Spring 2018
Volume 32, No. 1
AFRP 10-1

Features

Departments

The Big Data Imperative

Air Force Intelligence for the Information Age

Col Shane P. Hamilton, USAF

Lt Col Michael P. Kreuzer, USAF, PhD*

Big data is the subject of much discussion in the media and in the government today. It has been described as an "easy button," when combined with artificial intelligence, to reduce the human role of analysis. Some view this as a potential threat to the democratic order, and by others it is viewed as a lot of hype with few earth-shattering results to show.[1] What is big data, and why is it vital to the future of the intelligence community (IC) and combined military operations?

In this article, the authors argue that the information revolution has radically changed intelligence by dramatically increasing the number and variety of intelligence collectors. Thereby the collectors create a global network of analysts and

*The authors would like to thank those who provided key insights and reviews for this article, including Kenneth Bray, Dr. Jon Kimminau, Lt Col Shawn Smagh, and Maj Shaun Lee.

machines that facilitate the rapid sharing of data and information. This network also increases the appetite of operators for faster and more operationally relevant assessments about threats and targeting opportunities. Further, it has reshaped the threat environment by creating new centers of power and collection in the cyber domain—where adversaries can recruit members, plan strikes, and exploit both ordered and inspired attacks through online collectives. Our current manpower and resource-constrained environment—combined with these factors—necessitates new strategies for planning and executing intelligence, surveillance, and reconnaissance (ISR) operations, and investment in organizing, training, and equipping analyst Airmen with the tools to succeed in the modern information environment. Big data conceptually sits at the core of this environment and will drive our understanding of how we collect, structure, and analyze data, information, and intelligence in the future.

Cutting through the Hype—What is Big Data?

As the name implies, *big data* is ultimately about the gathering, storing, and processing of large volumes of data and information. Intelligence analysts will quickly point out that there is nothing new about gathering and storing large volumes of information, as it has been a central purpose of intelligence entities for centuries. Nonmilitary analysts regularly sort through large volumes of data to make quantitative assessments of complex problem sets based on tens of thousands of case observations across multiple variables. So, what makes big data new and different? The phrase first appeared in the early 2000s, when industry analyst Doug Laney defined big data as distinct from previous models by three main factors dubbed the "three Vs:"[2]

- **Volume**—The information age enables both the acquisition and storing of data and information that can be preserved and regularly accessed and analyzed on scales not seen before. Most previous databases for analysis could be contained in a single database (such as a Microsoft Excel database) with lines ranging from tens to tens of thousands of lines. Big data enables the collection of millions to billions of data points.
- **Velocity**—The volume of data and information is acquired at an unprecedented speed and must be dealt with promptly. Twitter, for instance, received 500 million updates (tweets) per day in 2013;[3] each tweet constituting a single data point of information.
- **Variety**—Data and information come in numerous formats from diverse sources. In the past, the analyst or entity requiring the information could shape what was collected and how it was stored, but the combination of volume and velocity today necessitates building systems to manage and incorporate data in the form in which it is acquired; from an image to a Twitter or Facebook entry to a transcript of a conversation or speech.

As awareness of big data has grown, many scholars today have added to these three Vs with other dimensions such as variability and complexity. In the USAF, among other institutions, we add a fourth "V" to this list:

- **Veracity**: The volume, velocity, and variety of data accessible via big data include a significant amount of noise and irrelevant data to the problem set. This creates potential abnormalities in data analysis and opens the door for analytic bias in the selection of what data is important and how to analyze it. Big-data strategies must include processes to keep data "clean" and an analytic awareness of the big data working hazards.

After big data emerged, a new phrase—*big-data analytics* —came into vogue.[4] These terms are often thrown about interchangeably but represent two distinct sides of the same coin. Big data represents a process for rapidly compiling, storing, and accessing large amounts of data and information from numerous sources and with varying structures. Big-data analytics represents the tools, tradecraft, and processes that can transform big data into insights—from intelligence preparation of the operating environment to threat warning to predictive battlespace awareness to targeting. These insights in turn shape decisions across the range of military and diplomatic operations, from strategic deterrence operations to near- real-time (NRT) tactical engagements.

Debates about big data's potential versus hype stem largely from misunderstanding both big data and big-data analytics.[5] Big data's cheerleaders have historically made four exciting claims about big data that are at best optimistic oversimplifications: (1) data analysis produces uncannily accurate results; (2) sampling is unnecessary because big data allows us to capture all possible data points; (3) high levels of correlation in big data makes qualitative debates about causation passé; and (4) statistical models are similarly irrelevant because "the data speaks for itself."[6] In truth, big data doesn't eliminate traditional challenges in data collection and data analysis; it does radically reshape where and how the snags occur. The main challenge stems from the final claim: data never speaks for itself. The manner in which data is gathered, organized, and processed shapes the message that the data sends to the user. Complex algorithms perform many of these functions to enable big data analytics, but those algorithms, even facilitated by machine learning, must be programmed by humans and tailored to answering prespecified questions.[7] This means big data is still subject to biases in collection, display, and analysis of which analysts must be acutely aware. Big data enables access to exponentially increasing data points to facilitate faster analysis from more data points, but bad big-data analysis begets bad analysis.

How Big Data Reshapes Intelligence

Of the four Vs of big data, analysts have until recently had to contend mainly with the first and third "V," but on a smaller and more manageable scale. The pace of collection, the relative consistency of threats posed by state actors, and the stovepiping of analysis and production along intelligence discipline production lines (the INTs—signals intelligence [SIGINT], geospatial intelligence [GEOINT], imagery intelligence [IMINT], human intelligence [HUMINT], open-source intelligence [OSINT], and measurement and signals intelligence [MASINT]),[8] enabled the division of effort into separate data problems that could be analyzed in parts by specialists, with all source intelligence answers produced by combining component parts.

The information revolution's impact on USAF intelligence's core competencies (collection, analysis, targeting, and integration) focused first on collection and second on both threat and targeting analysis (see fig. 1). There has been a dramatic increase of collectors and sensors available, with globally integrated ISR enabling NRT exploitation. Concurrently, operational demands shifted analysis for both threat and targeting analysis toward NRT to get inside the adversary's OODA loop.[9] In an era of constrained resources with few signs of significantly increased manpower in the near future, changing intelligence production to meet today's operational demands is unlikely to come from further revolutionizing collections or analysis. Today, even within the INTs, the volume, velocity, and variety of data and information collection has grown to a point where analysts can no longer sift through everything collected sufficiently to even store—much less analyze—all of it without the aid of computer programs and automated processes. Further, the advent of the cyber age transformed the nature of collection from publicly available sources that open-source analysis has evolved from an information source to aid analysis to a true intelligence discipline in its own right—OSINT—with tradecraft, governance, and legal issues surrounding the collection, analysis, and production.

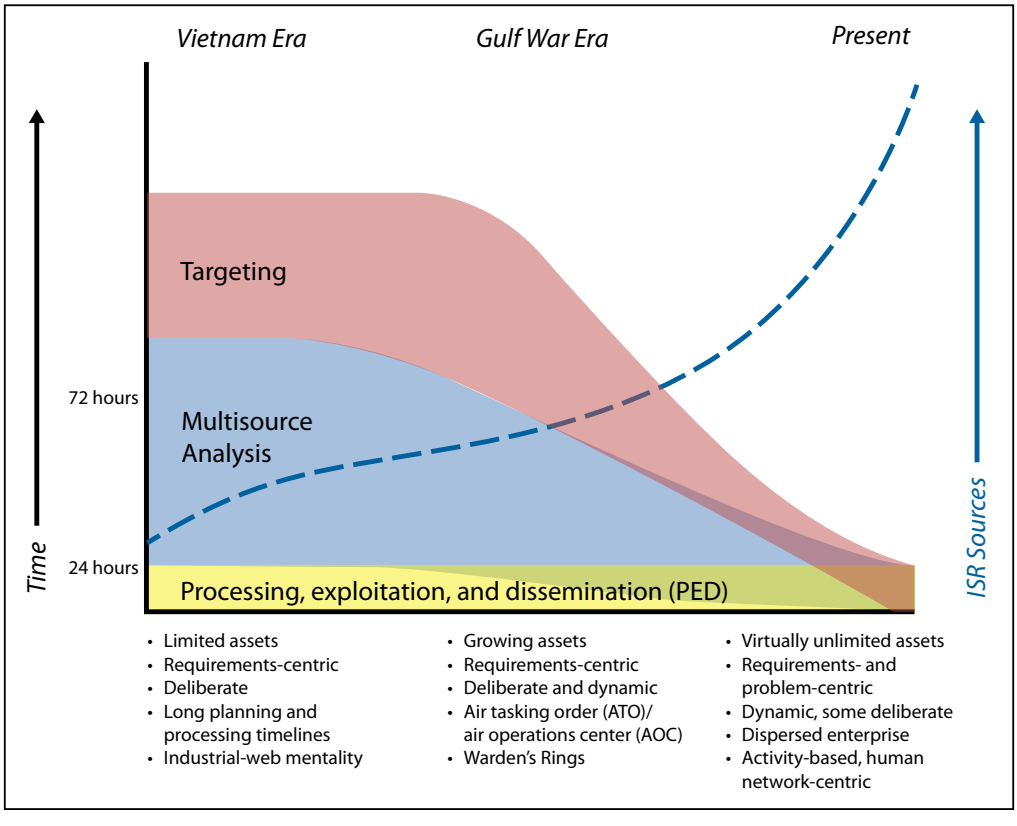


Figure 1. The information revolution's impact on collection, analysis, and targeting

The future is in data management and intelligence planning to facilitate problem-centric—rather than requirements-centric—USAF intelligence. Industrial models for production can no longer keep pace with the information environment. As National Geospatial Intelligence Agency director Robert Cardillo noted earlier this year, "If we were to attempt to manually exploit the commercial satellite imagery we expect to have over the next 20 years, we would need eight million imagery analysts. Even now, every day in just one combat theater with a single sensor, we collect the data equivalent of three NFL seasons—every game. In high definition!"[10] Analysts have more access to information than ever before and more tools at their disposal to gather information to fill gaps in knowledge. Empowering those analysts to shape the commander's knowledge of what is known, what is assessed, what is unknown, and shaping the right set of tools to answer the remaining intelligence questions is the way to get the right information to the right decision maker at the right time. Flexibility and versatility must be applied to planning and executing effects-based ISR campaigns the same way they are applied to offensive air operations.

The Four Vs and Intelligence Collection

The character of the War on Terrorism, combined with the information revolution's innovations of precision targeting, has shifted the balance of USAF efforts from the volume of ordinance dropped to the demand for ISR collection. Figure 2 illustrates the dramatic shift in balance between the aircraft and intelligence required to execute an air strike for strategic effect since World War II—with three hours of intelligence supporting 293 bombers in the 14 October 1943 Schweinfurt raid over Nazi Germany compared to more than 600 hours of intelligence work to support one 15-minute segment of a sortie in the Abu Musab al-Zarqawi raid in 2006. Precision strike requires precision intelligence, which flips the manpower burden from flying operations to processing, exploitation, and analysis to facilitate the strike operation. Recognizing the increased demand for intelligence to increase the ability to strike has resulted in a steady and sharp increase in collection platforms, sensors, and bandwidth to support "reach-back" operations, but not necessarily a commensurate increase in manpower to analyze the sheer volume of collection within the time requirements to facilitate operations. At the same time, the shift in emphasis to reach-back operations combined with the strengths and vulnerabilities of operations in the information age further muddies the historic delineation of a front and rear area of operation, rendering this concept of the operating environment an archaic notion to modern air forces.

For GEOINT, this manifested itself most visibly in an explosion in the demand for full-motion video (FMV) collection. For much of the last decade, the USAF has been awash in FMV, and it is not alone as Army organic capabilities, special operations, and partner nations press to expand the size of their fleets, increase the number of remotely piloted aircraft (RPA) sorties, and invest in the bandwidth to sustain the near insatiable demand.[11] High workloads associated with "deployed-in-place" status led the IC to steadily hollow out its workforce up to 2015, losing imagery analysts at a faster rate than they could be trained.[12] Several quality-of-life initiatives

implemented since that time reduce hours and combat the strain but also result in reduced capacity. In 2015, the USAF briefly reduced its number of RPA patrols from 65–60 to help the pilot, sensor operator, and intelligence workforce get healthy,[13] but operational realities forced the military to supplement its active duty RPA force with contractors to meet the demand.

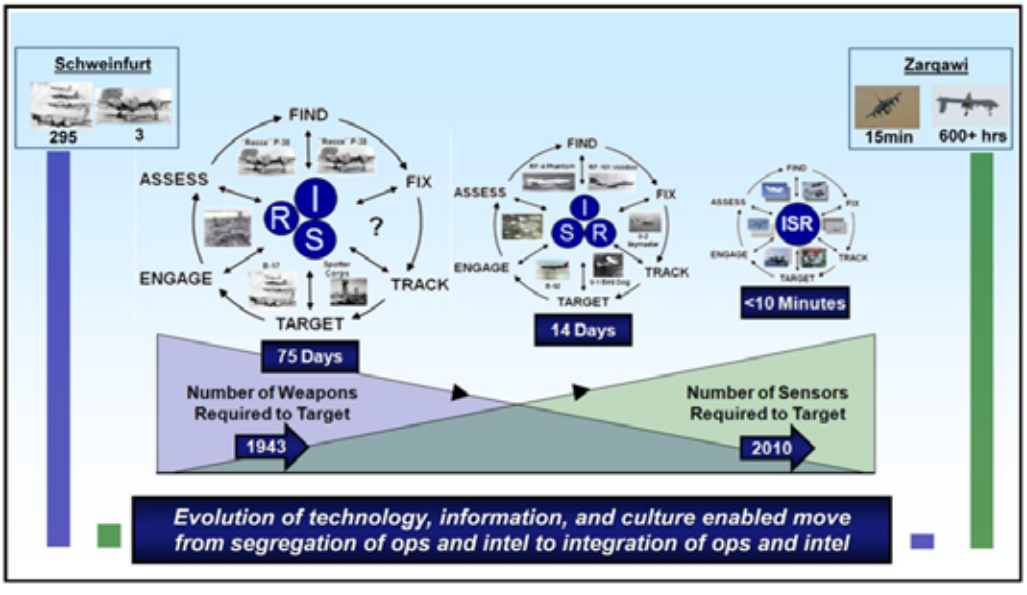


Figure 2. Implications of the information revolution for USAF targeting. (Reprinted from: Curtis E. LeMay Center for Doctrine, Development and Education, *Air Force Doctrine Document 2-0 Global Integrated Intelligence, Surveillance, and Reconnaissance Operations*, 6 January 2012, 2, https://fas.org/irp/doddir/usaf/afdd2-0.pdf.)

FMV gained the most attention outside the IC, but even within the realm of GEOINT/IMINT it represents just one source of intelligence that exploded in demand to meet operational needs. The needs for multispectral imagery, hyperspectral imagery, and ground-moving target indicator sources all continue to rise in demand across numerous operating areas;[14] including Iraq, Syria, and Afghanistan, among others. Specialized sensor suites provide the USAF with collection capabilities unrivaled in previous generations. However, those suites come with a training, manning, and time-intensive quality of analysis tail, which makes each sensor manpower intensive, straining the limited supply of imagery analysts available to process the rising collection.

The explosion of GEOINT sensors and collection capabilities introduces another significant challenge to effective analytics without the aid of big data solutions. The variety of data information collected in various graphics formats is "undiscoverable" to analysts, or what is sometimes characterized as *dark data*. Exploited GEOINT generally has textual summaries that can be searched, through queries similar to a Google image search, but absent text to cue the analyst, the relevant imagery may remain buried and undiscoverable in data archives. Big-data algorithms and automated

exploitation templates can allow all images, in NRT, to be tied to geographic coordinates, aligned to known locations, and automatically archived in searchable layered databases with related images over time. While the current model for ISR is operations-centric, requiring new sorties to gather geospatial information (particularly for problem sets like pattern-of-life), big-data analytics will provide future analysts access to a library of historical data and the tools to rapidly sift through potentially thousands of images to see changes over time and analyze the significance.

GEOINT is not alone in seeing an exponential increase in demand for collection and analysis. The increase in collection platforms also led to an increase in collector payloads across intelligence disciplines, including SIGINT payloads. As the number of collection opportunities rises, and as global connectivity rises in the information age with global-networked threats emerging, the volume, velocity, and variety of signals collected continue to rise, often at a rate faster than our ability to recruit and train analysts.[15] Just as hours of video acquired by RPAs may go unanalyzed for years without the prospect of big-data analytics to aid in cueing analysts to key segments of analysis collection, hours of intercepted communications may go without being analyzed absent automated tools to sort through the petabytes of collection. Beyond SIGINT and GEOINT, MASINT has similarly seen a boom in both collections and demand for production, with synthetic aperture radar and coherent change detection, among other capabilities in increasingly high demand.[16]

Open-source Intelligence

Perhaps no example illustrates the sea change of collection regarding the four Vs of big data more than the creation of OSINT as a true intelligence discipline. When we say OSINT is a new discipline, many Cold War-era analysts will caution, "No, we've always had OSINT, and the Central Intelligence Agency's (CIA) Open Source Center is proof."[17] Indeed, a common rule of thumb cited for decades, dating to a statement from then-CIA Director Allen Dulles, is that more than 80 percent of intelligence analysis is ultimately derived from open source. All this is true, but it would doctrinally be better characterized as *open-source information*. OSINT as an intelligence discipline is directly tied to the proliferation of the internet and social media, and with it the need to develop new tradecraft for search and discovery of information, oversight to ensure relevant laws and orders protecting citizens and safeguarding information are observed by the IC, and governance of the process. Absent big-data analytic solutions, it would be impossible for analysts to sort through the billions of data points available (volume, variety, and velocity), identify the relevant and irrelevant pieces of data (veracity), safeguard the rights of citizens and follow other applicable laws and regulations, and discover relevant intelligence insights to meet customer needs.

The information revolution led to a new online culture of sharing, and what many characterize as oversharing.[18] The upside for the IC is that through Twitter, Facebook, Snapchat, blogs, and numerous social media sites not even invented yet, intelligence has access to tens of millions of passive collectors all over the world. In the 1990s, analysts faced the prospect that battle damage assessment might be

conducted on CNN before they had time to complete the intelligence cycle for assessment. Today, if an RPA loses connectivity and crashes, it is likely to be reported on Twitter and retweeted multiple times before the aircraft is confirmed lost. Academic research and intelligence analysis now rely on sentiment analysis, in essence, a sophisticated and tailorable version of "trending" on Twitter, to determine the sentiments of populations as a potential predictor of future activity (civil unrest, and so forth).

Time Demands of Operations

In most commercial discussions of big data, velocity focuses on how rapidly information is acquired. For intelligence operations, velocity can equally apply to how rapidly operators, commanders, and other decision makers require intelligence outputs to facilitate operations. The campaign against the Islamic State has been for the United States predominantly an air-centric campaign, emphasizing both deliberate and dynamic targeting to isolate and degrade a proto-state with limited fixed infrastructure and which readily blends into the population for defense from strikes.[19] This combination, along with the necessity to minimize the risk of collateral damage, has only served to add to the demands for ISR. This includes both finding and characterizing targets, maintaining overwatch of potential targeted locations, and understanding patterns of life among the population. Lt Gen Charles Q. Brown Jr., the coalition forces air component commander, made the point explicit in May 2016, stating, "Because what it helps me to do is develop targets so we can strike at the same time as we develop those targets. The more ISR I have, I can minimize the risk to civilian casualties and continue the precision air campaign that we have."[20]

More in this context has both volume and time dimensions as the time the information will be of value in a dynamic strike is minimal, especially compared to a more traditional target such as an airfield, a command bunker, or a portion of a communications network. The NRT nature of FMV and its critical role in the engagement/finish phase of operations led many observers to conclude targeting is easier to do today in real time, but in practice this represents the tip of the intelligence iceberg that facilitated the strike. Coalition forces require a globally synchronized network of analysts to rapidly fuse imagery, electronic intercepts, and tips from informants to cue potential targets for a strike. Globally-integrated ISR facilitates these networks via timely access to more collection but with it a significant veracity problem. At the same time, this system is simultaneously raising critiques from human rights organizations with civilian casualties concerns and from advocates of more traditional air campaigns that the overall numbers of targets being struck are insufficient even by the standards of recent campaigns.[21] The ISR community, and the IC more broadly, must face the complex management problem of distributed operations, quality control of analysis, and management of data sets to give both the ISR enterprise and operators acting in real-time full visibility to target development progress.

The Threat Environment

The Islamic State in Iraq and Syria's (ISIS) regular appeals to "lone wolf" terrorism through what has been called the *digital caliphate* highlights the challenge the internet poses to security in the West.[22] Before that, cyber collectives like 4chan/"Anonymous" were exploiting online connectivity to build anarchic communities of information sharing that ultimately facilitated collective action on a number of issues.[23] As US military intelligence has traditionally regarded conventional military dominance as the focal point of its mission, in the information age weaponized narrative is rapidly gaining focus as a theater of operations for national security.[24] Understanding the threat environment in the information era will only be possible with access to, and the effective utilization of, big data solutions. While countering this challenge will likely ultimately fall to non-DOD entities such as the State Department, the USAF's mission demands awareness and defense of the cyber domain. As such, USAF intelligence analysts must be at the forefront of analyzing and discovering threats in the cyber domain.

The past decade of counterterrorism and counterinsurgency operations has made USAF intelligence analysts well-versed in monitoring and evaluating terrorist networks in conflict zones, particularly in Iraq as was the case with al-Qaeda in Iraq and with Taliban-linked groups in Afghanistan. Cyber collectives represent a distinct challenge, however. Cyber collectives lack a centralized command structure, instead operating largely through online community norms and values. Their membership is open, without formal recruitment or retention mechanisms, and their strategic planning is minimal. Most tend to resist anyone emerging as a leader or spokesperson for their group; influencers might emerge for limited periods, but the open and diverse nature of membership prevents anyone from emerging for an extended period without fracturing the group. Smaller communities might develop stronger internal hierarchies as limited membership brings with it homogenous ideologies, but this serves to limit the global reach and influence of larger collectives.[25] Figure 3 illustrates the distinctions in brief between a hierarchy, a network, and cyber collectives.

The character of intelligence collectives provides a forum that can be infiltrated to spark lone wolf or wolfpack attacks; information simultaneously spread among a circle of the collective initiates an action —think a flash mob—with little to no warning. At the same time, the anarchic character of collectives tends to make their justifications anarchic as well; their *modus operandi* is often to oppose authority figures and abuses of power, not to actively seek to replace it with a new dominant ideology. For this reason, many lone wolf and wolfpack strikes launched by individuals recruited through collectives, even when inspired by organizations with specific ideologies, do not necessarily show an affinity for specific ideological positions; only their reactionary nature. As one example, Orlando nightclub shooter Omar Mateen may not have understood the difference between ISIS, al-Qaeda, and Hezbollah, despite there being significant sectarian and strategic distinctions between these groups.[26] In line with the characteristics of cyber collectives, however, these groups are linked online by anti-Western sentiments and an anarchic perspective toward the Western order. Calls to incite chaos to avenge moral wrongs propagate in

that environment, while specific ideological messages and more formal alignments with specific groups may not.

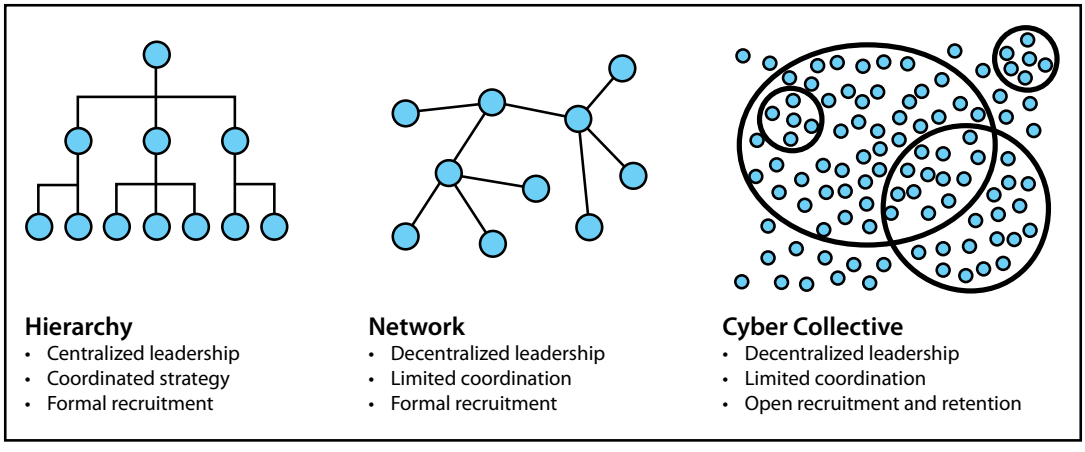


Figure 3. Hierarchies, networks, and cyber collectives. (Derived from sourcing in Max Sterling, "The Cyber Collective Threat: A Pack of Lone Wolf Terrorists," *The Project on International Peace and Security, Institute for the Theory and Practice of International Relations, College of William and Mary,* April 2017, http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Sterling.Max.pdf.)

The challenge for intelligence agencies stemming from this new decentralized organization is the prospect of infiltration of collectives as part of a multipronged strategy aimed simultaneously as destabilizing adversaries through deep state attacks while concentrating more organized and strategic violence against local governments through both networked and hierarchic organizations.[27] Figure 4 illustrates how this hybrid model might look, with a central strategic leadership core directing actions across multiple departments for recruitment, propaganda, training, direct action operations, coordination with networks, and online propaganda infiltration of cyber collectives. As broad and diverse as these networks are, traditional network mapping is not possible given how rapidly they can shift and how fast messages can be shared through collectives. Identifying influencers within the network requires big-data solutions to follow volume of message traffic, identify what themes might be trending and what messages might be receptive in what areas, and to identify shifts in trends in those messages which might presage a change in attack strategies (mass shootings, crashing vehicles, and the next evolution of threats). This level of understanding of adversary organizations and messaging is vital to countering adversaries directly at the operational level and above, but potentially more importantly for tactical indications and warnings for force protection.

Just as adversaries can use the cyber domain to carry out operations through influence, they can use cyber tools to thwart intelligence and to amplify their messages. One of the most prominent today is the use of bots;[28] software robots designed to automatically propagate messages via social media and other online venues. These can distort data for sentiment analysis, sway public opinion through a bandwagon effect by making it appear more popular, automatically spread disinformation

through cyber collectives, and to amplify recruitment. Investigations of Russia's potential activities in the 2016 election have focused not so much from the threat of hacking in the traditional sense, but social engineering executed by bots with messages aimed at specific groups.[29] Going forward, analysts operating in a complex multidomain environment must understand the emerging nature of threats posed by the cyber realm.[30] Maintaining basic situation awareness, much less gaining operational understanding, can only come through a better understanding of big-data analytics and recognition of both its power as a tool and its vulnerabilities.

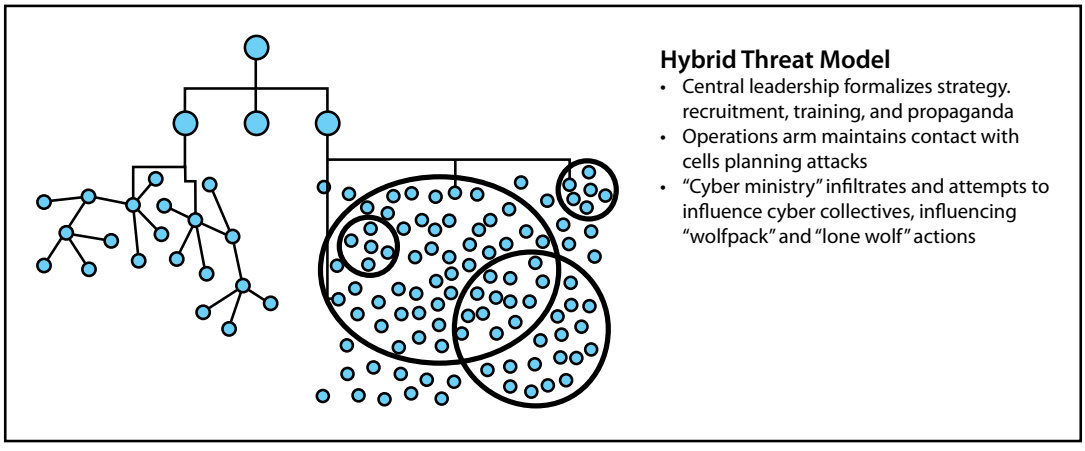


Figure 4. The hybrid threat of infiltrated cyber collectives

The Industrial Age Intelligence Model versus the Information Age Model

The three Vs of big data, combined with their implications for friend and foe alike, necessitate a rethinking of our industrial model for intelligence production. All intelligence operators are trained from their basic courses in the five-step intelligence cycle known as planning and direction; collection; processing, exploitation, and dissemination (PED); analysis and production; and dissemination (PCPAD).[31] This structured and repeatable process ensures clarity of the steps of production and provides checks and balances over analytical processes. It also contains bureaucratic elements, particularly for large organizations such as USAF intelligence that correlate steps of the PCPAD cycle with different units/offices. An information age model of intelligence must find ways to move beyond the bureaucratic model alone (not replace it, but supplement it), and facilitate data management across a distributed enterprise to support decision-quality intelligence for operational demands. Data science must be viewed as a core competency of the intelligence community in the information age, and traditional intelligence analysts must work hand-in-hand with skilled computer scientists and data managers to facilitate intelligence production.

Another challenge/opportunity for USAF intelligence is the conflation of intelligence and ISR. The DOD defines ISR as "an activity that synchronizes and integrates

the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function."[32] Although it is a combination of intelligence and operations, it represents a subset of the overall intelligence cycle. Tasking represents the final portion of the planning process, where units are assigned requirements through the ATO, while collection and PED mirror those stages of the PCPAD cycle, as illustrated in figure 5.

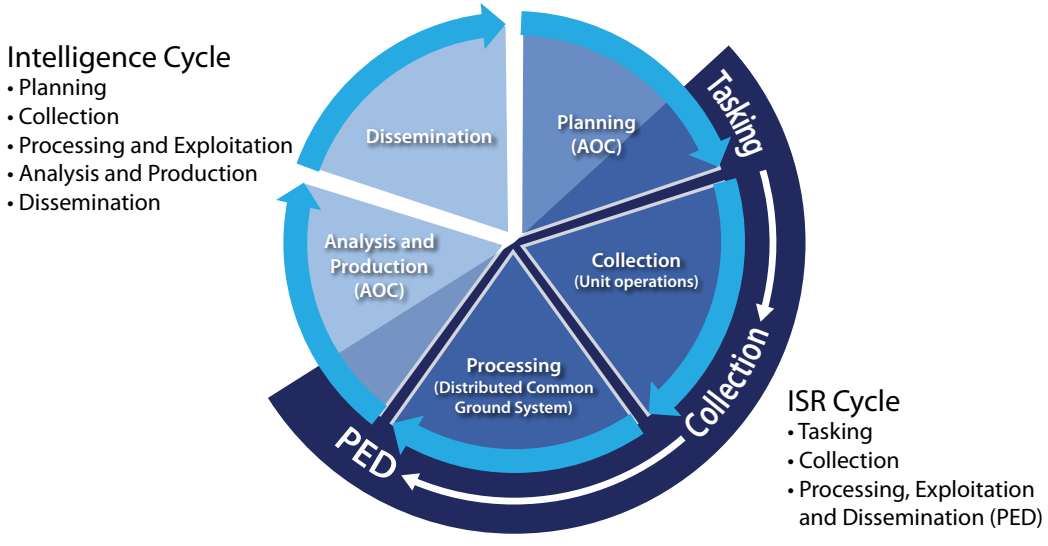


Figure 5. Industrial model of intelligence production

This model sets up an infrastructure for intelligence analysis that proved effective in evaluating state actors, but its time-sequenced character has in practice placed a limiting factor on the USAF's ISR OODA loop. ISR planning is executed through the 72-hour ATO tasking cycle and is governed by a collection management process whereby commanders' priorities for collection targets (sites to be imaged or otherwise collected) are racked and stacked through a boarded or refereed prioritization process before ATO execution. This is followed by an analysis process which can add days to the process for operational-level analysis within the USAF, or weeks for all-source production at national agencies. This interferes from an ISR standpoint with the USAF principle of flexibility, which should enable ISR operators to mass and maneuver ISR effects to critical points in the operating environment for integration in time, space, and purpose.[33] Further, as ISR sources have grown more complex and the stockpile of underlying intelligence data and information grows, it is unlikely that traditional models for developing priority intelligence requirements, commander's critical information requirements, and other intelligence collection requests in the future will remain an efficient means of prioritizing collection assets.

In the mid-2000s, ISR operators faced the challenge of explaining to customers, "Don't request an asset like Predator; request a capability like FMV." Today, the

problem is compounded as collection sources are much more specialized and numerous, leaving ISR tacticians best positioned to determine which ISR source is best positioned to fill an intelligence gap. Adding passive sensors like OSINT and discoverable big-data analysis of existing HUMINT, SIGINT, GEOINT, and MASINT data may rapidly answer a customer perceived problem absent the need for additional collection to a confidence level sufficient to justify not retasking the asset. While the vast majority of assets and collection allocations will, for the immediate future, continue to be tasked through this standard process, a share of airborne ISR assets and analytic capability must be dedicated to an information age alternative to directly shape the air campaign in NRT.

The alternative for the information age is problem-centric intelligence, spearheaded by an ISR task force. Rather than tasking collection, the operations input to the ISR process should be perceived intelligence problems, which ISR specialists can then translate to refined ISR problems, intelligence gaps, and prioritize ISR sensors in a combined scheme of maneuver to fill those gaps. An ISR task force, empowered by a single commander with organic collection requirements management and collection operations management authorities, is empowered to build an integrated ISR plan for a specified operational objective. This is the next step in the advancement of USAF Central Command's 2009 directive codifying ISR mission-type orders (MTO) as critical to supporting operational contingency operations.[34] Absent a specified ISR task force with ownership of ISR assets and authority to task them, the current MTO construct is more akin to an ISR coordination card for retasking than a true mission type order as defined in Joint Publication 3-50, *Personnel Recovery*.

This ISR task force model, outlined in figure 6, restructures the planning process for organic airborne ISR assets to a problem-centric mold, incorporating big-data analytics to refine the tasked ISR problem. The "IC Cloud," composed of access to NRT OSINT data and the full database of multi-INT analysis from across the IC, allows analysts in the earliest stages of the process to shape answers to the customer's problem, while refining their intelligence questions based on a refined understanding of what is actually known by the IC. ISR tacticians can then match the best collection platform to answer the intelligence gap. ISR operations can then be readily retasked by the ISR task force, under the authority of the commander through the intent of the MTO; in practice by a designated operator with sensor tasking authority. This provides NRT refinement of collection in concert with PED and fusion entities, maximizing the utility of the sensor. ISR task force products can then be distributed in NRT simultaneously to operational customers for planning and targeting decisions and to the larger IC for further analysis and ultimately incorporation into the IC Cloud for future exploitation.

Enabling this big-data solution to intelligence analysis and ISR tasking also requires the USAF intelligence community to think bigger about its personnel choices moving forward, as depicted in figure 6. The IC to date has accepted specialists in a number of scientific fields beyond intelligence officers and enlisted personnel. To make big data work in the future, the USAF intelligence enterprise must incorporate data scientists, computer programmers, and social scientists with expertise in the cyber domain to comprehend the nature of the data we access, and effectively analyze the operating environment of the cyber domain.

