are time-sensitive, which is likely to be the case with many targets, would equally be susceptible to dynamic targeting (with its six distinct find, fix, track, target, engage, and assess [F2T2EA] steps), with the "fix" step the most involved in determining attribution.[32] After appropriate weaponeering, the target could be struck, either with conventional munitions or other military capabilities, from electronic warfare to Space-Enabled Cyber Operations to the employment of USSOCOM forces, all of which would be followed by standard battle damage assessment processes.

A principal sticking point of delineating the type of cyber intrusion, and who is responsible for responding, is an ongoing debate of legality. When does a cyber attack become a law enforcement matter versus one of national security concern to the US? When is a computer exploitation attack considered a case of espionage? Is it election hacking or the theft of sensitive or classified information? When is a cyber attack an act of war? Would it be an act of war for a cyber threat actor or APT to disrupt or degrade the utility or telecommunication service belonging to one of the critical sectors described in PPD 21? These are questions that combatant commanders should field to the Joint Staff and Office of the Secretary of Defense so that they can begin working with Congress and the national security enterprise to clear up the current state of ambiguity. If positive attribution to a cyber attack has been achieved, particularly in US Northern Command (USNORTHCOM) where the preponderance of the US critical infrastructure and homeland defense mission resides, what is the USNORTHCOM commander's, or any other impacted combatant commander's, roles and rights in inherent self-defense? What about liaising with USCYBERCOM, the Cyber National Mission Forces, and other supporting forces tasked with critical infrastructure protection? Until the theater ROEs are defined, CCDRs have little option but to absorb the blow and maintain a largely defensive posture. If ROEs were sufficiently mature, combatant command planners could instead start generating more active civil and military critical infrastructure defense-related flexible deterrence options and flexible response options per JP 5-0 *Joint Planning*.

Beyond the legal authorities and implications inherent in the homeland defense mission, international concerns also need to be addressed. Maj Gen Didier Tisseyre, commander of France's Cyber Defense Command, has several adroit observations about cyber defense and notes, "If an organization such as NATO is attacked, then France is, by principle, against collective attribution. . . You have to be able to prove it, and the state that has been blamed might not appreciate having the finger pointed at it."[33] Therein lies further discussion, particularly with US's North Atlantic Treaty Organization (NATO) allies about its views, the ROEs for when and how we would respond, and thus the ROEs for when and how we would invoke Article 5 of the NATO treaty for mutual defense against a cyber attack.

Although both policy changes and attribution present large hurdles, something must be done to unmask, and continually confront, cyber threats, APTs, and similar rogue actors. By not establishing bright lines and systematically identifying and targeting these adversary forces, and by not meting out "retribution," we allow "evil to continue." In times of crises and conflict, not only will we face the continuing taunts of threat groups like GandCrab unabated, we might have to do so under candlelight—if we even have connectivity at all at that point.[34] ✪

Maj Lou Nguyen, USAF

Major Nguyen is the deputy chief, Vulnerability Management Branch, J34, Joint Force Headquarters-DOD Information Network at Fort Meade, Maryland when he is on active status with the Air Force Reserve. Previously, he was deputy chief, Strategy Plans Division, 9th Combat Operations Squadron at Vandenberg AFB, California. In his private civilian career, he is the senior cybersecurity engineer for a large natural gas utility in the United States.

Lt Col Jeremy L. Sparks, USAF

Lieutenant Colonel Sparks is the commander, 333rd Training Squadron, Keesler AFB, Mississippi. Previously, he was the weapons and tactics branch chief and Joint Access Operations Center chief at US Cyber Command, Fort Meade, Maryland.

Notes

1. Joie Salvio, "GandCrab Threat Actors Retire. . . Maybe," *Fortinet Threat Research*, 24 June 2019, https://www.fortinet.com/.

2. Brian Krebs, "Who's Behind the GandCrab Ransomware?," *Krebs on Security*, July 2019, https://krebsonsecurity.com/.

3. The National Institute of Standards and Technology defines an *advanced persistent threat* as: "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)," https://csrc.nist.gov/.

4. Walter Isaacson, "How to Fix the Internet," *The Atlantic*, 15 December 2016, https://www.theatlantic.com/.

5. Garrett Hinck and Tim Maurer, "What's the Point of Charging Foreign State-Linked Hackers?," *LawfareBlog*, 24 May 2019, https://www.lawfareblog.com/; and Department of Justice, "Report of the Attorney General's Cyber Digital Task Force," July 2018, https://www.justice.gov/.

6. Curtis E. LeMay Center for Doctrine Development and Education, *Challenges of Cyberspace Operations*, in "Annex 3-12, Cyberspace Operations" (Maxwell AFB: Air University, 11 November 2011), https://www.doctrine.af.mil/.

7. Department of Defense (DOD), *Department of Defense Strategy for Operating in Cyberspace,* July 2011, https://apps.dtic.mil/.

8. DOD, *Summary: Department of Defense Cyber Strategy*, 2018, https://media.defense.gov/.

9. Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, 27 February 2019, https://www.washingtonpost.com/.

10. Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access."

11. David Alexander, "U.S. Reserves Right to Meet Cyber Attack with Force," *Reuters Technology News*, 15 November 2011, https://www.reuters.com/.

12. Twitter's account of the Israel Defense Forces: "CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed," 5 May 2019, https://twitter.com/.

13. Elias Groll, "The Future Is Here, and It Features Hackers Getting Bombed," *Foreign Policy,* 6 May 2019, https://foreignpolicy.com/.

14. US Cybersecurity Solarium Commission, March 2020, 23–25, https://www.solarium.gov.

15. David Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, 15 June 2019, https://www.nytimes.com/.

16. Dr. Panayotis A. Yannakogergos, "Strategies for Resolving the Cyber Attribution Challenge" (Maxwell AFB, Air University: May 2016), 58–59; and U.S. Cybersecurity Solarium Commission, 2–7.

17. Presidential Policy Directive 21, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, 21 February 2013, https://obamawhitehouse.archives.gov/.

18. James Walker, "GandCrab Closure Will Lead to 'Power Vacuum' in Ransomware Market," *Daily Swig,* 20 June 2019, https://portswigger.net/.

19. Martin Chulov, "How an Arrest in Iraq Revealed Isis's $2bn Jihadist Network," *The Guardian*, 15 June 2014, https://www.theguardian.com/.

20. Darren Pauli, "Crims Shut off Ukraine Power in Wide-Ranging Anniversary Hacks," *The Register*, 12 January 2017, https://www.theregister.co.uk/.

21. Will Grant, "Mexico's Bid to Detain El Chapo Son 'a Failure of Everything,'" *BBC News*, 18 October 2019, https://www.bbc.com/news/.

22. Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *Center for Naval Analyses*, March 2017, 13; and Scott D. Applegate, "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare," *IEEE Security and Privacy* 9, no. 5 (September 2011): 16–22.

23. Michael Safi, "Iran Denies Launching Drone Attacks on Saudi Oil Facility," *The Guardian*, 15 September 2019, https://www.theguardian.com/.

24. Chairman of the Joint Chiefs of Staff (CJCS), *Joint Publication (JP) 3-25 Countering Threat Networks* (Washington, DC: Department of Defense, 21 December 2016), II-1–III-9, https://www.jcs.mil/Portals/; and Mitre, "Groups," https://attack.mitre.org/.

25. CJCS, *JP 3-25, Countering Threat Networks* (Washington, DC: Department of Defense, 21 December 2016), IV-4, https://www.jcs.mil/Portals/.

26. CJCS, JP 3-25, V-1–V-16.

27. David Vergun, "Reserve, Guard Leaders Provide Cybersecurity Updates," 26 March 2019, https://www.defense.gov/.

28. Department of Homeland Security (DHS), "Cyber Information Sharing and Collaboration Program (CISCP), 23 November 2015, https://www.cisa.gov/, and DHS, "Einstein," 21 August 2015, https://www.dhs.gov/cisa/einstein.

29. Curtis E. LeMay Center for Doctrine Development and Education, *The Joint Operation Planning Process for Air*, in "Annex 3-0, Operations and Planning" (Maxwell AFB, AL: Air University, 4 November 2016), https://www.doctrine.af.mil/.

30. Danny Bradbury, "Iran's APT33 Sharpens Focus on Industrial Control Systems," 22 November 2019, https://nakedsecurity.sophos.com/.

31. Curtis E. LeMay Center for Doctrine Development and Education, *Contingency and Crisis Execution: The Tasking Cycle*, in "Annex 3-0, Operations and Planning" (Maxwell AFB, AL: Air University, 4 November 2016), https://www.doctrine.af.mil/.

32. Curtis E. LeMay Center for Doctrine Development and Education, *Dynamic Targeting and the Tasking Process*, in "Annex 3-60, Targeting" (Maxwell AFB, AL: Air University, 15 March 2019), https://www.doctrine.af.mil/.

33. Christina Mackenzie, "France's New Cyber Defense 'Conductor' Talks Retaliation, Protecting Industry," *Defense News*, 30 September 2019, https://www.fifthdomain.com/.

34. Kelly Jackson Higgins, "Latest Ukraine Blackout Tied to 2015 Cyberattackers," *Dark Reading,* 10 January 2017, https://www.darkreading.com/.

Redistributing Airpower for the Spectrum of Warfare

LCDR Trevor Phillips-Levine, USN*

Redefining Relationships

Many of the air assets in the US inventory are expensive machines of war, designed to confront a peer adversary in high-end warfare. However, the majority of operations that have required US military resources for the past two decades did not require such high-end equipment.[1] Expensive fighter aircraft and bombers (e.g., F-15, F-16, F-22, F/A-18, F-35, and B-1B) have been used against an enemy that lacks an air force and credible integrated air defense systems, which is far less challenging than the environments for which these aircraft were designed. Additionally, the continuous use of high-end aircraft has depleted its useful life at an unprecedented pace, eroding overall readiness. While defense appropriations have increased recently, fiscal forecasts indicate that the trend of requiring the military to "do more with less" will continue, and budgets are expected to shrink into the future.[2] The full "spectrum of warfare"—from low-end insurgencies or irregular warfare to high-end peer conflicts—have notable differences in required capabilities, cost, and priorities.[3] Since airpower is integral to all forms of modern warfare, the US military must be prudent in the allocation of air capabilities within the service components to ensure adequate coverage. This allocation strategy is best accomplished by specializing procurement, roles, and responsibilities while identifying areas of unnecessary overlap or redundancy. The net effect would be increased effectiveness and efficiency of the joint force with each service component bringing unique capabilities. While the spectrum of warfare affects all service components, the focus of this article is between US Air Force and Army relationships in the land area of operations. Since counterinsurgency (COIN), stability, and hybrid warfare or low-end operations typically involve land components, the predominance of airpower is there to directly support the land mission. Close-in support is best accomplished with assets that are familiar with land component doctrine, which inherently includes land component tactics, techniques, and procedures (TTP). This approach is evidenced when examining the definitions of

*Editor's note: The following article represents the views of the author and not those of the *Air & Space Power Journal*, nor is it the official position of the US Air Force. LCDR Andrew Tenbusch, USN, contributed to this article.

roles, administrative and operational control, and the lack of a return on investment when utilizing multirole over specialized platforms. When aggregated, an argument can be made for a fundamental shift in traditional US Air Force roles and mission. Therefore, while it may be a controversial topic, it is the author's opinion that the US Air Force should focus on high-end capabilities to confront peer adversaries. Simultaneously, the responsibility for low-end, close-in support airpower requirements of the land force should predominantly fall to the land component, traditionally the US Army.

Roles and Control

Historically, the US Air Force and Army have been at odds over the role of airpower in warfare dating back to when the Air Force was part of the Army as the US Army Air Corps. Before World War II, airpower advocates led by Billy Mitchell argued that airpower should be used to strike at enemy centers of gravity, bypassing the stalemate of trenches while simultaneously destroying the vital organs of a country's war machine.[4] In other words, the use of airpower should be used with a strategic focus and for targets that could not be ranged by artillery. Conversely, US Army staff argued that airpower's purpose lay with close support and enabling the maneuver and objectives of ground forces.[5] During the Korean War, the theater commander, US Army Gen Mark W. Clark, received blunt feedback from US Air Force Gen Otto P. Weyland regarding competing airpower priorities. In August 1952, General Clark penned the following in a letter to his subordinate commanders regarding the friction between the differing opinions on Air Force and Army priorities:

> It should be borne in mind that the theater commander, rather than any single service, bears over-all responsibility for successfully prosecuting the Korean War. Each component contributes its own specialized capabilities to the attainment of the theater commander's over-all mission and in so doing assists the other components; however, no single service exists solely or primarily for the support of another.[6]

General Clark effectively stated that the US Air Force and other service components were all working toward a common objective, but that no single component had primacy over another in the attainment of that objective. Differences remained regarding the application of airpower and were once again brought to the forefront with experiences in Vietnam. The US Army fielded a light-attack aircraft, the OV-1 Mohawk, to good effect within its special forces community; however, infighting with the Air Force over the Army possessing fixed-wing

light-attack aircraft helped hasten the eventual abandonment of the program.[7] A 1972 Rand Corporation study stated the following:

> . . . the close air support issue manifests itself in a variety of differences between the Air Force and the Army. It is central to the establishment and maintenance of an effective relationship between air and ground elements in combat operations. The two services consider close air support an essential part of their missions and an essential element in their capabilities. There can be little doubt that the Army has established a de facto role for itself in close air support and this role is permanent. Nevertheless, the prospect for the future seems to be continued resistance by the Air Force to Army acquisition of additional responsibilities and capabilities for the function. But such resistance can be effective only if the Air Force demonstrates willingness, imagination, and responsiveness to the Army, and provides more versatile capabilities to perform the function.[8]

The close-in support role ideally falls to the land component, the Army. While the Joint Force commander (JFC) will have assets assigned to fulfill his or her objectives, it matters which service component has administrative control. The reason is that administrative control includes the responsibility for organizing, training, and equipping assets.[9] These responsibilities are influenced by service component doctrine and TTPs. Despite various service component assets being under the operational control of the JFC, ultimately, those assets will utilize service component doctrine at the tactical levels of execution.

Further evidence that close-in support should rest with the land component can be found by examining the construct of a conventional battlespace. The fire support coordination line (FSCL) is the defining boundary in which direct coordination with the land component is required.[10] The FSCL does not dictate the type of missions allowed short or beyond it and is primarily used for command and control and planning.[11] The air component is responsible for striking targets beyond the FSCL through air interdiction (detection, location, and engagement of targets of opportunity), in addition to performing air superiority missions.[12] Short of the FSCL, friendly ground maneuver elements may be operating, requiring that all fires be coordinated.[13] This situation highlights two main points: (1) coordination short of the FSCL is required to prevent fratricide; and (2) since ground maneuver elements are operating within this zone, fires may be in direct support of the ground scheme of maneuver. Placing dedicated close-in support aircraft under the Air Force purview may require aircrews and ground controllers to receive additional training to bridge doctrinal differences between the air and land components to maximize effectiveness. Additionally, the risk remains of competing priorities between Air Force and Army requirements during platform acquisition and mission execution.