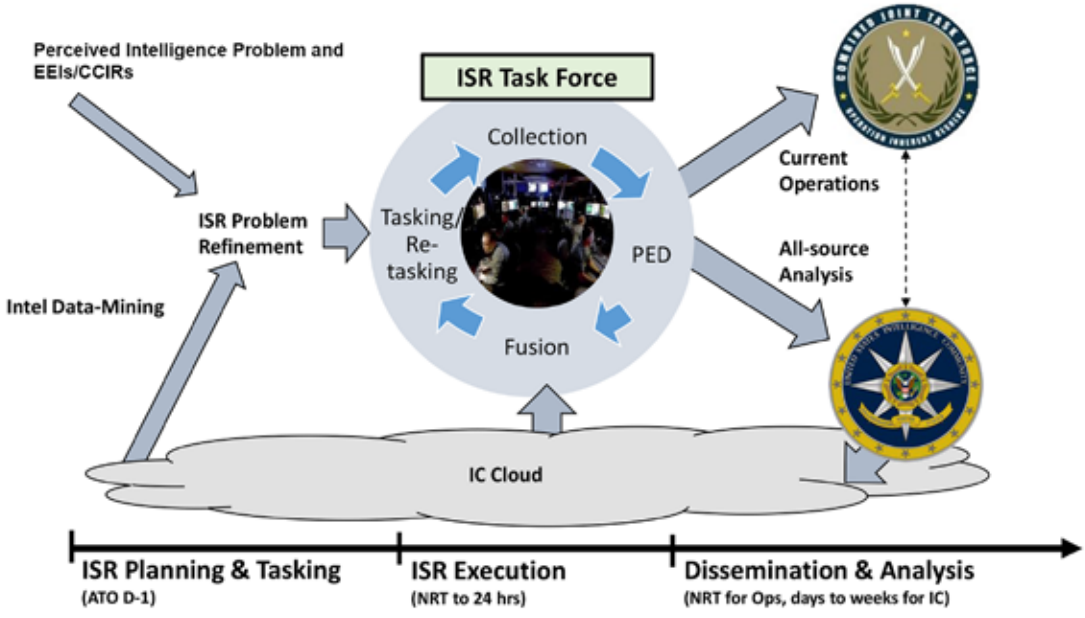


Figure 6. Intelligence, surveillance, and reconnaissance task force model for airborne intelligence. (Source: Maj Michael P. Kreuzer and Maj Denis A. Dallaire, "Targeting the Islamic State," The Mitchell Institute for Aerospace Studies, 14 April 2017, http://docs.wixstatic.com/ugd/a2dd91_4892807f169341188b7ebcd2f775671d.pdf.)

Conclusion

To paraphrase an old quote, you may not be interested in big data, but big data is interested in you.[35] Big data shapes the modern information environment, and through information sharing and access to the cloud, big data is already radically restructuring how analysts access and interpret data. Adversaries exploit the complex cyber environment to recruit, influence populations, and execute attacks against US interests in a manner that can only be detected through big-data solutions. Our ability to collect and store raw data continues to exceed our ability to process what we have collected, meaning we likely already have, somewhere in our vast databases of information, the answers to the puzzles intelligence customers have today and the ones they will pose tomorrow. Absent big-data solutions to manage the data and information we continue to collect and bring it to ISR planners rapidly to facilitate smarter, timely collection, the USAF intelligence community will face information overload resulting in decision paralysis. Getting the right information to the right customer at the right time means rethinking ISR planning, and embracing big-data solutions to the ISR challenges we face. ✪

Notes

1. David Rotman, "How Technology Is Destroying Jobs," *MIT Technology Review*, 12 June 2012, https://www.technologyreview.com/s/515926/how-technology-is-destroying-jobs/; Zeynep Tufekci, "The Machines are Coming," *New York Times*, 18 April 2015, https://www.nytimes.com/2015/04/19/opinion/sunday/the-machines-are-coming.html?_r=0; Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zacari, Andrej Zwitter, "Will Democracy Survive Big Data and Artificial Intelligence?," *Scientific American*, 25 February 2017, https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/; and Tim Harford, "Big Data: Are We Making a Big Mistake?," *Financial Times*, 28 March 2014, https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0.

2. SAS Institute, "Big Data: What It Is and Why It Matters," 24 May 2017, https://www.sas.com/en_us/insights/big-data/what-is-big-data.html.

3. Richard Holt, "Twitter in Numbers," *Telegraph*, 21 March 2013, http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.html.

4. SAS Institute, "Big Data Analytics."

5. Geethika B. Peddibhotla, "Gartner 2015 Hype Cycle: Big Data is Out, Machine Learning is in," *KD Nuggets*, http://www.kdnuggets.com/2015/08/gartner-2015-hype-cycle-big-data-is-out-machine-learning-is-in.html.

6. Harford, "Big Data."

7. SAS Institute, "Machine Learning: What It is and Why It Matters," 24 May 2017, https://www.sas.com/en_us/insights/analytics/machine-learning.html.

8. Office of the Director of National Intelligence, "What is Intelligence?," 24 May 2017, https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

9. Developed by John Boyd in the 1950s and introduced to Air Force training in the 1960s and 1970s, the "OODA Loop" (observe, orient, decide, and act) represents one model for decision making across four phases with the implication that a faster and better OODA Loop than your opponent is essential to gaining an advantage in combat. For a brief example, *see* Richard Feloni and Anaele Pelisson, "A Retired Marine and Elite Fighter Pilot Breaks Down the OODA Loop, the Military Decision-making Process that Guides 'Every Single Thing' in Life," *Business Insider*, 13 August 2017, http://www.businessinsider.com/ooda-loop-decision-making-2017-8.

10. Robert Cardillo, "National Geospatial Intelligence Agency (NGIA) *2017* Symposium Remarks," (lecture, NGIA Headquarters, Springfield, VA, 5 June 2017), https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/GEOINT-2017-Symposium.aspx.

11. Christopher Drew, "Military Is Awash in Data from Drones," *New York Times*, 10 January 2010, http://www.nytimes.com/2010/01/11/business/11drone.html; Kevin McCaney, "Pentagon Plans to Boost Drone Flights by 50 Percent," *Defense Systems*, 17 August 2015, https://defensesystems.com/articles/2015/08/17/pentagon-to-increase-drone-flights-50-percent.aspx; and Julian E. Barnes, "NATO Invests in More Bandwidth for New Data-Hungry Drones," *Wall Street Journal*, 27 March 2017, https://www.wsj.com/articles/nato-invests-in-more-bandwidth-for-new-data-hungry-drones-1490601588.

12. Pratrap Chatterjee, "The Side of Drone Warfare No One Is Talking About," *Nation*, 13 July 2015, https://www.thenation.com/article/the-side-of-drone-warfare-no-one-is-talking-about/.

13. Marcus Weisgerber, "Air Force Trims Drone Ops to Get Workforce 'Healthy,'" *Defense One*, 18 May 2015, http://www.defenseone.com/business/2015/05/air-force-trims-drone-ops-workforce-healthy/113122/.

14. Joey Cheng, "Hyperspectral Sensor Lets Drones See through Camouflage, Spot Explosives," *Defense Systems*, 25 February 2015, https://defensesystems.com/articles/2014/02/25/air-force-aces-hy-hyperspectral.aspx?admgarea=DS.

15. National Security Agency (NSA), "Signals Intelligence," *NSA*, 24 May 2017, https://www.nsa.gov/what-we-do/signals-intelligence/.

16. "RQ-4A/B Global Hawk HALE Reconnaissance UAV, United States of America," *Air Force Technology*, 24 May 2017, http://www.airforce-technology.com/projects/rq4-global-hawk-uav/rq4-global-hawk-uav6.html.

17. Central Intelligence Agency (CIA), "Open Source Center," *CIA*, 24 May 2017, https://www.cia.gov/careers/games-information/view-our-advertising/pdf/OSC%20Insert.pdf.

18. Mary D. Harrington, and Lisa E. Heffernan, "Oversharing: Why Do We Do It and How Do We Stop?," *Huffington Post*, 3 February 2014, http://www.huffingtonpost.com/grown-and-flown/oversharing-why-do-we-do-it-and-how-do-we-stop_b_4378997.html.

19. Maj Michael P. Kreuzer and Maj Denis A. Dallaire, "Targeting the Islamic State," *The Mitchell Institute for Aerospace Studies*, 14 April 2017, http://docs.wixstatic.com/ugd/a2dd91_4892807f169341188b7ebcd2f775671d.pdf; and Dave Majumdar, "Pentagon: ISIS Adapting to Air Strikes, Targeting Becoming 'More Difficult,' " *USNI News*, 11 August 2014, https://news.usni.org/2014/08/11/pentagon-isis-adapting-air-strikes-targeting-becoming-difficult.

20. Kristina Wong, "US Commander: Lack of Intelligence Assets Slowing Down ISIS War," *Hill*, 7 June 2016, http://thehill.com/policy/defense/282457-isis-air-war-commander-short-on-intelligence-assets.

21. Eric Schmitt, "U.S. Says Its Strikes Are Hitting More Significant ISIS Targets," *New York Times*, 25 May 2016, https://www.nytimes.com/2016/05/26/us/politics/us-strikes-isis-targets.html?_r=0.

22. Haroon Ullah, "Taking on the 'Digital Caliphate' in Our Fight Against ISIS," DIPNOTE: *US Department of State Official Blog*, 27 March 2017, https://blogs.state.gov/stories/2017/03/27/en/taking-digital-caliphate-our-fight-against-isis.

23. Max Sterling, "The Cyber Collective Threat: A Pack of Lone Wolf Terrorists," *The Project on International Peace and Security, Institute for the Theory and Practice of International Relations, College of William and Mary*, April 2017, http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Sterling.Max.pdf; and Dale Beran, "4chan: The Skeleton Key to the Rise of Trump," *Medium*, 14 February 2017, https://medium.com/@DaleBeran/4chan-the-skeleton-key-to-the-rise-of-trump-624e7cb798cb.

24. Brad Allenby, "Weaponized Narrative is the New Battlespace," *Defense One*, 3 January 2017, http://cdn.defenseone.com/b/defenseone/interstitial.html?v=7.5.0&rf=http%3A%2F%2Fwww.defenseone.com%2Fideas%2F2017%2F01%2Fweaponized-narrative-new-battlespace%2F134284%2F%3Foref%3DDefenseOneFB.

25. Sterling, "Cyber Collective Threat."

26. Adam Taylor, "Omar Mateen May Not Have Understood the Difference between ISIS, al-Qaeda and Hezbollah," *Washington Post*, 13 June 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/06/13/omar-mateen-may-not-have-understood-the-difference-between-isis-al-qaeda-and-hezbollah/?utm_term=.4718e23fe6f5.

27. Charlie Winter, "What I Learned from Reading the Islamic State's Propaganda Instruction Manual," *Lawfare*, 2 April 2017, https://www.lawfareblog.com/what-i-learned-reading-islamic-states-propaganda-instruction-manual.

28. Matthew Bondy, "Bad Bots," *The Project on International Peace and Security, Institute for the Theory and Practice of International Relations, College of William and Mary*, April 2017, http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Bondy.Matthew.pdf.

29. Gabe O'Connor, "How Russian Twitter Bots Pumped Out Fake News During The 2016 Election," *NPR*, 3 April 2017, http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election.

30. Tech Sgt Robert Barnett, "Goldfein: Future of War is Networked, Multi-domain," *US Air Forces Central Command*, 22 March 2017, http://www.afcent.af.mil/News/Article/1127569/goldfein-future-of-war-is-networked-multi-domain/.

31. CIA, "The Intelligence Cycle," *CIA*, 24 May 2017, https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html.

32. The Joint Staff, *DOD Dictionary of Military and Associated Terms*, 118, March 2017, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf.

33. Curtis E. LeMay Center for Doctrine, Development and Education, *Volume 1, Basic Doctrine: Flexibility and Versatility*, 27 February 2015, https://doctrine.af.mil/download.jsp?filename=V1-D82-Flexibility-Versatility.pdf.

34. Capt Jaylan M. Haley, "An Evolution in Intelligence Doctrine: The Intelligence, Surveillance, and Reconnaissance Mission Type Order," *Air & Space Power Journal*, October 2012, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-26_Issue-5/ASPJ-Sept-Oct-2012.pdf.

35. Ken Blackwell and Bob Morrison, "Like It or Not, War Is Interested in You," *American Thinker*, 23 April 2013, http://www.americanthinker.com/articles/2013/04/like_it_or_not_war_is_interested_in_you.html.

Col Shane P. Hamilton, USAF

Colonel Hamilton (MS, USAFA; MS, School of Advanced Air and Space Studies (SAASS), Embry-Riddle Aeronautical University; MS, Industrial College of the Armed Forces) is the deputy director of intelligence, Headquarters Air Combat Command (ACC). He has commanded at the squadron and group levels, led Joint Intelligence Fusion for US Forces Korea, and most recently served as ACC's director for the Intelligence Analysis, Targeting, and Collection Management Directorate. He is a graduate of the USAF Weapons School and the SAASS.

Lt Col Michael P. Kreuzer, USAF, PhD

Lieutenant Colonel Kreuzer (BA, USAFA; PhD, Princeton University; MPA, University of Alaska–Anchorage; MSI, American Military University) is the executive officer, ACC Directorate of Intelligence. He is a career intelligence officer who has served as director of special programs in counter-improvised explosive devices and collection management for Multinational Division North in Iraq, the intelligence staff officer of the Kapisa Provincial Reconstruction Team in Afghanistan, and chief of USAF Intelligence Officer Formal Training.

Semper Optiones: 21st Century Intelligence

COL David Pendall, USA

There is no American airpower, space power, land power, maritime power, or international political power without the knowledge provided by US intelligence professionals. Intelligence (INT) serves well today, but most importantly, needs to be better in the future. The thesis of this contrarian article is that technology has enabled, and always will enable, many different ways—options—to "do" intelligence. Consequently, we should continually seek better ways of "doing," organizing better structures for, and leveraging of new insights to plan, collect, analyze, synthesize, present, and use the data and information we call "Intelligence" today.[1] Intelligence now, in the United States, means the congressionally-endorsed organizational missions, authorities, and capabilities to collect data and information to produce insight and trusted judgment to government and military leaders and policy

makers in support of decisions and actions regarding national security and protection of US interests globally. The ideal is to understand everything, all the time.[2]

In plain language, this article argues that today's Intelligence technologies, processes, and structures are now, or may soon be, inadequate for the future. Plain language obviates the need to use many US Intelligence buzzwords and buzz phrases, the competing lexicons of "unified information theory," or picking sides in those bureaucratic or academic battles, though interesting and handy they may be. This argument begins with the obvious and ends with the contentious in the movement from upstream (where data is created and captured) to downstream (where it is converted, exploited, and enriched for decision and action). Most importantly, the article continues with the examination of significant implications for defense Intelligence processes, structures, security, and viability.

Upstream

Everything collected by any sensor upstream can be transformed directly or indirectly into zeros and ones downstream and then be progressively organized for processing, whether it is exquisite, phenomenologically-centered data, or data from multiple sources. Once processed, the collection can be analyzed and exploited for some purpose. The purpose may be as mundane as a business *predicting* what individual consumers have a high likelihood of purchasing or as elegant as *predicting* the location and behavior of "high-value targets:" individual terrorists, money launderers, or the wealthy "whales" upon whom the gaming industry depends. The business of Intelligence is the business of knowing. Premiums are placed on predicting behaviors and future operating conditions with high degrees of accuracy.

As for upstream collection, if it can be done by us, it is also being done by others (sometimes to us); with both good and bad intentions. Adversaries generally have the same ability to acquire and exploit the same commercially and publicly available data as the US. Here's a sample of what's available upstream:[3]

- full-motion video and electro-optic imaging from space, taskable with high periodicity (revisit), emplaced through multinational commercial investments
- environmental sensing and weather interactions affecting ground, sea, and air mobility and activities
- cyber transactions across the Open Web (internet), Deep Web (high-end commercial, industrial and academic exchanges), and the Dark Web (usually illicit and criminal transactions)
- online persona and behavioral graphing with resolution to the individual and internet protocol (IP) levels
- space-based collection and visualization of physical structures and city-scale assessments and characterizations for the insurance and risk assessment industries
- mobile smartphone transaction and location data supporting traffic pattern analysis, density graphs, behavior patterns, and current demographic flows

- social media sentiment and trending data based on issue, interest, and intensity, which can be further resolved to demographic segment and social status
- global interactions of distributed actors, devices, and affiliations based on IP connections and commercially-captured internet traffic, collected by manufacturers and sold to data brokers and marketing ventures, usually from application-based automated reporting (application programming interfaces). Internet of Things ([IoT] "smart" devices) reporting is also included.
- still image and video object extraction, recognition, and characterization, including facial recognition and database comparison matching, as related to internet-scale image and video posts—in near - real-time

YouTube, for example, ingests 400 hours of video every minute and distributes 5 billion hours of viewing content each month. YouTube does not just host the video, but scans it, characterizes it, stores it, and indexes it for many purposes.[4] Facebook and YouTube often contain exploitable data—evidence—of criminal, or other, activities we may need.[5]

The data exist. Exploiting it smartly is where the advantage lies in this decade and beyond. It is because of the beneficial or nefarious dual uses, reuse, and repurposing of the ever-expanding open-data universe that US Intelligence must learn to exploit it for predictive use—and at speed and scale. Operational success will depend on the creation of prescient intelligence at the velocity of data creation. The rules of the collection game are changing rapidly. To keep up with the changes requires a continuously adaptive Intelligence system to create knowledge out of data. This is the Intelligence-value proposition.

Useful information is becoming ubiquitous. The information collected and made available through direct sale, commercial data brokers, marketing venues, and social media is also held by the major data-capture corporations with analytical chops (Amazon, Google, Facebook, and Apple). These entities could train existing algorithms (artificial intelligence [AI] in its various manifestations) or craft new ones (deep learning) to answer almost every basic national security or defense question today. It has become an urgent matter of organizing this openly-available data for national security use. Exploiting and enriching it with the incomparable insights and knowledge that only US Intelligence and its partners possess, is part of the future value proposition.[6]

In today's world, the fact of the collection of these data, and as a result, exposing behaviors, relationships, and artifacts within these data, is inescapable. The concern of society, therefore, is more reasonably centered upon the **use** of the collected data—for good or evil—rather than the simple, inescapable fact of collection, and permanent archiving itself. Prevention or subsequent punishment of abuse and purposeful **misuse** of data, by governmental and nongovernmental entities, is where the societal concern should be. The sanctity of privacy and freedom in a world driven by the ubiquity of data and information on the individual is fundamental.

The logic of this model also holds that commercial and private entities may be much more adept, capable, incentivized, resourceful, and efficient in capturing and exposing data than any government entity. Therefore, the business of foreign intel-

ligence in the future will focus on the tailored assembly and synthesis of these globally-generated and available data (exploitation) for their intelligence consumers.

As we better understand, and begin to agree, that the information generated and commercially or publicly available today—a volume produced and stored digitally that is exponentially larger and richer than any in human history—the focus on information collection from solely government-developed, purpose-built, and "owned and operated" will diminish in overall merit and value.[7] We will move inevitably from an Intelligence culture dominated by vestigial beliefs and their associated behaviors reflecting information scarcity, excessive security, and a perceived disproportionate value placed on unique, singular contributions from large single-purpose workforces, INT bureaucracies and infrastructures, to one which embraces data abundance and a belief that "it's just data."

To exploit the upstream, the Intelligence culture will reflect a smaller, higher-end, integrated, and unified workforce, shared "back-office" services, and senior leaders who realize the profession ultimately exists to perform data synthesis and analysis, delivering meaning at the scale and speed relevant to decision makers and actors across all levels—tactical through strategic—simultaneously. The culture also must include public-private partnerships to further the development and exploitation of varied kinds of data; a pioneering pursuit presently being proposed by the National Geospatial-Intelligence Agency for geospatial information.[8]

In Transit

"In transit" has two aspects. The first aspect is the data moving downstream from sensor to a processor. The second, and profoundly affecting the first aspect, is the technological transit between now and the postquantum computing future. The logic of the model is that the three major entities pursuing quantum computing must be entities profiting from fast and increasingly accurate prediction: US Intelligence, on the one hand, but also the for-profit bodies like Amazon, Google, Facebook, and Apple on the other. (To murder a metaphor, the "third hand" is the academic and corporate communities that support the other two hands.) A major difference between the two hands is that Intelligence and their overseers are scrupulous and law-abiding: controlling the access and use of data in the best interests of national security. Commercial entities on the other hand—may not be as conscientious.[9]

Not all—read "only some of"—these forms of data and information require the same protection mechanisms that are currently afforded or were afforded in the last century to create competitive advantage. If the data in transit are encrypted, it may be an arduous and time-consuming process for a thief to render usable. If the data are unencrypted, theoretically any entity that can receive the data and immediately use the data. In the postquantum computing world, one may ask whether or not cryptography as we know it will survive. Our answer is "Yes, cryptography will

survive, but not as we know it." The issue raised here is a potential game-changer for all varieties of accessible data—at rest and in transit: US Intelligence may find it difficult to succeed in a world where the US is the fast second in quantum computing.[10] And that is second place in an unforgiving competition.

Downstream in Use

When the data arrive at the consumer and enter the consumer's associated processing workflows, the chore is to use it as rapidly as possible to discern changes and to make predictions. The further downstream use of the data is to comprehend the discerned relationships, and it is in understanding the patterns within the data that create competitive advantage. In business, uses include marketing-based information with the geospatial resolution of consumer patterns with retrievable buying and location histories, as one example. The data brokering of information on personal buying patterns and internet behaviors are bought, resold, and exploited in near- real-time for speculative action. Rarely do these business groups face mortal risks and consequences if their analysis is errant or their predictions are wrong. This is not so for intelligence professionals.

In intelligence, an army of people—subdivided into large and small groups, distributed globally (including aloft, afloat and submerged)—simultaneously need "just-right" information extracted from a mind-boggling mass of data every moment. The requirement to understand everything all the time begins with parsing the "everything" to focus on the sets of things—changes, movement, people, technologies, and so forth—that US forces and decision makers need to be knowledgeable of—right now.

Future Implications

In the future, the differences across Intelligence organizations should only be defined by the creativity and sustained pursuit of the advantage they can muster for their customer. The customer defines the end purpose or use (for good or evil) of information. The customer is agnostic to the original source and processing of single streams of unique data, much of which is losing its value as a distinct element. Simply stated, the source is irrelevant so long as the data is accurate. Single-source classified data, its legacy use, and its assessed value stemming from classified collection systems are rapidly being both rivaled and supplanted by an exploding universe of ubiquitous, commercially captured, common, and commoditized data.

For much of the emerging data, we do not yet fully understand its current value for defense intelligence or potential future uses. Before 9/11, we would not have associated anomalies of pilot training and one-way tickets. Similarly, we cannot fully develop smart insights among disparate data such as timber prices, cardboard boxes, and electronic product launches. There are insights to be educed. The value of collected and curated data, or its application, is difficult to predict. Some uses and analytic frameworks (tailored algorithms) have not yet been invented, and others already in use will evolve. As it evolves, the intense competition for data scientists and data curators will leave Intelligence and its supporting industry without

the full complement of the right human talent. How to hire, develop, compensate, and retain this type of talent must be addressed.[11] Perhaps outsourcing much of the workforce to a commercial firm with the ability to do this offers a solution. If so, Intelligence needs to rethink what its core functions and competencies really are in this century. We have moved from an industrial age to an information age, which requires new models for operating, teaming, and thinking that are dynamic to needs, time, and data creation. The industrial-age world was organized to perform linear processing and interrogation of hard-to-acquire, scarce data. In the twenty-first century's digitally integrated and dependent societies and nations—where quintillions of data bytes are generated daily—the processes must move from the linear to the nonlinear, commodity-based extractive model, and be as flexible and agile in this exploitation as is the dynamism of the emergent requirements and tempo of competition.[12] We often don't know what we need to know, until it is too late. We continuously incur global risks because of a lack of knowledge or understanding. In Intelligence, too many of our "analysts" are merely "processors" of data who are inadequately supported by insufficient automation. Worse, some parts of our Intelligence community seem satisfied with the status quo.

Technological Implications

The value created from data is centered on the conversion step that transforms it into an understood format. The transformation from a unique format to an enterprise-wide compatible and intelligible format is the point where a disproportionate value is created.[13] This point is where data can be of value to a wide range of applications. It is this step that commoditizes the data—placing it into the broader data universe, thereby allowing correlation, synthesis, pattern exploitation, and given the right algorithms, predictions.

Transforming signature data from discrete stovepipes and unique formats—understood by few—into commonly understood formats, across a data universe available to many, magnifies its value. Commercial data brokers and application makers know this and this is why data capture and marketing for future use and reuse are so lucrative. It is also one of the reasons that Amazon, Google, Facebook, and Apple trade at such high values: The *stored value* of that which they possess and the combinatorial potentials of what might be possible with such data. Technologies such as Blockchain and other distributed information and transaction security technologies, potentially contributing to creating this assured data universe for Intelligence, and further protected by quantum cryptography, may hold promise.

The material acquisition community (and defense contractors), military, and defense budget process managers, will need to adapt because this means an end to industrial-age procurement practices. This change disrupts current processes because it is not calling for large system procurements and programs to sustain "stuff"—sensors on platforms, multiple sea and air fleets, motor pools of ground platforms, maintenance shops, logistics, services, and so forth. This model is the opposite of that of the industrial era of mass and mechanical machines. Humans and machines communicating through algorithms is poorly understood and will initially be disruptive

to Intelligence. Nonetheless, recall the world leader who asserted that the control of AI would be crucial to global power?[14] AI control and quantum computing are our generation's race to the moon.

Organizational and Operational Implications

To the extent one believes Intelligence as a whole has made great strides under the leadership of James R. Clapper, had he continued to serve, he would have possibly continued to transform and integrate the Intelligence community.[15] To continue the transformation, as directed by its executive leaders, supported by its legislative overseers, and led by the US director of national intelligence, US Intelligence should be summoned to "start with the easy stuff:" organizing and centralizing the business processes of finance, acquisition, security, infrastructure, information technology architectures, and human talent management as the first steps toward dismantling "The Stovepipes" and recreating Intelligence. These modest business process reformations will be disruptive to some and gut-wrenching for many, but they are not only the barriers to exit from the present archaic and antiquated model (being kept alive by old laws and life support), but also barriers to entry into a revitalized model that puts analysis—and the human analyst—and human creativity at the forefront.

At the vanguard of the critical-for-differentiation-and-survival thrust in a new model, there needs to be an organizational blueprint that creates a data acquisition team, a data curation team, a data exploitation team, and a data visualization and distribution team apart from the existing phenomenologically-conditioned INT structure.

The data acquisition team is continuously scanning the information available and emerging from commercial and public sources and create the legal and practical mechanisms to bring these data or data accesses into the Intelligence architectures and workflows. The main consideration will be the data's use and relevance in supporting foreign Intelligence missions.

A data curation team is charged with reviewing and rating the internal qualities and veracity of the data itself, including its pedigree, source quality, and inherent flaws and use limitations under policy and legal statutes. Importantly, it is also the leader of the information assurance function.[16]

A data exploitation team should be empowered to design and create algorithms that deliver what lower- and higher-level analysts demand from their communications with the artificial intelligence in machines: knowledge of the present informed by the past and increasingly accurate predictions regarding the future. They should understand the flaws, implications, veracity, and composition of the data and data synthesis they create. A major component of the new organization's value will be its ability to create decision-quality information from smartly designed data models and algorithms (informed by domain team input) that work at enterprise/global scale and speed, producing competitively advantaged insight.

At the capstone, there needs to be a conscience: a data solution, process challenge, and innovation team. This team is the keeper of the current process/framework models and are also the "red teams," capable of and empowered to challenge

existing frameworks and the maturing data synthesis processes. While understanding and advocating for the organization's methodologies/tradecraft, they are simultaneously always looking for the outliers and "one-off" examples that current methodologies/tradecraft missed or insufficiently addressed. They thoughtfully challenge the existing views. They offer and build alternative models. Some models will be adopted and become the mainstay and some will be retained in hold status. The innovation component will be scanning the horizon for new data sources, emerging exploitation techniques, the creation of new best practices, and deeply evaluate the latest information science and technology trends.

All the teams—and their fixed and mobile elements, in the archaic terms of "forward and rear"—must be linked digitally and effortlessly into domain reference teams with depth and data on the history, economics, politics, demographics, ideology/culture, "military capabilities," and organizational behavior of other nations and rivals or potential rivals.[17] This group must be linked to the "conscience," engaged and contributing to the models helping humans discern and deeply understand "how things work" in the practical, physical, and human worlds.

There should be mutually supportive and explicit relationships among the domain reference teams and the data exploitation teams. Whenever the data exploitation team's views (or algorithms or results) diverge from the domain team's views (or algorithms or results), a deeper evaluation must be conducted to understand both "why" and also "how" to modify the algorithms that contributed. This evaluation is an especially important feedback mechanism to produce better insights and learning for the future performance of the organization and its ability to create meaningful and actionable knowledge—its central purpose. The logic of the model demands, multidata synthesis, and exploitation generate meaning and implications for decision and action. Single-data sources can complement or tip/cue data acquisition teams or data exploitation teams to adjust their acquisition or algorithms.

The workflows and familiarity of the production factory "task, collect, process, exploit, post" process must transform into an "access, synthesize, exploit" sequence. This sequence is tailored and decentralized, heavily dependent on domain awareness and team-based collaboration. It is not an industrial-age, assembly-line process or a linear assembly of resultant facts for a fixed report or product, but a synthesis of multivariate data and the tailored exploitation of meaning for a desired outcome and consequence that lives inside decision tools and the visualizations of future conditions. The interconnected world and the speed of interaction make it necessarily so.

Due to the complexity and the interdependence of people and things in the twenty-first century, there will be no single-source monopolies. All behavior creates a multitude of unique data (signatures) in the data universe. This data will either be directly sensed or enabled/made observable through correlated proxy data, providing the context, meaning, and implications. Finding the right signals in the noise of this man-made universe is dependent on the consumer's stated or discerned use of the data. It will vary as the needs of the consumer change, and the problem to solve is identified and clarified. Asking the right questions matters, correspondingly, to the qualities of the answers.

As far as the protection of the data itself—or the "fact" of collection—it exists and will in greater amounts and varieties whether we like it or not. It is, and will always

be, accessible to a wide variety of consumers, exploiters, brokers, or other entities (seeking to both good and evil). The very idea of "protection of sources and the collection capability" may not hold in the twenty-first century.[18] No longer will the protection requirements be in the form of protecting the fact of original collection, but must be applied to the intended and actual use of the data.[19]

Twenty-first Century Competitive Advantage

In this century, we have rediscovered, through aggregated data and the ability to find once hidden patterns and relationships in the data, that there are many interdependencies and signatures created simply from positive (or even passive) existence. We have also found that any single-sourced view into a phenomenon or activity is likely to miss more than it discovers or illuminates. That is why the twenty-first-century model must synthesize and exploit multivariate data from the points of collection earlier and faster in the workflows, assessed and expressed coherently, to orient the decision frameworks. Without this, decisions are likely susceptible to bias, deception, cumulative risk, and an artificial sense of certainty.[20] There is no 100 percent certainty in any man-made framework, but the old model is less capable of producing higher fidelity and veracity than the model for the near-future proposed here.

The goal is to develop a data acquisition and exploitation framework supporting a sense of reality that allows the organization to maintain a level of unrivaled competitiveness. This means a posture that surpasses the other competitors by supporting better decisions and actions at the tactical through strategic levels in a given field of competition. In a way, this is the twenty-first century OODA (John Boyd's "observe, orient, decide, and act") loop, enabled by the digitization of data (all zeros and ones). It is the observe phase that results from the collection of relevant digitized data, fed into organizationally tailored algorithms, processed into meaning (creating organizational orientation), and then fed into the decide and act frameworks. This phase is done at all scales and speeds, aggregated and disaggregated, continuously. This is less a schema to *predict* the future, although it will contribute, but rather one to help *create* the future. The future is created by providing the capabilities to navigate unfolding circumstances, wherein the winner maximizes competitiveness, the value of decisions, and the consequence of actions, while reducing risk and the chances of catastrophic failure or inexcusable setbacks (for a business and organization of the nation).

In our future, identifying the emergent need is essential for understanding at the speed of competition. To achieve this, the universe of data must be mined, exploited, synthesized, and presented at a speed and scale offering an advantage in decision and action, relative to actors who compete against us or are preparing to harm us. This—no harm—is the inescapable imperative. The need for an understanding of specific conditions, relationships, actor intent, and emergent potentials is what drives the clever data collection, extraction, and tailored assembly into useful insights that maintain our competitiveness. Clever means the ability to disproportionately or efficiently monetize, act, retain options, or otherwise smartly maintain an

advantage, whether these competitive behaviors occur in the market or for the national interest. That specific need for relevant data may be identified by a human—or more likely—an algorithm (human-built or, increasingly, machine-built) and will be occurring continuously and globally, at the speed of light (input-process-output-repeat). It may well be that Intelligence will get more value from commercially available information in the future than what it collects on its own today. The use of the commercially available data it accesses may create faster, more usable, and more important insights than Intelligence produces today.

The very idea of single INT supremacy or a single INT having a disproportionate influence or value in contributing to understanding is based on an industrial model and linear processing frameworks.[21] As with discoveries in investing, there are no single trend performance data across investment classes and assets that carry the day in making decisions. Collectible multivariate data generated from sensors capturing meaningful behaviors or "facts" of physical existence or "being" (location, material composition, dimensional properties, and so forth) will have strong correlations and tendencies to move together in ways that provide insight to those who are aware (and have the frameworks to create awareness). At the same time, there needs to be a set of data monitored in the same domain that is uncorrelated or has not followed the trends as another veracity metric, to balance the risk of taking too strong of a position (analytic judgment) on an unfolding set of circumstances or to reinforce the position (analytic judgment).[22] The most informative data sets balance correlations and trending across interdependent data streams to inform the decisions about what to do or how to act for advantage.

Since much of the data is generated by "social" interactions—whether it is the interaction of devices, machines, humans, or organizations—the creation of one's reality and the future is largely through the ability to integrate and interpret the data. One's view of the world becomes dependent on what information portals and personal interactions to which one has access. Whether one's world view is really an "echo chamber" or shaped by a refined and broadened set of inputs, it will still be subjective and limited. Objective truth for a human or an organization is a myth, which is not to trivialize the power of either faith or hope, while simultaneously rejecting the inappropriateness of myth, faith, or hope as lifelines for national security. Hence, the conclusion is that re-thinking our options for recreating, and then recreating Intelligence, would be a singularly valuable contribution to our national security. Even if we reject challenging today's structures and models, there are few forces beyond bureaucratic inertia that make it likely that the single INT, separate INT, structure will exist two decades hence.

Conclusion

Let's close with a thought from Edward Teller and a question for honest reflection. Teller observed that "The past is done. Finished. The future does not exist. It must be created microsecond by microsecond by every living being and thing in the universe."[23] We are cocreating the future of Intelligence, and hence US military and US global power, even as you read this.

The AI and quantum revolutions create the twenty-first-century arms race that is being pursued by our most capable adversaries. They will have no mercy in exploiting these arms and weaponized data, creating a future whereby our national security and elements of national power are undermined. Absent our recognition of this and a political will to make significant change ahead of this already unfolding curve, we will see our future disadvantaged. It is the fast-moving train we need to step onto, even if that means leaving some of our baggage behind. We know our adversaries are already ticketed and preparing to jump on (or are already traveling on) this train.

The reality of continuous co-creation begs a question to my sisters and brothers in the Intelligence profession—and to you, the ones whom we proudly serve. That is, "To what degree has Intelligence embraced the October 2004 summons to find ways of bringing *creativity and imagination* back into the Intelligence business and, more importantly, what more should we be doing?"[24]

Rest well, teammates. We never sleep.[25] ✪

Notes

1. The capitalized "Intelligence" refers to the apparatus and the product of present and future entities providing the information and insights essential for the preservation of our nation's security. The lower-case "intelligence" describes the activity of exploiting information for less lofty motives.

2. Our nation should choose better ways to understand everything all the time, not just because we can, but because we must. Some of these methods require learning from "intelligence" in business. Business intelligence is analogous although collection may be narrower, and the objective is to monetize insight.

3. A collection of capabilities regularly covered in industry and Intelligence open-source forums and public literature.

4. Armed Forces Communications and Electronics Association Europe Stockholm Chapter, "Google Federal Cloud presentation" (presented at the Technet Europe 2017 conference and expo, Stockholm, Sweden), 9 October 2017.

5. "According to a recent survey by LexisNexis Risk Solutions of more than 1,200 law enforcement professionals with federal, state, and local agencies. 83% of the respondents are using social media, particularly Facebook and YouTube, to further their investigations. More than two-thirds (67%) of respondents believe that social media helps solve crimes more quickly." John Patzakis, "Five Case Studies of Social Media Evidence in Criminal Investigations," *Next Generation eDiscovery Law and Technology Blog*, 16 November 2012, https://blog.x1discovery.com/2012/11/16/5-case-studies-of-social-media-evidence-in-criminal-investigations/.

6. Tailored insight, decision support, and enablement for consequential actions are the keys to providing intelligence value. Because of the artificial intelligence (AI) component of our future, China, Russia, and even well-financed transnational criminal organizations may possess nearly the same abilities.

7. Commercial entities currently seem better poised than the US government to collect and assemble big data. Consider: (1) how to protect/defend against the illicit use or adversary access/use, (2) how to prevent commercial entities from nefarious use or abuse, and (3) how does the intelligence community (IC) access this commercially created/collected data for national security? (Consider Apple: they are building their entire business on the sanctity of the personal data of their users. This is why they would not cooperate with the IC in accessing the San Bernardino, California shooter/terrorist's iPhone.) The author thanks COL Ron Corsetti, USA, for several key observations and suggestions throughout this article.

8. National Geospatial-Intelligence Agency (NGIA) Director Robert Cardillo made these remarks at the 2017 GEOINT Symposium, 5 June 2017, https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/GEOINT-2017-Symposium.aspx.

9. This was as demonstrated, for example, by the sale of advertising to US adversaries in the 2016 election and supporting the simultaneous concoction and dissemination of multiple fictions helpful to adversary interests, both of which must be judged as being less than conscientious. The judgment on entities like the Office of Personnel Management and Equifax is that they lacked the diligence to operate in a connected world of rivals.

10. Consider the protection of data at rest and the fragility of AI algorithms. An AI algorithm will only work well if the quality of the data can be assured. Otherwise, the algorithm will break. If the data is good in the first place, how can it be protected from accidental or purposeful corruption?

11. This would—because it must—include more clever and appropriate policies for duty location and flextime, geographic assignment, professional development, student loan payback, family leave, acceptance of diversity, and other human needs presently un- or under acknowledged. Worse, the multistovepiped Intelligence members may begin to "fight" with one another to acquire the same human talent.

12. More than 3.8 billion people interact on the internet daily and millions of self-synchronizing smart devices are added daily. These numbers are growing and in 2017 the data generated daily is measured in hundreds of "quintillions." The US alone generates more than 2.5 billion gigabytes per day. We will need to make up new measurements for the data by 2020. Tom Hale, "How Much Data Does The World Generate Every Minute?," *IFuc***gLoveScience*, 26 July 2017, http://www.iflscience.com/technology/how-much-data-does-the-world-generate-every-minute/.

13. Once a bit or byte moves from a form that can only be understood by a unique processor and is transformed into a format understood by a broader community of applications, machines, or humans, it has exponential value and use.

14. David Meyer, "Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World," *Fortune*, 4 September 2017, http://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/.

15. Robert Cardillo, who for the past three years has led the NGIA, probably has a better sense than most as to the "what comes next" for intelligence, having worked very closely with former Director James R. Clapper. Consequently, it would be prudent to developments in NGIA to anticipate what comes next. Among what is observable so far are: importing talent from other intelligence agencies and—more importantly—the world of commercial technology to fill high level NGIA positions; building and strengthening global military partnerships; creating formal and informal networks of commercial affiliates; rationalizing personnel policies and practices; creating an empowered organizational structures; prototyping products created only from open sources; expanding the intern program; creating a "Ventures" office to accelerate innovation; and, jump-starting computational thinking, coding, machine augmentation for analysts, and beginning to sortie into the world of AI.

16. If the data cannot be assured and protected from corruption, manipulation, and so forth, the artificial community will break or become unreliable.

17. Little today is effortless for the human analyst, and too much is brute force or manual workarounds to access and share enterprise data.

18. The counterintelligence functions include understanding how the data may be exploited, who is acquiring the data, and understanding adversarial data transactions. Both nation-states and nonstate actors (transnational and domestic) have the means to leverage much of the same data for their own uses and advantage.

19. The protection of data in the past was also related to the loss of value if it is compromised (we spent X during Y years to acquire it and its resultant data stream in world of information scarcity), and now that the unique source is compromised, we lose the source and any future value it could produce. Loss regret is also related to the "shame" factor—whereas, individuals or organizations would be shamed or embarrassed if the artifacts or knowledge of their behavior were made public, accepting that what does, or should, shame varies by culture and by generation within a culture or peer/reference group. Privacy was valued, transparency was a risk. The loss of individual or organizational privacy could mean lawsuits, prosecution, loss of status, liability for harm, or other penalties, not to mention the loss of trust. Also, these perceived negative consequences imply socially or could legally determine the behavior was not something acceptable in the social or legal frameworks within which the individual or organization operates. As far as the "cost" of compromise of a unique source when a target becomes aware of the collection capability or method and changes its behavior or institutes countermeasures—

that may still happen, however the multitude of commercial and other data collection existing reduces the overall value of unique sources and provides a wide variety of both direct and proxy data that illuminates the targeted entities activities, relationships, intent signals, and other strategically, though tactically relevant, data for decision and action. Even crowd-sourced, socially exchanged data will contribute to an understanding of threats or adversarial intent.

20. "Machine bias is human bias," according to Daniel Newman. *See* Newman, "Your Artificial Intelligence Is Not Bias-Free," *Forbes*, 12 September 2017, https://www.forbes.com/sites/danielnewman/2017/09/12/your-artificial-intelligence-is-not-bias-free/#5d879ef8c783.

21. As realists, we accept that some aspects of single intelligence capability will persist, much like the Panda's Thumb or the QWERTY keyboard. The National Reconnaissance Office (NRO)—a very large "office" indeed, self-described as a "hybrid organization consisting of some 3000 personnel"—for example, cannot conceive of a world without an NRO. Others can easily envision such a world. See http://www.nro.gov/about/nro/who.html.

22. The late Alvin Toffler cautioned that watching trends for their predictive power was inadequate since it may very well be that the countertrends are the ones that create history.

23. Air University, *SPACECAST 2020 Final Report* (Maxwell AFB, AL: Air University, 22 June 1994), http://www.au.af.mil/au/awc/csat/2020/monographs/process.pdf.

24. "National Commission on Terrorist Attacks upon the United States, *Report of the 9/11 WMD Commission* (Washington, DC: 9/11 Commission, 1 October 2004), 20,410.

25. As Tom Greco, G2 for US Army Training and Doctrine Command, remarked, "Actually we do, but AI doesn't have to!"

COL David Pendall, USA

Colonel Pendall (MS, Army Command and General Staff College; MA, Central Michigan University; BA, Ohio University) is the deputy chief of staff for Intelligence (G2), the senior intelligence officer for the US Army–Europe (USAREUR). He was commissioned in 1990 through the Ohio University Army ROTC Program. Colonel Pendall was also an Army War College Fellow at the Massachusetts Institute of Technology's (MIT) Security Studies Program in 2012–2013. Previous assignments include service with the 11th Armored Cavalry Regiment in Fulda, Germany; battalion and brigade combat team intelligence and security positions within the 1st Cavalry Division (CD); commander, Company A, 312th Military Intelligence Battalion (MIB) (Operation Joint Forge), Multi-National Division-North, 1st CD; officer-in-charge of operations and training, 741st MIB; strategic planner, National Security Agency, Signals Intelligence Directorate; Joint Staff strategic plans and policy planner, US Central Command Forward; intelligence planner and analysis and control element chief (ACE), Multi-National Corps-Iraq; USAREUR ACE chief, 24th MI Battalion/66th MI Brigade; USAREUR intelligence, surveillance, and reconnaissance plans chief, intelligence plans officer; North Atlantic Treaty Organization/International Security Assistance Force Joint Command Headquarters; senior intelligence officer, Combined Joint Staff Branch for Intelligence, Regional Command–East, concurrently serving as the 1st CD G2; and the Department of the Army G2 liaison officer with MIT Lincoln Laboratory. His deployments include Bosnia–Herzegovina, Qatar, Iraq, Turkey, and Afghanistan. The colonel's preceding assignment was commander, 66th Military Intelligence Brigade.

Air Mobility Liaison Officer Promotions: Perception and Reality

Lt Col Nicholas Conklin, USAF*

Our Airmen should continue to serve in joint positions, both on the staff and operationally, and capitalize on joint experiences, education and training. Our culture must value those who serve in these joint positions. We then must promote what we value and invest in Total Force Airmen who are joint warfighters.

—USAF Chief of Staff Gen David L. Goldfein,
"CSAF Letter to Airmen," 13 October 2016

*The author expresses his gratitude to key supporters of this research: Dr. Jeffery Weir for topic advice, feedback, and keeping him on schedule; Lt Col Brian Broekemeier for providing air mobility liaison officer (AMLO) background material and timely insight and assistance in topic development and solutions; Pamela Bennett Bardot for research assistance; and Lt Col Robert O'Keefe for invaluable insight into the current AMLO selection process and for his assistance and mentoring through the research process.

Introduction

General Goldfein's second letter to Airmen addressed the "important, timely, and worthy" issue of strengthening and addressing joint development of Airmen. Currently, air mobility liaison officer (AMLO) assignments present an opportunity for Mobility Air Forces (MAF) officers to "purposefully and systematically gain proficiency in joint warfare." Every rated officer in MAF does not need to be an AMLO, and there are many good reasons why a pilot or navigator may not want to volunteer for an AMLO assignment. However, the perception that an AMLO assignment negatively affects an officer's promotion opportunity likely prevents many officers from volunteering for an AMLO assignment. This article will provide a brief history of the AMLO program and explores the perception that an AMLO assignment negatively affects an officer's career advancement and determines if that perception is true.

AMLO History

Modern-day AMLOs can trace their origins back to the Vietnam War. The early stages of the Vietnam conflict saw a marked increase in airlift demand from the Army, with a corresponding need for close coordination.[1] While the USAF was able to meet much of this surge, the Army expressed dissatisfaction with the Air Force's ability to meet the Army's requests for rapid airlift. In mid-1966, Maj Gen (then Lt Col) Thomas M. Sadler proposed a solution to this problem. He recommended the Air Force experiment with temporarily assigning 30 airlift officers (mostly C-130 pilots) to various Army brigades and divisions on the ground in Vietnam. The original tasking for these men was to "be staff officers within the ground force unit, capable of planning and managing tactical air movements and resupply operations."[2] This experiment proved successful, and by mid-1967 the tactical airlift liaison officer (TALO) was a permanent billet assigned to Tactical Air Command (TAC) and located within Army divisions. Almost immediately, these men received praise from the Air Staff on the resultant decrease in rapid airlift response times and greater use of the preplanned airlift processes.[3]

After Vietnam, TALOs moved from TAC to Military Airlift Command (MAC). Here, TALO duties were expanded to include surveying drop zones, controlling airdrop operations, assisting with landing zone operations, joint training coordination, and exercise assistance. While under MAC, TALOs participated in many significant military events, including Operations Just Cause and Desert Storm. In 1992, after MAC was deactivated and Air Mobility Command (AMC) stood up, US Transportation Command agreed to establish a parallel program to support the US Marine Corps (USMC). In 2003, the TALO program merged with the AMC liaison officer program to become the new AMLO program, and AMC began allowing pilots and navigators with tanker backgrounds, including females, to serve as AMLOs.[4]

Since then, AMLOs have distinguished themselves in numerous conflicts including Operations Iraqi Freedom, Enduring Freedom, Inherent Resolve, and Freedom's Sentinel. AMLOs have also been active in a variety of humanitarian operations, including the Hurricane Katrina response, Operation Unified Response (the American response to the earthquake in Haiti and Operation United Assistance), and the US

Ebola response. In June 2015, the 621st Mobility Support Operations Squadron (MSOS) was activated under the 621st Contingency Response Wing.[5] This new squadron holds 49 billets for the AMC AMLOs embedded with 20 Army and USMC commands around the globe. While the majority of the Air Force's 63 AMLOs now fall under the 621st MSOS, an additional 8 AMLO billets fall under air support operations groups and squadrons in Pacific Air Forces and US Air Forces in Europe, and 6 additional AMLOs are stationed at nonoperational commands.

Problem Statement

Despite AMLO history and recent advancements within the community, a problem remains with real and perceived career progression issues regarding AMLOs. AMC's Deputy Chief of Staff for Manpower, Personnel and Services (AMC/A1) started tracking the promotion rates of prior AMLOs with the 2009 promotion boards. From 2009–2015, individuals who had previously served as AMLOs were promoted at a rate below their MAF peers.[6] According to AMC numbers, individuals who were AMLOs—or had previously served as AMLOs—had selection rates to lieutenant colonel below 52 percent (27 of 52 were selected for promotion). The promotion rates to major were similarly low for AMLOs. According to AMC, individuals with AMLO experience had a 73 percent promotion rate to major. This article seeks to investigate these low AMLO promotion rates, the perceptions that accompany them, and how much impact an AMLO assignment actually has on an officer's chances for promotion. To this end, two research questions must be answered: (1) Is there a perception in the MAF that an AMLO assignment will negatively affect career advancement? (2) Does having an AMLO assignment in your record affect your promotion opportunity?

To answer the first question, all 49 operational support squadron (OSS) commanders were surveyed within Eighteenth Air Force. This is an appropriate sample group because these commanders represent all major weapons systems in the MAF, have proximity to line flyers, possess influence in the assignment decisions of MAF captains and majors, and are required to mentor line aviators. If there are perceptions about the AMLO community in the MAF, it will be known by, if not originate from, these squadron commanders. These individuals were asked various questions about the AMLO career field using a combination of open responses, responses utilizing the Likert scale, and responses requiring rank-ordering.[7] The goal was to select questions designed to uncover any bias against recommending an officer to pursue an AMLO assignment. As such, Air Force Institute of Technology (AFIT) professors, senior Air Force leaders, current squadron commanders and various MAF instructor and evaluator pilots were all consulted during the question formulation of this survey. AFIT professors were consulted to ensure the survey met the academic standards required for this research. Senior Air Force leaders were consulted to ensure that the survey covered all of the issues surrounding AMLO assignments, and that the questions were at the appropriate level for squadron commanders. Finally, current squadron commanders (outside of Eighteenth AF) were

consulted to determine how the survey could be improved, and to ensure that the list of potential assignments was complete.

To answer the second question, data on all mobility pilots or mobility navigators in the Air Force during 1995–2015 were analyzed. The data were first focused to only look at individuals who pinned on major during 1 June 2000–31 July 2008, and individuals who ascended to captain from 1 January 2000–31 December 2008. Determining exactly what variables to use was an important consideration for this research. AMC publishes a Force Development Ribbon Chart for its officers to complete to see what career milestones have been met. The milestones that are on this document include whether or not an individual has accomplished the following items: Squadron Officer College (SOC), flight commander, main weapons system instructor pilot, boarded programs, executive aide, intermediate developmental education (IDE), and staff. Because AMC uses this as a barometer to see how mobility officers are progressing throughout their careers, these data points should give a statistically significant answer to how influential an AMLO assignment is in mobility officer promotions. Also, Capt James W. Bruns and Capt Lawrence A. Eichhorn found that age and commissioning source were significant predictors of promotion for Air Force Officers, and these two variables were included in the analysis.[8] Finally, because both pilots and navigators can and have served as AMLOs, an Air Force Specialty Code was used a variable.

A logistic regression of nonperformance factors was used to determine how much each plays into whether or not an officer is selected for promotion. A logistic regression analysis should show whether or not an AMLO assignment makes it less likely for an individual to be promoted and how statistically significant an AMLO assignment really is in determining promotion outcomes.

Limitations of Research

Before discussing the results of this research, it is appropriate to mention some of the limitations of the data in this article. First, and significantly, individual performance data were not available for review. This information includes officer performance reports, promotion recommendation forms (PRF), and training reports (TRs). TRs reveal officer performance in formal training, including distinguished graduate (DG) status. While AMC/A1 lists performance as the most important factor in promotion selection, the data analyzed consisted entirely of nonperformance factors.

Second, the data did not include promotion board results. Whether or not an officer made lieutenant colonel was determined by whether or not an individual was a major at the time of his board to lieutenant colonel, and whether that officer appears as a lieutenant colonel at any time in the records. Potentially, officers could meet their lieutenant colonel promotion board, make lieutenant colonel but separate before pinning on. While this would represent a small number of officers, there is a potential that this could affect the overall results.

Third, this research does not account for when specifically in an officer's career he or she serves as an AMLO. For example, when looking at promotion to lieutenant colonel, the data simply reflect whether or not an individual had served as an

AMLO prior to their primary lieutenant colonel board. However, timing may be a factor. An officer who does an AMLO tour as a young captain certainly pays different opportunity costs than an officer who serves as an AMLO as a senior major. While exploring the correlation of timing and promotion may be useful for future research, it was not explored for this article.

Fourth, this article defines career progression in terms of selection for promotion, appreciating that this is only one measure of career progression. This definition was also made clear to surveyed members. However, not everyone defines career progression strictly in terms of promotion. Other measures of career progression include school-select status, below-the-zone selection, selection for squadron command, and promotion to colonel or general officer.

Finally, the data analyzed do not cover any time period past 2013, and as such, do not account for the recent drop off of AMLO promotion rates. Specifically, from 2013–2015, only 38 percent (11 of 29) AMLOs were selected for promotion to lieutenant colonel (see table 1).

Table 1. AMC promotion data (promotion to major 2009–2014)

	AMLO				*MAF*		*AF*	
	Maj		*Lt Col*		*Maj*	*Lt Col*	*Maj*	*Lt Col*
2009	6/9	66.7%	2/4	50.0%	91.8%	72.9%	93.7%	74.0%
2010	7/8	87.50%	3/4	75.0%	85.7%	73.4%	89.1%	73.7%
2011	4/5	80.0%	4/5	80.0%	88.7%	71.4%	89.3%	75.3%
2012	2/6	33.3%	7/10	70.0%	86.7%	76.4%	88.9%	75.4%
2013	n/a	n/a	4/10	40.0%	n/a	71.0%	n/a	74.4%
2014	6/6	100.0%	3/8	37.5%	92.2%	69.9%	91.8%	67.0%
2015	n/a	n/a	4/11	36.4%	n/a	66.4%	n/a	72.0%
AMLO totals	25/34	73.5%	27/52	51.9%				

(Source: Derived from data sent to the author from Air Mobility Command Deputy Chief of Staff for Manpower, Personnel and Services (AMC/A1KO) and information retrieved from the AMC Rated Officer Force Development Roadshow, a presentation prepared by AMC/A1KO.)

Literature Review

The USAF has unique considerations in its promotion process. Research suggests that nonperformance indicators can effectively predict promotion results in the Air Force.[9] Bruns and Eichorn performed a regression analysis on nonperformance data for individuals promoted within the Air Force and found that among their criteria, SOC DG status, graduating from a service academy, being a pilot, and completing professional military education (PME) in-residence as all being positive and significant indicators of future promotion. Because there is no formal guidance on how promotion boards in the Air Force are to consider nonperformance criteria and because what the service values is continually evolving, these specific criteria may not still be relevant today.

It is worth examining the current (2016) qualifications required for an officer to be considered for an AMLO tour. The AMLO career field is governed by Air Force Instruction 13-106, dated June 2013, which has not been updated to reflect the recent creation of an AMLO squadron. This publication states that the basic qualifications for an officer to be an AMLO are: the "ability to authoritatively represent the Air Force, explain mobility systems. . . and capabilities to their supported unit." Further, it stipulates that officers need only be "qualified mobility pilots or navigators with airlift and airdrop experience highly desired." Despite, or perhaps because of, the lack of explicit requirements, AMC has decided to recruit to a higher standard. The *AMC Rated Officer Force Development Roadshow* presentation (2015) lists the qualifications for AMLO as: major weapons system (MWS) instructor, a score higher than 90 on the Air Force Fitness Test, and appropriate level of PME completed. This presentation also references the Rated Staff Allocation Plan (RSAP). The FY 2015 RSAP dictates that ALOs/AMLOs will be filled to between 95 and 100 percent before any additional rated staffs are filled. This makes AMLO assignments "must-fill" billets, which puts additional pressure on squadron commanders, AMC and Air Force Personnel Center staffs to fill these positions, regardless of "volunteer" status.

Finally, it is appropriate to briefly discuss the method used to analyze the promotion data. Because promotion is a binary variable (an officer is either selected or not selected for promotion)—and many of the nonperformance variables that determine promotion are either binary or categorical—an ordinary Least Squares Model will not sufficiently describe its characteristics.[10] In this case, a Linear or Logistic Least Squares Regression Model is a more appropriate method of analysis. Logistic regression is appropriate for describing and testing hypotheses about the relationship between categorical outcome variables and categorical predictor variables.[11] The logistic regression is based on the concept of the "logit" function (the natural logarithm of the ratio of probabilities of Y happening to Y not happening). The logit introduces the logarithmic function to the variables, which ultimately gives researchers the ability to apply linear models to cases with nonlinear outcomes.

Chao–Ying, Joanne Peng and others further stated that researchers should address the following information when analyzing and presenting a logistic regression: an overall evaluation of the logistic model, statistical tests of individual predictors, goodness of fit statistics, and an assessment of the predicted probabilities. The whole-model test in the SAS Institute's *JMP 8 Statistics and Graphics Guide* provides an overall evaluation of the logistic model, determining if the change in the independent variables has a statistical effect on the dependent variable. The extent of this effect can be seen in the p-value, where a p-value less than .05 shows a statistically significant difference.

The statistical significance of individual regression coefficients is best tested using the Wald Chi-square Test.[12] In this test, each variable and the intercept are tested for significance, and then evaluated, using its p-value. The p-value represents the probability of getting, by chance alone, a Chi-squared value greater than the one observed.[13] For variables, they are held to be significant if the p-value is less than .05.

Goodness of fit can be evaluated by looking at the area under the receiver operating characteristics (ROC) curve. The ROC curve plots the probability of detecting a true signal versus a false signal for the entire range of data.[14] To express the curve

as a single, scalable value, researchers use the area under the curve (AUC).[15] The AUC is a number between 0 and 1.0, giving the analyst an idea of how well the model predicts an outcome (The closer to 1.0 the AUC is, the better the model is at prediction, with .7 being the minimum of the acceptable region).[16]

Finally, researchers can use a confusion matrix to evaluate how accurately the model predicts the actual outcome. The confusion matrix (see fig. 1) displays the results in four categories: true positives (results that the model predicted to be true that were actually true), false negatives (results that the model predicted would be false but were actually true, false positives (results that the model predicted would be true but were actually false), and true negatives (results that the model predicted would be false and were actually false). To determine the accuracy of the model, the sum of the true positives and true negatives are divided by the total number of samples.[17]

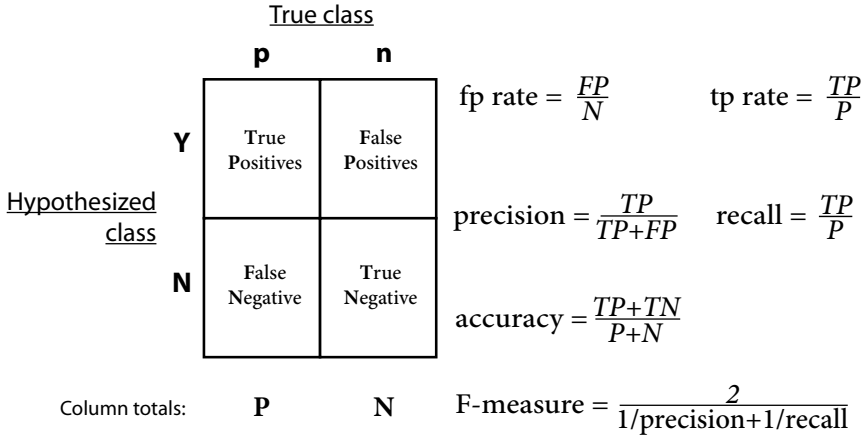


Figure 1. Confusion matrix and common performance metrics. (Source: Tom Fawcett, "An Introduction to ROC Analysis," Pattern Recognition Letters 27, no. 8 [2006]: 861–74, https://dl.acm.org/citation.cfm?id=1159475.)

Results and Analysis

The methodologies employed in analyzing the data revealed distinct answers to both research questions. The survey administered to 18th AF squadron commanders revealed a perception in the MAF that AMLOs do not enjoy the same career advancement opportunities as other mobility pilots and navigators. The analysis of the Air Force personnel data revealed that having an AMLO assignment in duty history is not a factor for individuals who are not promoted to either major or lieutenant colonel.

Survey Results

The individuals who responded to the squadron commander survey represented a broad cross-section of the MAF. Every major weapons system was represented, with 15 of the respondents being commanding officers within the airlift community (C-130, C-17, or C-5 aircraft), 12 commanding officers of the tanker community (KC-135 and KC-10 aircraft), and the remaining 3 members commanding operational support aircraft (OSA) (DV aircraft, including the C-21 and C-40) (see fig. 2). Interestingly, none of the respondents had previously been an AMLO or remotely piloted aircraft (RPA) pilot, but all other assignment types were represented by multiple individuals.

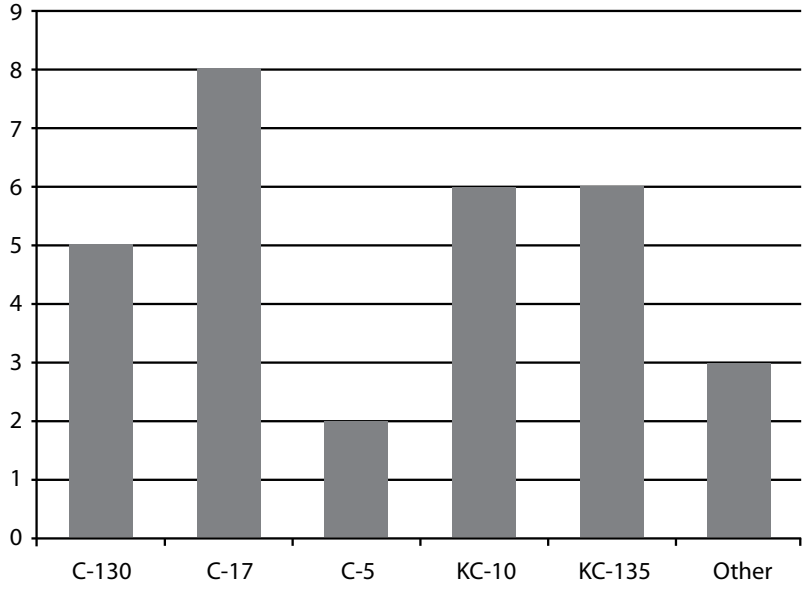


Figure 2. Primary aircraft of surveyed squadron commanders

Generally, respondents seemed to view AMLO assignments as valuable to the MAF. When asked to rank-order the different assignments generally open to MAF pilots and navigators at the captain and major level, the surveyed squadron commanders ranked AMLO as the sixth-best assignment for providing an officer with the best opportunity for professional development defined in the question as "deepen and/or broaden the individual's knowledge, skills, and abilities in the MAF and as an overall leader" (see fig. 3). Statistically, the possible responses divided themselves into three distinct categories. We can say with 90 percent confidence that respondents viewed AMLO, regional affairs specialist/political affairs specialist, Air Education and Training Command (AETC), and an additional operations assignment as better than OSA/VIP assignments and an RPA tour, but worse than the three Phoenix programs, USAF Weapons School Weapons Instructor Course (WIC), and a staff assignment, as these assignments relate to professional development.

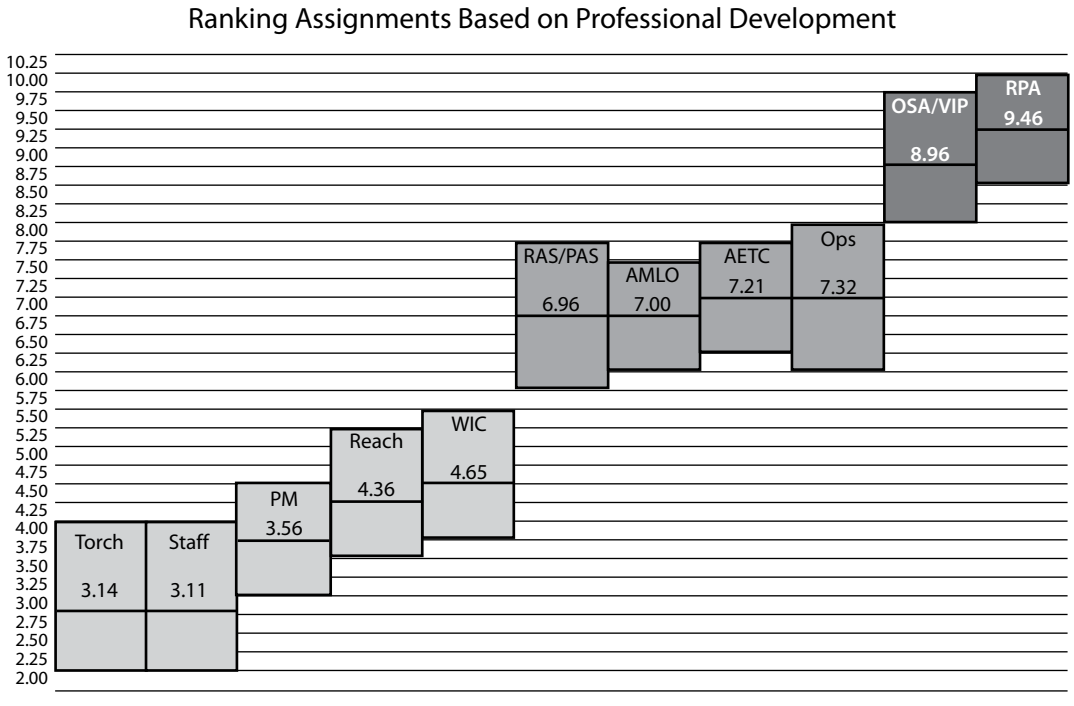


Figure 3. Ranking of assignments based on professional development

Further, 82 percent of respondents considered AMLO an effective use of rated officers, and only 10 percent of the respondents disagreed with the statement, "An AMLO assignment makes a mobility pilot/navigator a better officer and leader." These results show that MAF squadron commanders see value in the work that AMLOs do.

However, the survey results also indicate that squadron commanders feel that AMLO assignments do not benefit an officer's career progression. When asked to rank assignments in terms of which assignments make the officer more likely to be promoted to the next rank, the mean for AMLO assignments ranked 9 of 11. Again, the responses categorized into three groups. However, for this question, at the 90-percent confidence interval, it is now not possible to differentiate between AMLO and OSA/VIP and RPA assignments. The AMLO assignment dropped in relative value, revealing that respondents saw an AMLO assignment as having a greater benefit to professional development than to career progression (1.46 regression) (see fig. 4). Interestingly, all other assignment options stayed within .53 points except PM (1.10 improvement), Phoenix Torch (.9 improvement), and RAS/PAS (.68 improvement).

Further, when asked to respond to the statement that "an AMLO assignment hurts an officer's career development," only 20 percent disagreed (6 of 30 respondents) (see fig. 5). Finally, when asked how likely they were to recommend an AMLO assignment to a top performer in their unit (defined as the top one-third of his or her peer group), 66 percent (20 of 30 respondents) responded either "Not Likely" or "Would Not Recommend" (see fig. 6). The survey responses clearly show

that MAF squadron commanders perceive that an AMLO assignment is not good for an individual's career progression and promotion opportunities.

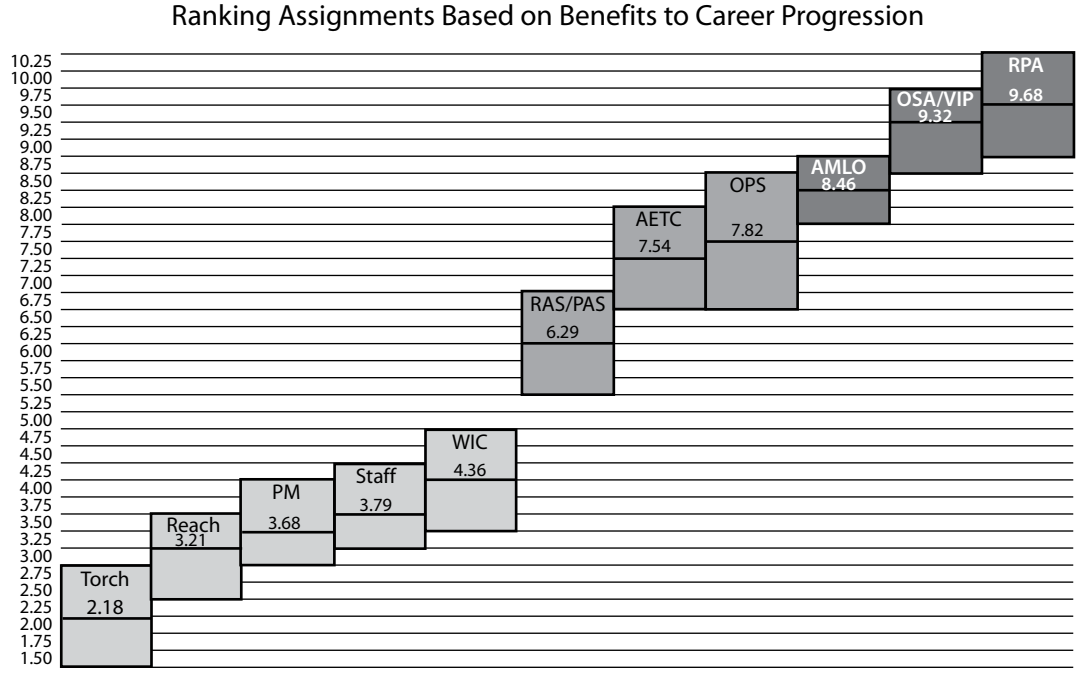


Figure 4. Ranking of assignments based on career progression

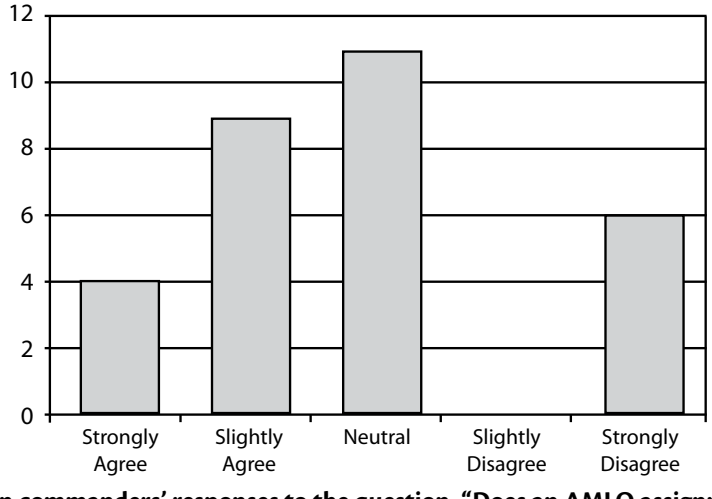


Figure 5. Squadron commanders' responses to the question, "Does an AMLO assignment hurt an officer's career development?"