At issue is the adherence and steadfastness of the US Air Force and Army to previous agreements, namely the 1948 Key West Agreement, from which the previous and current iterations of the Department of Defense Directive (DoDD) 5100.01 were derived. The Key West Agreement was intended to resolve internal conflicts between the various service components about inherent capabilities. Some interpret the agreement as setting the limits of Army aviation and Air Force responsibility to provide Army air support requirements. However, the wording of the agreement mentions only that components should apply the "maximum avoidance of duplication in operations" and that "no component should develop or maintain, on an appreciable scale, forces which already exist in another component."[14] The Key West Agreement and the DoDD 5100.01 have gone through numerous revisions, including the Goldwater-Nichols Defense Reorganization Act that further empowered joint combatant commanders and sought to improve efficiency between the services.[15] Despite the revisions and updates to commensurate changes with technology and global priorities, the roles and missions remained relatively unchanged.[16]

The wording is vague and open to broad interpretation. Still, it does not prohibit the Army from developing and operating its own specialized fixed-wing attack platforms, especially if that capability does not reside within the Air Force. More recently, an *Air & Space Power Journal* article by Col Jon Wilkinson and Dr. Andrew Hill, in addition to a threat from Congressman Michael Waltz to allow light-attack procurement by the Army, indicate both external and internal criticisms remain regarding the effectiveness of Air Force fulfillment of the close-in support mission.[17]

Currently, the United States has found itself embroiled in frustrating insurgencies that led to its involvement in its longest war. Insurgencies develop when a faction or group lacks the resources to directly confront a superior adversary and is a form of irregular warfare. Insurgency or guerrilla warfare is difficult to prosecute with traditional military methods. Per Fleet Marine Force Reference Publication (FMFRP) 12-18:

> Guerrilla war is not dependent for success on the efficient operation of complex mechanical devices, highly organized logistical systems, or the accuracy of electronic computers. It can be conducted in any terrain, in any climate, in any weather; in swamps, mountains, in farmed fields. Its basic element is man, and man is more complex than any of his machines.[18]

The American Revolutionary War was one that had mostly an insurgency flavor with militiamen ambushing British supply lines and soft targets. Mao Tse-

tung advocated insurgency or a protracted war (People's War) as the prime mover for political change and resistance to oppression.[19]

The key takeaway is the asymmetric nature of an insurgency (a form of irregular warfare) with measurements of strength and effectiveness not tied to conventional definitions of warfare. The other takeaway is that an insurgency is based on people and the requirement for a haven for insurgents to operate beyond the reach of conventional methods. These havens are in the form of territory, whether being remote regions or population centers. To the point of Colonel Wilkinson and Dr. Hill, irregular warfare does not require the expensive systems that comprise the majority of US Air Force combat air arms or the US military writ large due to its permissive environment and unconventional methods. It is also important to divorce the notion that close air support (CAS) and COIN operations are synonymous. True, a considerable number of air operations performed during the War on Terror have been CAS. This number was due to the large presence of security and stability operation forces and the inevitability of coming into contact with the enemy. Per Joint Publication (JP) 3-09.3, *Close Air Support*:

> Close air support (CAS) is planned and executed to support ground tactical units. The air apportionment recommendation and allocation process for joint air operations, which includes CAS, occurs at the operational level. CAS planning focuses on providing timely and accurate fires in support of friendly forces in close proximity to the enemy. CAS can be conducted at any place and time friendly forces are in close proximity to enemy forces. The word "close" does not imply a specific distance; rather, it is situational. The requirement for detailed integration because of proximity, fires, or movement is the determining factor. At times, CAS may be the best available means to exploit tactical opportunities in the offense or defense by providing fires to destroy, disrupt, suppress, fix, harass, neutralize, or delay enemy ground forces.[20]

Low-end warfare, which can be thought of as synonymous with stability or COIN operations, is a protracted war with success not tied to volume or frequency of munition expenditures by airpower. Additionally, engagement with the enemy may be sporadic, localized, and over vast territories. This engagement makes US Air Force air control doctrine, utilizing fixed air tasking order cycles (ATO), and conventional fixed-wing fighters and bombers analogous to using an expensive sledgehammer to drive a nail.[21] As Colonel Wilkinson and Dr. Hill pointed out, the Air Force air control construct, as it stands with its fixed ATO cycles, is inefficient for low-end warfare because it lacks responsiveness and adaptability.[22] Historically, the joint forces air component commander has been held by the US Air Force. Conceptually, it can also be held by a Naval component indicating that these shortcomings are not unique to the US Air Force. This

viewpoint does not mean that US Air Force or Naval air control priorities need to change since they are optimized for the full spectrum of a robust conventional battlespace. Instead, the divestiture of requirements to support low-end warfare to components of the armed forces that are more invested in COIN and stability operations is a better solution.

Traditionally, the brunt of these operations has fallen upon land components that are comprised mostly of Army, Marine Corps, and special operation forces units. Since air support is ultimately to further or support ground objectives in COIN and stability operations directly, this is where low-end air capability should reside. For instance, the Army views its aviation assets as another unit within the ground force.[23] The result is that Army aviation elements exercise lower levels of coordination when compared to CAS procedures in what was formerly referred to as close combat attack.[24] JP 3-09.3 states the following:

> USA [US Army] AH [Attack Helicopter] units support maneuver commanders as a subordinate maneuver unit. They are given mission type orders and execute these orders as a unit. USA AH units can conduct attacks employing CAS TTP [tactics, techniques, and procedures] when operating in support of other forces. However, their proficiency will be limited unless they have been trained as part of SOF [special operations forces] or CAS TTP have been coordinated in advance.[25]

The main difference is that Army aviation and rotary-wing five-line CAS briefs are friendly-centric, whereas, in most CAS procedures, they are target-centric.[26] In effect, the priority of an Army or rotary-wing asset is to ascertain with high confidence friendly position(s) before employment. Also, Army aviation does not require a specialized controller, known as a joint terminal attack controller (JTAC), or the clearance to release munitions while operating organically, potentially reducing kill-chain timelines. With organic use, any individual with a radio can request fires with no specific training. When supporting outside units, Army aviation utilizes JP 3-09.3 procedures. The most efficient procedure is the Army aviation or special operations force (SOF) call-for-fire (CFF) that is modeled after the artillery CFF format and does not require a JTAC to execute. A ground unit requesting fire could also utilize the rotary-wing five-line CAS brief, similar to a CFF. However, it requires a separate clearance be given (by a JTAC) in addition to the five-line CAS brief to authorize munition expenditure.[27]

The Air Force has one asset that utilizes SOF and Army aviation CFF procedures—the AC-130 gunship. The AC-130 is enabled through its twin high-fidelity electro-optical sensors, orbit, and gyro-stabilized direct-fire artillery platform. But Air Force AC-130s are primarily used by special operations, and their use to support conventional units is not the norm. The fluid and flexible response

SOF and Army aviation procedures offer seem ideally suited in an irregular environment where flexible and adaptable responses are required. While traditional fixed-wing strike assets performing CAS can perform similar procedures, it is typically associated with emergency CAS (E-CAS) scenarios with an increased risk of fratricide. In these *extremis* situations, aircrew assumes all responsibility for ensuring deconfliction from friendly ground forces before releasing ordnance. It is considered a deviation from normal JP 3-09.3 procedures.

Another type of mission executed in low-end warfare is high-value individual (HVI) and high-priority human target (HPHT) targeting. These missions are typically associated with special operations that fall under the purview of Special Operations Command (SOCOM). While SOCOM is comprised of US Air Force, Army, Navy, and Marine Corps assets, the Air Force contributes the predominance of air capability through its Air Force Special Operations Command (AFSOC). Within AFSOC, the Air Force supplies specialized intelligence, surveillance, and reconnaissance (ISR) aircraft, including armed variants, attack consisting of AC-130 gunships, and lift. In terms of air support, the Army supplies specialized rotary-wing (non-tiltrotor) assets through the 160th Special Operations Aviation Regiment (SOAR).

If the US Air Force desires to maintain relevancy in the low-end, then AFSOC is where it should invest its capability. However, the Army's 160th SOAR is an equally opportune location to place dedicated special operations light-attack and tactical ISR support. In 2017, Sen. John McCain published a budgetary white paper titled "Restoring American Power." He argued the need for the US Air Force to procure 300 light-attack aircraft, 200 by 2022, to preserve the fleet life of existing 4th and 5th generation fixed-wing platforms while maintaining capability in low-end conflicts.[28] The likely light-attack procurement cost is between $6–$7.5 billion, not including aircrew training requirements or operational costs.[29] Instead, the US Air Force has opted for a more measured approach, agreeing to buy a handful of planes for Air Combat Command and AFSOC.[30] The focus appears to be on programs that will be geared toward building partner capacity through tactics development and airborne advisor integration.[31] Building capacity in partner-nation air forces is important in building host government credibility and capability for eventual self-sustainment.[32] While this is an ideal mission for the US Air Force advisors, it does not solve the close-in support requirement for conventional ground forces. Also, increasing coverage of conventional ground forces by AC-130 gunships would remain inadequate due to their limited availability.

If the Air Force does not wish to maintain any capability in low-end conventional operations, it should divest its air advisor mission to the Army. The Army already maintains a robust aviation advisor mission, focused on rotary-wing. Since

the Army is also training host-nation forces in COIN and stability operations, adding light-attack may help ground and aviation forces better integrate by uniting under a unified doctrine.

Instead of trying to reconcile the criticisms, the US Air Force should drop its aversion to the Army operating fixed-wing light-attack. Critics may fear an erosion of US Air Force relevance and opening Pandora's Box regarding the Army attempting to take more and more airpower roles under its cognizance. However, they only need to look at history when airpower advocates and Army staff argued the true purpose of airpower. The Army's desire for airpower is to facilitate close-in support of ground maneuver elements and further its function of land dominance. DoDD 5100.01 lists some of the Army's functions are to "conduct prompt and sustained combined arms combat operations on land in all environments and types of terrain, including complex urban environments, in order to defeat enemy ground forces, and seize, occupy, and defend land areas" and "interdict enemy sea, space, air power, and communications through operations from or on the land."[33] These functions can be interpreted to mean that while the Army may utilize organic air assets, using air assets is strictly for furthering land dominance missions. The reason Air Force relevance is not in question is because the interdiction of enemy elements not related to close-in support of a ground force maneuver engaged in a land campaign (e.g., targets beyond the FSCL) falls under the purview of the air component.[34] Furthermore, the overall responsibility for airborne logistical support is specifically delegated to the US Air Force.[35]

The precedence for the divesture of capability is already set. Ceding the MC-12 ISR aircraft to US Army control, once operated by the Air Force, shows that the Army has the capacity and capability to absorb airpower missions.[36] In fact, the transfer of MC-12 assets to the Army was described as "seamless" and resulted in no mission interruptions.[37] Additionally, the Army operates armed ISR capability with MQ-1C Gray Eagle drones. The ability of the Army to absorb and perform airpower missions, while maintaining mission effectiveness in low-end operations, lends credibility to the argument that a return to specialization within the service components is warranted to cover the full spectrum of warfare.

Specialization Versus Multirole

The spectrum of warfare spans from the low-end to high-end. COIN, counterterrorism, and stability operations are characterized by permissive environments and fall into the low-end of the spectrum of warfare.[38] Permissive environments lack conventional air-to-air threats, and surface-to-air threats consist of man-portable air defense systems (MANPAD) and/or light air defense artillery. Friendly forces maintain air superiority, if not supremacy. While the land domain may be

contested, air, space, and cyberspace domains are largely uncontested. This operating environment has been the assumed baseline for most environments in the War on Terror. The nature of this environment makes low-altitude systems the most vulnerable, with higher flying platforms minimizing or avoiding threats through altitude sanctuaries in the battlespace. For these reasons, strike and medium-to-high altitude remotely piloted aircraft (RPA) are usually operating at low risk. Consequently, the risk to the mission from hostile fire is low for fixed-wing aircraft, while rotary-wing aircraft may experience elevated risk levels in this environment.

High-end warfare is characterized by countering anti-access/area denial threats.[39] Adversaries can contest many or all of the domains simultaneously with integrated air-defense systems and military capabilities in land, sea, air, space, and cyberspace. High-end warfare can be thought of as warfare with modern, state militaries in direct confrontation with one another.[40] The upper-low segment of the spectrum can be thought of as *hybrid warfare* where state actors may supply advanced weaponry to forces (proxies) that they would not possess otherwise, or that utilize weapons captured from state militaries (as is the case with the Islamic State in Iraq and Syria [ISIS]).[41]

Colonel Wilkinson and Dr. Hill's article from 2017 illuminates the dilemma some circles within the US Air Force are experiencing. Their article portrays an Air Force that is on the path to irrelevance by prioritizing high-end specialization while ignoring the low-end. Cited as evidence was the divestiture of MC-12 reconnaissance aircraft and the near-retirement of A-10s before congressional intervention. These events illustrate Air Force management was indeed prioritizing specialization into the high-end with the long-term focus being on peer competitors.[42] Meanwhile, both Colonel Wilkinson and Dr. Hill contend that the US Air Force ignoring the low-end conflicts and not investing in specialized, cheaper technologies imperils its relevance and places American strategic objectives at risk. This is a narrow viewpoint. It places the US Air Force as the sole proprietor of airpower capability and ignores the joint force as whole. High-end capabilities are expensive in terms of time to develop, resources (including manpower), and money, but necessary. Research and development costs have been steadily marching upward throughout history and have been making up larger percentages of expenditures on weapon programs. Further, high-end requirements are necessitating the return of specialization not only in terms of platforms but also in terms of missions.

For example, an article in *Military Review* discussed how US Air Force multirole aircraft were larger than necessary, overly complex, and costly despite onboard technology designed to mitigate capability gaps.[43] Multirole is an attempt at economy by requiring aircraft and operators to be capable of multiple missions; however, this reduces combat effectiveness since neither the platform nor the op-

erator is optimized for any particular requirement. This reduction in effectiveness makes it less likely that the force will accomplish the combatant commander's mission objectives.[44] It is precisely for these reasons that the US Air Force needs to focus on the high-end capability since specialization in this area ensures the ability to dominate complex-networked battlespaces. Colonel Wilkinson and Dr. Hill are right that the United States cannot afford to ignore low-end warfare without seriously jeopardizing strategic security and the ability to win future conflicts. However, the US Air Force should not and does not need to shoulder this burden alone, nor should it seek capabilities that overlap with other forces within the joint force.