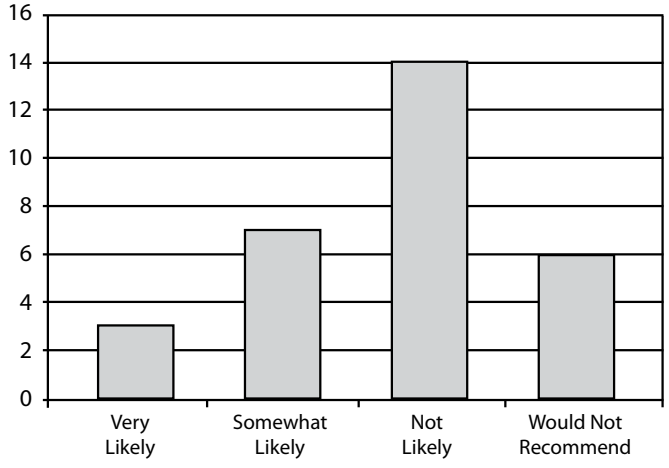


Figure 6. Squadron commanders' responses to the question, "How likely are you to recommend AMLO to a high-performing member of your squadron?"

Promotion Results

The analysis of the promotion results demonstrated exactly what influence being an AMLO had on whether or not a mobility officer was promoted. The analysis focused first on how having previously been an AMLO influenced whether an officer was not promoted to the rank of major (see tables 2–4 and fig. 7), and then whether having been an AMLO affected promotion to lieutenant colonel (see tables 5–7 and fig. 8). Both sets of results are presented in accordance with established standards: a whole model test was used to evaluate the overall model, a Wald chi-square test was utilized to evaluate individual predictors, the area under the receiver operating characteristic (ROC) curve was used to evaluate the goodness of fit, and a confusion matrix was utilized to assess the prediction capabilities of the logistic regression analysis. For both sets of data, the dependent variable was nonselections for promotion (1 = not selected for promotion; 0 = selected for promotion), to see what factors significantly affect an officer's chances of being passed over (not selected for promotion).

Nonselection to Major Model

The data show that most aspects of the major model suggest a good fit; however, the goodness of the fit test fell below the satisfactory level. The whole-model test (see table 2) shows that the model provides a significant improvement over the intercept-only model ($p < .0001$). Also, the Wald Chi-square test reveals that there are a number of statistically significant factors that influence who is not promoted (see table 3). Further, the Wald Chi-square test shows with certainty that AMLO is not a statistically significant factor ($p = .9323$). An analysis of the confusion matrix (see table 4) reveals that the nonselection for major model has an accuracy rate of 80.6

percent (3196/3963) in predicting who was and was not promoted to major. However, when evaluating the model's goodness of fit, this model only covered 68 percent of the area under the ROC curve (see fig. 7), which is just below an acceptable level of discrimination (.7).[18] This is likely attributed to the fact that performance is such a large factor in determining promotion to major. For promotion, performance is reflected by Distinguished Graduate status, officer stratification among peers, and recommendation for promotion on the PRF. None of these data were available for review, and it would appear that this information would provide a more accurate determination of who would and would not be selected for promotion to major.

Table 2. Whole-model test for promotion to major

Model	*-Loglikelihood*	*DF*	*Chi-square*	*Prob>Chi-sq*
Difference	147.18	11	294.36	<.001*
Full	1821.13	n/a	n/a	n/a
Reduced	1968.31	n/a	n/a	n/a

Table 3. Parameter estimates for promotion to major

Term	*Estimate Study*	*Error*	*Chi-square*	*Prob>Chi-sq*
Intercept	-3.31	0.983	11.35	0.0008*
Instructor as captain	-0.19	0.117	2.60	0.1072
AMLO as captain	0.03	0.328	0.01	0.9323
Evaluator as captain	0.32	0.096	10.92	0.001*
WIC as captain	1.78	0.393	20.48	<.0001*
Flt/CC as captain	0.52	0.084	38.58	<.0001*
Executive as captain	0.76	0.096	62.15	<.0001*
Pilot	0.61	0.145	17.91	<.0001*
USAFA	0.05	0.157	0.12	0.7293
ROTC	0.27	0.142	3.55	0.0594
BDE[a] in-residence	1.22	0.129	89.00	<0001*
Age	0.08	0.028	7.55	0.006*

[a]BDE-basic developmental education

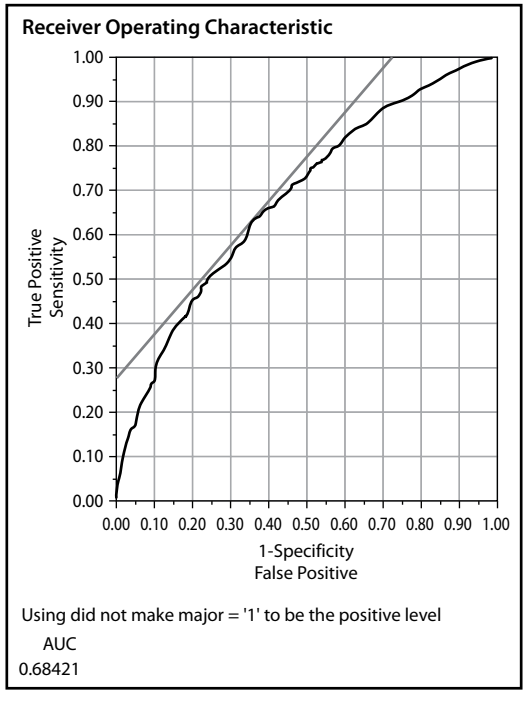


Figure 7. Area under the receiving operating characteristics for promotion to major

Table 4. Confusion matrix for promotion to major

	0	1
0	3132	49
1	718	64

Nonselection to Lieutenant Colonel Model

Next, the effect of an AMLO assignment on making lieutenant colonel was analyzed (see tables 5–7 and fig. 8). Overall, this model showed encouraging results in all four of the standardized tests. The whole model test reveals a good fit for the model (p-value less than .0001). This model again shows that there are numerous variables that are statistically significant in determining promotion to lieutenant colonel, and that AMLO is not a statistically significant factor ($p = .5322$). This model covered 90 percent of the area under the ROC curve (see fig. 8), giving it a superior level of discrimination. Finally, the accuracy of this model is at 87.9 percent (1934/2200). These results seem to show that nonpromotion to lieutenant colonel can be accurately predicted using the variables presented, and that the AMLO variable is not a statistically significant factor.

Table 5. Whole-model test for promotion to lieutenant colonel

Model	*-Loglikelihood*	*DF*	*Chi-square*	*Prob>Chi-sq*
Difference	682.78	13	1365.57	<.0001*
Full	766.92	n/a	n/a	n/a
Reduced	1449.7	n/a	n/a	n/a

Table 6. Parameter estimates for promotion to lieutenant colonel

Term	*Estimate*	*Study Error*	*Chi-square*	*Prob>Chi-sq*
Intercept	11.52	1.47	61.19	<.0001*
Evaluator	0.64	0.136	22.15	<.0001*
WIC	0.15	0.295	0.25	0.6161
Instructor	0.52	0.332	2.44	0.1182
Pilot	0.35	0.198	3.17	0.0749
Staff	0.73	0.138	28.30	<.0001*
Flt/CC	0.15	0.131	1.35	0.2449
Exec	0.79	0.141	31.19	<.0001*
AMLO	0.24	0.377	0.39	0.5322
USAFA	-1.24	0.221	31.34	<.0001*
ROTC	-0.65	0.199	10.72	<.0001*
IDE completed	8.29	1.02	66.12	<.0001*
IDE in-residence	2.76	0.475	33.80	<.0001*
Age	-0.52	0.029	327.13	<.0001*

Table 7. Confusion matrix for promotion to lieutenant colonel

	0	*1*
0	1320	66
1	200	614

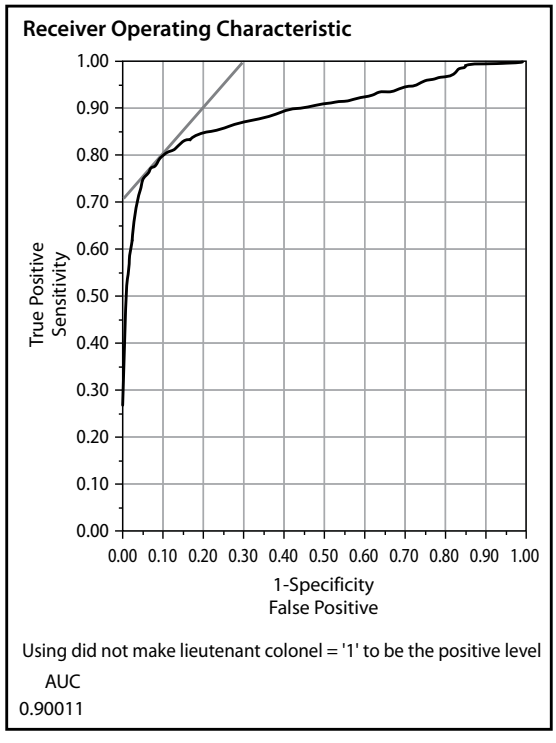


Figure 8. Area under the receiver operating characteristics for promotion to lieutenant colonel

Summary of Results

The survey data reviewed here clearly show that MAF squadron commanders see AMLO as an assignment with a negative impact to career progression relative to other assignment options. Only 20 percent (6 of 30) of squadron commanders slightly or strongly disagreed that an AMLO assignment hurt an officer's career development. Further, squadron commanders are unlikely to recommend AMLO assignments to their top performers. Clearly, there is a perception among MAF squadron commanders that an AMLO assignment is harmful to an officer's career. However, the promotion data analyzed do not support this perception. When promotion to major was analyzed, the data show that whether or not an officer had been an AMLO did not influence the likelihood that that individual was not promoted. Similarly, having been an AMLO did not influence whether or not officers were promoted to lieutenant colonel. This research collectively shows a perception among squadron commanders that an AMLO assignment hurts an officer's promotion potential, when in fact, the data show that having been an AMLO is not a statistically significant indicator of nonpromotion.

Recommendations for Action

Senior leaders have the opportunity to use this research to affect positive change. First, the mobility community should be educated that an AMLO assignment does not affect an officer's promotion potential. This information should be presented to all levels of MAF officers. First, sitting squadron commanders should receive this information to better mentor rated officers under their command. An excellent opportunity for this presentation would be the AMC Squadron Commanders Course. Also, junior MAF pilots and navigators who are potential AMLOs should receive this information. To simply show low promotion rates with no analysis drives a negative perception of the AMLO community. Education is the ideal way to eliminate the perception that having been an AMLO will make an officer less likely to be promoted.

However, education efforts by themselves are not enough. This research has shown that the lower promotion rates of AMLOs and former AMLOs are not because of the assignment. Mobility leaders should put policies in place to ensure that the officers selected for AMLO assignments are individuals who are most likely to succeed at the unique challenges of an AMLO assignment. This would include ensuring that potential AMLO candidates met minimum requirements (MWS instructor, worldwide deployable, no unfavorable personnel actions on record, eligible for a top-secret security clearance, excellent physical fitness scores, and PME completed, commensurate with rank), and that the MSOS commander was integral in the selection. There have been many successful AMLOs who were not selected for promotion to the next rank, and it would be unwise to base any criteria solely on increasing promotion rates. However, a list of requirements would present the AMLO squadron commander a point of departure and allow her or him to have a voice in the AMLO selection process. Giving the MSOS/CC a voice in AMLO selection based on a list of agreed-upon requirements would improve the community, since ostensibly that individual would know exactly what qualities would make for a good AMLO in the current operations tempo, and the requirements would increase the likelihood that future AMLOs are selected for promotion.

Finally, AMLO promotion rates would become a nonfactor if AMC began to offer incentives for individuals to become AMLOs. These incentives would offset, and eventually overcome, any negative perceptions of an AMLO assignment. Incentives available range from priority in follow-on assignment (including having AMLO outplacement reviewed by the MAF Developmental Team), to joint or staff credit, to raising the AMLO program to the level of other force development programs in AMC (Phoenix Reach, Phoenix Horizon, Phoenix Torch, and so forth). Each of these incentives comes with a trade-off, and it is valid to question if every program in AMC needs to be incentivized.

Conclusion

This article demonstrated that there is a perception that an AMLO assignment is detrimental to an officer's career progression, and that this perception is unsupported by data. The perception was uncovered through a survey of Eighteenth AF operational and OSS squadron commanders, asking them directly if they thought

AMLO assignments were detrimental to an officer's career progression, and indirectly by having them rank-order 11 assignments by how likely they were to advance an officer's career. The perception that AMLOs are promoted at a rate below their peers was shown to be false by examining the career advancement of mobility pilot and navigators of nine separate year groups. These data demonstrate that having previously served as an AMLO is not a statistically significant factor in predicting promotion, and that the lower AMLO promotion rates are because a number of individuals prone to not be promoted have served in AMLO positions.

General Goldfein expressed his desire that the Air Force should develop Airmen who can succeed in the joint environment, as this helps both the Air Force and the broader joint force. An AMLO assignment is one avenue that the MAF has to provide this development opportunity to its future leaders. An AMLO assignment immerses an officer with a sister service, often providing direct involvement with multiple joint task forces. However, partly because of a false perception, many officers either do not volunteer for these positions or are mentored to avoid them. MAF leadership should strive to correct this perception and continue to develop potential, current, and graduated AMLOs to ensure that future MAF leaders are "ready to provide the crucial airpower component and JTF leadership whenever and wherever needed."[19] ✪

Notes

1. R. L. Bowers, *Tactical Airlift: The United States Air Force in Southeast Asia* (Washington, DC: US Government Printing Office, 1982).
2. Ibid.
3. Ibid.
4. Air Mobility Command (AMC) historian, AMC 2003 History (Scott AFB, IL, 2003).
5. 1st Lt Jake Bailey, "New Chapter for AMC as AMLO Squadron Activates," US Air Force Expeditionary Center, 29 June 2015, http://www.expeditionarycenter.af.mil/News/Article-Display/Article/787939/new-chapter-for-amc-as-amlo-squadron-activates/.
6. Force Development Branch of the Personnel Division of the Directorate of Manpower Personnel and Services at Air Mobility Command emailed this information to the author in November 2015.
7. Rensis Likert, "A Technique for the Measurement of Attitudes," *Archives of Psychology* 140 (June 1932), https://legacy.voteview.com/pdf/Likert_1932.pdf.
8. Capt James W. Bruns, USAF, and Capt Lawrence A. Eichhorn, USAF, "A Comparison of Non-Performance Characteristics with United States Air Force Officer Promotions," (master's thesis, Air Force Institute of Technology, Wright–Patterson AFB:, 1993), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA273967.
9. Bruns and Eichhorn, "Comparison of Non-Performance Characteristics."
10. Daryl Pregibon, "Logistic Regression Diagnostics," *The Annals of Statistics* 9, no. 4 (July 1981): 705–24, https://www.jstor.org/stable/2240841?seq=1#page_scan_tab_contents.
11. Chao-Ying Joanne Peng, Kuk Lida Lee, and Gary M. Intersoll, "An Introduction to Logistic Regression Analysis and Reporting," *The Journal of Educational Research* 96, no. 1 (September–October 2002): 3–14, https://www.jstor.org/stable/27542407.
12. Peng, Lee, and Intersoll, "Logistic Regression Analysis and Reporting," 3–14.
13. SAS Institute Inc., *JMP 8 Statistics and Graphics Guide*, vols.1 and 2, (Cary, NC: SAS Institute, Inc., 2008).
14. Tom Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters* 27, no. 8 (2006): 861–74, https://dl.acm.org/citation.cfm?id=1159475.
15. Fawcett, "Introduction to ROC Analysis," 861–74.

16. Ibid., and Jesse M. Pines, Christopher R. Carpenter, Ali S. Raja, and Jeremiah D. Schuur, *Evidence-Based Emergency Care: Diagnostic Testing and Clinical Decision Rules* (Hoboken, NJ: John Wiley & Sons, 2012).
17. Fawcett, "Introduction to ROC Analysis," 861–74.
18. Pines, Carpenter, Raja, and Schuur, *Evidence-Based Emergency Care*.
19. Gen David L. Goldfein, USAF, "CSAF Letter to Airmen," *Air Force News Service*, 13 October 2016), http://www.afsoc.af.mil/News/Article-Display/Article/972444/csaf-letter-to-airmen/.

Lt Col Nicholas Conklin, USAF

Lieutenant Colonel Conklin (BS, USAFA; MPA, University of Illinois–Springfield; MS, Air Force Institute of Technology) is a senior pilot with operational experience in both the C-130 and KC-135. Lieutenant Colonel Conklin was previously an air mobility liaison officer with the 82nd Airborne Division and is currently the operations officer of the 906th Air Refueling Squadron, Scott AFB, Illinois.

Developing Air Force Field Grade Officers for Joint Leadership

Lt Col Daniel L. Magruder Jr., USAF, PhD

With the centrality of airpower in contingency operations, it is puzzling that more Airmen have not served in joint leadership positions throughout task forces and combatant commands. From Syria and Iraq to Afghanistan, partnered and enabled operations are catchphrases used to articulate current military action. The phrases are intended to capture the partnered, enabled operations the coalition is conducting against our enemies. Other than "train, advise, assist, and accompany" operations, American airpower has been the dominant form of direct influence in current military operations. For both, force finally counts. However, what our partners do on the battlefield is up to them to decide—a task for which American military ways and means are not ideally suited to directly influence. Critical warfighting functions that enable our partners' ground scheme of maneuver in current campaigns grind to a halt without airpower. These critical war-fighting

functions are: intelligence, surveillance, and reconnaissance (ISR) and target development, mobility of troops and material around the battlefield, combat search and rescue, medical evacuation, precision strike, and ensuring air superiority. Because Airmen already perform extraordinary heavy lifting in current conflicts, it is reasonable Air Force officers should gain experience necessary for joint, strategic-level leadership. The historical record shows otherwise.

The epitome of joint, strategic leadership is embodied in the command of a joint task force or a geographic combatant command. Even if the Goldwater-Nichols Reorganization Act was designed 30 years ago to foster joint-mindedness, many issues remain unresolved. The chairman of the Joint Chiefs of Staff (CJCS) commissioned a "Joint Forces Next" initiative which reviewed the training, education, and experience required to lead in the future. Gen David L. Goldfein, Air Force chief of staff, made joint leadership development a top priority and stated his intent is "that we can step in, and not only support, but lead any of those operations."[1] Other senior officers think the Air Force has a problem since "our best and brightest are able to offer only tired and uncreative strategies is not as important as what we need to do now."[2] While tides may have changed recently at the senior levels, in decades past, the Air Force has a troubled record developing joint force leaders.[3] Until 2013, the service that prides itself as "strategic" has only fielded seven combatant commanders since 1947.[4] Therefore, it could be productive to ask how the Air Force prepares field grade officers (FGO) for future joint leadership roles?

This article argues that the Air Force does not sufficiently develop FGOs for joint leadership roles.[5] It begins to explain why the Air Force needs—but has not developed—many FGOs who become leaders within the joint community. At field grade level, the net must be broadly cast because we cannot predict who will develop into joint senior leaders. This article does not cast blame outside the Air Force, but it does highlight internal challenges. It may be underwhelming to some, but it does not advocate for Air Force leadership of current operations. Instead, it is inward looking, meant to spur productive discussion within the Air Force about our institution's role in developing FGOs as joint leaders for the nation.

Does the Nation Need Joint, Strategic Air Force Leaders?

While some may argue that the nation is better served by drawing on the talent in the Air Force, many do not agree with this proposition. A reason why some may not envision themselves as leaders of the joint force is that the vast majority of conflict scenarios do not require Air Force leaders. In these scenarios, airpower does not contribute the preponderance of forces or effects but is employed as an enabling component to land power. Taken to the extreme, some advocate we abolish the Air Force entirely.[6] Far too often, the bar for a successful air campaign is set so high it cannot be met. Serious airpower advocates do not argue that an independent, strategic bombing campaign can bring about swift victory. By the same standard, ground power acting alone has had a grim record. No recent ground campaign has singlehandedly secured victory. Alternatively, even if the Air Force does not provide the preponderance of forces to a campaign, the air component may be providing the majority of the effects for the joint force commander. In this light, air, land, and sea

power are most effective at bringing about military and political goals if they work in concert.

National security is improved if all services are given a voice to add their perspective and, if qualified, opportunities to lead joint forces. This view recognizes the service as not just a force provider, but can put its best leaders forward to solve joint problems. Former Chief of Staff of the Air Force Gen Norton A. Schwartz stated "that [if] we don't fully use airmen in all joint war fighter roles, then it will catch up with us and our overall national security—sooner rather than later."[7] This has borne out in combat operations in the past. For example, before Operation Anaconda, the air component was largely excluded from planning until the final stages that resulted in the incomplete integration of airpower. Lt Gen David A. Deptula, a key air planner at the time, recalled that only three lines in the 145-page operations order addressed air operations.[8] Additionally, former Air Force Secretary Michael W. Wynne recognized that "When you don't have that Air Force general in command, you lose the air perspective over time."[9] JFCs facing operational problems can often influence the long-term institutional decision making of service chiefs. For example, wartime requirements articulated by combatant commanders of the post-9/11 world drove both the Army and Air Force to adapt in serious ways.[10]

This article advocates that only under certain circumstances should Air Force leaders be considered for joint leadership positions. This is congruent with the "most qualified" model for selection of joint leaders.[11] When faced with a crisis, contingency, or selecting combatant commanders, national leadership often looks to the most qualified candidates. What justifies the most qualified candidate depends on the context of the problem and background of the candidates. National leaders consider the types of problems facing potential commanders and select individuals accordingly. If this is the case, then the Air Force cannot complain if it does not privilege the development of individuals with requisite joint skills and experience. To be sure, it would be worse to place unqualified individuals in positions of leadership just for the sake of inclusion.

Regardless of one's position on whether the Air Force should produce joint leaders, it's understanding joint matters that makes better USAF officers. Whether a specialist or generalist in the Air Force, we must understand how our efforts contribute to a JFC's overall objective. A JFC is responsible for crafting a multidomain approach to achieve effects that facilitate a political end state. In terms of airpower effects, understanding the ground or naval scheme of maneuver will help Airmen optimize the tactical and operational design to meet the JFC's intent. Second, the structure and processes that guide the allocation and command and control of airpower need to meet the commander's intent. For example, in current fights more emphasis is placed on ISR and close air support assets. Interestingly, understanding how those ISR, strike, and mobility assets enable the political will and the ground scheme maneuver of our partners is a huge force multiplier. Precisely because they are predominantly terrestrial operations, a premium is set on the integration of airpower with coalition partner plans in Iraq and Afghanistan. To this point, CJCS Gen Joe Dunford, USMC, said: "The pace of our bombing is driven by the pace of operations of our partners. . . ."[12] This logic demands USAF officers have a basic grasp of joint warfare and how their actions tie into the ground scheme maneuver of partners.

Challenges in Developing Joint Leaders

Some may argue the Air Force is shut out of joint leadership opportunities. According to Gen Colin Powell, during his tenure as CJCS, it was not due to ill will.[13] A less parochial and more accurate argument is that national leaders select senior joint leaders based on the "most qualified" model. On this count, the Air Force has shied away from producing joint leaders. As recent as 2010, Wynne admitted the USAF would save "our 'A' people for the Air Force staff and the 'B' people for the joint staff."[14] This is corroborated by an earlier assertion by Col Phillip Meilinger, USAF, that: "The epitome for airmen was to be Chief or ACC (Air Combat Command) commander. . ." all else was ". . . table crumbs."[15] Besides a proclivity to centralize talent within service roles, the Air Force's current culture works at cross-purposes to building joint leaders. There are at least three reasons why the Air Force struggles to develop FGOs as joint leaders: (1) a service culture that prides itself on the particular and technical, (2) structural constraints, and (3) a bias for action over reflection.[16]

Tactical and Technical Focus

The Air Force privileges technical skills applicable at the tactical level. In terms of service culture, if one is asked "What do you do?," most will respond with a specialty such as pilot or intelligence officer. Tactical performance determines who gets promoted, but this may not translate into operational or strategic aptitude. For example, it is much easier to learn standard operating procedures in a known environment than it is to integrate those actions into a larger operation designed to elicit military effect for political purpose. This is because training is focused toward certainty. Realistic training puts individuals in simulated experiences to build pattern recognition and stress inoculation. However, the realm of operational planning deals with a multitude of unknowns that places the onus of being prepared for a wide range of scenarios. At higher levels of command, specific training will help marginally, but education and preparation for uncertainty will help exponentially.

A focus on the technical has its roots in many of the Air Force's institutions. The highly technical nature of service dictates an USAFA curriculum that emphasizes technical skills and engineering over social science or humanities. This is mirrored by USAF Weapons School instruction. By and large the curriculum is focused on training tactical experts, albeit with a culminating exercise, that integrates everyone. It is not until the final phase that the operational level of war is addressed, but they are single missions of increasingly difficulty rather than one scenario against an evolving enemy.[17] Fundamentally, the focus on technology and sound tactics is preeminent. At the Air Command and Staff College, "the service teaches 'people, processes, and products' that make up the Air Operations Center (AOC)."[18] To be sure, knowing the narrowly focused functions of air, space, and cyber within the AOC is important. However, there are disparities between a process-centric conception of air campaigning and activities that strive to achieve joint effects across all five domains.[19] The latter requires synchronizing effort in a campaign at the operational level of war.

A related issue is that technology employed tactically is a substitute for sound operational approaches. Former Air Force Chief of Staff Gen T. Michael Moseley, acknowledged "we risk being associated with—if not defined by—the material means of strategy, rather than its ends and ways."[20] To this point, airpower theorist Carl Builder admits that keeping "faith in ideas rather than things is difficult when institutions and resources are focused on things."[21] High-end technology is no substitute for strategy because "technical proficiency cannot substitute for an ability to analyze issues critically and apply every asset available to achieve a specific end in differing political and military contexts."[22] Strategic thinker Colin Gray himself admits, "It is paradoxical that air forces willing and able to expend billions of dollars on technical and tactical education typically devote a trivial amount to understanding what they do or might do strategically and why they are asked to do so by their political owners."[23] Operationally, this is borne out through the focus on optimizing complex processes.[24] Builder argues the Gulf War "was mostly a demonstration of operational and tactical virtuosity," and that because airpower is being applied to tactical ends "the strategic flame has dimmed."[25]

Structural Constraints

The second barrier to developing joint FGOs is structural constraints which limit USAF officers from gaining broad leadership experience. For example, when a typical Air Force lieutenant colonel is compared to an Army or Marines Corps peer, the latter has already commanded at least twice at the platoon and company levels.[26] However, it is remarkable to note that the average "fast-track" Air Force colonel (graduated wing commander) may, on average, command three times in their career—squadron, group, and wing levels.[27] At the same time, the equivalent Army colonel may have commanded at least four times in their career—platoon, company, battalion, brigade/regiment levels. Further restricting broadening opportunities, the Air Force has two colonel commands and requires less time to make general officer.[28] These factors combine to limit the breadth and scope of leadership experiences of potential joint leaders.

Although a generalization—both in garrison and deployed—USAF commanders do not exercise commensurate responsibility as joint force partners of the same rank. Anecdotally, some fighter squadron commanders in the F-22 and F-15C communities have between 20–35 people assigned—a vast majority of whom are officers. An average Air Force squadron numbers a couple hundred Airmen whereas an Army battalion can range from 5–800 soldiers. The size disparity drives a qualitative difference in scope between the two. Second, because of the size of a battalion, it requires a staff. This provides key developmental lessons to young captains and majors who work on those staffs to coordinate functions for the organization. Beyond disparities of scale, once an officer reaches the pinnacle of tactical leadership—wing command—there are more gaps.

It is not until the group or wing level that Air Force commanders actually command (organically) their own logistics support, communications, and sustainment on a truly large scale. Joint basing has made this more difficult for the Air Force to

develop experience in directing large organizations. For example, the fighter wing commanders at Elmendorf AFB, Alaska and Joint Base Langley–Eustis, Virginia only own the operations and maintenance functions while the remaining support functions report to a separate air base wing commander.[29] It should be no surprise then, that different command chains would set different priorities when addressing challenges facing service leaders at joint bases. Second, at the wing- and base-level, commanders start to interact with the surrounding community. This is too late in one's career to be expected to develop skills to interact with high-ranking civilians or partner nation leaders. Finally, because there are a limited number of officers on the operations/command track in the Air Force, it limits the pool of potential joint operational leaders.[30] All of these factors contribute to a shortage of officers who even have a chance of becoming a "most qualified" candidate for joint leadership opportunities.

Analytical Skills Required for Strategic Thinking

The final theme that cuts against the development of FGOs is a reliance on personal experience and intuition rather than reflection to guide decision making.[31] A bias for action over analytical deliberation is endemic to the military profession that largely shuns "independent thought and critical inquiry."[32] Lt Gen H. R. McMaster, USA, national security advisor, wrote that in terms of avoiding mistakes of the past "our record of learning from previous experience is poor."[33] Exercising sound judgement is the essence of decision making. Armed with strong critical-thinking skills officers can create fresh perspectives to address current challenges.[34] Gen John R. Galvin concluded the key elements to a developing strategic intellect are: "advanced schooling, operational experience, and lifelong development."[35] Writing is thinking because "the elements of good writing. . . bear a demonstrable relation to the powers of the mind."[36] Recognizing this, the Army has produced numerous scholar-warriors.[37] Many challenged the status quo in public forums to advance the national interest, and some knowingly and courageously imperiled their careers advocating policies to advance the national interest.

A symptom of a bias for action over reflection is the lack of Air Force officers debating strategic issues in a public forum. Serving as chief of staff, General Moseley said, "I see a need to increase the quality and quantity of Airmen's voices in the strategic debate."[38] Similarly, a group of senior strategists lamented the fact the Air Force "is arguably the most strategic service but lacks individuals making the intellectual arguments to support it."[39] Current trends are in contrast to the heyday of Air Force strategic thinkers such as Generals Billy Mitchell, Henry H. Arnold, Curtis E. LeMay, or much less known Glenn Kent and Nathan F. Twining. In the past two decades, the most prolific Air Force authors have been a lawyer, Maj Gen Charles Dunlap, and a more well-known air strategist, General Deptula. Before then, Colonels John Boyd and John Warden were thought leaders within the Air Force but outsiders based on temperament. Another symptom is a systemic devaluation of serving in academic instructor roles.[40] Again, this runs counter to the trend that 31 of 35 of the men who rose to become corps commanders in World War II taught at service schools at some point in their career.[41]

There are two main ways military officers improve their judgment skills: self-study or formal education. Historically, intellectual development was done on personal time.[42] A lifelong passion for self-study is the most common theme among all great strategists because ". . . development is progressive, with each level building on preceding levels."[43] While General Patton is recognized as the best fighting general of World War II, he only spent 13 months on the battlefield in combat with the bulk of his career spent "reading, for reflection, for prethinking the next phase of operations, and for writing a vast compendium of letters, diaries, speeches, and studies."[44] Modern air warriors think along the same lines. Maj Gen R. Mike Worden said: "Air strategists make time to study war—in the classroom, seminar, or conference—but mostly in a professional life devoted to self-study and reflection."[45]

The second way to develop an analytical aptitude is through dissimilar education such as civilian schooling or through fellowships in think-tanks and the interagency. The goal of dissimilar developmental experiences is to get officers comfortable with ambiguous situations. Ideally, officers build intellectual skills to make the uncertain more certain. A focus on inductive skills sharpens one's ability to discern what is conceptually at stake within a debate, build consensus, persuade with logic/evidence, and achieve outcomes that matter on the battlefield. Successful strategists can synthesize large amounts of data and understand the means and ends—which are skills directly linked with problem-solving.[46] Indeed, many claim dissimilar experiences exponentially increased their intellectual and professional growth.[47]

Success Stories

Despite barriers to Airmen becoming joint leaders, there are examples of Airmen who have become joint leaders. There have been at least seven Air Force combatant commanders since 1947. Confirming the assertions of the most-qualified model, USAF leaders have emerged when they have careers steeped in the required expertise. As of 2008, the Air Force has served in 21 of 71 opportunities to command JTFs.[48] From 1990–2009, just 17 percent of all JTF leaders were Air Force. However, these JTFs were decidedly noncombat-related.[49] As the RAND Corporation study found, "The 5 'combat' JTFs enforced no-fly zones (NFZs) in northern and southern Iraq and Bosnia and conducted an air campaign from Turkey during Operation Desert Storm."[50] As the record shows, the Air Force fares much better in functional commands such as US Transportation, Strategic, and Cyber Commands.[51] Even as the Air Force has not excelled in war-fighting roles, there are anomalies that bear special consideration. Lt Gen Brent Scowcroft (two-time NSA) and Gen Paul Selva (current vice CJCS) both received advanced social science education and spent more than a decade in the joint, interagency environment.[52]

A Modest Proposal for the Air Force

As depicted in the focus on core skills in the figure, prospective joint leaders should have consecutive building blocks throughout a career that develop a capacity to plan, prepare, and execute joint, combined arms across all war-fighting domains

and functions. In a career, officers are faced with a choice between remaining a functional expert within an Air Force specialty and broadening to become equally skilled at integrating joint combat power. If the USAF desires to develop strategic leaders, it must start early because the most precious resource in a career is time. The problem for the Air Force is that it must plant the "seed-corn" at the FGO ranks to build joint leader candidates. Three modest proposals are offered below to address the main challenges inhibiting the institution's development of leaders of the joint force.

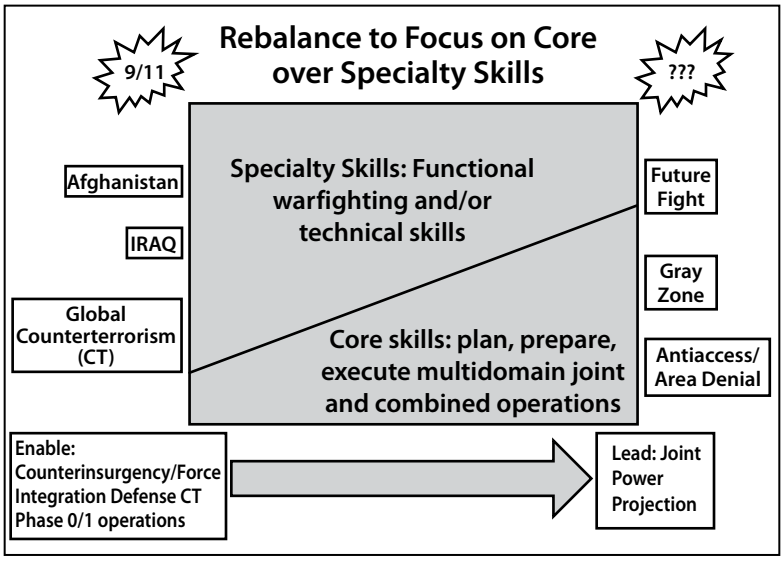


Figure. Paradigm shift from enabling to leading joint operations

First, the Air Force should slightly alter how it utilizes FGOs. Tactical officers should rightfully be focused on executing commensurate tasks. However, as officers are promoted to field ranks they should begin to integrate multidomain aspects into campaigning operations.[53] This distinction is on an officer's ability to shift away from specialty and functional war-fighting skills employed in particular situations toward core tasks used across the spectrum of conflict. Specialty and functional skills are specified by Air Force Special Code, which typically dictates a certain career path within a functional specialty. These types of capabilities have been extremely important to enable operations since 9/11 in Iraq, Afghanistan, Libya, Phase 0/1 tasks and, more broadly, global counterterrorism efforts. However, these tactically focused efforts may not necessarily translate into improving operational or strategic performance that's required in uncertain environments of the future: deterring aggression and malign influence, antiaccess/area-denial, or gray zone operations. These challenges require expertise to plan, prepare, and execute a wide swath of multidomain operations with joint, combined, and/or interagency partners. This does not discount the requirement to have technical and functional experts. However, it does require acknowledging that building and maintaining experts to enable joint operations is not

enough. To maximize contributions to national security, the Air Force should endeavor to develop experts in planning, preparing and, most importantly, leading the execution of joint operations.

Second, to address structural limitations, the Air Force could take a radically different approach to officer career paths. By selecting a career track around the 10-year mark, it could gain efficiencies to carve out time for specific development in desired areas. A new construct could offer one of three career tracks: USAF specialists, generalists, and joint-focused officers. Air Force specialists would not be on the "command track," but instead would be technical specialists focused on wielding technology and remaining the most tactically proficient air force in the world.[54] Second, Air Force generalists are the officers who have less interest in joint matters, but prefer to lead USAF organizations. This is largely the status quo in the Air Force and representative of those of who advance "up the organization" but not out as many specialists opt to do so. They would still serve in the requisite joint qualified assignments to gain breadth, but they would primarily lead Air Force formations. Finally, the smallest cohort of officers may opt into the pool of candidates to serve in a series of joint assignments. These are officers who may not be the Air Force specialist or generalist but will represent the perspective of airpower on joint staffs nonetheless. Doing this may allow the Air Force to focus efforts on a smaller, more manageable cross-section of future leaders to develop.

Finally, and equally important to the types of commands and assignments, is the type of educational opportunities that aim to develop intellectual competencies required for joint, strategic leadership. To the Air Force's credit, the School of Advanced Air and Space Studies produces strategists rather than planners but to maintain its quality of instruction must limit throughput. More opportunities should be given to USAF officers to gain the diverse education required to tackle uncertainty. In addition to learning the standard planning processes taught in professional military education, more one-year assignments to top-notch civilian graduate programs to study strategy, history, or international relations should be available. Indeed, the focus on improving inductive reasoning is a good balance to the deductive reasoning employed in planning doctrine.[55] In today's system, a small number of officers are afforded fellowships at civilian organizations, foreign schools, or opportunities to pursue advanced civilian degrees.[56] These opportunities should be focused in intermediate developmental education so the USAF maximizes its return on the investment.

One the one hand, as the Air Force orients itself to develop officers steeped in joint matters, it is a paradox that one cannot get the job without experience. On the other hand, one cannot get the experience without a job that builds joint credibility. To overcome this dilemma, the Air Force must intently develop a small cross-section of high performing FGOs for joint roles.[57] Only when the service creates a crop of individuals steeped in joint experience can they begin to be considered for commensurate leadership opportunities. An Air Force commitment to better prepare officers is not self-serving to the institution because it improves the service's contribution to national security in terms of offering capable, qualified joint leaders. However, this requires the Air Force be given opportunities to succeed. One way to gain trust and credibility is to seek first to understand joint force requirements and take steps to prepare officers to that end. Perhaps by focusing a small cohort to

learn to become the best teammates, we will, one day in the future, find some of our best officers leading the joint force. ✪

Notes

1. "Goldfein's Gambit: Former Air Force Chiefs Weigh in on His Ambitious Plans," *Air Force Times*, 18 September 2016, https://www.airforcetimes.com/2016/09/18/goldfein-s-gambit-former-air-force-chiefs-weigh-in-on-his-ambitious-plans/.

2. Brig Gen Scott Bethel, Col Aaron Prupas, Col Tomislav Ruby, and Col Mike Smith, USAF, "Developing Air Force Strategists: Change Culture, Reverse Careerism," *Joint Force Quarterly* (*JFQ*) 58 (July 2010): 83, http://www.au.af.mil/au/awc/awcgate/jfq/bethel_af_strategists.pdf.

3. A number of current general officers have held significant joint leadership posts: Gen Lori Robinson, commander, US Northern Command (NORTHCOM); Lt Gen Charles Brown, deputy commander, US Central Command; Lt Gen Scott Howell, vice commander, US Special Operations Command (SOC); and former commander, Special Operations Joint Task Force–Afghanistan; and Lt Gen James Vechery, deputy commander, military operations US Africa Command (AFRICOM).

4. Gen Lauris Norstad, Supreme Allied Commander Europe (SACEUR), 1956–62; Gen Joe Ralston, SACEUR 2000–03; Gen Douglas M. Fraser, US Southern Command (SOCOM) 2009–12; and Gen Phillip Breedlove, (SACEUR) 2013–16. NORTHCOM has had three Airmen as commanders: Gen Ralph Eberhart 2002–04, Gen Victor Renuart 2007–09, and most recently General Robinson. Notably, Gen Charles Holland served as SOC commander during the busy post–9/11 era. Similarly, there have been a small number of Air Force deputy combatant commanders: Gen James Jamerson, General Brown, and Lt Gen Timothy Ray.

5. Unfortunately, there is no definition of "joint leadership." See Dan McCauley, "Rediscovering the Art of Strategic Thinking: Developing 21st Century Strategic Leaders," *JFQ* 81 (March 2016): 28–29, http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-81/Article/702006/rediscovering-the-art-of-strategic-thinking-developing-21st-century-strategic-l/.

6. For this argument, see Robert Farley, *Grounded: The Case for Abolishing the United States Air Force*, (Lexington, KY: University of Kentucky Press, 2015).

7. Michael Hoffman, "Air Force Four-Stars Left Out of Top War Jobs," *Air Force Times*, (1 November 2010), 26.

8. Lt Gen Russell Handy, "Opening the Aperture. . . Ending Service Branding of US Unified Commands," (master's thesis, Air War College, 2003).

9. Hoffman, "Air Force Four-Stars Left Out," 26.

10. Rebecca Grant, "Why Airmen Don't Command," *Air Force Magazine*, March 2008, 48, http://www.airforcemag.com/MagazineArchive/Pages/2008/March%202008/0308command.aspx. Another example is the significant increase in drone combat air patrols.

11. Lt Col Howard Belote, USAF, "Once in a Blue Moon: Airmen in Theater Command," *CADRE Papers* 7, https://media.defense.gov/2017/Nov/21/2001847040/-1/-1/0/CP_0007_BELOTE_ONCE_IN_BLUE_MOON.PDF (Maxwell AFB, AL: Air University Press, 2000).

12. Andrew deGrandpre, "U.S. Troops Will Be Needed in Iraq after Mosul Falls, Pentagon Chief Says," *Military Times*, 10 January 2017, https://www.militarytimes.com/news/your-military/2017/01/11/u-s-troops-will-be-needed-in-iraq-after-mosul-falls-pentagon-chief-says/.

13. Handy, "Opening the Aperture," 2–4.

14. Hoffman, "Air Force Four-Stars Left Out," 26.

15. Grant, "Why Airmen Don't Command," 47.

16. For an overview and Air Force perspective, see Tom Ruby, "Flying High, Thinking Big," *The American Interest*, http://www.the-american-interest.com/2009/05/01/flying-high-thinking-big/. For Army perspectives see, Nate Finney, https://medium.com/the-bridge/anti-intellectualism-in-the-army-a802d98c3611#.n65y0y7q3, and Don Snider, "Whiskey over Books, Again? Anti-Intellectualism and the Future Effectiveness of Army 2025," *Strategic Studies Institute*, February 2016, http://publications.armywarcollege.edu/pubs/3333.pdf.

17. This is from the author's personal experience as a weapons and tactics officer. While Special Tactics did not have a "patch" program at the time, the author attended all academics phases in Class

2008–Bravo and facilitated multiple "mission employments" with combat controllers and pararescuemen in 2006 and 2007. Most recently, the author led a 108-Airmen element in the execution of ground special operations forces Vuls (flying windows) during the winter 2016 Weapons School integration.

18. Bethel et al., "Developing Air Force Strategists," 84.

19. Ibid., 84.

20. Gen T. Michael Moseley, "Airmen and the Art of Strategy," *Strategic Studies Quarterly* (*SSQ*) (Spring 2007): 15, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-01_Issue-1/Moseley.pdf.

21. Carl H. Builder, "Keeping the Strategic Flame," *JFQ* (Winter 1996–97), 83, http://www.dtic.mil/doctrine/jfq/jfq-14.pdf.

22. Ruby, "Flying High, Thinking Big."

23. Colin Gray, *Airpower for Strategic Effect*, (Australia: Military Bookshop, 2012), 27.

24. This is borne out in the focus placed on the Combined Air Operations Center at the operational level of war.

25. Builder, "Keeping the Strategic Flame," 80.

26. Admittedly, this article focuses on the operational Air Force specialties which are most likely to lead to joint operations, plans and policy, and joint command roles. Also, it is not reasonable to equate leadership of a typical operational Air Force aviation flight (which could number just a handful of officers) to a platoon that can average 40 personnel.

27. Some may argue that the flight is another level of command, but for many rated individuals—which this article focuses on for their potential to become joint operations and plans leaders—they do not supervise a large number of people.

28. Bethel et al., "Developing Air Force Strategists," 86.

29. It is also worth noting that these wings are small when compared to their service counterparts. The 1st Fighter Wing has about 1,000 members.

30. According to the Air Force Personnel Center, there are 12,681 pilots and 3,285 navigators. These groups account for roughly 25 percent of the total officer strength of the Air Force. These Air Force Specialty Codes predominantly make up the officers the types of officers who advance up the operations/command track in joint assignments. See http://www.afpc.af.mil/Air-Force-Demographics. On the other hand, the Army has about 82,000 officers, 40 percent of who are in operations jobs. See FY 2014 data at: http://www.armyg1.army.mil/HR/demographics.asp. While this may contribute to a disproportionate Army representation in joint commands, it cannot fully account for why and how Army leaders historically outnumber other services in top joint posts.

31. Maj Gen Robert Scales, "Too Busy to Learn," *Proceedings*, US Naval Institute, February 2010, 32. For an Air Force perspective, see Col Tomislav Z. Ruby, "The Impact of Anti-Intellectualism in the US Air Force" (PhD diss., Air University, n.d.), bgcts.com/wp-content/uploads/2015/02/bgcts_usafantiintellectualism.doc (site discontinued).

32. Greg Foster, "Research, Writing, and the Mind of the Strategist," *JFQ* (Spring 1996), 112, https://wss.apan.org/s/JSOFUN/Shared%20Documents/WriteAndRead/Research_Writing_and_the_Mind_of_the_Strategist.pdf.

33. Lt Gen H. R. McMaster, "The Pipe Dream of Easy War," *New York Times*, 20 July 2013, http://www.nytimes.com/2013/07/21/opinion/sunday/the-pipe-dream-of-easy-war.html.

34. Bethel et al., "Developing Air Force Strategists," 88.

35. Gen John R. Galvin, "What's the Matter with Being a Strategist?" *Parameters* 19 (March 1989): 2–10, https://pdfs.semanticscholar.org/7986/16b51c46ad816a324900e05303ce0fc9e15f.pdf.

36. Foster, "Mind of the Strategist," 115.

37. For example, Generals John R. Galvin, William E. Odom, David H. Petraeus, H. R. McMaster, Daniel P. Bolger, Robert H. Scales and a cohort of nonflag officers in Andrew Krepinevich, Andrew Bacevich, John Nagl, and Paul Yingling.

38. Moseley, "Airmen and the Art of Strategy," 15.

39. Bethel et al., "Developing Air Force Strategists," 83.

40. Unless instructing at the USAF Weapons School, academic billets are not typically command track career choices.

41. Scales, "Too Busy to Learn," 32.

42. The list of war fighters in history who could also be categorized as intellectually curious or voracious readers is impressive: Generals Winfield Scott, Ulysses S. Grant, Fox Connor, Douglas MacArthur, George C. Marshall, Dwight D. Eisenhower, George S. Patton—and most recently, Secretary of Defense James Mattis.

43. George Forsythe, "The Preparation of Strategic Leaders," Fort Belvoir, Defense Technical Information Center, 1992, 44, http://www.dtic.mil/dtic/tr/fulltext/u2/a528179.pdf.

44. Roger Nye, "Whence Patton's Military Genius," *Parameters* 21 (Winter 1991–92): 60–73.

45. Maj Gen Mike Worden, "Developing Twenty-First-Century Airpower Strategists," *SSQ* (Spring 2008), 23, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-02_Issue-1/worden.pdf.

46. Bethel et al., "Developing Air Force Strategists," 88.

47. Barak Salmoni, Jessica Hart, Renny McPherson, and Aidan Kirby Winn, "Growing Strategic Leaders for Future Conflict," *Parameters* (Spring 2010), 78, http://ssi.armywarcollege.edu/pubs/parameters/articles/2010spring/40-1-2010_salmonietal.pdf . The following officers benefitted from service-supported civilian education: Generals Peter W. Chiarelli, Martin Dempsey, John Galvin, and David H. Petraeus; Admirals Michael Mullen and James G. Stavridis; Lt Gen Dan Bolger and Lt Gen H. R. McMaster; and Maj Gen Robert H. Scales. General Petraeus proposed six benefits of civilian graduate school: it forces you to move out of an intellectual comfort zone, increases appreciation for diverse and divergent views, exposes yourself to a huge range of topics and knowledge, develops oral and written communication skills, improves critical thinking skills, and imbues intellectual humility. See General Petraeus, "Beyond the Cloister," *American Interest* 2, no. 6 (July 2007), https://www.the-american-interest.com/2007/07/01/beyond-the-cloister/.

48. Grant, "Why Airmen Don't Command," 46–47.

49. Of the 15 Air Force–led JTF headquarters, four were humanitarian relief operations, two were to help evacuate noncombatant evacuees, and four provided support to other forces. See Michael Spirtas, Thomas Young, Rebecca Zimmerman, *What it Takes: Air Force Command of Joint Operations*, (Santa Monica, Ca: RAND, 2009), 10–11.

50. Ibid., 10–11.

51. For example, Gen Darren W. McDew is the current commander of US Transportation Command.

52. Lt Gen Brent Scowcroft did not serve as the national security advisor twice by accident. His biographer cites many of the same themes that contribute to joint, strategic leader success. General Scowcroft was widely reputed as a consensus builder who tackled problems in a no-nonsense manner, held numerous posts well outside the Air Force norm, and was deeply intellectual (an intelligence officer, completed a doctorate from Columbia University, and taught political science at the USAFA). See Bartholomew Sparrow, *Strategist: Brent Scowcroft and the Call of National Security* (New York: Public Affairs, 2015). The second individual is a contemporary leader, the vice chairman of the Joint Chiefs of Staff, Gen Paul Selva. General Selva spent the bulk of his career as a functional specialist while serving in Air Mobility Command and eventually commanding US Transportation Command. In terms of professional military education, after graduating from USAFA with a degree in aeronautical engineering, he completed two social science degrees. However, General Selva spent two years as a field grade officer (FGO) in the Office of Net Assessment and then more than five years split between US Transportation Command and the Joint Chiefs of Staff as a general officer. With almost a decade of service in joint commands, General Selva is an example of how the Air Force's functional specialists can serve at the highest levels in the joint community.

53. In fact, promotion from company grade officer to FGO is the historical distinction from focusing on tactical tasks to integration of many elements of combat power by coordinating through staff actions.

54. This is already informal with the Guard and Reserve force or individuals who voice this desire as their intention.

55. This is an extremely important point. On the one hand, planning military operations is heavily influenced by key facts and assumptions that are givens based on the policy preferences of civilians or senior military leaders. On the other hand, inductive reasoning is more likely to lead to creative approaches because it may challenge the very assumptions upon which these arguments are made. For example, if military planners make strident arguments about the efficacy of military force in certain situations it may obviate negative unintended consequences. It is probably naïve, but this is exactly the type of moral courage and intellectual environment needed to advance national interests.

56. This is currently done primarily through faculty development programs at the USAFA and the USAF School of Advanced Airpower Studies. However, it is very difficult for those who serve as faculty at those schools to compete with their peers who remained steeped in the operational world.

57. This assumes the appropriate personnel actions are taken to systematically manage and reward individuals identified as future joint leaders.

Lt Col Daniel L. Magruder Jr., USAF, PhD

Lieutenant Colonel Magruder (BS, USAFA; MA, American Military University; MA and PhD, University of Chicago) is the commander, 22nd Special Tactics Squadron, Joint Base Lewis–McChord, Washington. He has led special tactics forces during Operations Enduring Freedom, Iraqi Freedom, Willing Spirit, Freedom's Sentinel, and Inherent Resolve. Lieutenant Colonel Magruder has served as a weapons and tactics officer, as well as in a variety of joint staff positions at Special Operations Command (SOC), Central. He has numerous publications, including most recently the book, *Counterinsurgency, Security Forces, and the Identification Problem: Distinguishing Friend from Foe*. Lieutenant Colonel Magruder is currently deployed, serving as chief of staff, Combined Joint Special Operations Task Force–Syria serving in a deployed, joint position as commander, SOC Command and Control Element, northwest and southern Syria (SOCCE-NWSS). SOCCE-NWSS is responsible for a battalion-sized element that commands and controls vetted Syrian opposition.

The Elements of an Effective Squadron: An Air Force Organizational Study

Maj Jason M. Newcomer, DBA, USAF*
Lt Col Daniel A. Connelly, PhD, USAF, Retired

During the past two decades, the US Air Force has reduced squadron-level support functions, manpower, and appropriations to cut costs through consolidation at higher organizational levels. In 2016, Chief of Staff of the Air Force (CSAF) Gen David Goldfein identified "revitalizing the squadron" as his number one priority during his four-year tenure. According to the CSAF, the squadrons—and similar support entities—are the foundational organization in the service.[1] They provide the appropriate level of leader-to-Airman ratio, setting, and tactical focus to

*The authors would like to extend a sincere thank you to the 30 graduated squadron commanders who dedicated their time to participate in this research. Additionally, the authors appreciate the Air Command and Staff College research department, the Air University research oversight office (ROO), and the US Air Force ROO for their assistance during the approval process of this study.

foster the most nourishing environment for personal and professional development, esprit de corps, and mission excellence.

Problem Statement

According to Air Force Instruction (AFI) 38-101, *Air Force Organization*, "squadrons are the basic building-block organizations in the Air Force, providing specific operational or support capability."[2] Since the implementation of the Budget Control Act (BCA) of 2011, US defense spending was decreased and congressionally frozen for three years from 2013–2015.[3] The frozen spending levels, which did not account for inflation, reduced the DOD's purchasing power to an equivalent of the 2008 budget.[4] Although the funding crisis impacted organizations throughout the DOD, many of the problems directly affected squadron-level operations. Reduced manning, increased Airmen stress, consolidated functions, and degraded training are some examples. Despite the foregoing challenges, many squadrons in the Air Force continue to receive "effective" and "highly effective" inspection ratings, and many Airmen claim to have come from "great squadrons." The specific problem explored during this research was the identification of the elements of organizational effectiveness in squadrons that made them effective, even in resource-constrained times.

Purpose Statement

The objective of this qualitative phenomenological study was to explore the experiences of graduated squadron commanders to identify organizational conditions that lead to effective squadrons. Several benefits emerged from this research:

- This study provided empirical evidence of best practices for current and future commanders to consider for implementation.
- The results of this research can increase the quality of education in professional military institutions that teach command and/or leadership.
- The study identified problem areas Air Force senior leaders can focus at the squadron level as part of the ongoing effort to revitalize the squadron.

Research Questions

The following research questions guided the exploratory study:

1. What conditions or activities impact squadron effectiveness?
2. What future research can positively impact squadron effectiveness?

Methodology

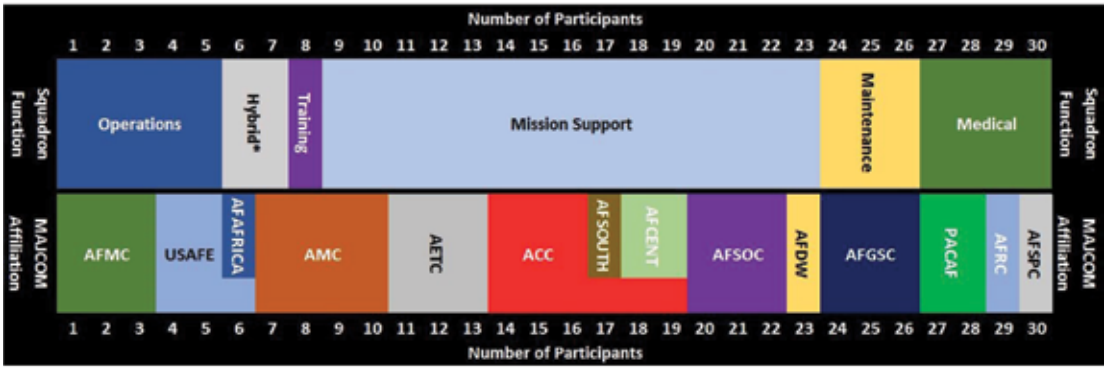
Method and Design

To obtain the depth of knowledge necessary for the research questions, a qualitative phenomenological research method and design were most appropriate. The

qualitative method allowed for the depth necessary to understand the frequencies that occurred in the research.[5] The phenomenological design provided a framework for exploring the experiences of each graduated squadron commander.[6]

Population and Sampling

To obtain the specific sample of graduated squadron commanders and to ensure a diverse demographic that represents the USAF population, a purposeful sampling method was most appropriate for the research. Following approval from the USAF research oversight office (ROO), Air Command and Staff College and Air War College students and faculty with recent squadron–command experience received email invitations. Although the sample was recruited from one location, they all relocated from various career fields and major commands as depicted in Figure 1. The sample (n = 30) met qualitative research rigor requirements, which typically range from 6–30 participants.[7] We found it important to maximize the sample to obtain the richest data for analysis in the study.



Major Command (MAJCOM)
Air Force Materiel Command (AFMC)
US Air Forces in Europe (USAFE)
Air Forces Africa (AFAFRICA)
Air Mobility Command (AMC)
Air Education and Training Command (AETC)
Air Combat Command (ACC)
Air Forces Southern (AFSOUTH)
US Air Forces Central Command (AFCENT)
Air Force Special Operations Command (AFSOC)
Air Force District of Washington (AFDW)
Air Force Global Strike Command (AFGSC)
Pacific Air Forces (PACAF)
Air Force Reserve Command (AFRC)
Air Force Space Command (AFSPC)

Figure 1. Sample demographics**

* Hybrid squadrons are those with cross-functional mission areas (as in air base squadrons, air advisory squadrons, and so forth).

** Function and MAJCOM numbers do not align. Participant number one was not an operations commander in AFMC. The figure only reflects frequencies (as in five operations commanders and three AFMC commanders).

Reliability and Validity

We ensured the reliability, or the consistency of the data, by using an interview protocol that was vetted through the Air University and USAF ROO offices. The protocol served as a checklist for consistent interview questioning and data collection. Participants were then questioned in a 30-minute to 1-hour interview when they responded to items on the interview protocol. To guarantee reliable data, each participant

received a copy of their interview record to review for accuracy with any errors corrected before data analysis.

Results

During the interview, participants were asked to rate their personal perception of the effectiveness of each theme area in their unit (see table 1). This self-reporting mechanism was not used for statistical analysis but instead served as a basis for placing qualitative comments into categorical bins. For example, participant one might have rated leadership a "five" and stated, "Having a strong relationship with my first sergeant and operations officer made it much easier to lead the unit." Participant two might have rated leadership a "two" and stated, "My operations officer was the only other officer in my unit and was not very good. We could have done so much more if the situation was different." In both cases, these items were coded as "leadership team strength impacted quality" (see table 2), and the nature of that impact was described in the discussion section of the article.

Table 1. Descriptive statistics on participant self-reported effectiveness

Theme	*n*	*Minimum*	*Maximum*	*M*	*SD*
Leadership	30	2	5	4.2	0.85
Training	30	3	5	3.97	0.8
Customer service	30	3	5	4.47	0.68
Performance improvement	30	3	5	4.1	0.68
Change management	30	2	5	4.17	0.74
Communication	30	3	5	4.1	0.8
Employee Relations	30	3	5	4.27	0.58

Node Frequencies

The node frequencies in table 2 reflect the number of interviews when participants felt that these items were of the most importance to their units' effectiveness. It is important to note here that when given an open-ended question, several items were so consistent that they appeared during 10 or more interviews. These key nodes served as the strongest findings in the study and are described in more detail in the discussion. Other minor nodes emerged within the various themes. Only the top three (based on frequency) scored nodes were included in this study; however, there were many more nodes in each theme and several other interesting benchmarks that were noted later in the discussion section.

Table 2. Coded themes, nodes, and frequencies (*f*)

Theme	*Nodes*	*f*
Leadership	• Leadership team strength impacted quality	17*
	• Focus on strategic tasks vs. fighting fires	8
	• Airmen need to understand their role in the big picture	8
Training	• Leaders focused on training	17
	• Use realistic training	10
	• Needed assigned unit training	8
	• Resources directly impacted quality	8
Customer service	• Focused on the customer	15
	• Resources directly impacted quality	8
	• Interunit relationships matter	8
Performance management	• Awards program directly impacted performance	16
	• Set high standards	9
	• Effectively manage talent	8
Change management	• Communicated regularly	15
	• Transparency creates trust	11
	• Airmen need to understand their role in the big picture	9
Communication	• Leadership by walking around	17
	• Open-door policy was effective	11
	• Unit size mattered	10
Employee relations	• Policy to outline respect	10
	• Social events regularly	7
	• UCA as a tool for improving relations	7

* Key nodes are those that comprise 1/3 of the sample.

Node Relationships

In qualitative research, understanding the relationship of nodes is as important, if not more important, than the frequency. Figure 2 depicts the horizontal dendrogram that reflects the organization of themes based on phrase similarity in the interviews. This means that the conversations regarding the grouped areas were qualitatively similar regarding content.

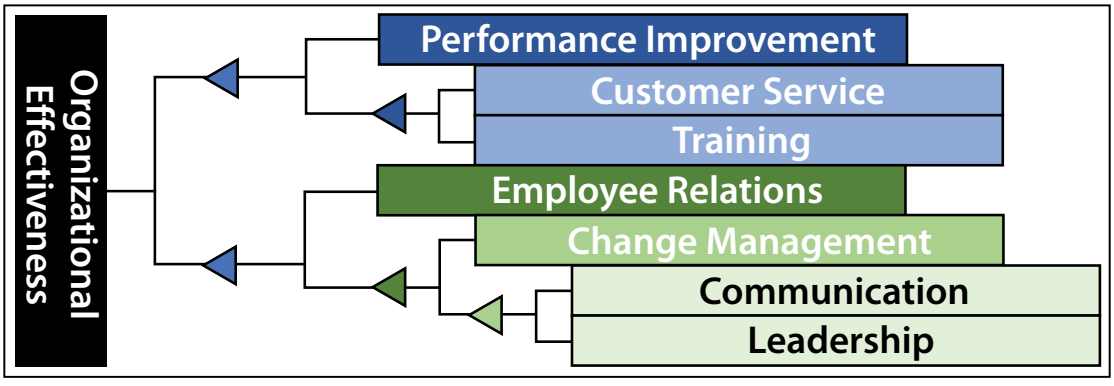


Figure 2. Horizontal dendrogram of nodes clustered by content similarity

We conducted a cluster analysis on nodes that appeared across multiple themes. Eight nodes had multiple connecting themes, and all themes had 2–5 connecting nodes. From an investment perspective, the results in Figure 3 identified areas that commanders can focus on that will impact multiple elements of organizational effectiveness. Transparency was the most impactful node, reaching customer service, communication, leadership, performance improvement, and, most significantly, change management. One finding, completely out of a commander's control, is that unit size will moderately impact employee relations and leadership, while it strongly impacts communication.

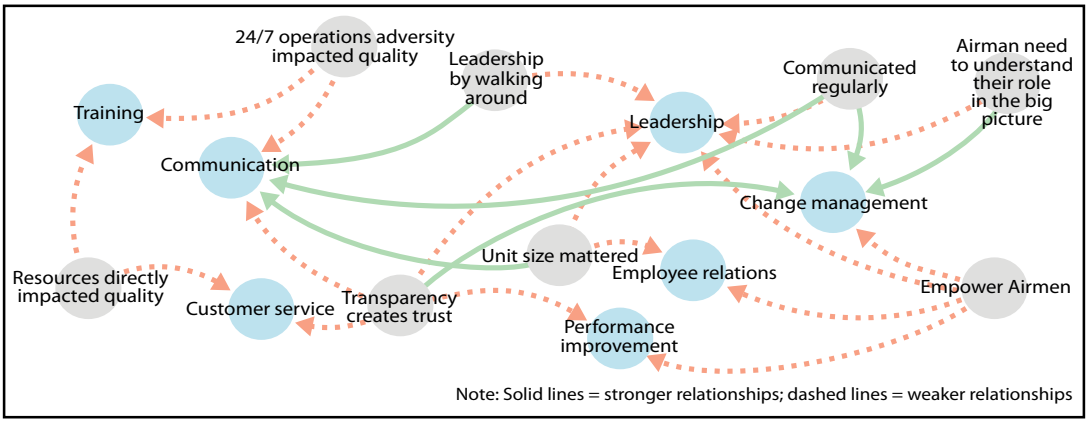


Figure 3. Cluster diagram depicting nodes with impact on multiple themes

Discussion

Leadership

Leadership team strength impact quality. Commanders reported that the cohesiveness of their leadership team was the most significant factor in their leadership effectiveness—good or bad. While the command team varied based on unit size and function, the references consisted of a mix of commander, first sergeant, operations officer, superintendent, and flight commanders. Smaller units also consider the senior noncommissioned officer (SNCO) part of the leadership team, while larger units generally did not. Effective teams had trained and proactive leaders who mentored junior members (or tier groups) and kept the commander from micromanaging. Creating that culture required the commander to be receptive to feedback, ensure open lines of communication with her or his team, and empower the team to act in their respective roles. Commanders with weaker teams noted that their staff was typically underexperienced, or there was an unusual rank structure. For example, some commanders had vacant chief master sergeant positions and/or had operations officers who were lieutenants—a rank that generally lacks the required experience for effectively leading a squadron-level unit.

Focus on strategic tasks versus fighting fires. Commanders who focused on strategic tasks, or those high-level tasks where only they could make the decision, were more effective than those who struggled with the foregoing. Focusing on strategic tasks was a mutually beneficial approach: (1) it allowed the commander to maximize the use of her or his limited time, and (2) it empowered lower-level leaders to lead people and manage resources under their authority.

Airmen need to understand their role in the big picture. Airmen who understood the unit's mission and their specific contribution to the overall wing mission were more motivated to accomplish goals. These findings are congruent with recent messages to Air Force leaders urging that the millennial generation of Airmen—comprising most Airmen in ranks Airman basic through technical sergeant and second lieutenant through young majors—work better when they have consistent feedback and understand "why" they are performing tasks.[8] Support squadrons found this approach most useful since their Airmen are often disconnected from the direct operations of the wing. Commanders suggested sending Airmen to their customer units for orientations, familiarization flights, and other similar integration practices. The Airman Comprehensive Assessment (ACA) also provided an excellent forum for integrating this practice into the culture of a unit.

Training

Leaders focus on training. Commanders felt strongly about the importance training had on unit success. While fiscal resources and time often limited their ability to do what they wanted, commanders who focused energy on unit training often felt it was worth the investment. Medical and support units preferred establishing training down-days while operations, maintenance, and hybrid units most benefited from quality assurance programs. In either case, the commander's engagement

was critical to the success of the programs. Commanders spoke often of the importance of proactively and aggressively requesting training money and manpower from their leaders.

Use realistic training. Commanders agreed that the benefit of computer-based training paled in comparison to realistic training. Focusing on obtaining realistic training, such as exercises, practical courses (that is, jump school and physical security school), and on-the-job training paid much higher dividends, especially when taking over a unit with a defunct training program. Commanders who were limited in resources would substitute courses with local subject-matter experts who could provide training. Additionally, some commanders would establish on-base mock deployment sites, such as alternate duty locations, for expeditionary training.

Assigned unit training managers (UTM) matter. We saw that in many cases, commanders either benefited from having an assigned 3S2X1 UTM or wished they had one. Some small units had UTMs while other larger units did not. After investigating several points of contact at the wing and MAJCOM level, we learned that the requirements for who gets a UTM and who does not were not well known. The Air Force Manpower Agency provided a copy of the manpower standard that identified how units with 110 or more authorizations may have an assigned UTM.[9] The foregoing reinforced the "unit size mattered" theme.

Customer Service

Focus on the customer. Units that excelled in customer service emphasized the customer from their vision statement to their active feedback solicitation. Geographically-separated units, varying operations tempos, and diverse customer requirements often made it increasingly difficult to have rigid procedures for providing support. Since much lot of customer service is personality dependent, successful commanders often discussed their focus on personality and flexible approach to delivering value to their customers. Some practices noted were:

- Treating someone on the phone the same as if they were in person
- Positioning top-performing Airmen in roles that directly interact with the customer
- Fully staffing customer-interfacing elements
- Establishing outreach programs to educate Airmen and customers on each other's roles
- Creating a client-based approach where the customer was part of the solution

Resources directly impact quality. Commanders—especially those in support functions—identified the need to prioritize services due to limited resources. It was unrealistic to expect to fulfill the needs of all customers, so instead some of them developed priority lists where units closer to the "tip of the spear" were first served. The priority lists created some unrest, however, being transparent about the process and priorities tempered complaints. Current or future commanders should expect that they will likely be in a resource-constrained unit and need to accept similar

risk. Regardless of the type of risk accepted, being transparent with the customer will help maintain constructive relationships.

Interunit relationships matter. Find a way to get to "yes" was a mentality that facilitated cooperative interaction between units. Commanders found that in very rare cases "no" was the only answer to a problem. Successful units actively sought alternative means of satisfying the customer's needs. In some cases, "we can't do that, but we can do this" was the most effective approach to providing services in a way that still met the customer's requirements. Direct interunit conversations between commanders and operations officers improved effectiveness, especially in situations when a service was shared between two or more units (that is, airfield construction requires cooperation and input from civil engineering, contracting, and operations support squadrons).

Performance Improvement

Awards program directly impacts performance. Formal and informal recognition activities formed the foundation of performance improvement in the units of most interviewed commanders. Positively affecting people's attitudes through deserved awards and decorations instilled unit pride, motivated Airmen, and reinforced desired behaviors. Commanders described various states of awards programs upon arrival to the unit. Some programs were well established and required little work, while others were nonexistent or grossly neglected and required a lot of the commander's time to get going. Establishing "murder boards" as forums where different groups reviewed packages to vet and improve quality improved the success rate of performance awards. Presenting awards and decorations to those who deserved it was just as important as not "handing out" the same to those who were not deserving. It was important to set high standards and reward those who met or exceeded them.

Set high standards. Several commanders identified the establishment of high standards as a pivotal performance improvement decision. Even those who came to command units that were not performing well found that once they set and enforced higher standards, the unit adapted, and improved morale and performance followed. In some cases, commanders were directed by higher-level commanders to set higher standards, a decision they regretted not making on their own.

Effectively manage talent. Putting people in places where they could succeed was the best approach to talent management. To do so, commanders had to know the strengths and weaknesses of their Airmen. In several cases, commanders met with each Airman in their units to discuss their potential in the unit. Unfortunately, many of these commanders also had to remove Airmen who did not adequately perform their duties. Those who did not fire underperformers, when perhaps they should have, expressed regretting that decision well after their command ended. Commanders of selectively-manned units found that they had little trouble with managing talent and performance issues since they could screen their new hires before assignments were issued.

Change Management

Communicate regularly. Frequent communication positively impacted the change management, communication, and leadership themes in various ways. From a change management perspective, regular communication on the upcoming change—why the change is happening, what impact the change will have, and what conditions will exist after the change—was an effective way to help manage the change process. Commanders found that communicating regularly helped to control the "rumor mill"; however, it was important to convey with each update that things are in flux, and the plan today might not be the plan tomorrow. Balancing how much to share and when to share it was a common struggle. In some cases, information sharing was heavily restricted by higher-level authorities; an often unfavorable practice that would create transparency issues between the commander and the unit.

Transparency creates trust. During an organizational change, Airmen want to know what is happening, even if the news was negative. Commanders found that when they were transparent with their Airmen, even when it was negative information, they received less resistance during the change process. These findings are congruent with recent research that demonstrated how transparent communication instilled trust, improved employee perception of the leader and enhanced the reputation of the organization.[10] Transparent communication was found to be so significant that it impacted five of the seven themes (see fig. 3).

Airmen need to understand their role in the big picture. We addressed this node in the *leadership* theme; however, the context of how it impacted change management was slightly different. During discussions, commanders emphasized how important it was for them to explain to their Airmen the role they played during and following the change. In many cases, commanders assigned a portion of the change process to their lower-level leaders for implementation. For example, during the release of the recent enlisted evaluation system overhaul, commanders delegated to their top three the role of educators for the unit. While all leaders were educated on the program, the top three translated the program changes to their junior enlisted and explained how the changes would benefit them, as well as some of the challenges they would bring during implementation.