When examining the DoDD 5100.01, it may appear that it is directing overlapping capabilities regarding CAS. It lists CAS as a US Air Force, Navy, and Marine Corps mission. Maintaining capabilities in CAS does not equate to the requirement to maintain specialized assets to perform the mission.[45] Instead, the interpretation is that when required, US airpower shall be able to integrate effectively and further a ground force commander's objective while enemy forces are within proximity to friendly positions. To be effective, airpower needs only to deliver effects on target when called upon. Korea, Vietnam, and both Gulf Wars utilized existing aircraft to support CAS missions and were largely effective. A myth developed during the Korean War: the Army believed that propeller aircraft, like the outmoded F-51 (formerly the P-51), were better CAS and ground support platforms.[46] This belief was due to the initial basing of jets at the limits of their endurance, defective ordnance, and air control construct.[47] In reality, jet aircraft proved to provide higher readiness rates, greater survivability, and once bases were moved closer, identical loiter capability.[48] The success of the F-51 and similar propeller platforms was only possible through Allied air superiority, a prerequisite with any modern battlefield requiring CAS.

The F-16, F-15, and F/A-18 have performed CAS adequately, and upgraded weapons, developed mostly out of necessity with targeting within urban centers, have improved their accuracy and effectiveness. Even strategic bombers (e.g., the B1-B and B-52) demonstrated limited capability in CAS in Afghanistan and, most recently, against the Islamic State. The F-35, the newest arrival to the US military air arm, has had its utility in CAS questioned due to flight profiles dictated by its preferred tactics, techniques, and procedures. Additionally, its sensor suite is not optimized for close-in support. Nonetheless, it has been shown capable of executing airstrikes in support of ground forces in addition to a host of other capabilities for which it was explicitly designed.[49] At issue is the expense of the utilized platforms and the flexibility of the current air control construct when applied to the low-end, since the majority of current and future Air Force platforms can conduct CAS and ground support missions when required.

In high-end warfare against a peer adversary, there may be situations where the only survivable and effective aircraft are fifth-generation platforms because air superiority is temporary and localized. A scenario in which high-end CAS is required is a defensive one where friendly forces do not hold the initiative and are operating reactively. For example, the first and second phases of the Korean War were periods that necessitated CAS to repel large-scale assaults and prevent friendly forces from being overrun. During the second phase, the enemy leveraged geopolitical boundaries by staging supply lines and airbases on the Chinese side of the Yalu River, a no-go area for US and United Nations forces.[50] A similar environment exists today in eastern Ukraine, where the fear of escalation puts geopolitical boundaries on airpower that allow for havens of enemy strategic surface-to-air systems and fighter bases. Russia supplied and, in some cases, operated surface-to-air systems to provide defensive umbrellas from their territory to support government-backed insurgents.[51] This scenario would require low-observable platforms if US ground forces were involved.

The Army desires a flexible and visible airpower presence that has sufficient loiter, weapons payload, and austere operations capability. In other words, the Army seeks operational control of low and slow "bomb trucks" and surveillance platforms. These platforms would possess the capability to be forward-deployed in austere conditions to allow for distributed airpower coverage and in which the visible presence of airpower alone may be sufficient to rally friendly troops while simultaneously demoralizing the enemy. Presently, the Air Force has been favoring relatively fast and stealthy platforms for its strike and fighter aircraft. While these aircraft have demonstrated capabilities in ground support functions, their preferred tactics and weapons necessitate higher employment altitudes, speed, and greater standoff to maximize survivability. Also, these platforms typically require extensive logistics to operate. The Air Force viewpoint is that with the proliferation of advanced threats, lower and slower aircraft (the type the Army has traditionally championed) lack satisfactory survivability in environments other than permissive. There is data to support this viewpoint. In Korea, low-flying F-51s performing close-in support missions suffered the highest US Air Force loss rates of any other aircraft.[52] Since Korea, the predominance of US Air Force air combat losses has been due to ground fire.[53] The lower and slower an aircraft flies, the more vulnerable it is to ground fire consisting of small arms, MANPADs, and air defense artillery.

Advancements in aircraft sensors and guided low-collateral weapons have mitigated some of the requirement for close-in support aircraft to routinely fly at low altitudes. Previously, unguided weaponry and the lack of sophisticated electro-optical sensors required pilots to employ closer to targets to increase accuracy and

minimize the dispersion of gun systems; this also reduced the chances of fratricide. Requirements to be low and close naturally led to lower operating airspeeds and increased vulnerability. The option now exists, for what historically would have been more vulnerable aircraft, to employ at increased standoff ranges without sacrificing accuracy. The problem is that when standoff or stealth are not required, and there is a desire or need to move a platform closer to targets or troops, only two aircraft in the US Air Force—the A-10 and AC-130—are explicitly designed with that capability in mind.

In May 2018, the Mitchell Institute published an article on the light attack program. In it, the author examined the many benefits of utilizing specially procured light-attack aircraft for low-end conflicts. The article noted, "The attributes of light combat aircraft—tremendous endurance, respectable weapons loads, high weapons delivery accuracy, ability to operate from austere locations, and low acquisition and operational costs—make them an excellent choice for today's low-intensity conflicts."[54]

Examining how airpower has been applied during the past two decades, one can see the potential savings for the US military. Traditional Air Force strike-fighter assets have required aerial refueling support, established bases with infrastructure, high operational costs, and experienced erosion of the assets' fleet life. By comparison, a light-attack aircraft can be flown for anywhere between $2,000–$2,800 per flight hour compared to $19,168 per flight hour for an F-16C.[55] Additionally, existing fixed-wing light attack platforms (e.g., A-29 and AT-6B) have an internal fuel endurance of 2.6 hours that can be increased to 7.1 hours by adding external fuel tanks at the expense of combat load.[56] A light-attack aircraft's speed, payload, and altitude capability allow it to affect targets beyond the reach of a rotary-wing attack. Since 2016 within Afghanistan, the Afghan Air Force has been using its relatively small fleet of A-29s to good effect while suffering no combat losses. To date, Afghan A-29s have conducted 311 successful strikes with 2,427 enemy troops killed in action and zero incidents of fratricide.[57] More importantly, these strikes have no reported incidents of civilian casualties.[58]

In COIN and stability operations, tactical ISR is just as important as dedicated CAS assets.[59] It is not unusual for airborne strike aircraft to fly nontraditional ISR (NTISR) missions when higher priority taskings do not exist. This mission makes for an expensive ISR platform and one not optimized for the role. Light-attack aircraft (i.e., A-29 or AT-6B) can be utilized to fly NTISR missions at an hourly cost similar to MQ-9 Reapers and with greater loiter time than conventional strike-fighter aircraft (when combat load is reduced to facilitate carrying additional fuel).[60] While using RPA may seem like an attractive solution for most

COIN and stability airpower requirements, it is important to note RPA strengths and shortcomings. The Mitchell Institute article noted:

> The advent of the armed RPA, such as the MQ-9 Reaper, provides an astounding ability to target high-value targets that are time-critical, fleeting, or are identified with no other strike assets in proximity to respond. However, using RPA as a tool of first choice for routine light-attack missions risk undermining other vital mission imperatives fulfilled by these aircraft.[61]

RPAs provide a level of persistent loiter, low acoustics, and high-fidelity sensors that are more aptly suited for collecting intelligence or locating and finishing higher priority targets. In COIN and stability operations, these targets are typically HVIs and HPHTs. As a manned platform, light-attack aircraft are not as susceptible to weather or threats when compared to a RPA, capable of modifying their flight profiles to avoid weather or defend against threats.[62] This distinction makes light-attack better suited to prosecute the majority of targets associated with conventional ground operations not necessarily tied to HVI or HPHT targeting.

Conclusion

Specialization and the elimination of unnecessary capability overlap between the services will result in a more efficient and effective joint force. As the US military retools for peer competition, it is important to maintain capability in the low-end as these types of conflicts are likely to persist in the future. Also, ignoring the low-end provides an asymmetric advantage to peer adversaries who may employ hybrid warfare to exploit the perceived vulnerabilities. Lessons from COIN and stability operations have shown that the Army's theory of airpower is most applicable to the low-end as these conflicts lack strategic targets when referencing conventional definitions for Air Force air control construct to be truly effective. Instead, administrative and operational control of close-in direct support assets resting with the land component, for low-end warfare, is more effective.

In more traditional warfare, a high-low mix of aircraft is required to ensure the economical prosecution of any future war.[63] Conceivably, once air superiority is established, US Air Force assets would be conducting air interdiction and air superiority missions beyond the fire support coordinating line (FSCL). Concurrently, Army rotary-wing and light-attack aircraft would prosecute targets short of the FSCL in close-in support of ground forces with Air Force assets augmenting where required. Senator McCain advocated the procurement of 300 light-attack aircraft to rebuild American military power, but the US Air Force should not fulfill this order. Instead, limited procurement to fulfill its advisor missions, as it already has, is the extent to which the Air Force should wade into low-end ca-

pabilities if it does not divest this capability altogether to the Army. The predominance of the remaining light attack numbers should go to Army aviation with the 160th SOAR or AFSOC procuring small numbers for direct special operations support. In this way, the US military can ensure responsive, flexible, and effective airpower delivered to ground commanders in direct or close-in support roles at a fraction of the cost. Should the Air Force maintain its resistance to the Army possessing fixed-wing light attack, the fleet life of high-end assets will continue to erode, and providing tailored airpower to ground commanders in COIN and in stability operations will remain difficult. In consequence, the fears of Colonel Wilkinson and Dr. Hill will take a breath; a low-end capability gap is ripe for any adversary to exploit. ✪

LCDR Trevor Phillips-Levine, USN

Lieutenant Commander Phillips-Levine (BS, US Merchant Marine Academy) is an active duty F/A-18 pilot and squadron department head with 12 years of service in the US Navy. Lieutenant Commander Phillips-Levine has served as a joint terminal attack controller and fires support officer with Naval Special Warfare (NSW) and deployed with Special Operations Task Force–West in support of Operation Inherent Resolve. While serving with NSW, he worked closely with various air and ground entities, including Air Force Special Operations Command, Air Force Weapons School, and Marine Special Operations Command.

Notes

1. Lt Col Michael Buck, USAF, retired, "Light Combat Aircraft: Looking at O/A-X and Beyond," Mitchell Institute Policy Papers 11, May 2018, 2, http://docs.wixstatic.com/.
2. Luke Strange, "A Troubling Outlook for Future Defense Spending," *Real Clear Defense*, 6 November 2018, https://www.realcleardefense.com/.
3. Paul Scharre, "Spectrum of What?," *Military Review*, November–December 2012, 73, https://www.armyupress.army.mil/.
4. LTC Michael J. Chandler, *Gen Otto P. Weyland USAF: Close Air Support in the Korean War* (Maxwell AFB, AL: Air University Press, March 2007), 10.
5. Chandler, *Gen Otto P. Weyland USAF*, 10.
6. Chandler, *Gen Otto P. Weyland USAF,* 72.
7. Joseph Trevithick, "The OV-1 Mohawk Was One of the U.S. Military's First Forgotten Light Attack Planes," *The Drive*, 12 July 2018, https://www.thedrive.com/.
8. Alfred Goldberg and Lt Col Donald Smith, "Army-Air Force Relations: The Close Air Support Issue," *United States Air Force Project Rand*, October 1971, 49, https://www.rand.org/content/.
9. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, IV-16, https://www.jcs.mil/; and Department of Defense Directive (DoDD) 5100.01, "Functions of the Department of Defense and Its Major Components," 21 December 2010, 25, https://www.esd.whs.mil/.
10. JP 3-09, *Joint Fire Support*, A-5, 10 April 2019.
11. JP 3-09, *Joint Fire Support*, A-5.
12. JP 3-09, *Joint Fire Support*, A-5.
13. JP 3-09.3, *Close Air Support*, III-59, 10 June 2019; and JP 3-09, *Joint Fire Support*, A-5.

14. Kenneth Condit, *History of the Joint Chiefs of Staff—The Joint Chiefs of Staff and National Policy*, Vol. II, 1947–1949 (Washington, DC: Office of Joint History, 1996), 93.

15. "White Paper: Evolution of Department of Defense Directive 5100.01," Office of the Secretary of Defense, Revised January 2014, 21.

16. Bob Taradash et al., "Zone Defense: A Case for Distinct Service Roles and Mission," Disruptive Defense Papers, *Center for New American Security*, January 2014, 8, https://www.cnas.org/.

17. Marcus Weisgerber, "U.S. Lawmaker Threatens to Give the Next Attack Plane to the Army," *Real Clear Defense*, 12 September 2019, https://www.realcleardefense.com/.

18. Fleet Marine Force Reference Publication (FMFRP) 12-18, "Mao Tse-tung on Guerrilla Warfare," 5 April 1989, 7, https://www.marines.mil/.

19. FMFRP 12-18, "Mao Tse-tung on Guerrilla Warfare," 20.

20. JP 3-09.3, *Close Air Support*, xi.

21. Col Jon C. Wilkinson and Dr. Andrew Hill, "Airpower against the Taliban: Systems of Denial," *Air & Space Power Journal* (*ASPJ)* 31, no. 3, 50, https://www.airuniversity.af.edu/ASPJ/.

22. Wilkinson and Hill, "Airpower against the Taliban," 53.

23. Maj Patrick Ryan Wilde, "Close Air Support Versus Close Combat Attack," United States Army Command and General Staff College, 2012, 38, https://sobchak.files.wordpress.com/; and JP 3-09.3, *Close Air Support*, III-86.

24. Wilde, "Close Air Support Versus Close Combat Attack," 42.

25. JP 3-09.3, *Close Air Support*, III-86.

26. JP 3-09.3, *Close Air Support*, III-91.

27. JP 3-09.3, *Close Air Support*, III-91.

28. Sen John McCain, "Restoring American Power," *Future Defense Budget Recommendations*, 16 January 2017, 12, https://news.usni.org/.

29. Betsy McDonald, Sierra Nevada Corporation, message to the author, email, 26 September 2019.

30. Aaron Mehta, "US Air Force Officially Buying Light-Attack Planes," *DefenseNews*, 25 October 2019, https://www.defensenews.com/.

31. Mehta, "US Air Force Officially Buying Light-Attack Planes."

32. Maj Michael M. Trimble, *Asymmetric Advantage: Air Advising in a Time of Strategic Competition*, LeMay Paper no. 5 (Maxwell AFB, AL: Air University Press, August 2019), 83, https://www.airuniversity.af.edu/AUPress/.