Similarly, during unit restructuring, some commanders had their flight commanders and/or Top Three create Post-it notes with all their functions and aligned them on a board where they fit best to create the new organization's structure. This collaborative effort created a sense of ownership in the new unit, gained the support of the leadership team, and made it easier to translate a common message to the unit regarding the change. It was also easier for supervisors to explain their Airmen's logical place in the unit and how they connected to the other sections.

Communication

Leadership by walking around. The majority of commanders agreed that walking around the unit was one of the most productive ways to be an effective leader. Walking around the unit familiarizes the commander with the people, hot issues, and unit climate.[11] Walking around, unlike electronic communication, provides connectedness and clarity; a clarity that is sometimes critical to a message. It

opens lines of communication and lets Airmen know that their commander values them enough to spend direct time with them.[12]

Open-door policy is effective. Although the implementation of open-door policies varied among the interviewed commanders, the idea that it created an avenue for Airmen to freely approach their commander and improved communication remained constant. Some commanders maintained a completely open door, while others stated, "my door is open unless it's not." The latter implied that when the door is closed, Airmen can make an appointment to be seen as soon as possible.

Unit size matters. The most impactful element—and outside of the commander's control—mentioned during the interviews was how the size of the unit impacted various themes (see fig. 3). Of those themes, communication was the most impacted by unit size. As units grew larger, commanders experienced more complexity when it came to communicating with their Airmen. Increased levels of supervision, distributed work environments, varying shifts, and access to communication mediums all presented challenges. Security forces, aircraft maintenance, and operations support commanders experienced significant challenges in these areas. Commanders wishing to communicate in these environments often held multiple commander's calls, came to work after standard hours to see various shifts, and made it a point to travel to various work sites—even when geographically separated. Some commanders emphasized the importance of overcoming generation barriers and capitalizing on social media as a medium for communicating with the unit. The organization's social media groups and feeds also created a medium where unit members could collaborate and improve intraunit relations.

Employee Relations

Policy to outline respect. Respect in the workplace improves retention, productivity, and team building, thus leading to a more effective organization.[13] Commanders must set the tone and be clear on their policies that outline workplace respect. Clearly communicating, demonstrating, promoting, and enforcing such policies fuels a transformational process that results in improved employee relations and a more positive organizational climate.

Several medical and support squadron commanders described a culture where individual opinions were respected, and everyone's contributions were valued. In these cultures, there was no prestige or relevance in rank or titles. Instead, pride generated from how well each member of the team did their part in accomplishing the mission. Airmen of all ranks were welcome to voice ideas and contribute to organization objectives.

Regular social events. Research has proven that social activities build camaraderie and community within workplaces, as long as those activities reflect the values of the organization.[14] The research participants echoed those findings through their many stories about establishing squadron sports teams, attending dining events, and creating a family-inclusive culture. One of the greatest hurdles to codify such a culture was dissolving some of the social clicks that prevented inter- work-center interaction. Identifying those clicks required immersion in the unit and one-on-one conversations with the Airmen.

Unit climate assessment as a tool for improvement. Several commanders found value in using the unit's past climate assessments to gauge the evolution of the organization's climate upon taking command. The surveys, now called Defense Equal Opportunity Management Institute's Organizational Climate Survey, provided commanders with anonymous quantitative and qualitative data points for highlighting the climate of the unit during a multiyear period. They also allow commanders to gauge their current assessment with past assessments to identify any upward or downward trending during their command.

Assumptions and Limitations

Two major assumptions underlaid the research:

1. The confidentiality promised to participants created enough trust between them and the research team to provide honest, information-rich feedback.
2. The qualitative reasoning behind their explanation of key themes and nodes were transferable to other squadron-level command scenarios.

Two limitations impacted this study:

1. Resources in time and travel money impacted the ability to survey/interview various units to couple the Airmen's perspective with the commanders' input.
2. The interviews provided an extensive amount of information which required us to constrain this article to only the top nodes in each theme with only the most common explanations for each node.

Recommendations for Future Research

This study identified several research opportunities to explore farther the problem of squadron organizational effectiveness:

1. Although the goal of this study was to identify key nodes across multiple career fields that lead to effective organizations, future research should focus on functional-specific practices for success. Large organizations, like the Air Force, have an overall organizational culture, but they also have various subcultures where occupational shared values and norms impact the organization's culture and effectiveness (that is, fighter squadrons having a bar).[15] These more specific commander challenges could then be incorporated into the respective MAJCOM squadron commander and Air University Commanders' Professional Development School courses.
2. The Air Force Inspector General's office manages the Inspector General Evaluation Management System (IGEMS), which collects data on four major graded areas: management of resources, leading people, improving the unit, and executing the mission.[16] A mixed-methods study examining the quantitative and qualitative data points from IGEMS would provide significant insight into squadron effectiveness. Quantitative data points derived from converting the

rating system (that is, satisfactory, effective, highly effective) into a Likert-type scale would reveal immediately useful information regarding command and functional effectiveness. A deeper qualitative investigation into the inspector and unit member comments would highlight specific details that led to the ranking system.

3. As indicated in the study's analysis of phrase similarity depicted in Figure 2, an intriguing connection surfaced between the themes of customer service and training. A review of the raw data led to the suggestion that perhaps the quality, stability, and frequency of training indirectly affect the predictability of positive interactions with customers. In short, the level of prioritization and organization of a squadron's training program may have enough impact on customer interaction to allow commanders more control over the quality of those interactions than they may realize. More research is required to unpack the possible linkages here, but the proposed relationship of these two themes to performance improvement highlights this question as an important one for commanders.
4. The cohesion strength of the leadership teams in each unit directly impacted the unit's effectiveness. How do we improve the strength of not just the commander, but the entire team? Are the senior squadron positions so important that they deserve some more development? Commanders and first sergeants attend formal courses; however, operations officers learn the job on the job. Additionally, not all squadrons are large enough to be authorized a diamond-wearing first sergeant and instead appoint an additional-duty first sergeant who typically does not have the formal education. Does a unit's size directly relate to the importance of having a trained first sergeant as the senior enlisted leader? Why not authorize additional duty first sergeants to attend the distance learning first sergeant course to afford them more training and credibility?

Conclusion

The specific problem explored during this research was the identification of the elements of USAF squadron organizational effectiveness. Our qualitative phenomenological approach, using 30 graduated squadron commanders as a sample, provided a tremendous amount of data that we analyzed to address our research questions. While the research recommendations were proposed, we offer the following conditions or activities that make squadrons effective:

1. During our research, we explored seven areas of organizational effectiveness: (1) leadership, (2) training, (3) customer service, (4) performance improvement, (5) change management, (6) communication, and (7) employee relations. The empirical results of this research can serve as a guide for incoming squadron commanders. Reviewing the key nodes identified in this study and knowing how they impacted unit effectiveness in other squadrons can help commanders be better prepared to step into their new role (see table 2). Additionally, understanding how the nodes related to each other and the other themes of organization effectiveness can help time- and resource-constrained

commanders focus those resources on the key nodes that impact multiple areas of the unit (see fig. 3). Commanders that focus on positively impacting the key nodes identified in this study will improve their chances of having an effective squadron over those who do not.

2. The dendrogram in Figure 2 visually depicted the centrality of the role of communication in leadership, in that communication is the basis of both relationships and command. Years ago, British journalist, philosopher, and writer G. K. Chesterton pointed out that one of the reasons that the topic of education is misunderstood is because people see it, not as a method or medium, but as a discrete academic subject such as physics or history. In the same way, leaders can misunderstand communication's centrality by seeing it as "another element" of leadership rather than *the medium* of leadership. Leadership is not a purely mental event, but it is a lived event that must occur in relationships and only with communication—or it has never actually taken place. A review of the raw data suggests that, just as communication is the mechanism through which leadership occurs, it is also the basis upon which change management succeeds and employee relations thrive. The bottom line is that it would be a mistake for commanders to assume that the quality of communication in a unit—and from themselves—is merely another "leadership element" to be handled as time allows and de-emphasizes in the face of competing demands and when facing a crisis. The solution would be to accept that *communication IS leadership*. While communication can be consciously improved before a crisis, it is a most powerful predictor of the outcome of that crisis. ✪

Notes

1. Gen David Goldfein, "CSAF Letter to Airmen," *af.mil*, 9 August 2016, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/ 873161/csaf-letter-to-airmen.aspx.
2. Air Force Instruction (AFI) 38-101, *Air Force Organization*, 31 January 2017, 13, 2.2.8. http://static.e-publishing.af.mil/production/1/af_a1/publication/afi38-101/afi38-101.pdf.
3. Angelina Fleming, *Defense Spending and War Funding: Budget Control Act Impacts and Issues* (Nova Science Publishers: New York, 2015), 1.
4. Ibid., 2.
5. John W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 3rd ed. (Los Angeles, CA: Sage, 2009), 4.
6. Ibid.
7. David P. Nalbone, "A Quantitative Look at a New Qualitative Methodology" (2012), *PsycCRITIQUES* 57, no. 8 (January 2012), doi: 10.1037/a0026557.
8. Col Clinton Hinote and Col Timothy J. Sundvall, "Leading Millennials: An Approach that Works," *Air & Space Power Journal* (*ASPJ*) 29, no. 1 (Winter 2015): 133–134, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-29_Issue-1/C-Hinote_Sundvall.pdf.
9. Air Force Medical Service (AFMS), *10S1000–10S1 Squadron Orderly Room* (Washington, DC: AFMS, 2015), 10, Table A2.2.1.
10. Linjuan Rita Men, "Internal Reputation Management: The Impact of Authentic Leadership and Transparent Communication," *Corporate Reputation Review* 17, no. 4 (1 October 2014): 254–72, http://www.ingentaconnect.com/content/pal/crr/2014/00000017/00000004/art00003 /.

11. Maj Steven Minkin, "Reflections on Command," *ASPJ* (Winter 2006): 44–51, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-20_Issue-1-4/2006_Vol20_No4.pdf; and Gen Hal M. Hornburg, "Senior Leader Perspective," *ASPJ* (Spring 2005): 4–16, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-19_Issue-1-4/spr05.pdf.

12. Brig Gen Raymond A. Shulstad, USAF, Retired, and Lt Col Richard D. Meal, USAF, Retired, "Leading and Managing through Influence," *ASPJ* (Summer 2010): 6–17, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-24_Issue-1-4/2010_Vol24_No2.pdf.

13. Astree Augsberger, Wendy Schudrich, Brenda G. McGowan, and Charles Auerbach, "Respect in the Workplace: A Mixed Methods Study of Retention and Turnover in the Voluntary Child Welfare Sector," *Children and Youth Services Review* 34, no. 7 (2012): 1222, https://econpapers.repec.org/article/eeecysrev/v_3a34_3ay_3a2012_3ai_3a7_3ap_3a1222-1229.htm.

14. George Manning, "To Party or Not to Party," *Journal of Employee Assistance* (January–March 2005), 10.

15. Edgar H. Schein, *Organizational Culture and Leadership* (San Francisco, CA: Jossey-Bass, 2010), 2.

16. *AFI* 90-201, *The Air Force Inspection System*, 10-11, 7 December 2017, http://static.e-publishing.af.mil/production/1/saf_ig/publication/afi90-201/afi90-201.pdf.

Maj Jason M. Newcomer, DBA, USAF

Major Newcomer (DBA, Walden University; MA, Air University; MAS, BS, Embry–Riddle Aeronautical University; AAS, Community College of the Air Force) is the 84th Radar Evaluation Squadron director of operations, Hill AFB, Utah. He oversees the operations of 84 personnel in two flights and four operating locations in New York, Washington, Hawaii, and Alaska. Major Newcomer supports nine major radar evaluation programs encompassing 480 air defense, air surveillance, and counternarcotic radar sensors worldwide. He is an assistant professor of leadership and aeronautics at Embry–Riddle Aeronautical University and has 16 publications in various military, aviation, and management journals covering leadership issues on those topics.

Lt Col Daniel A. Connelly, PhD, USAF, Retired

Dr. Connelly (PhD, Auburn University; MA, American University) is an assistant professor in the Department of International Security, at the Air Command and Staff College, Maxwell AFB, Alabama. He is a retired USAF officer whose background includes operational tours at headquarters and flying unit echelons and deployments to Southwest and Far East Asia. Dr. Connelly teaches courses in international security, leadership studies, airpower theory, the Just War tradition, and Russian studies. He has published on topics ranging from leadership theory and higher education to Former Soviet Union affairs, and has participated in multiple empirical investigations related to these topics. Previously, Dr. Connelly served as the dean of academic affairs at the Squadron Officer College.

Terror from Above

How the Commercial Unmanned Aerial Vehicle Revolution Threatens the US Threshold

Maj Bryan A. Card, USAFR

Amazon is not the only organization interested in using unmanned aerial vehicles (UAV) to deliver packages. Soon, terrorist organizations may also employ UAVs for their diabolic purposes. The US is on the cusp of a burgeoning commercial UAV revolution. Federal Aviation Administration (FAA) regulations have limited commercial employment of UAVs within the US; however, this is changing with newly implemented FAA guidelines.[1] As the regulatory impediments to using UAVs in the US for commercial purposes continue to decrease, commercial demand will increase, and UAV technology providers will develop more capable and user-friendly UAVs and control systems. Unfortunately, greater commercial accessibility to UAV technology will make UAVs more attractive as a delivery method for terrorist attacks, and policy makers should consider different courses of action to combat this emerging threat.

The DOD classifies UAVs into five different groups, based on the gross weight, operating altitude, and speed of the UAV.[2] This article will focus on the small UAVs in groups 1 and 2, which include UAVs under 55 lbs., flying under 3,500 feet above ground level, and under 250 knots. There are two primary reasons for focusing on these UAVs. First, the FAA has created a new remote pilot certification for UAV operators, no longer requiring UAV operators to hold a recreational, sport, or commercial pilot's license for unmanned aircraft weighing less than 55 lbs.[3] With this new regulation, it is anticipated that most commercial development into pilot-less systems in the US will fall into unmanned aircraft of this size. Second, it is more likely that individuals or a small group can build a group 1 or 2 UAV in a garage, on a small budget, for use in a terror attack without attracting suspicion.

Definitions

First, it is helpful to look at some of the terms and acronyms associated with unmanned aerial vehicles:

- *Unmanned aerial vehicle* (UAV): UAV refers to an actual air vehicle, sometimes simply referred to as an unmanned aircraft (UA).
- *Unmanned aerial system* (UAS): This term typically refers to the entire system of systems that allows a UAV to fly and perform its mission, including the ground station, telemetry, communication and navigation equipment, sensor package, and the UAV itself.
- *Remotely piloted aircraft* (RPA): An unmanned aircraft controlled by a trained pilot; this is a term primarily used by the USAF to denote unmanned aircraft.[4]
- *Drone*: A common term used to refer to UAVs but can refer to any form of automated robot or machinery.

Despite the distinctions among these terms, they are often used interchangeably. This article will primarily use the term *UAV* unless referencing a complete system of systems, in which case the term *UAS* will be used.

Last, the following terms will be used to characterize potential terrorist targets and assets that law enforcement and defensive planners wish to protect.

- *High-value target*: A target whose loss will significantly bolster the terrorist's campaign, due to several factors that could include the symbolic nature of the target and the amount of media attention the target would generate.[5]
- *High-risk personnel*: Personnel who, by their position, grade, assignment, or symbolic value, are likely to be attractive terrorist targets.[6]
- *High-risk event*: An event that due to its symbolic value, mass attendance, or media attention, is likely to be an attractive and accessible terrorist target.

Current Assessments of Unmanned Aerial Vehicles as Threats to National Security

Until recently, the literature discussing the threat from UAVs focused on either large-scale UAVs that pose an external threat to US security or on domestically operated UAVs that could threaten the privacy of citizens. Recent events, such as the UAV crashing on the White House lawn and UAV sightings in France—throughout Paris and at nuclear power plants throughout the country—have brought attention to the use of small UAVs and the potential danger they pose.[7]

One of the most critical pieces of research to date examining the threat of UAVs to the US homeland is a RAND Corporation study entitled *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, henceforth referred to as the *Novel Threats* study. This 2008 study conducts a "Red" analysis of alternative attack modes, comparing "the suitability of cruise missiles and UAVs against other options, such as vest bombs, car bombs, and mortars."[8] The success of potential attacks is based on three primary tactical outcomes:

1. Targeted individuals are injured or killed.
2. Property is damaged or destroyed.
3. An activity in or by the target state is disrupted.[9]

To determine if an attack mode could successfully achieve these tactical outcomes, the study considered: (1) warhead effectiveness (measured by weight of payload); (2) the type of ordinance delivered; (3) the accuracy of the weapon; and (4) the probability of reaching the target. Generally speaking, the larger the payload that can be delivered, the less accuracy required to achieve the tactical objective.

The study concludes that UAVs and cruise missiles best provide the following five operational advantages:

1. Circumventing perimeter defenses
2. Attacking from outside national borders
3. Staging multiple simultaneous attacks
4. Sustaining protracted terrorist campaigns and
5. Dispersal of unconventional weapons.[10]

Despite these operational advantages, the study claims that UAVs are unlikely to be widely embraced due to their "greater complexity, technological uncertainty, cost, and risks."[11] The authors do concede that attack methods are "driven by the actions of the defense or security measures" in place; however, they conclude that significant soft targets within the US exist to make it unnecessary for terrorists to employ UAVs for attacks.[12]

In arriving at their conclusion, the *Novel Threats* authors failed to take into consideration two important factors that will contribute to terrorist use of UAVs. First, they do not consider communication, or "messaging," as a tactical objective of terrorist violence. Second, the study does not account for the commercial expansion of

UAVs that the US is now beginning to experience or the effects commercialization is having on the costs and accessibility of UAVs. Consideration of these two factors will demonstrate that the use of UAVs in terrorist attacks can no longer be dismissed as highly unlikely.

Terrorism as Communication

A key component of terrorism is communication. In *Communicating Terror*, Joseph Tuman proposes that terrorists engage in violence to send a message to a target audience. He writes: "The primary audience will be those who witness and observe the violence and destruction and engage in discourse about what they have seen."[13] Thus, the message is not the violence or destruction itself, but rather the message is either embedded within the violence or follows from it in subsequent messaging.[14] Therefore, the tactical output of a terrorist action may not be the people killed or the damaged property but rather the message it sends to a target audience that is separate from those targeted in the attack.

By striking a particularly high-value target, such as a high-ranking political figure, celebrity, or athlete, a terrorist organization can demonstrate its ability to overcome the defensive capabilities of the state, displaying the terrorists' strength and the state's weakness. The more attention the action will garner—through sheer destruction or due to the target's high value—the more lucrative a particular target becomes. Simply assuming that terrorists will attack soft targets rather than protected ones due to the additional operational complexity is simplifying the issue too much. By failing to address the idea that terrorism is communication through violence, the *Novel Threats* authors discount the real possibility that terrorists may choose an accurate delivery method capable of circumventing perimeter defenses to strike at a high-value target and thus garnering the terrorists a high degree of attention and infamy. By not addressing terrorists' propensity for choosing targets of symbolic significance or for media attention, the *Novel Threats* study comes to the rebuttable conclusion that UAVs are not a probable threat. UAVs are indeed a probable threat.

The Commercialization of Unmanned Aerial Vehicles

A second factor the *Novel Threats* study fails to account for is the burgeoning commercial UAV revolution. Missy Cummings, a former Navy fighter pilot and the director of the Humans and Autonomy Lab at Duke University, has stated:

> *We're going to see many commercial applications and much more civilian development than in the military. In 15 years, you could look up in the sky and see UAVs doing window washing and building inspections. You also could see every jealous ex-husband or wife following their significant other around. For good or bad, we are on the cusp of a new era.*[15]

One's imagination may be the only limiting factor to the multitude of uses for UAVs. Current commercial uses include aerial photography, monitoring oil fields and pipelines, transporting critical goods, and conducting search and rescue operations. One example of this new demand for UAVs is provided by University of Nebraska

journalism professor Matt Waite, who spent almost two decades as a reporter covering natural disasters. At a digital-mapping conference he saw the GateWing X100 UAV, which can fit in the back of a sport utility vehicle, is hand-launchable and equipped with a downward-facing high resolution camera. Controlled by a tablet computer using a digital map, one simply touches the screen and tells it where to fly—no piloting skills required. The X100 is extremely useful for reporting on fires, floods, hurricanes, and tornadoes—just about any situation where it is prohibitively dangerous to fly a manned aircraft.[16] This utility was demonstrated recently in the aftermath of Hurricane Harvey, where the FAA issued at least 43 authorizations to fly commercial UAVs in support of recovery efforts, helping local authorities "assess damage to homes, roads, bridges, power lines, oil and gas facilities, and office buildings."[17]

Human supervisory control is one of the largest advantages of UAV technology, allowing those with minimal training to control these aircraft. Instead of having to understand aeronautical principles and the complex controls of an aircraft—as a pilot must—UAV operators are performing, human supervisory control, a higher-level function where the operator "encourages" the aircraft to do what she or he wants.[18] Thus, you have UAVs that fly themselves to waypoints without the operator having to know the first thing about aerodynamics. Engineers, surveyors, search and rescue crews, and other professionals who would benefit from a UAV can simply go through minimal training and operate the aircraft themselves.

In one of Cummings' experiments with human supervisory control, micro-aerial vehicle visualization of unexplored environments (MAV VUE), researchers had an operator in Seattle, Washington controlling a micro-UAV in an open field in Cambridge, Massachusetts.[19] The controller used an iPhone connected to the internet via a wireless hotspot while the UAV communicated with a ground-station, also connected to a wireless hotspot. The operator had two levels of control—waypoint control and nudge control. Using waypoint control, the operator simply clicked on a digital map to tell the UAV where to fly. Using nudge control, the operator, with the help of a forward-facing view from the UAV's camera, flew the UAV by tilting the iPhone in the direction she wanted it to go. The researchers also selected random passersby to control the UAV to demonstrate how a minimally trained operator could easily operate a small UAV. Test subjects received three minutes of instruction and were able to successfully control the UAV and perform tasks like identifying people through the video feed sent to the iPhone from the UAV's camera. Such technology allows operators to move away from traditional command and control systems that require them to micromanage the behavior of the vehicle, and to concentrate instead on the more mission-relevant part of command and control.

Additionally, the relatively low cost of group 1 and 2 UAVs will make them a viable delivery mechanism for terrorists. Exemplifying the increased accessibility of UAVs is the hobbyist website *DIYDrones.com*. *DIYDrones.com* is dedicated to helping drone enthusiasts gather and exchange ideas and information about how to build and operate drones. Through it, a person can learn to build a UAV equipped with high-definition (HD) cameras, telemetry, and control systems. These hobby-built UAVs can be assembled with a full telemetry kit and autopilot for a cost of between $2,000–$10,000.[20] Chris Anderson, founder of *DIYDrones.com* stated, "If we make the technology cheap, easy and ubiquitous, regular people will figure it out."[21] Cer-

tainly if your average person can build a UAS, so can a terrorist, and the $2,000–$10,000 price range falls well within the historical costs of many terrorist attacks.[22]

In 2012, Cummings stated, "companies are chomping at the bit" to integrate UAVs into their operations, "and there's no technical reason we can't do this now. . . the only reason we don't is regulatory issues."[23] Now, with the barriers to operating UAVs in the US diminishing, we will see a rise in commercial development, leading to greater accessibility for individuals and businesses. Unfortunately, such increased accessibility will also make UAVs more attractive to those who would use them for nefarious purposes, thus eliminating the barriers to entry into the realm of airpower.

The Attraction of Unmanned Aerial Vehicles

With the understanding that terror attacks are communication through violence and that the technical and monetary costs of using UAVs are decreasing, we will now highlight some of the characteristics of UAVs that make them well-suited for terrorist attacks. The *Novel Threats* study argues that the primary reason UAVs are attractive as a delivery mechanism is their inherent mobility—the ability to conduct attacks over perimeter defenses. While many potential terrorist targets in the US lack perimeter defenses or barriers, "individual protected targets may still be attractive to an adversary if a successful strike on such a target is viewed as particularly valuable in advancing the group's goals."[24] For instance, it is not hard to imagine the media sensation that would occur if terrorists are able to successfully fly a weaponized UAV into a huddle of football players during the next Super Bowl, an outdoor music concert, or an elementary school playground at recess. Another frightening example would be if a UAV were flown toward the US president at the next inauguration. Even a minimal 1–2 lb. explosive charge could cause deaths and severe injuries, all while 100 million people watch in horror.

This ability of a UAV to bypass perimeter defenses is exemplified by several recent events. In 2013, at a campaign event in Dresden, German Chancellor Angela Merkel and Defense Minister Thomas de Maizière were interrupted by a quadcopter flying onto the stage (fig. 1).[25] In January 2015, a quadrotor UAV crash landed on the White House lawn and three months later a gyrocopter—the size of a larger UAV—landed on the lawn near the US Capitol, flying unimpeded through restricted airspace.[26] In these examples, no one was injured, and there was no demonstrable malicious intent on the part of the operators; however, they show how easily UAVs can access secure areas. Either of these events could have been tragic had the operator's intent been nefarious and the aircraft carrying energetic material.

A second reason terrorists will adopt UAVs is their ability to lower operational risks to the terrorists themselves. While some terrorists have shown a willingness to sacrifice themselves for their cause, others may be attracted to the ability to commit a terrorist attack with a much lower risk of apprehension, allowing for the possibility of conducting a protracted terror campaign. The MAV VUE project demonstrates how a UAV operator can be 3,000 miles away, controlling a UAV over the internet. Someone would certainly need to be on the ground to deploy the UAV; however, a UAV equipped with a 3G or 4G cellular phone can be controlled from

virtually anywhere. Such operations would significantly complicate law enforcement investigations because of the limited footprint that terrorists would leave on the ground near the attack. A weaponized UAV could be launched miles away from the intended target, forcing law enforcement to greatly expand the search area for potential witnesses and/or physical evidence.

Courtesy of ArsTechnica

Figure 1. German chancellor Angela Merkel smiles as a Parrot AR drone comes in for a crash landing during a Christian Democratic Party campaign event 15 September 2013. (Reprinted from "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs," ArsTechnica, 8 September 2013, https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

A final reason that UAVs are attractive to terrorists is that it would be difficult to thwart an attack in progress. It is difficult to detect UAVs using radar, the traditional method of detecting air defense threats. The gyrocopter that landed on the Capitol building lawn exemplifies this difficulty. White House spokesman Josh Earnest said that the low-speed, low-altitude flight made it difficult to detect the small gyrocopter on radar.[27] Marcus Weisgerber, a *Defense One* writer, stated, "Radars can only see above the treeline so if he's flying on the treeline they are going to have a hard time spotting him."[28] Additionally, the small size of UAVs makes them difficult to detect on radar, since "(existing radar systems) are not designed to look for something like a quadcopter."[29] Finally, by the time UAVs are detected, their high speed (70–plus mph) can make them difficult to defeat or evade.

There are already weaponized, small-scale UAVs developed for military application, designed to be rapidly deployable, easily controlled and equipped to destroy soft targets. AeroVironment's "Switchblade is designed to provide the warfighter

with a back-packable, non-line-of-sight precision strike solution with minimal collateral effects."[30] The Switchblade weighs 2.8 kg, carries a 0.45 kg payload, and can reach an estimated top speed of 80–100 mph.[31] AeroVironment claims "the vehicle's small size and quiet motor make it difficult to detect, recognize and track even at very close range."[32] While the Switchblade may well never fall into terrorist hands due to sales and export restrictions, the principle of the Switchblade—a small, fast UAV with an onboard camera for targeting—provides an important example of the potential of this threat.

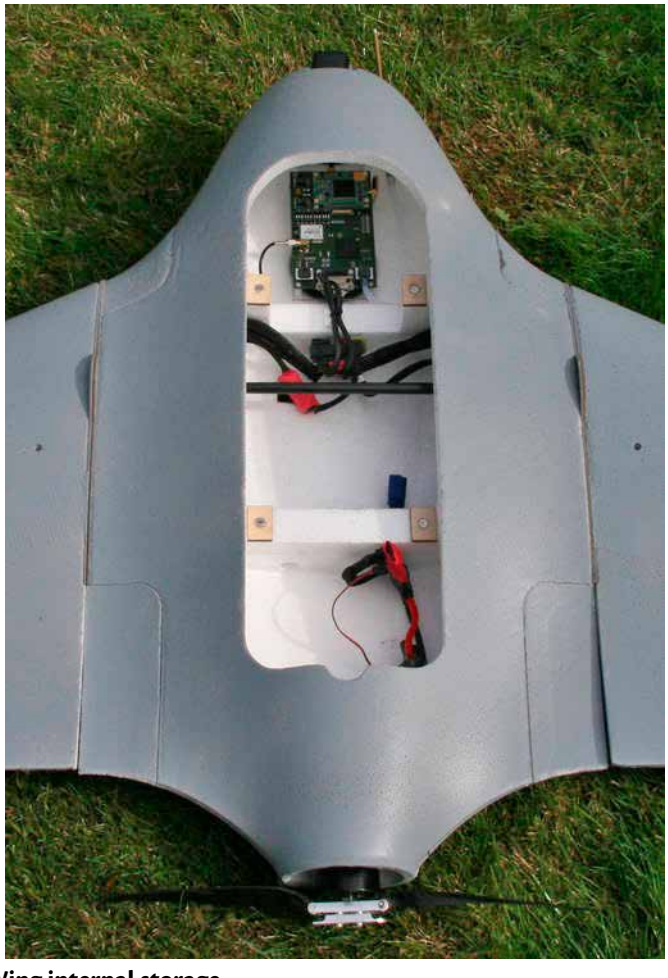


Figure 2. X8 Flying Wing internal storage

One example of a hobbyist remote control (R/C) aircraft that can be converted into a weaponized UAV is the X8 Flying Wing. The X8 has ample space for electronics and a small explosive. (fig. 2) It weighs a mere 2.2 kg, is capable of holding an additional 2.3 kg payload, can cruise at 40 mph with a maximum speed of 70 mph, and has an endurance of up to three hours.[33] The base kit can be purchased for

$160; a complete system with an engine, autopilot, first-person view HD camera and video transmitter can cost an amount between $2,000–$10,000. There are also options to purchase the X8 as a turn-key UAS. Spain-based Airelectronics sells the X8 Flying Wing complete with a ground station, its U-Pilot autopilot, and a sensor suite. Airelectronics claims an endurance of up to three hours, with redundant navigation using dead reckoning if GPS signals are lost. This system is estimated to cost approximately $20,000.[34] The X8 is just one of several hobby-grade UAVs that can be used for attacks, highlighting once again the real terrorist threat UAVs pose today.

Defensive Approach

US military joint doctrine discusses both defensive and offensive methodologies for countering air threats.[35] Borrowing from this operational concept, we will examine both active and passive defense, as well as a more proactive approach utilizing intelligence and law enforcement operations before a possible UAV attack. Active defense consists of "direct defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile air" threats, while passive defense includes measures "taken to minimize, mitigate, or recover from the consequences of attack aircraft and missiles."[36] Finally, intelligence and law enforcement operations can be used to seek out and apprehend terrorists before they strike.

Active Defense

UAVs are not a traditional air defense threat as they are generally smaller than manned aircraft and fly lower and slower, making them harder to detect, thereby complicating the role of active defense. Radars can only detect objects within their direct line of sight, and the lower an object flies, the shorter the possible detection range due to being masked behind trees and buildings. Finally, the small size of UAVs further complicates detection with radars. Based on an Army Research Lab report, a small UAV may have an approximate radar cross-section (RCS) of -15 dBsm, or decibels referenced to a square meter, which is a logarithmic measure of how much a particular object will reflect electromagnetic energy.[37] This is comparable to a large bird (-20 dBsm), while, on the other hand, a large commercial airliner could have an RCS around 40 dBsm and a small jet might be in the 1–2 dBsm range.[38] Therefore, even if a UAV is detected on radar, it may be disregarded as a bird due to their similar size, altitude and speed.

To make matters worse, even if a UAV threat is identified, the options for dealing with the threat are limited. First, in urban environments, where attacks are more likely, law enforcement and the military will be averse to shooting UAVs down because any projectile used for a kinetic attack may cause collateral damage when it returns to the ground. Furthermore, many UAVs would likely be difficult to shoot down due to their light weight, requiring minimal lift to remain airborne.[39] UAVs made of Styrofoam, fiberglass or similar materials could likely take several hits and remain operational unless a critical component is damaged—such as the engine, navigation, or receiver. The use of an explosive ordinance could help alleviate this

issue, but it will add additional concern about collateral damage and public safety. Lastly, a kinetic model for defending a target in an urban environment could require several systems with trained operators to be in place along likely air avenues of approach to adequately defend the area. This model will increase the cost of defending against UAV threats, perhaps prohibitively so, which is one of the reasons the *Novel Threats* study does not recommend the development of a robust active defense system for this threat.

One form of active defense that does hold promise, however, is the use of jamming to block the command channel and/or telemetry of UAVs. Jamming can be particularly effective against hobby-grade UAVs because their command frequencies are regulated; therefore, anything purchased off the shelf will be in a frequency range that can be anticipated. By jamming the most common frequencies, one could effectively eliminate the ability of a terrorist UAV operator to conduct accurate targeting within the denied area. Additionally, unlike kinetic fires, jamming would not necessarily require the same type of tracking precision to engage the threat. Jamming can be omnidirectional, thus only requiring the threat be detected within a certain proximity, allowing for nontraditional methods of detection, such as acoustic and radio frequency detection.

There are three basic factors to consider debating when attempting to jam a UAV command channel or its telemetry data:

- Transmit power of both the control station and the UAV
- Antenna gain of the transmitters
- Radio-frequency (RF) noise level in the environment.

For a terrorist to conduct dynamic targeting, the control station and UAV need to communicate. By preventing this communication, an attack may be thwarted or, at a minimum, cause a loss of precision in targeting, which is critical when considering the small payload of these UAVs.

Theoretically, radio waves, by which the ground station and UAV communicate, travel infinitely; however, as they travel, they disperse, and their signal weakens by the square of the distance they travel.

$$\left(Intensity \times \frac{1}{Distance^2}\right)$$

This rule is known as the inverse square law of propagation, and it is the major determinant of the range in which a UAV control station can make contact with a receiver. Antenna gain also affects this distance in that the better the antenna can translate power into radio waves, the further the usable signal will travel. Third, the signal needs to overcome the RF noise level in the environment. Once the signal can no longer be discerned from the noise, it becomes unusable. Jamming works by effectively raising the RF noise level, preventing a useful transmission from reaching the receiver on the UAV. As the UAV approaches the defended asset and collocated jammer, the harder it is for the transmitter to overcome the RF noise of the signal jammer.

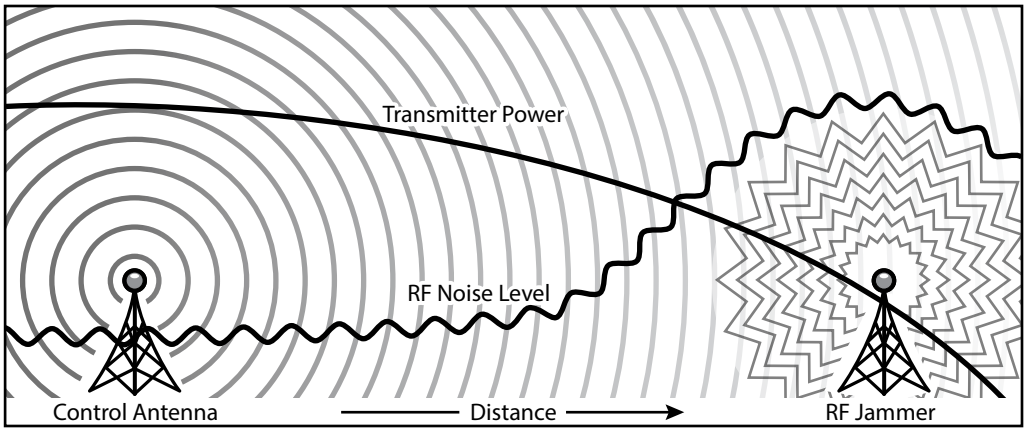


Figure 3. Transmitter power versus RF noise level

Figure 3 shows how such a jammer would work by raising the RF noise level in the vicinity of the area that is to be defended. Once the signal from the control antenna falls below the RF noise level, the operator would no longer be able to control the UAV. To overcome the signal jammer, the terrorist would then have to change frequency bands, increase transmit power, or get closer to the target area, none of which are particularly easy. Changing the frequency band or increasing the power output of the transmitter would require significant knowledge of electrical and radio frequency engineering, unlikely to be had except in the case of the most determined and/or technical of terrorists. Additionally, forcing the terrorist to move closer to the target raises the operational risk for the terrorist since he then may be observed and interrupted midoperation, thus negating some of the operational advantages of UAVs.

One of the downsides of using jamming against UAVs, however, is that there are many users of the electromagnetic spectrum, and jamming may disrupt legitimate users of the spectrum. R/C aircraft and UAVs are only authorized to utilize certain frequencies: 27 MHz, 49 MHz, 50 MHz, 53 MHz, 72 MHz, and 75 MHz for single channel use and 2.4 GHz for spread spectrum use.[40] Additionally, telemetry kits that send back video and positioning information can usually be found in the 433 MHz, 900 MHz, 2.4 GHz, and 5.8 GHz ranges. While the single-channel control frequencies would not be particularly problematic to jam, the 433 MHz, 900 MHz, 2.4 GHz, and 5.8 GHz ranges are part of what is known as the industrial, scientific and medical bands (ISM), and jamming them could cause undesirable interference. Common devices that use these bands include Bluetooth devices, cordless phones, and wireless internet protocol networks. Additionally, a complicating factor in the utilization of jammers is the use of cellular networks to control UAVs. To extend the range of UAVs and the telemetry they send back, terrorists may attempt to utilize cellular networks by integrating a smartphone or other wireless mobile device into their UAV design, as exemplified in the MAV VUE experiment. Jamming such signals would require interrupting cellular services within a given area. The general

public would likely disapprove of continuous, unnecessary interruptions of cellular services and other wireless functions in protected areas. Fortunately, there are ways to help mitigate undesired interference.

Active and passive detection systems—radars, acoustic sensors, and RF detectors—can help mitigate interference with the general public use of cellular services and the ISM bands by allowing jamming only when a UAV is detected within restricted airspace. Radars optimized against small, low, and slow UAVs—such as those using new holographic and micro-Doppler radar technology—may be effective at detecting and identifying UAVs operating in restricted airspace.[41] Additionally, nontraditional detection methods such as acoustic and radio frequency sensors may also prove useful in both detecting UAVs and distinguishing them from other objects like birds. Acoustic systems detect the relatively unique audio signature that UAVs produce from their propellers, while RF detection involves creating a mesh network of receivers "that can triangulate moving transmitters."[42] Thus, once a UAV is detected entering restricted airspace or approaching a high-risk event, jammers can then be turned on to defeat the threat, minimizing the interruption of cellular services and the ISM bands and alleviating public concerns.

Obviously, the choice to interrupt cellular service, wireless networks, and Bluetooth devices should not be taken lightly; however, when faced with the alternate choice of expending live ordinances over a population center in order to disable a threatening UAV, the prudent choice to use jamming is clear. The use of a warning network—radar, acoustic sensors, and RF detectors—to detect UAV threats combined with RF jamming of UAV command and telemetry systems seems to be a highly promising way to defeat such threats.

Passive Defense

One of the best methods of mitigating a UAV terrorist attack is through a strong passive defense. Passive air defense measures can include detection and warning systems, camouflage and concealment, deception, and hardening. One particularly effective passive method for defeating UAV attacks is to host high-risk events indoors. Most commercial structures provide adequate physical protection—hardening—from the warheads that small UAVs would be able to carry, approximately 1–5 kg. By merely hosting events inside, one could greatly reduce the likelihood of being targeted. While it may be possible to fly a UAV inside a structure, it is not desirable due to a lack of mobility, difficulty in route planning and the strong possibility of losing RF signals indoors. Hosting an event indoors removes the ability of the UAV to bypass perimeter defenses and would likely cause a terrorist to choose a different target or delivery method.

In case of an outdoor event, passive defenses can still be implemented. By utilizing detection systems to provide advanced warning, high-risk personnel can be moved to a sheltered area if a UAV were to enter into a restricted area. Since small UAVs cannot carry a large payload, this shelter could range from an armored vehicle to a nearby building. For outdoor events on a covered stage, deployable netting could prove effective at preventing a UAV from getting close to an intended target.

Passive defense can even act as a deterrent against attacks since terrorists may be led to believe that their weapons would not be able to reach the desired target.

Finally, traditional forms of operational security can help protect high-risk personnel from being targeted by UAV attacks. Such measures include using unpredictable transport routes and varying the times that high-risk personnel arrive and leave work and residences, as well as not announcing arrival and departure times of high-risk personnel at high-risk events. These measures generally make it harder for terrorists to target high-risk personnel using any method of attack, not just UAVs.

Intelligence

Currently, almost all of the technology related to hobby-grade R/C aircraft and UAVs is widely available, and it would be nearly impossible to stop the proliferation of this technology.[43] However, it may be possible to discover those who are building UAVs that can be operated beyond visual range. The one distinction between UAVs and R/C aircraft is navigational control. Navigational control can be separated into two distinct pieces of technology—GPS receivers and autopilots. While GPS receivers are commonplace, the autopilot fills a highly specialized role, as it is only procured by individuals operating aircraft or building UAVs. Because the development and use of a UAV require this highly specialized piece of technology, law enforcement, and intelligence agencies have something they can specifically look for in screening for potential terrorist threats.

If law enforcement and intelligence personnel gained the ability to monitor purchases of autopilots, they could then cross-reference those purchases against other indicators of terrorist activity, such as ties to extremist groups and the purchase of chemicals that can be used in making explosives. Similarly, the purchase of any commercial-off-the-shelf (COTS) UAV that includes an autopilot and is capable of holding a 1–5 kg payload (or more) could be monitored. Therefore, it is recommended that provisions be put in place that would enable law enforcement and appropriate intelligence agencies to monitor purchases of autopilots and COTS UAVs.

Conclusion

The employment of UAVs by terrorists is not a far-off threat. The commercialization of UAVs is occurring now and with the latest announcement from the FAA, creating an operator status for small UAVs, eliminating the costly requirement of a licensed pilot, we will see more commercial demand. UAV companies and technology providers will endeavor to make UAV technology even more accessible to both businesses and individual hobbyists to increase its marketability. Unfortunately, commercial development will make such technology more attractive and accessible to terrorists, as well.

Terrorists will seek to acquire small UAVs because of their significant potential benefits. Terrorists use violence as communication, and they understand that it is not necessary to kill numerous people to send a message. UAVs provide the ability to bypass defensive perimeters, allowing terrorists to strike high-risk personnel or

events, which can produce immediate, live media coverage and depict weakness in the government for its inability to protect such targets. Additionally, using UAVs provides a certain degree of safety for the terrorist by enabling him to be farther away from the target location, possibly allowing the terrorist to conduct subsequent attacks before being apprehended. Terrorists are now increasingly able to capitalize on the benefits of using UAVs through technological advances such as those in human supervisory control and through a decrease in the costs of obtaining a UAV. All in all, the likelihood of seeing UAVs used in terror attacks is significantly increasing.

While UAVs may be more difficult to defeat than traditional air threats, there are measures that can be taken to help mitigate the threat from small UAVs. Hosting high-risk events and the appearances of high-risk personnel indoors is probably the best way to protect against the threat from small UAVs. This passive defense measure also happens to have the fewest negative consequences and is probably the lowest cost option among the alternatives. Of course, it will not always be possible to host an event indoors. Events such as the Boston Marathon will still provide lucrative targets for terrorists; however, risk can be mitigated through active defense measures. Radar assets can be brought to bear to detect these threats, providing early warning that enhances passive defense. Also, jamming can be utilized as part of an active defense to disable UAVs once they are detected entering into a restricted area. Finally, by monitoring those who purchase autopilots and COTS UAVs that have built-in autopilots and a certain payload capacity can help law enforcement and intelligence operations can help discover, ahead of time, those who would use UAVs (among other tools) to harm us.

Unfortunately, the reality today is that UAVs complicate matters for security personnel and defensive planners. They democratize airpower, forcing the consideration of the third-dimension when thinking about potential threats to high-risk personnel and events. The advantages gained by utilizing UAVs will undoubtedly attract terrorists to potential targets that will now be more accessible. While resources may be limited to adequately protect the vast number of potential targets, small-scale UAVs are a growing threat and one for which the US government should be preparing. ✪

Notes

1. Federal Aviation Administration (FAA), "Summary of Small Unmanned Aircraft Rule (Part 107)," *FAA News*, 21 June 2016, https://www.faa.gov/uas/media/Part_107_Summary.pdf.
2. "United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047," (Washington, DC: Headquarters, USAF, 2009), 25, http://fas.org/irp/program/collect/uas_2009.pdf.
3. FAA, "DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems," 21 June 2016, https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515.
4. Air Force Instruction 11-202, vol. 3, *Flying Operations: General Flight Rules*, 10 August 2016, 69, http://static.e-publishing.af.mil/production/1/af_a3/publication/afi11-202v3/afi11-202v3.pdf.
5. This is similar to the term used by the DOD; *see* "Joint Publication (JP) 1-02, *Dept. of Defense Dictionary of Military and Associated Terms*," 15 March 2015, 108, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
6. JP 3-07.2, *Antiterrorism*, 24 November 2010, GL-6, http://www.dtic.mil/doctrine/docnet/courses/operations/icdjo/resources/JP3_07X2.pdf.
7. Michael D. Shear and Michael S. Schmidt, "White House Drone Crash Described as a U.S. Worker's Drunken Lark," *New York Times*, 27 January 2015, http://www.nytimes.com/2015/01/28/us/white

-house-drone.html?_r = 0; and Amar Toor, "Paris has a Drone Problem," *The Verge*, 26 February 2015, http://www.theverge.com/2015/2/26/8113291/paris-drone-uav-eiffel-tower-charlie-hebdo.

8. Brian A. Jackson, David R. Frelinger, Michael J. Lostumbo, and Robert W. Button, *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*, Rand Corporation: National Defense Research Institute, 2 March 2008, 8, http://www.rand.org/pubs/monographs/MG626.html.

9. Ibid., 13.

10. Ibid., 58–59.

11. Ibid.

12. Ibid.

13. Joseph Tuman, *Communicating Terror*, 2nd ed. (Los Angeles, Sage Publications: 2010), 34.

14. Ibid., 32.

15. Patrick Hruby, "Out of 'Hobby' Class, Drones Lifting Off for Personal, Commercial Use," *Washington Times*, 14 March 2012, http://www.washingtontimes.com/news/2012/mar/14/out-of-hobby-class-drones-lifting-off-for-personal/?page = all.

16. Ibid.

17. Aarian Marshall, "Above Devastated Houston, Armies of Drones Prove Their Worth," *Wired.com*, 4 September 2017, https://www.wired.com/story/houston-recovery-drones/.

18. Missy Cummings, "Can a 'Computer Co-pilot' Help Anyone Be a Surgeon?" *TEDTALK 2012*, 10 July 2012, http://www.tedmed.com/talks/show?id = 7355&videoId = 6923&ref = about-this-talk.

19. Tom Koehler, "Smart Phones Fly Mini Drones," *Boeing*, 29 August 2011, http://www.boeing.com/Features/2011/08/corp_drone_08_29_11.html.

20. This range includes the cost of the hobby aircraft, autopilot, telemetry kit, and ground-station. More information on various pricing options can be found on the *DIYDrones.com* website and the affiliated 3DRobotics website: http://www.diydrones.com and http://3drobotics.com, respectively.

21. Hruby, "Out of 'Hobby' Class."

22. Eben Kaplan, "Tracking Down Terrorist Financing," *Council on Foreign Relations*, 4 April 2006, http://www.cfr.org/terrorist-financing/tracking-down-terrorist-financing/p10356#p4.

23. Ibid.

24. Jackson et al., *Evaluating Novel Threats*, 29.

25. Sean Gallagher, "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs," *ArsTechnica*, 18 September 2013, http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

26. Shear and Schmidt, "White House Drone Crash Described;" and Krishnadev Calamur, "Florida Mailman Who Flew Gyrocopter onto Capitol Lawn Charged," *the two-way*, 16 April 2015, http://www.npr.org/sections/thetwo-way/2015/04/16/400195580/florida-mailman-who-flew-gyrocopter-onto-capitol-lawn-charged.

27. Calamur, "Florida Mailman Who Flew Gyrocopter."

28. Robin Young, "How Did This Pilot Make it All the Way to the Capitol Lawn?" *Here and Now*, 16 April 2015, http://hereandnow.wbur.org/2015/04/16/gyrocopter-capitol-security.

29. Tereza Pultarova, "Drone-detecting Air-traffic Radar Successful in Trials," *Engineering and Technology Magazine*, 6 May 2015, https://eandt.theiet.org/content/articles/2015/05/drone-detecting-air-traffic-radar-successful-in-trials/.

30. "Switchblade," *AeroVironment*, 13 June 2015, https://www.avinc.com/uas/adc/switchblade/.

31. "2010–2011 UAS Yearbook," *The Global Perspective—8th Edition*, June 2010, http://uas.usgs.gov/UAS-Yearbook2010/pdf/P161-195_World-UAS-Reference-Section.pdf; and Gary Mortimer, "Lethal Miniature Aerial Munition System (LMAMS) to be Deployed Soon?," *UAS News*, 1 January 2011, http://www.suasnews.com/2011/01/3260/lethal-miniature-aerial-munition-system-lmams-to-be-deployed-soon/.

32. AeroVironment, "Switchblade."

33. "Airelectronics X8 Flying Wing Datasheet," *Airelectronics* website, 13 June 2015, http://www.airelectronics.es/products/x8_brochure.pdf?PHPSESSID = itg7avr0agek17jv0o6njqt7h3.

34. Airelectronics does not publicly state the cost of the complete system, but the ground station, autopilot, and control software retails for approximately $16,000, which would be the bulk of the cost of the system.

35. "JP 3-01, *Countering Air and Missile Threats*," 21 April 2017, I-3, http://www.dtic.mil/doctrine/new_pubs/jp3_01_20172104.pdf.

36. JP 3-01, *Countering Air and Missile Threats*, I-6 and V-15.

37. Thomas J. Pizzillo, "RCS Measurements of a PT40 Remote Control Plane at Ka-Band," *Army Research Laboratory*, March 2005, http://www.arl.army.mil/arlreports/2005/ARL-TN-238.pdf.

38. J. A. Spruyt and Ph. van Dorp, "Detection of Birds by Radar," *TNO Physics and Electronics Laboratory*, August 1996, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA321060; and Merrill I. Skolnik, *Introduction to Radar Systems*, 2nd ed. (London: McGraw-Hill Book Co., 1981), 44.

39. Quadcopters may be more susceptible to kinetic fires due to their reliance upon multiple motors to maintain lift.

40. Academy of Model Aeronautics, "Frequency Chart for Model Operation," 13 June 2015, http://www.modelaircraft.org/events/frequencies.aspx.

41. Tereza Pultarova, "Drone-detecting Air-traffic Radar;" and P. Molchanov, K. Egiazarian, J. Astola, R. I. A. Harmanny, and J. J. M. de Wit, "Classification of Small UAVs and Birds by Micro-Doppler Signature," *Proceedings of the 10th European Radar Conference*, 9–11 October 2013, http://www.cs.tut.fi/~molchano/papers/EuRad2013.pdf.

42. Bryan Lifkin, "Detection Systems Listen for Drones Flying Under the Radar," *Gizmodo*, 18 May 2015, http://gizmodo.com/detection-systems-listen-for-drones-flying-under-the-ra-1704764102; and "Credible Personal Drone Detection Systems Now Available on Kickstarter from Domestic Drone Countermeasures LLC," *PR Newswire*, 13 June 2014, https://www.prnewswire.com/news-releases/credible-personal-drone-detection-systems-now-available-on-kickstarter-from-domestic-drone-countermeasures-llc-263016721.html.

43. Ajay Lele and Archana Mishra, "Aerial Terrorism and the Threat from Unmanned Aerial Vehicles," *Journal of Defense Studies* 3:3 (July 2009): 54–65, http://skyjack.co.il/pdf/jds_3_3_alele_amishra.pdf.

Maj Bryan A. Card, USAFR

Major Card (AB Stanford University; MS, University of Texas at El Paso) is the chief of weapons and tactics for the 710th Combat Operations Squadron, Joint Base Langley–Eustis, Virginia. He is responsible for training and tactics development and evaluation to support air component operations. He recently returned from the US Air Forces Central Command Combined Air Operations Center, where he worked as a nonkinetic duty officer, integrating air, space, and cyber capabilities into joint operations. Major Card is also a project manager with the US Army Fires Center of Excellence, Capabilities Development and Integration Directorate, providing command and control and tactical data link support to the Army and Joint Staff. Before joining the Air Force Reserve, he spent five years in the US Army, serving as an air defense artillery fire control officer, responsible for the control and coordination of surface-to-air missile fires. He also served as an infantryman before his commissioning through the Officer Candidate School. Major Card has deployed to Afghanistan and Qatar, and he is a graduate of the US Air Force Weapons School and the Joint Interface Control Officer Course.

Piercing the Fog of Data

Using Activity Based Intelligence to Combat the North Korea Missile Problem

Maj William Giannetti, USAFR

2017 was a banner year for Kim Jong Un and North Korea. Tensions between Pyongyang and Washington rose to an all-time high, and Kim has been eager to prove his credentials as a shrewd political thinker and military strategist. A provocateur like his father and grandfather before him, he launched 20 missile tests—all in violation of international sanctions.[1] Media sources reported that North Korea is irretrievably bent upon becoming a nuclear power. Since 2006 it has conducted six underground nuclear tests at Pungyee.[2] With probably its most hyperbolic rhetoric to date, the reclusive regime in Pyongyang threatened to launch "super-mighty" preemptive strikes against the US mainland and to turn Seoul into a "sea of fire."[3]

Officials in Washington expressed their exasperation about these developments. "The policy of strategic patience has ended," said Secretary of State Rex Tillerson on 16 March 2017, marking the White House's departure from Obama-era national security policy.[4] The USS *Carl Vinson* strike group was sent on a five-month deployment to the Western Pacific in a show of military might. The USS *Ronald Reagan* spent the summer patrolling the Sea of Japan. An advanced, missile-killing terminal high-altitude air defense (THAAD) battery deployed to South Korea to reassure our allies in Seoul and Tokyo. For almost eight years, the US and South Korea called, in vain, for a return to economic engagement with North Korea. Both nations offered to halt annual joint military exercises in the hopes that North Korea would reciprocate by curtailing its nuclear and missile programs. US and North Korean diplomats discussed the possibility of talks toward a peace treaty—a long-awaited event because the Korean War (1950–1953) ended in an armistice and an uneasy return to the *status quo ante*. Pyongyang seemed amenable to discussing a treaty in principle, but the nuclear issue was out of the question. "Diplomacy," according to *Foreign Affairs*, "has failed because Pyongyang remains determined to build its nuclear arsenal."[5]

Then, on 4 July 2017, things took a dramatic turn: North Korea test-fired an intercontinental ballistic missile (ICBM).[6] Even as President Donald J. Trump threatened "fire and fury" against it, Pyongyang stayed its course. In September 2017 Pyongyang undertook its largest nuclear test, which triggered an earthquake of 6.3 magnitude, a

seismic reading that suggests a thermonuclear weapon was detonated.[7] US and international pressure notwithstanding, in September and November Kim launched two more ICBMs.[8] His missile forces even threatened Guam, a US territory and the home of large Air Force and Navy bases, with a salvo of four intermediate-range missiles.[9]

With so much rhetoric and action from both sides, the risks of miscalculation have never been higher. Now, more than ever, the bedrock of Air Force intelligence assessments for senior leaders must be accurate data. Commanders from every service and at almost every echelon also demand the worldwide battlefield awareness the Air Force's Distributed Common Ground System (DCGS) provides. Yet, the DCGS' present challenge, from an intelligence, surveillance, and reconnaissance (ISR) standpoint, is to control the fog of "big data" that is enveloping it. According to a 2013 estimate, the DCGS processes 1.3 petabytes of data per month or about 1,000 hours of full-motion video (FMV) per day.[10] Our space-based assets provide sufficient warning of missile launches to America and its allies, but antiballistic missile defenses like THAAD are designed to destroy missiles as they reenter the Earth's atmosphere which, by then, might be too late. Time and lethality are of the essence; it will take a prudent combination of activity-based intelligence (ABI) and cyber-targeting to respond to Pyongyang.

Better ISR through ABI

As the North Korean threat has grown, the talk in Washington's intelligence and policy circles has turned to getting left-of-launch. This combination of science, technology, and operational art has the potential to disable or destroy North Korean missiles upon or within a few seconds of lift-off.[11] While this approach certainly seems tantalizing, there are two problems with it. First, a missile interceptor will have to be moving at hypersonic speed to destroy its target. This practice is so fraught with risk that military historians have likened it to "hitting a bullet with a bullet."[12] And, if the stakes are not high enough, shooting down one of North Korea's ICBMs upon ignition would put the US in a de facto state of war. Moreover, in some cases, a missile test is virtually indistinguishable from a hostile launch; intelligence that discerns between the two must be impossibly pristine. North Korea's military doctrine is modeled after the old Soviet *maskirovka*—a crafty, resourceful denial and deception campaign that makes positive identification of targets hard to attain.[13]

ABI demystifies North Korea's calculus and gives the DCGS the means to help military and civilian decision makers avoid a miscalculation. Chandler P. Atwood, a leading ABI advocate, defined the concept and its guiding principles handily in *Joint Force Quarterly*:

> ABI is an analysis methodology which rapidly integrates data from multiple [intelligence disciplines] and sources around the interactions of people, events, and activities, in order to discover relevant patterns, determine and identify change, and characterize those patterns that drive collection and create decision advantage.[14]

Many Airmen today—especially those who inhabit the DCGS—seek to stem the tides flowing from every sensor and to make sense of it, ideally without all the antiquated, human labor-intensive practices that come with processing, exploitation, and

dissemination (PED) of intelligence. With automation and machine-to-machine interaction, ABI can bridge the gaps between the virtual stovepipes our human intelligence (HUMINT), signals intelligence (SIGINT), geospatial intelligence (GEOINT), measurement and signatures intelligence (MASINT), and even open-source intelligence (OSINT) have become. Information from traditional intelligence sources such as these can be fused with data from nontraditional sources, such as moving target indicator (MTI) sensors, or space-based sensors such as overhead persistent infrared (OPIR) that captures IR emanations on the surface below them. This widens the information aperture and promotes the DCGS' transcendence from FMV imagery's narrow "soda-straw" view.[15] Fortunately, the bandwidth of our information technology systems is increasing at a rate that supports the surge of disparate data streams.[16] All-source analysts can correlate events quickly, discover anomalies and connections, and make comprehensive assessments with as much context possible. "The traditional process of stitching together sparse data," wrote Atwood, "is now evolving into a process of extracting conclusions from aggregation and distillation of big data."[17]

How can using ABI get us left-of-launch? Let's say we want to make a detailed examination of North Korea's missiles, not just ICBMs but the entire country's missile industry. ABI enables the automated georeferencing of the objects and entities associated with it—the people, places, and things that are responsible for the missiles' design, supply chain management, engineering, production, and deployment. ABI analysts determine remarkable events, locate them in space and time, and tune out extraneous information, so the identified problem can be solved more readily. It is in this stage where they put on their detective hats, looking forward and backward temporally, searching for activities that indicate missile checkouts from storage, possible routes to launch pads, or intercepts of communications between senior leaders in Pyongyang, to lower-ranking officers in North Korea's missile forces. Provided every facet of activity captured across the disciplines are georeferenced, with the aid of tools like Google Earth or ArcGIS, an ABI analyst can build an activity map that depicts the interactions between the target entities and then apply what Atwood calls "integration before exploitation."[18]

In the typical PED process, DCGS analysts look deeply into the intelligence discipline stovepipes, narrowly focusing on GEOINT for example, searching for the missiles themselves and their transporter erector launchers (TEL) moving from staging areas to hide sites or launch bays. In the old days, a correlation analyst might corroborate prelaunch activities by reaching into the SIGINT stovepipe for communications between missile convoys, or using OSINT to seek out provocative press statements from Pyongyang that might signal something is imminent. ABI moves analysts away from linear thinking and avails other intelligence disciplines for correlation analysis that may have otherwise been disregarded. It could have brought vital context to Pyongyang's threat to Guam, which certainly seemed menacing on its surface. But, a far different story takes shape when nontraditional sources of intelligence from MTI sensors are fused with information from other disciplines that correlate the threat itself with actual movements in time and space on the ground. Incorporating MTI data with an activity map might uncover if the North Koreans are using *maskirovka* to hide from our ISR assets, or bar us from seeing the total picture. Without bias for one intelligence means or the other ABI analysts

will give each piece of data equal consideration. SIGINT should not be favored over HUMINT because it is derived from more direct sources or technical means, and GEOINT should not be held up as absolute proof of movement to launch pads if MTI or electronic intelligence (ELINT) indicate facts to the contrary.

An ABI-focused approach considers every intelligence discipline as they interrelate with one another—spatially *and* temporally. This way, the analyst-as-detective can forensically judge if (or when) a launch might occur using a combination of historical data and data obtained in near real time. This is what Atwood calls "sequence neutrality;" a principle that considers "incidentally collected data" (information collected by happenstance) that "may be as significant or more significant than data collected in a more targeted fashion."[19] Of all ABI's principles, sequence neutrality is most important. It is the thing that permits analysts to take all present day and archival data into account when making fact-driven, unbiased, left-of-launch judgments about North Korea.

Weighing All the Options

In a left-of-launch scenario, a direct attack on North Korea's missiles would have little coercive value, and doing so could cause the situation to spiral perilously out of control. However, a cyberattack—if properly executed—would almost certainly cause less collateral damage and decrease the chances of a political liability for Washington. One of the revelations from the Stuxnet virus that infected Iran's uranium-enriching centrifuges was that it caused subtle variations in the machines' control code, causing them to spin out of control, and tear themselves apart.[20] These revelations beg the question—what industrial control systems (ICS) oversee the North Korean missile industry? Machine presses that heat, temper, and roll steel into tubes do a lot of the work—but mobile missiles tend to be air-gapped and isolated from any central command and control system that might be subject to interference or jamming.[21] Using the common space-based means of direction finding would be futile if enemy crews are instructed to halt any communications before launch. Small nations like North Korea are also adept at evading Air Force collection platforms, and their orbits would have to be adjusted to compensate for any loss of intelligence.[22] Applications that track commercial satellites are available on the open internet, making counterspace, as well as denial and deception, easy even for the most unsophisticated adversary.[23]

A good ABI analyst will have the entire North Korean missiles' industry charted with an activities map—from its machines down to the people who operate them. Collection managers could use these maps to reallocate assets and maximize potential so analysts will have the best available intelligence at the right time. Cyber operators can use the same data-driven technique to choose what logic ought to be discreetly implanted and at which missiles' manufacturer. A carefully crafted internet worm could circumvent all the obstacles; it could cause delicate, structural variations in metals that might defy the human eye. Missile production involves intricate engineering processes where the minutest defect in their engineering could cause catastrophic failure. Consider, too, that most of North Korea's missiles are mobile,

which is both a weakness and strength. Mobile missiles by their very nature are moving targets. But, once deprived of their mobility, they cannot evade detection or a counterattack. Wheels and tracks are comprised of common rubber and tires for mobile TELs. They are manufactured with antioxidants and stabilizers (like phenols) which prevent tread wear on the road and rot during storage.[24] Where do the North Koreans purchase them, or are they made domestically? In theory, for as much as Stuxnet caused nearly imperceptible damage to Iran's nuclear program, similarly "weaponized code" could decrease the shelf-life and reliability of North Korea's missiles and their TELs.[25]

The modern intelligence methods proposed here are just a few, but they cut through the fog of data smartly so that USAF intelligence analysts can decipher Pyongyang's true intentions and make recommendations that respond to it appropriately. In the meantime, forceful preemptive action has not been ruled out, but as Secretary Tillerson said, "All options are on the table."[26] His words signal each instrument of power will be evaluated deliberately before the US commits to action. If this is the case, then weaponized code applied precisely using ABI should be given its due consideration as well. Both make a powerful, one-two combination that will achieve the same effects as a conventional attack, but without the casualties an all-out war on the Korean Peninsula will surely bring. ✪

Notes

1. James Martin Center for Non-Proliferation Studies, "The CNS North Korea Missile Test Database," *Nuclear Threat Initiative*, accessed 27 December 2017, http://www.nti.org/analysis/articles/cns-north-korea-missile-test-database/.

2. Joseph S. Bermudez Jr., Jack Liu, and Frank Pabian, "The Games People Play: Has the Punggye-ri Nuclear Test Site Transitioned to Stand-by Status?," 19 April 2017, *38North*, http://38north.org/2017/04/punggye041917/#_ftn2.

3. Fox News, "North Korea: 'Super-Mighty Pre-Emptive Strike' Will Reduce US to Ashes," *Fox News*, 20 April 2017, http://www.foxnews.com/world/2017/04/20/north-korea-super-mighty-pre-emptive-strike-will-reduce-us-to-ashes.html. *See* Mason Richey, "Turning It Up to Eleven: Belligerent Rhetoric in North Korea's Propaganda," *Parameters* 46: no. 4 (Winter 2016–17): 95–96, https://www.hsdl.org/?view&did=799478.

4. David E. Sanger, "Rex Tillerson Rejects Talks with North Korea on Nuclear Program," *New York Times*, 17 March 2017, https://www.nytimes.com/2017/03/17/world/asia/rex-tillerson-north-korea-nuclear.html?_r=0. *See* Barack H. Obama, "National Security Strategy: February 2015," *Obama White House Archives*, accessed 5 May 2017, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

5. Joshua Stanton, Sung-Yoon Lee, and Bruce Klingner, "Getting Tough on North Korea: How to Hit Pyongyang Where It Hurts," *Foreign Affairs* 96, no. 3 (May–June 2017): 73, https://www.foreignaffairs.com/articles/north-korea/2017-04-17/getting-tough-north-korea.

6. The Department of Defense misclassified the 4 July 2017 missile launch as a test of an intermediate range missile. On 5 July, it was reclassified as an ICBM with a range of at least 5,500 kilometers. The missile was launched from Panghyon Airfield, an area 90 miles north of Pyongyang. The airfield

was not previously associated with North Korea's missile industry. *See* David Nakamura and Emily Rauhala, "Haley Hits China and Russia at U.N.," 6 July 2017, *Washington Post*, sec. A1.

7. Michelle Ye Hee Lee, "Analysis: N. Korea Bomb Test Was Far Larger Than Thought," *Washington Post,* 14 September 2017, https://www.highbeam.com/doc/1P4-1938384106.html. The article cites an assessment by the Air Force Technical Applications Center. It estimated the September 2017 explosion at Pungyee was between 70 to 280 kilotons. These yields surpass the Hiroshima bomb's strength, which was about 15 kilotons.

8. Anna Fifield, "North Korea's Latest Missile Launch Appears to Put U.S. Capitol in Range," *Washington Post*, 29 November 2017, https://www.washingtonpost.com/world/north-korea-fires-missile-for-the-first-time-in-more-than-two-months/2017/11/28/0c136952-d46c-11e7-9461-ba77d604373d_story.html?utm_term=.917a36b75f0e.

9. Anna Fifield, "More Than War, Kim Wants to Stay in Power, Experts Say," *Washington Post*, 11 August 2017, sec. A10.

10. Marc V. Schanz, "ISR After Afghanistan," *Air Force Magazine* 96, no. 1 (January 2013): 24, http://www.airforcemag.com/MagazineArchive/Magazine/2013/0113fullissue.pdf.

11. William Broad and David Sanger, "U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight," *New York Times*, 4 March 2017, https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html.

12. Michael J. Neufeld, "Hitting a Bullet with a Bullet: A History of Ballistic Missile Defense by Kenneth P. Werrell," *Journal of Military History* 65, no. 2 (April 2001): 574, http://www.jstor.org/stable/2677252.

13. Scott Gerwehr and Russell W. Glenn, *The Art of Darkness: Deception and Urban Operations* (Santa Monica, CA: Rand Corp., 2000), 33, https://www.rand.org/pubs/monograph_reports/MR1132.html.

14. Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Force Quarterly* 77 (April 2015): 26, http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-77/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/.

15. Ibid., 25.

16. During the opening days of Operation Iraqi Freedom, the United States used 30 times more bandwidth than it did during Operation Desert Storm in 1990, thus enabling the swift toppling of Saddam Hussein in 26 days. *See* Max Boot, "The New American Way of War," *Foreign Affairs*, 82, no. 4 (July-August 2003): 58, http://www.jstor.org/stable/20033648.

17. Atwood, *Activity-Based Intelligence*, 26.

18. Ibid., 27.

19. Ibid., 32.

20. Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, 14 April 2011, http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs.

21. John Schilling, "How to Hack and Not Hack a Missile," 21 April 2017, *38North*, http://38north.org/2017/04/jschilling042117/.

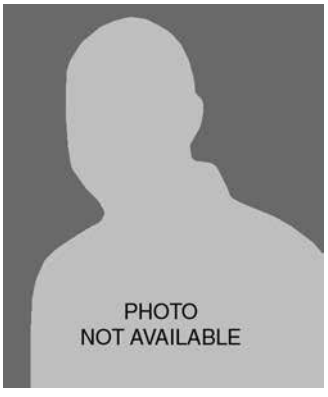
22. Gene H. McCall and John H. Darrah, "Space Situational Awareness: Difficult, Expensive—and Necessary," *Air & Space Power Journal* 28, no. 6 (November–December 2014): 7, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-28_Issue-6/SLP-McCall_Darrah.pdf.

23. Ibid.

24. Lawrence Fishbein, "Chemicals Used in The Rubber Industry: An Overview," *Scandinavian Journal of Work, Environment, and Health* 9, no. 2 (1983): 9, http://www.jstor.org/stable/40964975.

25. Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs* 92, no. 6 (November–December 2013), http://www.jstor.org/stable/23527014.

26. Sanger, *Tillerson Rejects Talks*.



Maj William Giannetti, USAFR

Major Giannetti (MS, St. Joseph's University) is an Air Force reservist assigned to the joint staff at the Pentagon, Washington, DC. His 20-year career spans time as a civil servant, Philadelphia police officer, and Department of Defense analyst. He was a part-time mission operations commander in the Virginia Air National Guard. Major Giannetti has also served two tours in Afghanistan.

Toward an Innovation Strategy for the US Air Force

Lt Col Christopher R. Cassem, USAF

In recent years, the US Air Force has made much of its history of innovation. The phrase, "Every Airman an Innovator" has been a popular mantra, and the tagline on our 70th-anniversary letterhead reads "Breaking Barriers Since 1947." As part of an effort to reinvigorate the Air Force's spirit of innovation, this year the chief of staff has tasked the USAF Blue Horizons fellowship to dig into rapid innovation processes. But no organization can suddenly become innovative overnight, even if it was born from an innovative past. This rule is especially true of an outfit as large and bureaucratic (and autocratic) as a military service. The Air Force needs a bona fide strategy to rebuild its innovative brand during the next several years.

This article proposes the groundwork for such an innovation strategy. The strategy begins with its diagnosis and guiding principles and concludes by suggesting some coherent actions necessary for implementation.[1] The key theme that will unite the elements of this story is that *Airpower is about Airmen, not airplanes* (or satellites or computers). Said another way, innovation is a people problem, not a technology problem. This Air Force innovation strategy, therefore, focuses on the human aspects of this issue, including empowerment, education, and evaluation.