33. DoDD 5100.01, "Functions of the Department of Defense and Its Major Components," 30.

34. JP 3-09, *Joint Fire Support*, A-5.

35. DoDD 5100.01, "Functions of the Department of Defense and Its Major Components," 34.

36. Wilkinson and Hill, "Airpower against the Taliban," 54.

37. SSgt Torri Ingalsbe, "ISR Aircraft Hones in on Strategic Agility," USAF, 10 November 2014, https://www.af.mil/.

38. Scharre, "Spectrum of What?," 73.

39. Scharre, "Spectrum of What?," 73.

40. DoDD 3000.07, "Irregular Warfare (IW)," 12 May 2017, 14, https://www.hsdl.org/.

41. Scharre, "Spectrum of What?," 78.

42. Wilkinson and Hill, "Airpower against the Taliban," 48; and Ingalsbe, "ISR Aircraft Hones in on Strategic Agility."

43. Maj John Q. Bolton, "Precedent and Rationale for an Army Fixed-Wing Ground Attack Aircraft," *Military Review*, May–June 2016, 79, https://www.armyupress.army.mil/.

44. Maj Kamal J. Kaaoush, "The Best Aircraft for Close Air Support in the Twenty-First Century," *ASPJ* 30, no. 3, 50, https://www.airuniversity.af.edu/ASPJ/.

45. DoDD 5100.01, "Functions of the Department of Defense and Its Major Components," 31–32, 34.

46. Chandler, *Gen Otto P. Weyland,* 41.

47. Chandler, *Gen Otto P. Weyland,* 41–42.

48. Chandler, *Gen Otto P. Weyland,* 42.

49. Tara Copp and Valerie Insinna, "Marine Corps F-35 Flies First Combat Mission in Afghanistan," *MilitaryTimes*, 27 September 2018, https://www.militarytimes.com/.

50. Chandler, *Gen Otto P. Weyland*, 27, 29–30.

51. David M. Herezenhorn and Peter Baker, "Russia Steps Up Help for Rebels In Ukraine War," *New York Times*, 25 July 2014, https://www.nytimes.com/; and Mike Corder, "4 Charged in Downing of Malaysian Airliner over Ukraine," 19 June 2019, https://apnews.com/.

52. David Legg, "Aircraft Survivability—The Korean War," *JASP Online Journal*, accessed 16 December 2018, http://jasp-online.org/.

53. Dr. Daniel Haulman, *No Contest: Aerial Combat in the 1990s* (Maxwell AFB, AL: Air Force Historical Research Agency, 2015), 8, https://www.afhra.af.mil/.

54. Buck, "Light Combat Aircraft," 4.

55. Buck, "Light Combat Aircraft," 8; and Jim Ickes, Sierra Nevada Corporation, A-29 Logistics vice president, message to the author, email, 27 August 2019.

56. "Built for the Mission," A-29 company website, n.d., accessed 18 August 2019, http://www.builtforthemission.com/.

57. Trimble, *Asymmetric Advantage*, 85.

58. Trimble, *Asymmetric Advantage*, 85.

59. Wilkinson and Hill, "Airpower against the Taliban," 54.

60. Winslow Wheeler, "2. The MQ-9's Cost and Performance," *Time*, 28 February 2012, http://nation.time.com/.

61. Buck, "Light Combat Aircraft," 11.

62. Capt James Schmitt and Capt John Taylor (USAF MQ-9 pilots), interview by the author, 9 September 2019.

63. Scharre, "Spectrum of What?," 78.

Minimum Force

Airborne Special Reconnaissance in War

Maj Nicholas T. G. Narbutovskih, USAF

The Need for ASR

On 30 January 2002, the International Security Assistance Force (ISAF) and US forces embarked on Operation Anaconda, the most ambitious and large-scale clearing operation of the war to that date. While considered a tactical victory, the casualties were relatively high, with eight Americans killed in action and another 82 wounded. The coalition forces experienced several problems, mostly the lack of effective coordination between airstrikes and ground forces and ineffective and incomplete reporting of enemy locations. The lack of coordination with intelligence assets on the front lines of a fast-paced modern conflict and the lack of a purpose-built air platform to find the enemy and report directly to frontline troops contributed significantly to the overall confusion and high casualty rate, despite the enemy force's lack of training and sophistication. One case study highlights these issues—the battle of Takur Ghar.

On 3 March 2002, a Special Operations Forces (SOF) team inserted from an MH-47 Chinook helicopter onto a mountain to set up a ground-based observation post, resulting in the loss of three helicopters and seven elite operators. The enemy presence on the hilltop proved significantly higher than expected, as was consistent with the entirety of Operation Anaconda.[1] Immediately after landing with the first portion of the SOF team, the first helicopter came under fire from a fixed heavy machine gun, small arms from at least three separate firing positions, and was struck by three rocket-propelled grenades. One stuck a critical radar system, and the aircraft lost almost all electrical power, including defensive miniguns.

Somehow still able to fly, the pilot elected to leave the landing zone (LZ) quickly before the SOF team could be ripped to pieces by the incoming fire. As the helicopter took off, Petty Officer 1st Class Neil Roberts fell from the open ramp of the MH-47. The pilots landed the barely functional helicopter in the valley below, and Roberts activated his infrared strobe to mark his position for the second Chinook. The second helicopter, aware of the hot LZ, made a combat landing, and the second half of the SOF team quickly left the helicopter and took up cover and concealment in the surrounding trees.

After searching but unable to make contact with Roberts during their advance, enemy fighters discovered the team. Heavy machine-gun fire pinned the team

down and prevented effective extraction. The team did have support from an AC-130H gunship, which orbited overhead providing fire support. However, as the sun rose, the aircraft had to depart to prevent the relatively vulnerable aircraft from becoming a second casualty. While on station, this aircraft was not wholly dedicated to finding the enemy positions as the gunship's primary mission is on-call close air support (CAS).[2]

With a tactical requirement to dedicate one of its two sensors to the friendly location to prevent fratricide, the gunship could find and engage only a single enemy position at a time. Also, communications with the ground forces were minimal and did not enable effective reporting of enemy positions to the friendly troops.[3] There was an intelligence, surveillance, and reconnaissance (ISR) aircraft overhead in the form of an MQ-1 Predator. This aircraft, however, was centrally-controlled and had no communication with the ground forces.[4] Ultimately, the SOF team managed to call for the quick-reaction force of Rangers, a Tactical Air Control Party, and USAF Pararescue to secure their exfiltration, but only after the death of seven Soldiers, Sailors, and Airmen over a battle that lasted the entire day. Petty Officer 1st Class Roberts was posthumously awarded the Silver Star for his actions, and USAF MSgt John Chapman was posthumously awarded the Medal of Honor.

Had there been a dedicated reconnaissance platform in constant communication with ground forces, the outcome at Takur Ghar might have been significantly different. The US military finally addressed the need for dedicated Airborne Special Reconnaissance (ASR) platforms. However, it was not until much later during operations in Iraq that the mission truly gained traction.

Large-scale movement in Operation Iraqi Freedom was over relatively quickly with the initial operations to secure the country over in only 21 days.[5] After this, the United States conducted targeted, specific, SOF raids in a counterterrorism and counterinsurgency role. These raids were often in urban environments that made traditional reconnaissance almost useless. Deep urban canyons and complicated terrain, as well as the warren of internal rooms, kept the enemy well-hidden and required military leaders to rethink tactics as well as assets. As a result of these conditions and in no small part to Takur Ghar and operations like it, senior military officials took action. By urgent operational needs statement, the United States Special Operations Command developed and fielded the first pure Airborne Special Reconnaissance (ASR) platform, the U-28A. First deployed in 2006, the U-28A, "provides manned fixed-wing tactical airborne ISR support to humanitarian operations, search and rescue and conventional and special operations missions."[6]

Despite the urgent operational needs and the platform's actual development and various standards and tactics, ASR does not yet exist in doctrine. Even with

the Joint Force's increasingly heavy reliance on light tactical fixed-wing reconnaissance platforms during the last two decades, there is no guiding doctrine on how best to integrate these platforms into the operational level of war, and there should be. The 2018 *National Defense Strategy* (*NDS*) refocuses the defense enterprise on peer competition *and* explicitly states that our armed forces will continue the low-end fight.[7] We need to capture these important lessons somewhere other than platform-specific tactics, techniques, and procedures (TTP) so that they can propagate to, and be adapted by, the future force. We must study what we know of the low-end fight, pass on those best practices to the next generation, and consider how we can use ASR to counter a high-end adversary. Gaining and maintaining a strategic advantage in future conflict will be a function of intelligence and reconnaissance.

Reconnaissance is critical to war fighting. The ability to know where the enemy is, what they are doing, and where your forces are engaged, is necessary for effective combat operations regardless of low-end or high-end conflict.[8] The side that has the best information usually wins.[9] Successful reconnaissance is measured in terms of speed, accuracy, and timeliness.[10] The advent of airpower improved reconnaissance across all three critical measures. With human flight, the rapid acquisition and dissemination of intelligence from the air became the norm for warfare.

World War I (WWI) saw the first large-scale use of air reconnaissance with three categories of sortie, the contact sortie, the tactical reconnaissance sortie, and the artillery observation sortie. Contact sorties served to cut through the fog of war and find friendly forces, assessed the situation in real-time, and reported back to commanders at higher echelon. The tactical reconnaissance sortie found the enemy and discerned its disposition and activities, while the artillery observation sortie spotted enemy artillery batteries, guided friendly bombardments, and enabled counterbattery firing. The effectiveness of air reconnaissance at providing counterbattery corrections was most useful to ground commanders and formed the foundation of the early air corps' mission.[11] This mission was revolutionary, but due to the low availability of air assets and the strategic importance of reconnaissance, commanders held operational control at the corps level, resulting in days to weeks before frontline units knew critical details about their enemy. This delay often led to gaps in front-line war-fighting unit intelligence, leading commanders to make un-informed decisions or rely on gut instinct as opposed to concrete data.[12]

The modern example of Takur Ghar is a pivotal moment in the evolution of airborne reconnaissance. This important milestone marked the foundational requirements of the first purpose-built manned SOF platform to address tactical intelligence needs. It integrated into that role so successfully that the demand for support skyrocketed. In June 2009, the Air Force developed the first conventional

asset to fill this new mission need—the MC-12W Liberty.[13] Parallel to the manned efforts, the remotely piloted aircraft mission evolved as well, with the MQ-9 Reaper capable of both finding enemy targets, providing real-time feed, and carrying a modest amount of ordnance providing precision strike and limited CAS capability.

Eventually, the focus of operations in Afghanistan and Iraq shifted from enabling ground forces to conducting precision airstrikes to target high-value individuals. The ASR aircraft again evolved, their flexibility and advanced sensors giving them the ability to find and fix targets extremely rapidly. They coordinated with armed aircraft to develop advanced TTPs to manage and deconflict airspace in the Tactical Air Controller-Airborne role. They also provided precision terminal guidance for weapons deliveries. The latest iterations of ASR platforms can perform a wide range of functions within the ASR mission from the support of friendly forces to filling roles for precision strikes. Between manned and unmanned platforms, the ASR mission has an unprecedented ability to provide real-time targeting and amplifying information on enemy positions to the frontline friendly forces that are directly engaged with the enemy.

This mission brings a unique blend of multidomain abilities to the battlefield and changes how air reconnaissance assets integrate into the Joint Force. A single ASR asset can simultaneously meet the reconnaissance and intelligence needs of multiple regimental sized units in real-time while providing that information to the Global Integrated ISR Network.[14] This capability means that ASR assets can operate effectively under much more decentralized control than current doctrinal ISR missions.

Modern Role of Ground and Airborne Special Reconnaissance

Modern Special Reconnaissance (SR) provides the commander with several types of data about the enemy as well as the terrain and environment the main force will encounter in an advance. Each branch organizes, trains, and equips its units to conduct this mission. SR must provide three common core functions to the ground force commander. Effective SR must accurately fix the threat's location, movement, and reserves, visualize the terrain, and anticipate the threat's actions.[15]

Fix the Threat

With modern engagements evolving and changing in minutes, reconnaissance must be even more decentrally executed than it has been in the past. Modern general-purpose maneuver forces rely on a nonlinear battlefield to use advantages and create a mass of force at times and locations that set conditions for victory.[16] Nonlinear battlefields require frontline commanders to have accurate, meaningful,

real-time information. Commanders must have an accurate perception of reality to achieve victory. Aircrews refer to this concept as situational awareness. With a centralized construct, intelligence products must flow back up to a headquarters element before they are sent to the frontlines. This situation creates unacceptable delays that result in old and inaccurate reconnaissance at the frontline commander's level, reducing the situational awareness of battlefield forces. The requirement for real-time intelligence is incompatible with the delay inherent in a centralized intelligence system. When providing accurate information, modern reconnaissance, it must flow directly to tactical commanders.

ASR can fix the threat several orders of magnitude faster than ground reconnaissance units and over significantly larger areas and provide critical elements of information rapidly. This rate increases the situational awareness of frontline units significantly better than other traditional ISR efforts. In addition to speed, ASR can leverage real-time links to national intelligence assets and offboard sensors on other aircraft, creating on-the-fly fusion of all-source intelligence to support the ground force commander's intent in real-time. Because of the aircraft's payload capability relative to man-portable systems, these links are far more robust, resilient, and agile than similar capabilities carried by ground special reconnaissance teams.

Visualize the Terrain

Visualizing the terrain is a key function of SR. A commander cannot plan effectively without knowing where the formation is going and what they will encounter. SR provides this function in several ways: verbal reports of the terrain, still and motion imagery, and through geographic and hydrographic surveys. Another key reason to request a terrain survey of SR is that it significantly reduces the chances for successful enemy deception.[17]

ASR can visualize the terrain across the range of the electromagnetic spectrum, covering large physical areas as well as conducting comparisons of change over time. ASR platforms usually carry on-board terrain data that can validate planning assumptions compared with real-world information or allow war fighter-centered realignment to meet emergent combat requirements. They can deliver this information to the Joint Force in real-time.

Anticipate the Enemy

Finally, and most importantly, effective SR must enable the commander to accurately predict the enemy's actions. This function is the most difficult aspect of SR because the characterization of enemy forces is entirely subjective. Sometimes, merely identifying enemy combatants is difficult. This characterization allows

commanders to predict the enemy's response and validate planning assumptions or trigger contingency plans. ASR can characterize individual actions, anticipate routes of march or travel based on enemy qualities and known capabilities, and even identify enemy combatants hiding among a population. The ability to anticipate the enemy from the air is a direct result of the specialized equipment and highly trained crews of ASR units.

Characteristics of Airborne Special Reconnaissance Missions

ASR can provide many essential elements of information to frontline troops and higher-echelon commanders simultaneously. Air assets bring other unique and disruptive abilities to the battlefield that directly enable multidomain operations.

The characteristics of ASR missions are clearly defined commander's scope and intent, delegation to the lowest practical authority, and full support from the Intelligence (J2) infrastructure.

USAF Annex 2-0 emphasizes the processing and dissemination of intelligence. This function is indeed essential in the construct of the centrally controlled employment of ISR the USAF currently uses. With this centralized construct, the information flow is inherently slow. Computers and technology make this much faster than during WWI, but the construct remains essentially unchanged and is insufficient for current and future combat.

ASR units do not have to pass information back up to the central authority for dissemination. They operate with autonomy from central headquarters, operating on mission command and clear commander's intent. They pass updates directly to the front, speaking with the war fighters on the ground in real-time, passing live video and other products directly. They are rapidly flexible to emergent mission requirements and can even support many units simultaneously. The aircraft's technology and connectivity allow much of this data to automatically feed back into the overall global integrated ISR effort, allowing the crew to focus on the war fighter.

By delegating tactical control (TACON) to the lowest practical unit, planners set the most optimal conditions for close working relationships between aircrews and ground forces. ASR working in close coordination with ground and air tactical command and control can rapidly turn the tide of battle.

The designation of supported force in the J2 commander relationship ensures the integrity of the ASR mission. With full J2 infrastructure support, the processing, exploitation, and dissemination (PED) process allows the data to inform operational and strategic decisions. The PED is passive. It does not interfere with the aircrew's ability to support their tactical level unit, nor do PED requests or requirements drive taskings to the aircrew.

Functions of Airborne Special Reconnaissance

According to Air Force Doctrine Document (AFDD)-1, the inherent flexibility of airpower allows a single platform to deliver tactical, operational, and strategic effects simultaneously.[18] For this reason, Joint Force commanders should not consider air assets to be "spent" once they are assigned to a given echelon of command. ASR missions can support any level of warfare when the needs of the force dictate. However, the nature of airpower and the character of ASR lend themselves to the tactical level. They are less effective when control is held at higher levels.

Strategic

Strategic reconnaissance is the gathering and dissemination of information that enables national-level strategic discourse and policy making. Strategic intelligence seeks to characterize general enemy operations, movements, and postures by casting the widest collection net possible. This ability is most useful to higher-echelon commanders and campaign planners at the highest operational echelon of warfare.[19] In general, strategic intelligence enables strategic planning that may or may not include the military instrument of power.

ASR is not an inherently strategic mission. With modern PED and connectivity, ASR missions may gather information and data that enable strategic planning; however, this is a second- or third-order effect. The primary focus of ASR is enabling tactical effects.

Operational

The operational level of war links strategy to tactics by providing a framework to guide campaigns and major combat operations. At this level, combatant commanders develop end states that will support and enable strategic objectives.[20] Arranging battles and undertaking major combat operations are critical pieces of the operational level. ASR mission fundamentals can provide the commander and staff with critical details before and during the onset of hostilities. We must establish operational-level doctrine that will allow planners to best integrate the unique and disruptive capabilities of ASR platforms into campaign plans.

The connectivity and J2 infrastructure support of ASR platforms mean that operational intelligence needs can flow to the right audience regardless of the TACON command relationship. Many other platforms have capabilities that can bridge the strategic and operational intelligence requirements; however, they are not purpose-built for tactical mission sets. As such, ASR provides a uniquely flexible tool to the Joint Force the must be effectively integrated into operational planning.

Tactical

The tactical level of warfare is that the lowest level at which tactical units and joint task forces plan and conduct battles and engagements.[21] Engagements and battles are the most critical component of warfare; the actions of the frontline troops, especially in today's hyperconnected and complex environment, can have immediate and far-reaching operational and strategic impacts.[22] As such, this level of war is where ASR can have the biggest impact on successful military operations.

ASR operators are highly educated and trained, and the best possible chances of overall mission success lie in giving them a clear commander's intent and autonomy of action. The relationship between ground and air at this level is a partnership, with both parties working towards a clear goal. Through standards, training, and education, ground force commanders can be confident that the reconnaissance they receive from ASR missions is relevant, timely, and accurate.

The table is a brief overview of the relative comparison between the existing doctrinal mission set of ground special reconnaissance and airborne special reconnaissance. While each service has its unique capabilities in special reconnaissance just as each airborne platform does, the general characteristics allow a quick, surface level grasp at the similarities and differences between the two missions.

Table. Comparisons between the roles, characteristics, and functions of the special reconnaissance mission

Roles	Ground SR		Airborne SR	
	Positive	**Negative**	**Positive**	**Negative**
Fix the Threat	Precision, accuracy, hard to deceive, Identify equipment condition	Limited geographic scope, prone to deception in urban areas, single-mission reporting, delayed reporting (equipment-dependent)	Speed, volume of targets, rapid multimodal distribution, wide area coverage all-source intelligence fusion, multisource target correlation	Impacted by weather, mission duration usually <24hrs, vulnerable to deception in some situations
Visualize the Terrain	Precision, accuracy, soil type, load capacity, line of sight considerations hard to deceive, minimally impacted by weather	Requires high terrain for wide view, landmark obscuration, limited coverage area	Wide area coverage, no line-of-sight gaps holistic picture, real-time full-spectrum imaging, radar mapping, computer-assisted change identification, all-source intelligence fusion	Impacted by weather, unable to conduct geographic/ hydrographic survey to a high level
Anticipate the Enemy	Characterization of actions/intent, facial expressions, body language, id true activity levels, less vulnerable to deception/decoy	Line-of-sight only, delayed/minimal correlation with multiple sites	Large-scale troop movements, correlated activity at separate locations, tactical movements, thermal signatures, likely paths of travel, civilian locations/ considerations	Vulnerable to deception/unclear indicators, difficult to characterize intent

Characteristics				
Commander's Intent	Receive specific orders/objectives, operate under ROE, flexible within geographic range	Not easily retasked, equipment/capabilities limited by weight	Rapidly flexible, Operate Under ROE, access to datalinks and beyond LOS resources, wide area of responsiveness, multirole capability/loadouts	Duration limited by fuel, impacted by weather
Delegation of Authority	Limited battlefield scope and relatively high number of capable units drives best fit to tactical level	Usually unable to provide intelligence products directly to higher echelon, reporting delay due to bandwidth/equipment/tactical situation	Operates TACON at tactical level, provides operational and strategic support simultaneously	High-demand, low-density asset
J2 Support	Able to carry moderate products on equipment, thorough pre-mission briefs	Available products at beginning of mission are all that is available, limited connectivity while on mission	Real-time access to national intelligence resources, PED, cross-platform datalinks, all-source fusion products, support from and access to secure networks.	Prone to confusion and possibility of C2 push-pull issues if supported, supporting relationship not clearly defined
Functions				
Strategic	Hard truth of survey data, enemy disposition, characterization, equipments state confirms/denies planning assumptions. Limited ability to engage in action for strategic effect.	Significant time-delay compared to ASR, limited breadth of collection techniques/products, smaller available range of actions.	Real-Time reporting directly to strategic decision makers. Fusion of all-source intelligence into actions that have strategic effects. Wide-area responsiveness and flexibility.	High-demand/ low-density asset, weather dependent
Operational	Precise and accurate data to support operational planning and execution	Long transit times by ground, limited firepower, non-kinetic effects	Real-time support to operational and tactical units, precision strike on some platforms, significant non-kinetic effect options, parallel support and bridge between tactical and operational levels	Weather dependent, high demand/low-density assets, prone to deception in some situations
Tactical	Truth data on enemy, terrain, characterization allows high-confidence tactical decision-making, ability to conduct limited kinetic/non-kinetic operations at tactical level	Able to support limited number of units intelligence needs, delay in reporting, limited equipment and capabilities due to weight	Range of products, J2 support, network connectivity, datalink integration, full-spectrum imagery and sensing, TAC-A for control of supporting airborne assets	Weather dependent, high demand/low-density assets, prone to deception in some situations

Conclusion

ASR is an extremely valuable mission set to the Joint Force commander and can provide a critical edge across the competition continuum. Although ground commanders have always appreciated airborne reconnaissance, the implications of this mission have been far more clear in the minds of those who fly than their joint partners.[23] For this reason, it is critical that air-minded individuals have the guiding hand in creating the doctrine of ASR.

The ability to share reconnaissance information directly with the front echelon in real time enables the key component of mission command.[24] ASR can concurrently enable and augment the joint war-fighting functions of intelligence, information, command and control, fires, movement and maneuver, and protection. ASR missions can simultaneously support multiple ground units, conduct deep shaping fires and preparation of the operational environment, and contribute to theater-level situational awareness across all echelons of the Joint Force. ASR is most efficient when operating with the commander's intent and autonomy. The ability to find and fix enemy positions, visualize the terrain, and characterize the enemy over vast areas accurately and rapidly is the most important advantage in modern maneuver warfare and nonlinear battlefield operations. This ability has been the core advantage of aviation since WWI, and modern ASR aircraft are more capable, more lethal, and more effective than ever. ✪

Maj Nicholas T. G. Narbutovskih, USAF

Major Narbutovskih (BS USAFA; MSOM University of Arkansas; MMOAS, Air University) is a vice dean at Squadron Officer School, Maxwell AFB, Alabama.

Notes

1. Tommy R. Franks, *American Soldier* (New York: Harper Collins, 2004), 379.
2. USAF, *AC-130U* fact sheet, 20 January 2016, https://www.af.mil/.
3. Sean Naylor, *Not a Good Day to Die: The Untold Story of Operation Anaconda* (New York: Penguin Books, 2006), 335.
4. Naylor, *Not a Good Day to Die*, 340.
5. President George W. Bush, *President Discusses Beginning of Operation Iraqi Freedom*, 22 March 2003, https://georgewbush-whitehouse.archives.gov/.
6. USAF, *U-28A* fact sheet, 15 March 2012, https://www.af.mil/.
7. Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, technical report, 1 January 2018, https://apps.dtic.mil/, 3–4.
8. Peter Mead, *The Eye in the Air: History of Air Observation and Reconnaissance for the Army, 1785-1945* (Washington, DC: HM Stationary Office, 1983), 221.
9. Mead, *Eye in the Air*, 221.
10. Mead, *Eye in the Air*, 3.

11. Mead, *Eye in the Air,* 79.
12. Mead, *Eye in the Air,* 85.
13. USAF, *MC-12* fact sheet, 21 January 2016, https://www.af.mil/.
14. Curtis E. LeMay Center for Doctrine Development and Education, *Annex 2-0—Global Integrated ISR Operations,* 29 January 2015, https://www.doctrine.af.mil/, 2.
15. US Army (USA), *USA Field Manual (FM),* 31-20-05 *Special Reconnaissance* (Washington, DC: Department of the Army, 2015), 1–17.
16. USA, *USA FM* 31-20-05, 1–17.
17. USA, *USA FM* 31-20-05, 1–18
18. Mark A. Welsh, "Volume 1—Basic Doctrine," Curtis E. LeMay Center for Doctrine Development and Education, 27 February 2015, https://www.doctrine.af.mil/, 44.
19. Maj Tyler Morton, "Manned Intelligence, Surveillance, and Reconnaissance: Strategic, Tactical. . . Both?," *Air & Space Power Journal,* November–December 2012, 34–52, 38–39, https://www.airuniversity.af.edu/aspj.
20. Joint Chiefs of Staff (JCS), Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, JCS Electronic Library, 12 July 2017, https://www.jcs.mil/.
21. JCS, JP 1, I-8.
22. JCS, JP 1, I-8.
23. Mead, *Eye in the Air*, 221.
24. JCS, *Joint Operations*, II-2.

Table Stakes of the Advanced Battle Management System

Maj Rudy Novak, USAF

Imagine a system that instantaneously gives its user the majority of airborne battlefield data needed to make time-critical, potentially life-saving decisions. Now imagine that same system not only producing information but presenting a solution, shaving critical minutes from an observe, orient, decide, and act (OODA) loop.[1] This solution would allow the user to react before the enemy does, expeditiously placing weapons, sensors, and effects in the right place at the right time. This utopia is what the United States Air Force (USAF) imagines when it pitches the Advanced Battle Management System (ABMS), the service's answer, and impetus behind the Department of Defense's (DOD) Joint All-Domain Command and Control (JADC2) concept.

Many questions linger on what conceptually and physically ABMS entails and what it will provide to the war fighter. Is it a system or a system of systems? Is it autonomous, man-on-the-loop, or man-in-the-loop? What information will be shared? Will it control the pace of the battle, replacing C2 teams onboard the E-8 Joint Surveillance and Target Attack Radar System (JSTARS) or Combined Air and Space Operations Center, or will it be just a series of sensors that integrate into existing weapon systems?

This article cannot answer all these questions. Still, it will attempt to outline the fundamental table stakes that should guide architects and industry in the development of this future concept. While ABMS has evolved with the heightened influence of JADC2, this article will limit itself to its role in aerial combat. Integration beyond will be left for future scholars. Additionally, it will not discuss the technical means in which it could be designed but only the desired product to be delivered to the war fighter. ABMS must integrate the foundational table stakes of:

1. accessibility
2. synchronization
3. tailorability
4. built-in and upgradable artificial intelligence (AI)
5. decentralization and survivability
6. enabled communication
7. easily compartmentalized but accessible
8. centralized control and decentralized execution
9. employment of specialists

Through the implementation of these concepts, a tool will be created that will revolutionize the speed and capacity of decision-making and increase lethality and efficiency beyond what has ever been available to military commanders in the history of modern warfare.

Table Stakes

First and foremost, ABMS needs to make all relevant sensors, weapons, positioning, and battlespace deconfliction data *accessible*. Essentially, the ABMS is a more robust and user-friendly Link-16 network designed from the ground up to integrate seamlessly between platforms. The system-specific operator or AI could refine raw sensor data, which could then be broadcasted across the network to be actioned upon by other users. Ultimately, this would speed the kill chain by fulfilling an identification matrix faster or through the employment of weapons from different platforms other than providing sensor information. Weapon states, employment data, and engagement zones distributed to other users would allow for real-time accountability of available weapons and the timeline of engagements. Fighters sharing the tracking of airborne or surface adversaries, along with their quantity of missiles, would allow for timely distribution of forces and warning to commanders when risk is exceeded. The benefits of knowing in real-time the positions of all friendly and known enemy forces in every domain do not need to be explained, and ABMS can allow commanders to progress closer to that goal. Finally, airspace deconfliction measures such as kill boxes or restricted operating zones should be broadcasted, preventing fratricide and allowing freedom of maneuver and integration for assigned assets throughout different domains. Since air forces will not operate independently of other components, immediate deconfliction measures from artillery, unmanned aerial systems, and other assets sharing airspace could be transmitted. The sharing would increase awareness of the evolving battlespace and changing areas of responsibility.

Synchronization of data streams. ABMS must integrate data from "all domains" to streamline and heighten situational awareness in the battlespace. The ability to synchronize intelligence, data, and weapon or sensor effects on specific targets is a critical table stake. For example, when a potential target is identified, every entity collecting data, running an identification matrix, or providing an effect should have the ability to effortlessly place that data into a single file or log specific to the target. Cyber intelligence collections that identify centers of gravity, satellite or unmanned aerial systems imagery, airborne passive detection systems, or ongoing electronic attacks are among this information. All must be consolidated and ranked based on system accuracy to produce a single accurate model of a target's

location, condition, received effects, or other data that can be seamlessly synchronized for immediate lethal or nonlethal effects, or further collection.

The information, if provided as stated in the previous table stakes, would be of massive quantities in any large-scale operation, far more than any individual or team could digest in a meaningful amount of time. That ability is why information must be easily *tailorable*. This table stake would allow the user to effortlessly see only what they care about at the moment and not get bogged down with nonpertinent data. For example, in the dynamic task of tanker management, where aerial tankers provide fuel to other military aircraft, ABMS could allow a user to filter out only needed data such as an airborne tanker's available gas and a list of scheduled or added receivers updated by the air tasking order, tactical command and control (C2), or the tanker itself. Tailorability would also allow for higher priority items based on the commander's intent to be highlighted based on the focus of the day and mission set.

With artificial intelligence advancing at a dizzying rate, ABMS needs to capitalize on this potential third-offset capability.[2] ABMS must have *built-in and upgradable AI*. Adapting AI to conduct man-in-the-loop, man-on-the-loop, or fully autonomous battle management decisions is critical in speeding up the OODA loop and holding to the rules of engagement prescribed by its programmer. In the previously mentioned tanker management mission set, AI, once configured, could proactively work unplanned refueling and source available fuel within a theater based on receivers' needs and location. AI integrated into ABMS could directly speed up the kill chain by analyzing connected weapons systems to develop a solution of the best weapon system available to interdict a target. In a dynamic targeting scenario, AI could maintain a real-time inventory of airborne munitions not assigned targets. When a dynamic target is inputted into the system, ABMS could provide an operator with the best and alternative munitions available based on desired effects and collateral damage. With the weapon owner's concurrence, all targeting data could be instantly forwarded and all networked users notified that this specific aircraft is servicing the target. While these examples solve current aerial combat challenges, the upgradable portion of this table stake would adapt ABMS to integrate with AI being developed independently of this concept. Looking to the future, ABMS AI could be the system that fuses all sources of data, then forwards it to autonomous weapons that automatically neutralize a target based on the programmed commander's intent and collateral damage. This future AI utilizing ABMS would minimize human input and be the foundational language that future US military AI is designed.

The initial pretense for the USAF's decision to divest the E-8 JSTARS fleet and pivot to the ABMS concept was a perceived lack of survivability in contested en-

vironments and a desire to shift to a more modern decentralized concept. *Decentralization and survivability* are critical to any future battle management system, and ABMS must hold to this. An easy comparison is the cellular phone, built upon a framework of antennas, internet protocols, fiber-optic cables, and satellites. One can travel virtually anywhere in the world and still be connected. Importantly, if a signal is lost from one cellular phone tower, the device seamlessly connects to a new one. This decentralization requires survivability through the employment of protocols and other methods to prevent jamming or other forms of electronic attack. Add to this the requirement that all data sources are vetted through an active information assurance program that assesses for data corruption, and a robust system would be created. This protection is admittedly easier said than done. In designing and utilizing the system, developers and operators must always be mindful of the fact that if ABMS becomes compromised, so could the USAF's future war-making capability. However, if the USAF is voracious in its defense, utilizing the same vigor in which it protects its nuclear arsenal or other strategic assets, ABMS would be secure. To meet this table stake, ABMS must be made of devices able to connect and are resilient against the attack of individual nodes, keeping lines of communication open between every war fighter and commander.

Enable communication. From tactical chatrooms, direct messaging, and digital packets of data, ABMS must facilitate communication. Features like user/mission defined chatrooms and precanned missions, dynamic targets, close air support, and joint tactical air strike requests (JTAR) must be incorporated into the system. When a joint terminal attack controller requests air support, the DD Form 1972 Air Strike Request must be integrated. The request should be seamlessly sent through higher echelons and eventually forwarded to the aircraft that will service it. ABMS can eliminate the "telephone game," providing information directly from the organization requesting action. Finally, central updates to essential documents, like the air tasking order, or real-time mission impactful information need to have a way to be distributed. ABMS should be the method to so, broadcasting and updating pertinent communications to all players seamlessly.

While the United States must be prepared to fight a conflict independently, it is foolish to think that America would enter a major conflict without a coalition of the willing. American forces fight and train with allies and coalition partners daily, but often security classifications hinder complete integration. ABMS must be *easily compartmentalized but accessible* at varying levels of classification. Existing systems and policies often wholly cut out partners from accessibility, including portions that have been previously deemed releasable. Separate ABMS systems should not exist, but American users should have the ability to filter out data that must be withheld. Partner nations like the United Kingdom have already expressed their

interest in this idea,[3] and like the F-35 Joint Strike Fighter, ABMS must be designed with partners in mind. Our allies and coalition partners around the globe are critical to our national defense, and any future C2 systems must embrace them.

With its creation, the inevitable outcome with any C2 system is that a higher headquarters would have the ability and desire to influence decisions at the lowest possible level. While this is tolerable within a low-intensity operation, in a near-peer conflict, this mentality is impracticable. ABMS must enable *centralized control and decentralized execution.* The overarching design of ABMS must allow the war fighter to gather necessary data and carry out the mission based on the tactical situation, in accordance with the commander's intent. It cannot merely be a tool for commanders separated from the battle to direct action in a centralized execution model. This tool would only slow the actual war fighter's OODA loop, potentially giving an enemy an advantage or opportunity to exploit. USAF doctrine,[4] established through decades of successful air combat, must not be changed simply because a system comes online that promises all data to the commander. Tactical commanders must be empowered and have the ability to use the information provided to them to make critical decisions independently.

Nevertheless, tactical commanders must not be alone. ABMS must *employ specialists* trained to filter data and are empowered to make tactical decisions on behalf of this commander. These specialists should be tasked to maintain network integrity and act upon information produced within the system. This table stake does not imply information hoarding or limiting access to the war fighter. It means utilizing trained personnel to enable operations and assist the computer and commander where needed. Some within the DOD argue that ABMS data should immediately be sent directly to the user to influence their OODA loop. However, as many commanders know, the first battlefield report is often misleading or simply wrong. ABMS needs that filter and designated decision-maker and should not be designed to cut out tactical C2 operators nor intelligence analysis. A misguided expectation is that with ABMS, C2 decisions can be consistently delegated to the fifth-generation fighter or bomber pilot in their cockpit. While this pilot is more than capable of making time-critical tactical decisions within the specific mission, add a dynamic scenario featuring a multitude of mission sets, vast quantities of information, and the physical stressors within the cockpit that decision-making capacity simply breaks down. Tactical C2 teams have the innate ability to execute multiple mission sets, process dizzying amounts of information, and be the experts in interpreting the commander's intent within the confines of tactical or theater-wide operations. By integrating tactical C2 and the theater air control systems within ABMS, the Air Force will have a system that creates a force multiplier in which it envisions.

Conclusion

The USAF and the DOD must not settle for a system that delivers anything less than these table stakes. Only the best providers can meet them, but this model of the ABMS is obtainable. ABMS cannot be relegated or considered a "new" Joint Tactical Information Distribution System (Link-16); it can be so much more. It can be the baseline in which future generations of technology are built, and doctrine is evolved. Future autonomous wingmen, AI imagery analysis, and space-based sensors can all be designed to integrate and "feed" ABMS. The US can no longer have programs built for independent purposes, utilizing aftermarket technology to bridge communications. They must be built around this common next-generation system. Vast amounts of data will need to be transmitted, and current weapon systems will need to be modernized or replaced to support information flow. With the rise of near-peer threats and their evolving C2 enterprises, the USAF must evolve faster. No longer can the USAF rely on quantity but instead utilize the quality of weapons systems and sensors in the right place at the right time, faster than our adversaries. ABMS must be audacious and seize innovative opportunities and revolutionary changes wherever possible, but structured around the table stakes of (1) accessibility, (2) synchronization of data streams, (3) tailorability, (4) built-in and upgradeable AI, (5) decentralization and survivability, (6) enabled communication, (7) easily compartmentalized but accessible, (8) centralized control and decentralized execution, and (9) employment of specialists. In doing so, a tool will be created that will revolutionize the speed and capacity of decision-making and increase lethality and efficiency beyond what has ever been available to military commanders in the history of modern warfare. ✪

Maj Rudy Novak, USAF

Major Novak (BA, University of Michigan; MPA, University of Oklahoma) is a senior air battle manager with more than 1,800 hours onboard the E-3 Airborne Warning and Control System. Currently, he is the chief of group contingency plans, 552nd Operations Support Squadron, at Tinker AFB, Oklahoma.

Notes

1. Paul Tremblay, *Shaping and Adapting: Unlocking the Power of Colonel John Boyd's OODA Loop* (Quantico, VA: United States Marine Corps Command and Staff College, 2015).
2. Deputy Secretary of Defense Bob Work, *The Third U.S. Offset Strategy and its Implications for Partners and Allies*, speech, Washington, DC, 28 January 2015.
3. Development, Concepts and Doctrine Centre, *Joint Concept Note 2/17 Future of Command and Control* (Wiltshire, UK: UK Ministry of Defence, 2017).
4. Curtis E. LeMay Center for Doctrine Development and Education, "Centralized Control and Decentralized Execution," *Air University,* 27 February 2015, https://www.doctrine.af.mil/.

21st Century Power: Strategic Superiority for the Modern Era edited by Brent D. Ziarnick. Naval Institute Press, 2018, 208 pp.

"Deterrence," states Peter Sellers' titular character in Stanley Kubrick's *Dr. Strangelove: Or, How I Learned to Stop Worrying and Love the Bomb*, "is the art of producing in the mind of the enemy the *fear* to attack." In Kubrick's black comedy, the observation cynically underpins the film's satirical attack on Cold War nuclear policies in general and the USAF's Strategic Air Command (SAC) in particular. But for a man like Gen Thomas S. Power, SAC's commander from 1957–64 (the year of *Dr. Strangelove's* release), deterrence and nuclear war were matters of deadly seriousness. As the SAC commander during some of the most significant nuclear events of the Cold War, including the Soviet development of the "Tsar Bomba" (the RDS-220 hydrogen bomb and largest nuclear weapon ever tested) in 1961 and the Cuban Missile Crisis in 1963, General Power was responsible for preventing—but, ultimately, preparing to win—a nuclear war.

With *21st Century Power*, Ziarnick has curated a collection of writings and speeches from Power, who succeeded Gen Curtis E. LeMay as the third SAC commander. Even more so than the legendary LeMay, Power crafted SAC into the world's preeminent nuclear fighting force, modernizing air and ground nuclear alert systems, incorporating intercontinental ballistic missiles (ICBM) into America's nuclear arsenal, and establishing the around-the-clock crew schedules that provided SAC the ability to launch manned nuclear counterstrikes within 15 minutes of a nuclear alert. Power's innovations were extremely important. Indeed, they not only prevented nuclear war between the Soviet Union and the US but may also have been instrumental in the West's ultimate victory in the Cold War. Ziarnick's aim in *21st Century Power*, however, is not merely to celebrate Power's achievements; it is to illustrate the SAC commander's strategic thought. Even more specifically, it is to argue that Power's ideas related to nuclear grand strategy have renewed significance in addressing what some scholars have begun calling the "Second Nuclear Age"—a time when proliferation has allowed even smaller, less stable nations to develop and maintain nuclear weapons.

Ziarnick organizes his book into five chapters, each collecting writings or transcriptions detailing various facets of Power's strategic thought. The first two chapters provide overviews of Power's thoughts on nuclear deterrence generally and the development of the ICBM as a strategic weapons system specifically. These chapters collect examples of Power's shorter writings, including multiple pieces from *Combat Crew* (SAC's official magazine), a journal-length article from *Air University Quarterly Review*, a declassified memorandum to the SAC Alert Force, and several other pieces. Chapters 3–5 each provide a more singular focus. Chapter 3 collects, in its entirety, Power's testimony to the US Senate in opposition to the Limited Test Ban Treaty of 1963; chapter 4 provides a verbatim transcript of the general's remarks to one of the many civic groups that visited Offutt AFB, Nebraska during the mid-1960s to learn more about SAC's mission; and, finally, chapter 5 reproduces Power's last public speech while on active duty.

Ziarnick's organization is among the great strengths of his work. By offering examples of Power's advocacy for SAC's mission in a variety of situations, Ziarnick allows the reader to see Power as he was: a man with an unshakable belief in the importance of the American nuclear enterprise, with the wit and skill to adapt his message to advocate for that mission no matter his audience. Each of his many facets—Power as a steely-eyed SAC commander, urging his Airmen to be vigilant and mission-ready; Power as a respectful but vehement Cassandra, arguing in vain against the Limited Nuclear Test Ban Treaty; Power as a public advocate, explaining SAC's role to a public increasingly incredulous of the importance of nuclear deterrence—overlaps with the other and demonstrate his conviction that, in a nuclear world, the US must maintain both the military strength and the ideological resolve to protect the Free World from Soviet encroachment.

Perhaps the most interesting, although largely unexplored, aspect of *21st Century Power* is how Power's ideas regarding nuclear deterrence and strategy apply to modern warfare beyond the nu-

clear realm. Time and again in his writings, he returns to the themes of advancing technology, the compression of time in the winning or losing of war, the futility of the search for an "ultimate weapon," and the importance of resolve, preparation, and readiness in deciding future conflicts. All of these topics remain pressing in twenty-first century conflict, particularly within the new vistas of warfare to be found in space and cyberspace.

Given the emphasis on the renewed importance of Power's strategic thought to the Second Nuclear Age, this reviewer would also have liked to see a more complete explanation of how his writings regarding nuclear warfare specifically apply in the twenty-first century. Power planned to "win" a nuclear war (although he believed such a war would result only in losers to varying degrees) through the use of early warning systems, ICBMs, and around-the-clock alert crews ready to counterstrike in the event of a detected nuclear attack. But what does "confront[ing] the problem of fighting, not just preventing, nuclear war" look like in the modern era—particularly when, as Ziarnick points out in his introduction, a modern nuclear war is more likely to occur between "secondary" nuclear states?

21st Century Power is an excellent book for any scholar or casual reader interested in the history of US nuclear policy or the strategic underpinnings of nuclear warfare. It provides a fascinating and welcome insight into the mindset of a man who, in an almost literal sense, held the fate of the world in his hands. Although only about 200 pages in length, it is a wide-ranging volume that illustrates the passion of a military commander for his craft and his country. Finally, *21st Century Power* serves as a useful reminder that, far from being one of the self-aggrandizing madmen of *Dr. Strangelove*, General Power was a man who believed firmly that nuclear conflict must be prevented at all costs. Indeed, the man who, in October 1963, came closer to actually fighting a nuclear war than any of his predecessors or successors, did not think that American power was to be measured merely in megatons and nuclear stockpiles. For Power, true deterrence lies in "a sound economy," "prosperous industry," "scientific progress," "good schools," and "[m]ost of all... the determination of the American people to prevent and, if necessary, fight and win any kind of war, whether hot or cold, big or small" (p. 36).

Capt Jeremy J. Grunert, USAF

NATO's Return to Europe: Engaging Ukraine, Russia, and Beyond edited by Rebecca R. Moore and Damon Coletta. Georgetown University Press, 2017, 272 pp.

In *NATO's Return to Europe*, editors Rebecca Moore and Damon Coletta bring together seven leading political scientists, scholars, and historians to examine issues within the North Atlantic Treaty Alliance (NATO) while outlining options for the future. Employing the history of NATO as the backdrop to make sense of geopolitics in the Ukraine, the authors clarify the challenges facing the alliance while recommending future solutions to preserve NATO by returning the focus to European affairs.

Broken into seven chapters, *NATO's Return to Europe* primarily orients to the past 25 years of the alliance's history following the collapse of the Soviet Union. The authors argue that decisions made in adjusting NATO's membership and purpose in the wake of the Cold War directly contributed to challenges that would manifest in Georgia and Ukraine in the twenty-first century. Utilizing historical context effectively anchors various arguments in the book to make sense of Russian, European, and American decisions in the contemporary operational environment.

The seven chapters stand alone with independent arguments but also complement each other to form a holistic narrative and argument for how to galvanize the NATO alliance in the modern era. While the crisis in Ukraine is the primary event that spurs this analysis, consideration is also given to the rise of nationalism and anti-NATO rhetoric manifest within the alliance in 2016. The authors caution against these internal divisions with recommendations for commitment to NA-

TO's core principles alongside a deliberate strategy to provide security while prudently mitigating threats from Russia. This strategy focuses on a return to the basics of the alliance, as well as a focus on partnership to achieve cooperative security as the operational environment shifts from southwest Asia back to Europe.

While the book presents an exceptionally researched argument for NATO's return to Europe; the book predominantly orients to actions in the Ukraine as a lens to understand tensions within Europe and within the alliance. Focusing on Ukraine marginalizes other NATO challenges such as the rise of nationalism or the developing cybersecurity issues plaguing democracies worldwide. Despite this narrow focus, the authors still capture the alliance's history as well as the significant challenges for member states in an increasingly complex geopolitical landscape.

NATO's Return to Europe provides excellent insight into the challenges facing the NATO alliance. Comprehensively linking the alliance's history with current global events, the authors effectively deliver the argument for NATO's preservation with a return to Europe. This is an informative read for military professionals and scholars seeking to understand the complexities of NATO as well as the alliance's options in the future.

Lt Col Matthew C. Wunderlich, USAF

RAF: The Birth of the World's First Air Force by Richard Overy. W. W. Norton & Co., 2018, 150 pp.

"For good or ill, air mastery is today the supreme expression of military power and Fleets and Armies, however necessary, must accept a subordinate rank."

Thus ends *RAF: The Birth of the World's First Air Force,* with a 1919 quote from Winston Churchill. The new book by Richard Overy, a professor at the University of Exeter in England, details how the Royal Air Force was formed. Only 10 years after the Wright Brothers' first powered flight at Kitty Hawk, North Carolina, European militaries were investing and experimenting with military aircraft. Less than 15 years later, on 1 April 1918, the Royal Air Force was created as a separate and equal third service in the British military out of the six-year-old auxiliary Royal Flying Corps (RFC).

Overy starts his work in April 1912, with the establishment of the RFC. Proceeding chronologically, the narrative ends in 1919. Initially founded as an auxiliary service, the RFC was a necessary innovation. The RFC used small wood and cloth biplanes in reconnaissance in support of ground forces and artillery spotting roles across the Western Front. It was not until late 1915 that the RFC "classed counter-force operations as a key function." But the force grew rapidly, fielding tens of thousands of aircraft by the end of the war.

RAF focuses on the bureaucratic and administrative developments of the RFC and its transition to the RAF, with particular emphasis on the intragovernmental struggle to establish the new service. This focus is both the key strength and weakness of the work. Absent are the voices of the young pilot and mechanics themselves, as are the descriptions of aerial combat and austere aerodrome conditions. The exhilaration of dogfighting and the pain of counting far fewer planes return than sortied. But that does not seem to have been Overy's intent. He is much more comfortable detailing the more mundane but essential work of building a service. What uniforms will be worn? What is the official ensign? Will the new service use Navy or Army rank structures? All decisions that have to be signed off by King George V himself. *RAF* is more a book about the bureaucratic and political struggle to create a new service than about the men who flew over the battlefields in France.

The recent declaration of a Space Force in the US Department of Defense is an uncanny allegory. Like the creation of RFC which Ovrey labels "a political decision… not a decision dictated by military necessity," the Space Force was initiated by the civilian side of the government. Also akin to the RFC, the Space Force will pull existing commands and units away from control of the

Army, Navy, and Air Force in a move that is more consolidation than creation. If the allusion between the forces holds true, the Space Force will struggle for years before it is entrenched as a service. It took the RFC and RAF almost half a decade before they were finally free of Army and Admiralty attempts to dissolve them.

Overy writes about the strategic directions of the young force. During the war, German Zeppelin raids on London quickly brought home defense to the top of the British military's priorities list. RFC squadrons, which were initially used only to support the Army and Navy, were raised for the home front and tasked with combat air patrols. These units and the tactics they developed were the precursors to Churchill's "The Few" that protected Britain from the Luftwaffe in the Second World War. But eventually the British developed their own doctrine of strategic bombing in retaliation. Overy tells us that the tonnage of bombs the RAF dropped on "strategic targets" in the First World War could have been dropped by a dozen heavy bombers of the Second World War in a single raid. The raids on German cities, although insignificant in the tonnage of bombs dropped, foreshadowed the character of the next war 25 years later.

The author also misses an opportunity to contrast the development of the RAF with equivalent organizations in the US, Germany, Italy, and France. All of the major powers were rapidly developing air services during the war, but the other is mentioned only briefly. It is only a page toward the end of the work that he makes clear that the RAF was unique in its status as an equal and third service. The US Air Force was not established as a separate service until 1947, almost 30 years after the RAF. He also gives only the faintest tease of an analysis of the effectiveness of establishing a separate service. In almost all respects, the RAF entered the Second World War behind her counterparts, despite being a separate service. German aviation had mastered close air support operations, and Japanese and American aviation had made huge developments in carrier borne aviation. The saving grace of the RAF was their investment in home defense, which Overy paints as "the one element in the RAF that was technically up to date and reasonably prepared [in 1939]." A network of fighters, radars, and ground defense ultimately proved decisive in the Battle for Britain and bought the island nation enough time to upgrade the rest of her air forces.

RAF is a short read at less than 150 pages, but the bureaucratic focus keeps it from being a quick read. Absent from the treatise is a treatment of the development of the RAF up to 1939 and more content focused on the tactical and operational successes and failures. Discussion of the RAF during the interwar years and across the British Commonwealth would better balance the book. That said, the narrative will prove invaluable to anyone who is pursuing significant organizational change. It also elucidates some of the RAF's oldest traditions—even the structures and insignia that influenced the USAF. The story of the RAF is a study in institutional innovation—the challenge of building an organization that by 1918 would consist of hundreds of thousands of airmen and 10,000 aircraft in a few short years. *RAF* is a companion to similar books that detail the birth of institutions like the Special Air Service, the Royal Marine Commandos, or the Defense Advanced Research Projects Agency. It was an organization built around a new type of weapon and a new type of warfare, with every decision literally made on the fly.

1stLt Walker Mills, USMC

The End of Strategic Stability? Nuclear Weapons and the Challenge of Regional Rivalries edited by Lawrence Rubin and Adam N. Stulberg. Georgetown University Press, 2018, 328 pp.

In *The End of Strategic Stability,* editors Lawrence Rubin and Adam Stulberg bring together 17 regional experts to examine contested understandings of deterrence and strategic stability among existing and potential nuclear actors. Rubin and Stulberg are professors at the Georgia Institute of Technology's Sam Nunn School of International Affairs. They approach the idea of stability from three angles: regional approaches to strategic stability, their implication on multidomain deter-

rence, and practical recommendations for US policy. Their analyses enrich our understanding of the international security environment by examining how other nations conceptualize and articulate their national security interests.

The first section contends that there is no consensus among different actors on the meaning of strategic stability and deterrence. This is important because global order during the Cold War—and its immediate aftermath—was built on the assumed mutual understanding of strategic stability and deterrence. With the end of the Cold War, the US promoted a system for global strategic stability based on restraint, emphasizing risk reduction, and disarmament. The restraint-based approach to strategic stability does not translate well in regions where a balance-based understanding of stability drives calculations. Misaligned strategic priorities and historic and cultural context drive these discrepancies and are evident in both internal policy discourse and observed force posturing.

As an example, the contributors point to India and Pakistan where the idea of stability shows little correlation with parity and transparency. Challenging the traditional conceptions of strategic stability built on mutual second-strike capabilities, the disparity in conventional forces and the plausible risk of successful limited nuclear escalation may actually be one structural support for stability in the India-Pakistan balance, as long as both parties can mitigate potential crises at the political level. Ultimately, the contributors stress that cognitive flexibility to adapt current doctrine to operate in any gradient of the spectrum is key for enhancing stability. In fact, one of the contributors suggests in a possible reference to the latest US nuclear modernization efforts that actors who have traditionally exhibited restraint oriented behavior are shifting toward limited forms of balancing.

Part two examines how the lack of consensus on strategic stability, and ultimately the transparency behind the actor's intent, affects multidomain deterrence. Contemporary Russian and Chinese strategic discourse both emphasize the ability to fine-tune the strategic environment through the employment of kinetic and nonkinetic options in one domain to deter threats in another. Russia views its conception of new-generation warfare as a stabilizing measure reduces the chances of a kinetic escalation against North Atlantic Treaty Organization forces through the use of information operations. However, the inherent opacity behind the intent and scope of this approach has the potential to be highly destabilizing, especially as Moscow openly contemplates the use of limited tactical nuclear weapons in Eastern Europe as part of their deterrence posture.

The final section of this anthology outlines policy implications for the US. The unique historical, cultural, and geopolitical circumstances that prompt state actors to seek greater security through multidomain operations create sources of instability that must be carefully navigated on an actor-specific basis to prevent inadvertent escalation. The editors highlight the risk of entanglement, as regional actors can deliberately trigger a crisis to provoke US intervention in a conflict, exploiting the asymmetry in threat perception and tolerance for nuclear escalation with the goal of renegotiating the status quo on favorable terms. The editors conclude that while the absence of a shared understanding of stability is not necessarily a source of instability in itself, it is crucial for all parties to recognize and communicate the differences.

The timely research supporting this volume contribute important nuances and details to the strategic landscape described in the *2018 National Defense Strategy* and the *Nuclear Posture Review*. Readers should note that the volume predates significant shifts in regional balance, namely the suspension of the Joint Comprehensive Plan of Action in Iran, as well as denuclearization efforts on the Korean peninsula following the historic Singapore summit. This does not detract from the importance of the research and analyses presented in this volume, which make a powerful case for the need to rethink old models of stability given new regional actors and technologies. This book deserves a place on the bookshelf for scholars and practitioners who will

find in its well curated pages an insightful framework to further the discussion on formulating effective multidomain deterrence.

1st Lt John Lee, USAF

Four Guardians: A Principled Agent View of American Civil-Military Relations by Jeffrey W. Donnithorne. Johns Hopkins University Press, 2018, 192 pp.

The resignation of Chief of Staff John F. Kelly, USMC, general, retired, and Secretary of Defense James Mattis, USMC, general, retired, give pressing interest to Jeffrey W. Donnithornes' new book on civil-military relations: *Four Guardians: A Principled Agent View of American Civil Military Relations.* Donnithorne, applying social science methods, provides a model for readers to evaluate and anticipate future reactions by the USA, USN, USMC, and the USAF to policy changes. His book refines Dr. Samuel P. Huntington and Dr. Peter D. Feaver's writings providing more refined conceptions of service behavior. A comparable work of recent production is Austin Long's *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the US and UK*, which examines the effect of service culture on individual behavior. As Air University's chief academic officer and a former USAF pilot with a career of joint experience, Mr. Donnithorne is well-placed to comment on the behavior of America's four services. The book is a great read for field-grade officers preparing for joint staff or any assignment that requires making predictions on other services' behavior in policy debate. Donnithorne argues that thinking about the services' decision making through the lenses of bureaucratic self-interest and rivalry are inadequate models of behavior. A service's decision-making, he posits, is better understood as the product of unique service culture. Additionally, he states that the phase of the process—policy development or execution—and the clarity of the policy at hand are essential to guiding a service's decision. To illustrate this process, Donnithorne provides a quad chart that matrices the clarity of policy against the phase of the process against and service culture. The succeeding six chapters describe the four service cultures, two case studies, and two examples of future application.

The service analysis and selected examples make a great case for Donnithorne's thesis. Each analysis is useful for service members seeking to understand other services. He distills primary and secondary sources into easy-to-read service summaries that nevertheless capture their essence. For example, the author uses Russell F. Weigley's *The American Way of War* and the *History of the United States Army* to supplement his personal experience with the US Army. Donnithorne's case studies—the development of US Central Command (USCENTCOM) from the Rapid Deployment Joint Task Force and the signing of the Goldwater-Nichols Act of 1986—are the most important developments for the DOD in the twenty-first century. To support his case studies, he uses the memoirs and official correspondence of the personnel involved. The memoirs and correspondence lend great credence to his research and conclusions.

For social scientists, the measure of one's theory is its ability to supersede other available models on the market of decision-making. Mr. Donnithorne's book is very successful in this respect as readers with limited exposure to social-science models can easily learn and employ his quad chart to structure their thinking. Likewise, a novice to service culture will gain an understanding of the services. By putting the chart and anecdotes together, the reader rapidly gets a sense of the struggles in the Pentagon and on Capitol Hill. Although the book is unlikely to be read as popular entertainment, Donnithorne supports his book with enough details and spicy exchanges to keep the reader's interest.

The author's argument is quite convincing but not without its flaws. On two occasions, I think Donnithorne failed to adequately examine or explain phenomena that would impact his thesis. Donnithorne does not bring attention to the USA's domination of the United States European Command or the USN's domination of the previous United States Pacific Command during the

standup of USCENTCOM. The combatant commanders' proposals were the service's attempt to seize the power, prestige, and funding and he does not address this maneuver. In the second occasion, it seems Donnithorne overplays the Army's neutral status leading up to the Goldwater-Nichols Act. In his description, the USN appears to be a greedy manipulator while the USA appears as the humble American servant. The USA looks neutral because the policy gave the USA power over its rival, the USN. For these two examples, the less culturally-attuned bureaucratic actor model predicts the same behavior, but that model would require an in-depth knowledge on the readers' part. This is where Donnithorne redeems work. His ability to provide context to readers across the range of experience and a model, that does not require preexisting knowledge, gives the book its power.

I would recommend this book for mandatory reading for intermediate developmental education and for officers preparing for an assignment on the joint staff. Despite six years of joint experience, including five years on USA posts, I found new insights into understanding the other services. Officers never have enough time to read every book and crave quickly accessible wisdom. *The Four Guardians* is especially useful in this area because it can be read as a whole or by chapter and the author provides notes which accelerate the comprehension of his work. We are destined to fight together and Donnithorne's book prepares the reader for that destiny.

Capt F. Jon Nesselhuf, USAF

Flight Risk: The Coalition's Air Advisory Mission in Afghanistan, 2005–15 by Forrest Marion. Naval Institute Press, 2018, 376 pp.

America's 17-year war in Afghanistan has received significant attention from a wide array of chroniclers. Those authors who focus on the USAF's contribution usually discuss the service's unmanned aerial vehicles, the heroism of its battlefield Airmen, or the prowess of its ever-vigilant pilots. Curiously missing from the war's historiography, however, is a dedicated analysis on the USAF's longest air advising mission. *Flight Risk: The Coalition's Air Advisory Mission in Afghanistan, 2005–2015* by Dr. Forrest Marion, retired, is a desperately needed history on the service's quixotic mission to construct a modern air force in an impoverished nation in the midst of an industrial strength insurgency. Dr. Marion, a staff historian at the Air Force Historical Research Agency, interviewed scores of former senior Air Force officers to provide readers a peek behind the curtain on the USAF's most audacious mission in the Hindu Kush.

Dr. Marion's 300-page book primarily focuses on the North Atlantic Treaty Organization's effort—though an overwhelming American endeavor—to birth an Afghan Air Force (AAF). He devotes a few chapters chronicling other countries' endeavors before 11 September 2001, primarily focusing on the Soviet Union's similar mission in the 1980s. Dr. Marion rightly credits the USAF for making substantial progress during the past 12 years, especially considering the starting point. He also astutely dissects the USAF's overarching strategy of professionalizing the AAF and zeroes in on its inability to align its strategy with their Afghan counterparts' cultural norms. This lack of cultural interoperability significantly hindered the USAF's goal of creating a new, modern, and professional AAF.

These cultural missteps were varied and significant. For example, senior air advisors insisted on mimicking the air operations center by creating, financing, and then rebuilding an air command and control center despite the Afghans' cultural aversion to such a concept. Instead, AAF generals and senior Ministry of Defense officials routinely diverted missions for their predilections. Further, they were far more comfortable using "cell-phone C2" and circumventing a wester-designed process. Both sides also differed on the choice of platforms for the country's fledgling service. The Afghans were wedded to helicopters because they made grand, *wasta*-inflating noise upon their landing, much to the chagrin of their advisors who pushed for more operationally effective plat-

forms. These cultural chasms unnecessarily drained time and resources from an already difficult mission. Dr. Marion is spot-on in questioning the efficacy of trying to make the AAF a "professional" service, instead of focusing primarily on their counterpart's technical prowess. Indeed, while the phrase "Afghan good enough" was a constant mantra, senior air advisors often created the AAF in their image.

Dr. Marion also attacks some significantly engrained shibboleths. First, he astutely questions the decision to bring women into the service, considering the difficulties the Afghans had in recruiting qualified candidates, who had to learn English as well as fly a plane. He wisely notes that the Soviet Union tried to bring gender equality to the countryside, too, only to have it used as a rallying cry against them by the mujahedeen. Second, he highlights the devastating effect that the rash of Green-on-Blue attacks had on the air advisors, who suffered a gruesome attack in April 2011, which resulted in the death of eight Airmen and one civilian. Dr. Marion shows that the "Guardian Angel" program, while politically necessary to assuage concern at home, significantly hindered the rapport between the AAF and their advisors, a point that numerous advisors made in his book. More importantly, the author shows that other special operations advisors never utilized this program because they understood the devastating effect it would have with an honor-based culture.

Despite the book's overall value, Dr. Marion leaves some runners on base. First, Dr. Marion was spot-on in blasting the investigation of the April 2011 insider attack because senior air advisors deliberately obfuscated the complete investigation, fearing that it would reflect poorly on a beleaguered AAF that was struggling to get off the ground. However, he fails to highlight the irony in this abdication of responsibility by comparing senior air advisors' performance with that of their often-ridiculed Afghan counterparts. If the "world's greatest Air Force" sweeps unpleasant truths under the rug after a devastating attack that resulted in the deaths of eight Airmen, perhaps expecting professionalism from a burgeoning service engulfed in a four decade-long civil war is a bridge too far? Second, Dr. Marion never examines the efficacy in creating an AAF. Indeed, if his first two chapters of his book are any indication, the Afghan government has never been able to field a standing air arm despite consistent investment from outside powers. Moreover, how will future Afghan governments support such a technically advanced service without substantial financial assistance from a war-weary patron?

Nevertheless, Dr. Marion's book is an invaluable analysis of the USAF's longest air advising mission. He is unafraid of tackling controversial subjects and rightly questioning senior Air Force leaders' judgment. Moreover, he wisely highlights the problems that mirror imaging had on American advisors, who desperately wanted their counterparts to succeed but often forgot that *mission success* is an incredibly subjective term and his lessons learned incorporated into future doctrine to ensure our past missteps are not repeated—yet again.

Maj Will Selber, USAF

Satellite: Innovation in Orbit by Doug Millard. Reaktion Books, 2017, 208 pp.

What do you see when you look up at the stars? This is one of the fundamental questions that author Doug Millard, a deputy keeper of technologies and engineering at the Science Museum in London, tries to answer in his book *Satellite: Innovation in Orbit*. Millard dives into mankind's history and fascination with the universe beyond the planet that we inhabit and discusses the great minds and scientific achievements that made spaceflight and satellite launch possible. Written in a story-like fashion and densely illustrated, *Satellite* covers the full spectrum of launch into orbit and discusses the plethora of ways that satellites are integrated into daily life.

The organization of the book is presented logically, beginning with a discussion about the numerous physics discoveries contributing to the development and use of satellite systems. Sir Isaac

Newton and Johannes Kepler are both introduced in the first chapter, which provides original illustrations from both scientists on their laws of gravitation and motion. Konstantin Tsiolkovsky's contributions make up a good portion of this initial content as well, and he is mentioned throughout the book for his work on applying the theories of earlier discoveries to rocket and propellant design. Particularly interesting are the parallels that Millard makes between prominent science fiction writers, such as Jules Verne and H. G. Wells, and the research that was making that science fiction a reality. This connection to literary fiction helps to establish an early bond with the reader by referencing many familiar stories from these authors.

Millard quickly makes the transition from engineering theory to practice, as the militaries of the world turn their attention toward acquiring and operationalizing these prototype systems being developed. Multiple think tanks and advisory groups, such as the RAND Corporation and the British Interplanetary Society, began devising solutions to the problems inherent in space travel. He covers the notable contributions of individuals, such as Arthur C. Clarke and several prominent Russian enthusiasts, to the concept of space lift. Millard also includes detailed images of the hobbyist groups and prototypes in action, engaging the reader in the excitement of the time period and giving a sense of belonging and wonder to this early space era.

Millard then expands upon the inevitable realization that satellites are being launched and used for all humanity. Rightfully beginning with a dialogue on Sputnik, Millard includes discussions on the early systems that were deployed for government use. He accurately summarizes the space race occurring between the Soviet Union and the US, and the public fascination as it all unfolded. The American launch of Project Score initiated the Western foray into the communications satellite realm, relaying a message from President Eisenhower across the globe for the first time. Millard furthers the discussion of early satellite uses, including expansion into reconnaissance with TIROS and imaging with SENTRY, as well as infrared detection using MIDAS. The intelligence agencies made quick use of these capabilities, employing them for data collection as the Cold War began to take shape.

As more powerful rockets are developed, Millard informs, higher orbits became more accessible (p. 106). This development created a market for global communications as commercial companies leveraged these rockets to place satellites in geostationary orbits. Telstar, Intelsat-1, and other satellites brought new methods of information distribution to industry and government. Details are also given about other orbits designed to solve unique challenges, such as the Molniya orbit, to cover higher latitudes. Satellite costs became affordable enough that large networks could be built, such as the Iridium constellation of 66 satellites. In this segment, the author introduces the global positioning system, which revolutionized precision navigation, timing, and nuclear detonation detection for military use. Millard wraps up the intriguing discussion of satellite constellations with a couple of chapters on their scientific applications. He spends this segment discussing the onboard elements, fuel types, propulsion systems, and orbits. Arming the reader with the history and functionality of satellites, he concludes by pondering the future of both satellite systems and mankind's presence in space. He leaves it to the reader to decide what the future holds.

In conclusion, Millard uses this book to introduce readers to the story of the satellite. His intent is simply to inform the reader of how humanity reached into its imagination to put objects into space and how that imagination can be put to use to usher in a new space age. It is an excellent book to place on the coffee table to entertain guests or to casually glance through at leisure. For anyone looking for a technical manual, this book will not satisfy that desire but for anyone just looking to be entertained and informed on satellite history from concept to future application, this book certainly provides that.

1st Lt James Corcoran, USAF

Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks by Robert Mandel. Georgetown University Press, 2017, 302 pp.

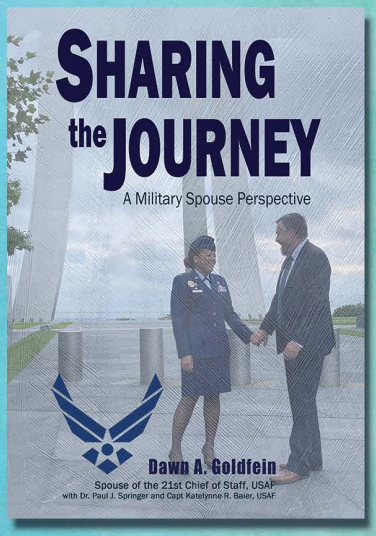
In *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*, author and professor Robert Mandel tackles one of the most relevant topics of the Information Age. In an interesting approach that focuses on deterring international cyberattacks rather than internal cyberattacks, the author makes the case that there are underexamined distinctions between cyber deterrence and other types of deterrence.

In the US, major cyber threats mark among the most prevalent security threats to the government and the private sector. With increasing global concern about a cross-border cyber threat, cyberattackers have increased diversity in their motivations, objectives, targets, and attack styles. In an exemplary case from October 2011–February 2012, the Department of Homeland Security reported more than 50,000 cyberattacks on private and government networks with 86 attacks on critical infrastructure networks. Mandel's work explores the rising and shifting nature of foreign cyber threat dangers and examines the hitherto moderately ineffective target responses. Following an excursion in cyber deterrence paradoxes revolving around ideal cyber deterrence dynamics, the author presents a list of hurdles to forward progress. Within this list, he addresses obstacles to meaningful cyber deterrence improvement and the roots of cyber deterrence failure. Perhaps the most intriguing section of the book details case studies from 12 major global twenty-first-century cyberattacks, which have been scrutinized in detail. Based on these findings, Mandel suggests specific, feasible ways to improve cyber deterrence planning and execution. Herein, needed conditions under the suggested approaches optimally serve the purpose of cyber deterrence, in addition to the counterpart approach of worst-case scenarios in cases where cyber deterrence is neglected are unveiled. This work omits to deter internal cyberattacks and focuses on major cyberattacks that threaten state and human security rather than cyberattacks with minor impacts or those which are non- security-oriented or profit-related. This demarcation provides a better understanding of cyber deterrence as a whole since the potential inclusion of additional shades of cyber deterrence could indeed complicate the reading comprehension. In concluding annotations an overarching analysis sheds light on ways to integrate and stabilize cyber deterrence, cogitate cyber deterrence legitimacy and ethics predicaments, address cyber deterrence paradoxes, and predict future cyber deterrence prospects.

Cyber deterrence entails a convoluted landscape for reader navigation. An intricate mixture of the deterrent declaration, penalty measures, credibility, and fear across subject areas such as cyberterrorism and national security effortlessly captures the reader in a whirlpool of arcane technical jargon and obscure acronyms. Nonetheless, one of the key strengths of this book is the author's decision to avoid such confusing elements. In this work, Mandel summarizes key insights in tables and figures, providing an opportunity for both novice readers and experts to gain insight into security opportunities, limitations, and trade-offs surrounding foreign cyber deterrence. Overall, this reviewer enjoyed reading *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks* and recommends it.

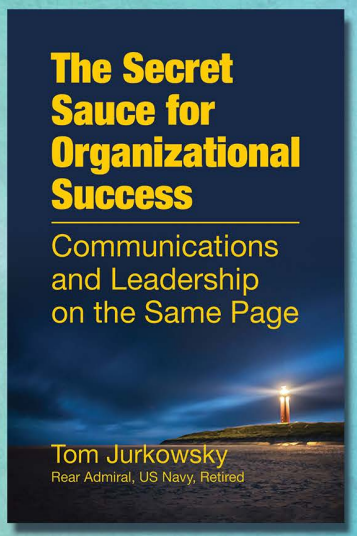
Dr. Amir S. Gohardani

Check out the latest publications from Air University Press



Sharing the Journey: A Military Spouse Perspective
Dawn A. Goldfein with Dr. Paul J. Springer and Capt Katelynne R. Baier

A unit's command team is the partnership among the commander, the senior noncommissioned officer (NCO), and a volunteer lead spouse. As the primary advisor, ambassador, and advocate for the spouses and families of members in the unit, finding the right person to undertake the critical role of volunteer lead spouse is one of the most important decisions a commander will make. Once a spouse in the unit decides to take on the role, it can be challenging and incredibly rewarding to navigate working with military leadership, state or local government, base programs and organizations, and other military spouses to take care of families. This book captures "words of wisdom" collected by Mrs. Dawn Goldfein, spouse of the 21st Chief of Staff of the Air Force and Gen David L. Goldfein over their 37-year career. For command teams that seek to understand and leverage the military "spouse network" of command, lead, key, and key spouse mentors within their unit or their installation, it offers a treasure trove of useful ideas and stories.



The Secret Sauce for Organizational Success: Communications and Leadership on the Same Page
Rear Admiral Tom Jurkowsky, US Navy, Retired

Admiral Jurkowsky's distinguished military career culminated in service as the Navy's Chief of Information, and he worked on a variety of events, from the Tailhook Scandal to various incidents at the Naval Academy. His book highlights the importance of honesty, clear messaging, and a positive relationship with the press in order to effectively manage strategic communications. The goal of The Secret Sauce for Organizational Success is for both communication practitioners and their leaders to learn from the author's experiences and motivate both, in tandem, so that they always do the "right thing."

AUP
AIR UNIVERSITY PRESS

https://www.airuniversity.af.edu/AUPress/
https://www.facebook.com/AirUnivPress/
https://twitter.com/aupress/