The Crossroads of Strategy and Innovation

An organization cannot simply decide to become innovative. Ideas are only the beginning of innovation, and hard work coupled with organizational change must follow.[2] However, businesses and air forces are purpose-built, and innovation is always at odds with the day-to-day accomplishment of those purposes.[3] So for innovation to take root and thrive in the USAF, it must be intentionally separated from day-to-day mission execution (or the "performance engine"),[4] and the conflict between innovation and mission accomplishment must be understood and addressed. This separate innovation requires a long-term plan or strategy.

Author Richard Rumelt teaches that effective strategies are built on a three-part kernel of a diagnosis, guiding policy, and coherent plan of action.[5] So let's take Rumelt's advice and begin our innovation strategy with a solid diagnosis of our current

situation. Airmen today can easily rattle off names like Billy Mitchell, Curtis E. LeMay, Hoyt S. Vandenberg, and John R. Boyd as great innovators, but the list tends to fade away with Colonel Boyd. Generals now must cast their nets pretty wide to fill their speeches with even the simplest example of our continuing innovative prowess, while corporate technology gurus have key instances at their verbal fingertips. Today, the F-35 is equipped with—by and large—the same types of air-to-air missiles that F-4s carried in Vietnam. Innovation, it seems, became a lost art somewhere along the way.

There are several reasons why innovation became difficult to achieve in the modern Air Force, but I highlight three below. First, we aren't new anymore. We were born as a service to renegade parents like Mitchell, and our first leaders were revolutionaries and mavericks. The Air Force today has evolved, as most organizations inevitably do, into a "performance-engine" culture.[6] As a result, decision making is consolidated at the top and is focused on near-term mission accomplishment. This organizational structure is effective, but doesn't encourage or reward innovation unless it can provide cheap and immediate capabilities. Second, we don't teach innovation well. The Air Force has a formal education system that doesn't deliberately incorporate instruction on creative or critical thinking in a recurring way. Third, our talent management system is incapable of identifying which officers might be exceptional innovators and which might be exceptional performance managers.[7] While several other factors affect our innovation potential (like the relationship between the military and the defense-industrial complex and the role of Congress in the military decision-making process), they are largely outside the direct control of the chief of staff and secretary, so they aren't covered in this article.

What these three factors (empowerment, education, and evaluation) have in common is that they're all human-centric. So if our diagnosis tells us that these areas are critical to rekindling innovation, and that they all center on people, then our guiding principle must likewise be focused on Airmen. In other words, our strategy must develop innova*tors*, not innova*tion*. This idea is consistent with the recent academic conclusion that modern military successes and failures are the results of human factors.[8] It is good, tech-savvy leaders, not simply good technology that will bring victory.

The first two pieces of the kernel for an Air Force innovation strategy are now clear: a focus on the deliberate development of innovative Airmen through organizational empowerment, formal education, and effective evaluation. The third part of Rumelt's strategic kernel, specific and coordinated action, is covered next.

The Innovation Reformation

A strategy without action is meaningless, and innovation without execution goes nowhere. So if innovation is truly an Air Force goal, the service needs to convert the diagnosis and principles discussed above into concrete steps that are within the power of Air Force leaders to affect. This section outlines plans of action for the three critical areas of empowerment, education, and evaluation.

Let's begin with organizational empowerment. The Air Force is undeniably a bureaucracy, but that isn't all bad. Any organization as large as the USAF needs a bureaucratic backbone to function or it disintegrates into chaos. We're also autocratic, which is a necessity for a military service. This autocratic bureaucracy has functioned reasonably well as a performance engine, but it doesn't innovate well (particularly across bureaucratic and security stovepipes). Performance engines like our major commands and line squadrons should be respected, but innovators need to think about organizing and planning very differently than performance engines because innovation is nonroutine and uncertain.[9] The Air Force, therefore, needs to adapt its current organizational structure to allow for the existence of innovation teams that can try and fail quickly.

These innovation teams don't need to be large, permanent or disruptive to the current structures we already have in place. Innovators should be brought together to solve finite problems, empowered to investigate and implement solutions, and then returned to their "day jobs."[10] The process to stand up temporary organizations in the Air Force should be made easier and delegated as low as wing commanders, and temporary hiring authorities should be granted to allow for "outside help" from the civilian world or our joint/interagency partners.[11] An innovation direct reporting unit should also be established to disseminate innovation best practices to these temporary units. Finally, autocratic Air Force leaders must be prepared to not only commission innovation teams but also to buy into their solutions if proven to be effective. If commanders don't implement innovative initiatives because they fear, mistrust, or misunderstand the solution (or its associated technology), any attempt at building a culture of innovators will fail.

A note here is needed on the annual Combat Air Forces Weapons and Tactics (WEPTAC) conference and the new AFWerX organization. While WEPTAC rightfully remains one of the crown jewels of American airpower, the practice of assigning a small group of tactical experts a major war-fighting problem and giving them four days to solve it is not effective. The keys to innovation are the root-cause analysis of the underlying problem and informed, creative thinking to develop targeted solutions. These things cannot be reasonably accomplished in less than a week. A more effective method might be to assign the problem to the team at the 2018 WEPTAC and have an outbrief of the results for the year-long innovation effort at the 2019 conference. AFWerx, on the other hand, offers a promising method of innovating new technologies for the war fighter. But one potential danger with AFWerx is that it becomes (or is perceived as) an alternative to the USAF requirements and acquisition process rather than a supplement to it. This concern should be closely monitored as the AFWerx process takes shape.

The second area for action is innovation education. Critical and creative thought is necessary for innovation, and both of those traits are teachable. Yet, remarkably, the Air Force doesn't deliberately teach these skills at its institutions of higher officer learning in a consistent or coordinated way, which doesn't make any intuitive sense. If you want your officers to know certain things or act in certain ways, you must teach them those things. Moreover, as current cognitive research tells us, you can't just tell them once.[12] The message needs to be interleaved and reinforced over time for it to be retained.[13]

Innovation requires education, and the Air Force has the perfect educational vehicle to reach its entire officer corps at least once or twice in their careers. Air University (AU) offers both correspondence and in-residence programs for captains (Squadron Officer College), majors (Air Command and Staff College) and lieutenant colonels (Air War College). While not all officers will attend all of these schools, most officers will attend one or two if only in correspondence. These schools should have their curriculums modified to include innovation skill sets so that officers are continually infused with an innovation culture at as many opportunities as possible.

In addition to teaching innovation in the formal officer education programs, AU should also target officer accession programs (like the Reserve Officer Training Corps, Officer Training School, and the USAFA), and develop stand-alone courses. AU's new Continuum of Learning program would be an excellent venue for these kinds of opportunities, as would the Air Force's formal enlisted education system. The key is that all these various educational methods must be coherent, and the innovation principles must be sound and consistent (although varied for the audience, so they continue to be value-added as the message is reinforced as Airmen become more senior).

However, despite the best efforts of educators, it's important to note that not everyone can be good at innovation.[14] This brings us to the final point: the Air Force must redesign its evaluation system to allow for even basic talent management. The current Officer Evaluation System consists of two forms: the annual officer performance report (OPR) and the promotion recommendation form (PRF), which aggregates data from the OPRs for review by a promotion board. Both the OPR and PRF are primarily based on a numerical stratification system (that is, Joe is my number 1 of 16 majors). The idea is that a collection of good stratifications over several OPRs will roll up onto a PRF, and a promotion board can get a good sense of how talented an officer is based on consistently strong stratifications (or lack thereof). This idea may seem like a reasonable way to manage a promotion system that processes many thousands of officers on any given board, but it is seriously flawed both quantitatively and qualitatively.

This stratification process is mathematically unsupportable in three ways. First, there is no possible way to compare the relative abilities of one officer ranked third of 82 majors and another ranked second of 23 majors. Who is better, the number three or the number two? Does the bigger denominator matter? What about the following two rankings: first of 37 and first of 12? Is one number one better than the other? There's no statistical method for direct comparison. The second reason this system isn't logical is that it uses objective mathematics to quantify subjective distinctions. As a result, there's no way to tell the relative gap in abilities between the major ranked second of 23 and the one ranked third of 82. Third, this system is susceptible to two known errors in the human brain: the availability heuristic and a phenomenon known as "What You See Is All There Is" or WYSIATI.[15] A common illustrative example is that officers with more direct daily contact with their senior rater are often stratified more favorably than their peers. But how does a wing com-

mander know her executive officer is truly better than the 81 other majors in the wing she doesn't see every day?

These mathematical shortcomings alone are enough to question the effectiveness of this process, but the bigger impact to innovation is the failure of this stratification system to account for any qualitative assessment. To illustrate, consider two majors with strong records with multiple number one/XX stratifications. Are they good? Probably. But what are they good at? Were they number ones because they were excellent technical experts (amazing pilots or engineers, for example), or because they possessed strong leadership talents? How do you know which of these consistent number ones is more articulate or more suitable for attaché duty because of skills in multicultural negotiations? You don't. Our system may tell you who the best seems to be, but it can't tell you what anybody is best at. So who are the best innovators? Who are the best performance managers? Who should I send to which developmental education program to develop those skills? We, collectively, have no idea, so we default to the only measure we have—who's number one?

The USAF needs a new evaluation system that captures the specific talents of our officers and dispenses with an artificial stratification system primarily focused on the promotion process. A talent management system needs to collect data on skill sets, not relative scales of greatness (especially scales with no means of direct comparison). A new system will allow the Air Force to identify innovation leaders, as well as other talents (instructors, joint-minded officers, testers, attachés, and so forth), and place them appropriately rather than randomly.

Three Es toward Innovation

The Air Force realizes that it must, in part, rely on innovation to stay current in an age of rapid obsolescence. However, innovation is a culture that must be built and sustained over time, and it relies on people to make it effective. In the end, airpower is made possible by Airmen, not the airplanes or the systems they operate. Similarly, humans perform the innovation; it is not done by the technology they inspire or adapt. With that in mind, the Air Force must create the conditions necessary for innovators to thrive by reforming three specific areas: organizational empowerment, formal education, and effective evaluation. These "3 Es" are all within the span of control of USAF senior leadership and are necessary and sufficient conditions to reestablish innovation as a core trait of our service. ✪

Notes

1. Richard P. Rumelt, *Good Strategy, Bad Strategy* (New York: Crown Business, 2011), 77.
2. Vijay Govindarajan and Chris Trimble, *The Other Side of Innovation: Solving the Execution Challenge* (Boston, MA: Harvard Business Review Press, 2010), 3.
3. Ibid., 11.
4. Govindarajan and Trimble, *The Other Side of Innovation*, 3.
5. Rumelt, *Good Strategy, Bad Strategy*, 77.
6. Govindarajan and Trimble, *The Other Side of Innovation*, 29–30.
7. Ibid., 51–74.

8. Azriel Lorber, *Misguided Weapons: Technological Failure and Surprise on the Battlefield* (Dulles, VA: Brassey's, 2002), 33–34.
9. Govindarajan and Trimble, *The Other Side of Innovation*, 15.
10. Ibid., 166.
11. Ibid., 53–59.
12. Peter C. Brown, Henry L. Roediger III, and Mark A. McDaniel, *Make it Stick: The Science of Successful Learning* (Cambridge, MA: The Belknap Press, 2014), 63–66.
13. Ibid.
14. Govindarajan and Trimble, *The Other Side of Innovation*, 174.
15. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus, and Giroux, 2011), 127–36.

Lt Col Christopher R. Cassem, USAF

Lieutenant Colonel Cassem (BS, University of Florida; MS, University of San Diego) is a fellow in USAF Blue Horizons, Maxwell AFB, Alabama. His research focus is the development of high-endurance offensive airpower through the use of radioisotope batteries. He is an F-15E instructor combat systems officer who has flown combat sorties in Operations Southern Watch, Enduring Freedom, and Iraqi Freedom. Lieutenant Colonel Cassem was previously the commander of the 28th Test and Evaluation Squadron, Eglin AFB, Florida and is a graduate of the USAF Weapons School.

The New Matrix of War

Digital Dependence in Contested Environments

Capt Keith B. Nordquist, USAF

> *Do you believe that my being stronger or faster has anything to do with my muscles in this place?*
>
> —Morpheus (Laurence Fishburne), *The Matrix*

Simply being stronger or faster is no longer enough when operations hinge on cyber capabilities, and this dependence exposes vulnerabilities. Since the end of the Cold War, the DOD has proven its strategic advantage across the spectrum of conflict in quantity, quality, and readiness. This kinetic strength is what allies rely upon and enemies fear, equating American dominance to mission assurance.[1] In the digital age, the cyber domain underpins this dominance and preserves the ability to project asymmetric kinetic power worldwide at any time.[2] In kind, adversaries are beginning to acknowledge America's reliance on digital tools in preserving its strategic advantage. As adversaries develop robust digital interference competencies, the conflict moves beyond an exclusively near-peer competition of conventional forces and becomes a comprehensive conglomeration of contested domains. The rhetorical question famously asked by Morpheus in *The Matrix* trilogy captures the essence of this digital dependence and the thoughtfulness it necessitates; strength and speed do not matter within the matrix.[3] The question's import is equally pertinent today; when projecting military muscle requires digital tools, virtual failures affect reality.

The strategic imperative for a new matrix of war is clear—cyber domain operations are the bedrock of American military strength today, and consequently, they are its greatest liability for tomorrow. In particular, those near-peer competitive advantages of the DOD in command and control, deployment and distribution, and weapon system technology exist because of the complementary and enabling nature of cyberspace.[4] Imagine prosecuting an operation at the tactical or strategic level without cyber tools enabling freedom of maneuver—even for just one day. If an adversary disrupts, interrupts, or denies US cyber capabilities, American superiority no longer matters—the DOD cannot employ its strategic advantage. A day without cyber could be catastrophic if the impact is a nullification of a capability to project power. Exercising a holistic vulnerability assessment, the cyber domain is critical to the application of kinetic power. Through reflection and analysis, the DOD must adjust in kind for the increasing risk it encounters when inextricably linking the military enterprise with the digital tools it needs to function.

The implicit charge is to understand and counter possible strategic shock from a cyber attack and appreciate the depth of capabilities that exist in cyberspace. By adjusting military planning cognitive associations, to appreciate the depth of capabilities that exist in cyberspace, the DOD can continue to assure mission success, even during cyber attacks and degraded operations. This change in DOD cognitive association would illustrate how kinetic effects are secondary to digital dominance and inform strategic solutions that deter and defeat cyber domain threats. The future requires constructing an updated, globally integrated strategy that recognizes a superior force attracts digital disruption. Contemplating a day without cyber means acknowledging risk across domains and understanding that conflict transcends physical battlefields, especially as the battlespace becomes more transregional, multidomain, and multidimensional.[5] The new matrix of war in the digital age necessitates concerted transformation, both to appreciate the current calculus of conflict and acknowledge the strategic shock of denied kinetic effect delivery.

Strategic Shock

Disruptive effects to digital tools in the cyber domain ignore the traditional kinetic understandings of conventional warfare. Currently, military planners tend to focus on two incomplete assumptions: (1) contested environments exist in the designated conflict theater, and (2) militaries win wars where kinetic force meets kinetic force.[6]

Assumptions like these fail to adequately address the evolving complexities and connectedness of the new matrix of war. If military planners do not accept that adversaries may achieve strategic outcomes without kinetic power, the US may be susceptible to *strategic shock*.[7] Strategic shock is similar to the principle of shock and awe—instead of overpowering an adversary's physical force to the point of paralysis, one strategically overwhelms their ability to orient themselves in policy or directing forces. In this context, strategic shock is cognitive in nature, encompassing the perceptions, experiences, and psychologies of the opponent.[8] Consequently, to induce strategic shock in an adversary, one must disrupt these cognitive associations.

The DOD's cognitive depth is rooted in its cyber capabilities, representing the crucial foundation of American military execution. However, DOD resources and energies remain focused on more institutionalized cognitive associations concerning employment—better managed forces, global deployability, and more advanced weapon technologies.[9] Understanding the need for a greater focus on cyber domain security requires a cognitive acceptance that the DOD's depth should be associated with its digital tools, not just its superior capability. Should an adversary attack the DOD's digital dependence without this association, the potential for strategic shock is disastrous. Specifically for the military, an adversary does not need to compete with the DOD's superior capacity, capability, or availability—they need only degrade the ability to employ its advantages to produce strategic effects. More broadly, an enemy can deliver superior effects over a superior force if they disrupt the cognitive depth of their function. A lack of cognitive association to that depth extends the vulnerability and exacerbates the effect. This widens the aperture for understanding DOD risk mitigation, and it expands planning from the frontline to the point of

embarkation and from the weapon system to its digital footprint. In particular, those strategic capabilities of the DOD most susceptible to strategic shock without a change in cognitive association are also its employment strengths—command and control (C2), deployment and distribution, and weapon system technology. Each of these strengths needs strategic solutions to deter and prevail in contested environments.

Contested Environments

The contested cyber domain embodies conflict that is no longer exclusive to an abroad, permissive battlefield.[10] Instead, digital tools extend the conflict to the homeland and limit access of the US; one will have to fight to get to the fight in the new matrix of war. C2 is the critical element needed to guide the projection of power from garrison to a conflict area. An examination of the cyber domain needed to enter conflict in a transregional, multidomain context encompasses the tools used for tactical execution, operational guidance, and strategic oversight.[11] Today, the systems to communicate up and down the chain of command are digital, from planning to tasking to executing. Whether through constellations of satellites or cyberspace networks,[12] DOD C2 and communication rely upon tools almost exclusively enabled through the cyber domain to enter an engagement. Designed for decentralized execution,[13] the demands on these digital tools require global awareness and dedicated focus to preserve access. However, each combatant command often employs C2 tools in isolation by centralizing their execution tools, requesting forces, and operating separately from geographic and functional partners. This operating construct represents the DOD's current cognitive association,[14] but it is limited to antiquated and conventional dynamics. The DOD should instead pursue more globally integrated planning for its C2 functions to embrace the comprehensive digital capabilities of its enterprise. Through a worldwide situational awareness, the DOD can cognitively associate C2 with tools that transcend terrestrial designations and authorities. If unaddressed, enforcing parochial C2 relationships in geographic areas of responsibility incurs greater risk of strategic shock.

A critical utility of capable C2 is to manage the deployment and distribution of the military, delivering and sustaining a decisive force to the place of need. Cognitively linking the battlefield to its distribution network expands the contested environment and thrusts logistics into a precarious, strategic center of gravity role.[15] No longer will the DOD be able to operate the global distribution network with impunity as it has for the last 70 years. Today, the end-to-end functionality of the system, from combatant commander request to sourcing and delivery, relies almost completely upon digital tools. The DOD must realistically account for the potential of denied access to these power projection tools so it can disperse the gravity from its logistics cyber dependency. Through cyber perseverance and resilience strategies, the DOD must fight through degradation and preserve the ability to deliver options to joint force commanders. Stove-piped cognitive associations of domain-specific conflict no longer support the global battlespace. Consequently, joint force power projection cannot just be about a capability to effectively and decisively distribute the force; it must also be about its enabling digital network. This multitiered and

worldwide view more accurately informs needs and requirements, countering the threat of strategic shock.

In a globally integrated battlespace, DOD weapon systems also depend on digital technologies to operate, and these physical tools are equally susceptible to cyber intrusions. Reliant upon GPS, operating software, and unclassified network acquisition processes,[16] weapon systems are subject to disruption possibilities from development to employment. Moreover, these same weapon systems are subject to attrition and mobilization complications.[17] Failing to consider and plan for cyber domain reliance undermines the survivability and movement of DOD weapon systems, the kinetic equipment needed when prosecuting campaigns. Without addressing how attrition, mobilization, and cyber vulnerabilities converge, the DOD may fail to defend against adversaries when moving resources and employing weapon systems at the speed of war. At worst, a failure to cognitively associate cyber threats with weapon system development may foreshadow fewer available options for joint force commanders, causing the DOD to lose potency when projecting power and lethality. Since losing options costs strategic outcomes, the DOD must address weapon system susceptibility to cyber attack to avoid strategic shock. If not, it could be unprepared to counter the extensive liabilities of the cyber domain.

Strategic Solutions

To deter, deny, degrade, or defeat the threat of strategic shock in C2, deployment and distribution, and weapon system technology, the DOD must holistically address the threat of cyber attack.[18] This requires investigating two broad problem sets with concerted focus: (1) how to preserve American superiority in increasingly contested environments, and (2) how to craft a superior strategy that protects our power projection ability across domains.

These focus areas consider the interdependent impacts of cyberspace problems as the strategic framework to engage the new matrix of war, illustrating the need for a paradigm shift. By balancing superior quantity, quality, and readiness of the force with superior strategy, the DOD can account for its digital dependence, deter aggressive action, and prevail when disrupted. The strategic solutions presented underline the DOD's required cognitive shift in understanding its depth, where superior kinetic effects are secondary to superior posturing with digital tools. Without fundamentally changing its focus to the actual depth of the military's power, it may fail to advance or even preserve its strategic advantage.

The globally deployable and dominant force of the DOD represents an inherent target for adversaries in the cyber domain.[19] Complicating this contested environment, the force is constantly under tension to balance superior quantity, quality, and readiness. Ostensibly, military planners should focus on all three—develop a robust organic capacity of the best technologies, ready to be deployed at a moment's notice.[20] However, budgetary constraints and fluctuating military demands make this difficult, if not impossible, creating a need to inject greater agility and velocity in the execution of military acquisition and operations processes.[21] Cognitively associating a superior force in contested environments with the cyber domain requires the explicit pursuit

of gains in force efficiency and globally integrated planning. Using advanced digital tools through the cyber domain, the DOD can prepare for the next high-end conflict by purposefully leveraging existing force quantity, quality, and readiness to generate more capability. Specifically, optimization can preserve a superior force by advancing efficacy in tasking and execution with evolving technologies like automation, machine learning, and algorithmic predictive analysis.[22] This data-driven mindset in managing, enhancing, and deploying a superior force spirals current quantity, quality, and readiness by reducing effort and waste. By making their equilibrium easier to manage and improve in resource-constrained and contested environments, the DOD also capitalizes on its inherent digital depth.

To deter and prevail against cyber attacks in this data-centric community, the DOD must better deny adversary access and promote greater redundancy.[23] Together, they preserve kinetic advantages as cyber assurance strategies. If an enemy is unable to penetrate a hardened network, whether through a securely enabled cloud-based infrastructure or robust authentication protocols from trusted transactions or quantum entanglement, the DOD minimizes vulnerabilities.[24] When the technological cost of entry increases, the eligible pool of capable hostile actors becomes smaller, enabling more tailored and direct address. However, a network barrier limiting access to these most capable adversaries does not disperse vulnerabilities or safeguard functionality. For the DOD to prevail and ensure the utility of its depth, it should move from a link-in-a-chain cyber processing dynamic to a portion-of-a-whole model.[25] Spreading the risk across both a physical and virtual web ensures the capability of a superior force by minimizing exposure and diffusing weaknesses across a network. A web model negates an adversary's ability to totally disrupt operations through the scope and level of effort required to affect them all. Together, synergizing a robust firewall with a dispersed digital footprint preserves the superior force's advantage, especially if called to action in cyber-degraded operating environments.

The evolving construct of contested environments presents a unique opportunity to strategically assess the cyber assumptions in military strategy and recognize how enemies seek asymmetric or unconventional advantages.[26] In particular, crafting a broader strategy matrix that acknowledges how C2 deployment and distribution, and weapon system technologies are contested through the cyber domain allow for a more global and comprehensive understanding of military operations. A broader strategy matrix also counters the potential for strategic shock by grounding the cognitive associations of the DOD within its digital dependence. With an organizational mindset that focuses on mission assurance in a cyber-enabled and potentially degraded environment, the DOD can not only promote the evolution of digital capabilities but also protect current, critical cyber functions from a disadvantage. It is empowered to transform with the evolved battlespace, blurring the lines between domains and systems through strategic planning to assure the mission.[27]

As cyber becomes more multidomain in execution and function through globally integrated planning, the DOD must also address roles and responsibilities, authorities, and dynamic prioritization in relation to the cyber threat.[28] Specifically, it must explore operational models that support its digital depth, leveraging current and future cyber tools to protect advantages, deny adversary access, and prevail against hostile action. Additionally, these operational models need to address the cognitive tension

between employing kinetic advantages and enabling them. The DOD cannot accept losing capability or forces in unacceptable numbers along this digital employment connection but may be susceptible to such losses with planning constrained to domain-specific outcomes.

To prevent strategic shock from stove-piped cognitive associations, strategic risk must continuously address the possibility of interference in those digital tools that connect the military planner to the warfighter, the cyber thread that connects all levels of the DOD.[29] The military should also reassess strategic risk with a global perspective, to redress the permissive geographic assumptions that have permeated conflict since the Second World War, centered on the belief that the US can operate at will. Future conflicts will not be limited to a single combatant command, so cognitive associations require adjustment to view kinetic effects as products of robust and global cybersecurity. Moreover, contested environments make the binary relationship between peace and war murkier due to persistent adversarial action in the cyber domain. Digital tools are constantly at risk, so preventing strategic shock requires relentless advocacy. As with preserving a superior force, DOD planners should focus on how the military enterprise is more resilient without linked or linear processes, spreading resources out into a web to promote survivability. The DOD's digital dependence cannot prevail with a sequential chain model and single points of failure.

A New Matrix

The cyber domain threats of tomorrow require understanding strategic shock today. Of note, the new matrix of war does not seek to supplant or undermine the importance of a superior force, whether through its C2, deployment and distribution, or weapon system technology. Instead, it merely acknowledges the DOD's digital dependence to employ these advantages, embracing a cognitive association between military depth, cyber domain capability, and strategic shock vulnerabilities. Much like the mythical Morpheus is the Greek god of dreams, the fictional character from *The Matrix* challenges military planners to see reality differently and appreciate virtual vulnerabilities. The DOD's reliance on cyber tools is like a dream, both incorporeal yet subject to influence, manipulation, and disruption. Without understanding how adversaries pursue asymmetric advantages against superior forces, the DOD cannot fully appreciate the risk it accepts through its digital dependence.

Projecting power into contested environments requires continuously examining DOD depth and thinking through operating without cyber capabilities as well. Success now requires highlighting key digital functions the military must have to operate, where cyber vulnerabilities need tactical and strategic awareness of permissiveness and freedom of maneuver. Empowered by a comprehensive discussion of global integration and interconnectedness, the American kinetic power advantage is only part of this equation for military planners. The DOD must understand how mission assurance to deliver kinetic effects is a product of securely operating in the cyber domain. To divest the two is to force an analog solution onto a digital age's problems, or as Morpheus might quip, to stay in Wonderland. The US cannot afford delusion and

must acknowledge how emboldened adversaries will seek to disrupt our advantages, attacking the military's cyber depth and not necessarily its conventional forces to achieve strategic effects. Strength and speed alone do not matter within the new matrix of war.

Further discussion, research, and policy are required to move beyond the limitations of the current cognitive association. To overcome paralysis and prepare for the unexpectedness of future contested conflicts, the DOD must relentlessly pursue solutions to deter cyber threats, prevail against them, and preclude suffering from strategic shock. The new matrix urgently requires better global integration, superior cyber security and resilience, and optimized dominance with fewer resources, demanding more investment into digital tools that promote efficiency and less focus on geographic authorities. The DOD can pioneer this future out of necessity, but only as fast as it can cognitively accept its digital dependence. If the US fails to institutionally associate power projection with the digital tools it requires, the DOD may not prevail in a day without cyber. ✪

Notes

1. Michael O. Wheeler, "The Changing Requirements of Assurance and Extended Deterrence," *Institute for Defense Analyses*, July 2010, iii–iv, http://www.dtic.mil/docs/citations/ADA550264.

2. Maj Gen Richard Weber, USAF, and Col Mark E. Ware, USAF, "Cyberspace Mission Assurance: A New Paradigm for Operations in Cyberspace," *High Frontier* 6, no. 4, (August 2010): 3–7, http://www.dtic.mil/docs/citations/ADA549792.

3. "Question Asked by Morpheus," *The Matrix*, directed by Lana Wachowski and Lilly Wachowski (1999; Burbank, CA: Warner Home Video, 1999), DVD.

4. Col Clinton J. Ancker III, USA, Retired, and Lt Col Michael Flynn, USA, Retired, "Exercising Command and Control in an Era of Persistent Conflict," *army.mil*, 3 May 2010, https://www.army.mil/article/38412/exercising-command-and-control-in-an-era-of-persistent-conflict/; Eric Peltz and Marc Robbins, "Leveraging Complementary Distribution Channels for an Effective, Efficient Global Supply Chain," *RAND Corporation*, 2007, vii–x, http://www.dtic.mil/docs/citations/ADA473027; US Government Accountability Office (GAO), *Defense Acquisitions: Assessments of Selected Weapon Programs*, Report to Congressional Committees (Washington, DC: US GAO, March 2017), 5–6, http://www.dtic.mil/docs/citations/AD1032079; and Joshua T. Hartman, "Exploring the Complementary Nature of Cyber and Space Operations," *High Frontier* 6, no. 4 (August 2010): 31–34, http://www.dtic.mil/docs/citations/ADA549792.

5. Jim Garamone, "Dunford: Command, Control Must 'Keep Pace' in 21st Century," *DoD News, Defense Media Activity*, 4 January 2016, https://www.defense.gov/News/Article/Article/639844/dunford-command-control-must-keep-pace-in-21st-century/.

6. Joint Chiefs of Staff, "The Joint Force in a Contested and Disordered World," *The Joint Operating Environment 2035*, 14 July 2016, ii–iii, http://www.dtic.mil/docs/citations/AD1012885; and Maj Paul J. Blakesley, British Army, "Operational Shock and Complexity Theory," monograph (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 26 May 2005), 69–71, http://www.dtic.mil/docs/citations/ADA437516.

7. Col Peter J. Lane, USA, "Strategic Shock: Managing the Strategic Gap," strategy research project (Carlisle Barracks, PA: Army War College, March 2013), 1–5, http://www.dtic.mil/docs/citations/ADA589203.

8. Maj Anthony L. Marston, USA, "The Efficacy of Cognitive Shock," monograph, (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, May 2015), 33–35, http://www.dtic.mil/get-tr-doc/pdf?AD=AD1001654.

9. Lt Col Thomas M. Jordan, USA, "Versatility and Balance: Maintaining a Full Spectrum Force for the 21st Century," this is capped in original document Strategy Research Project, (Carlisle Barracks, PA:

Army War College, 6 April 1998), 22–24, http://www.dtic.mil/docs/citations/ADA343362; Lt Col Russell F. Miller, USA, "Developing and Retaining Information Warriors: An Imperative to Achieve Information Superiority," Strategy Research Project, (Carlisle Barracks, PA: Army War College, 29 February 2000), 2–3, http://www.dtic.mil/docs/citations/ADA377713; and Justin A. Thompson, "Improving Department of Defense Global Distribution Performance Through Network Analysis," (master's thesis, Monterey, CA: Naval Postgraduate School, June 2016), 41–42, http://www.dtic.mil/docs/citations/AD1026843.

10. Peter C. Mastro, "So Near and Yet So Far: Choices and Consequences of the Stand-In and Stand-Off Approach," (master's thesis, Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 1 June 2015), 121–25, http://www.dtic.mil/docs/citations/AD1015800.

11. CDR Lawrence Rice, USN, "Technology's Impact on Command and Control: How Much Does the Operational Commander Need?," final report (Monterey, CA: Naval Postgraduate School, 19 May 1997), 13–14, http://www.dtic.mil/docs/citations/ADA328120.

12. Dan Shen, Genshe Chen, Jose B. Cruz Jr., Erik Blasch, and Martin Kruger, "Adapting C2 to the 21st Century: Game Theoretic Solutions to Cyber Attack and Network Defense Problems," conference paper (Rockville, MD: 12th International Command and Control Research and Technology Symposium, June 2007), 1–2, 16, http://www.dtic.mil/docs/citations/ADA481265; and Brig Gen Kurt S. Story, USA, and Peter M. Stauffer, "Delivering It to the Soldier," *High Frontier* 6, no. 4 (August 2010): 16–19, http://www.dtic.mil/docs/citations/ADA549792.

13. Lt Col Robert C. Johnson, USA, "Fighting with Fires: Decentralize Control to Increase Responsiveness," monograph, (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 2001), 37–41, http://www.dtic.mil/docs/citations/ADA403795.

14. Maj Richard McGlamory, USAF, "Defense or Diplomacy? Geographic Combatant Commands," (master's thesis, School of Advanced Air and Space Studies, Air University, Maxwell, AFB, 1 June 2011), 55–56, http://www.dtic.mil/docs/citations/AD1019397.

15. Thomas Lorenzen, "The Edge of Chaos: Emergent Factors in the Information Environment," *The Strategy Bridge*, 9 May 2017, https://thestrategybridge.org/the-bridge/2017/5/9/the-edge-of-chaos-emergent-factors-in-the-information-environment; and Maj Gen Arnold Punaro, USMC, Retired, Bill Phillips, John O'Connor, and Capt Garrett Campbell, USN, "Logistics as a Competitive War Advantage," technical report (Washington, DC: Defense Business Board, 20 October 2016), 2–5, http://www.dtic.mil/docs/citations/AD1020304.

16. Marc A. Thibault, Jr., "GPS: Public Utility or Software Platform?," technical report (Monterey, CA: Naval Postgraduate School, 1 September 2016), 57–62, http://www.dtic.mil/docs/citations/AD1030085; John B. Dickens and Dean R. Dukes, "Innovative Decentralized Decision-Making Enabling Capability on Mobile Edge Devices," technical report (Monterey, CA: Naval Postgraduate School, 1 September 2015), 85–88, http://www.dtic.mil/docs/citations/AD1008918; and Col Robert L. Tremaine, USAF, Retired, "Demonstrating Cyberspace Superiority in an Acquisition World," *High Frontier* 6, no. 4 (August 2010): 62–65, http://www.dtic.mil/docs/citations/ADA549792.

17. J. B. Bartholomess, Jr., "The Issue of Attrition," journal article (Carlisle Barracks, PA: Army War College, Spring 2010), 17–18, http://www.dtic.mil/docs/citations/ADA522310; and Maj Christopher G. Williams, USA, "Fielding a Division Staff in the Modern Day," technical report (Fort Leavenworth, KS: Army Command and General Staff College, 10 June 2016, 58–61, http://www.dtic.mil/docs/citations/AD1020377.

18. Martin Libicki and Lt Gen Robert Elder, USAF, Retired, "Mission Assurance in the Face of Cyber Attacks," *High Frontier* 6, no. 4 (August 2010): 24–27, http://www.dtic.mil/docs/citations/ADA549792.

19. Lt Col William D. Bryant, USAF, "Cyberspace Superiority: Dominating the Digital Frontier," (thesis, Maxwell AFB, AL, School of Advanced Air and Space Studies: January 2014), 47–48, http://www.dtic.mil/docs/citations/ADA622182.

20. Laura J. Junor, "Managing Military Readiness," *Strategic Perspectives*, 23 Institute for National Strategic Studies, (Washington, DC: National Defense University, February 2017), 1, http://www.dtic.mil/docs/citations/AD1030355.

21. Chad DeStefano, Kurt Lachevet, and Joseph Carozzoni, "Distributed Planning in a Mixed-Initiative Environment: Collaborative Technologies for Network Centric Operations," conference paper (Rome, NY: Air Force Research Laboratory, October 2007), 20, http://www.dtic.mil/docs/citations/ADA489219.

22. George K. Baah, Thomas Hobson, Hamad Okhravi, Shannon C. Roberts, William W. Streilein, and Sophia C. Yuditskaya, "A Study of Gaps in Cyber Defense Automation," Technical Report no. 1194

(Lexington, MA: Massachusetts Institute of Technology, Lincoln Laboratory, 13 October 2016), 39–40, http://www.dtic.mil/docs/citations/AD1021685; Liang Xiong, "On Learning from Collective Data," (doctoral thesis, Carnegie Mellon University, Machine Learning Department, December 2013), 142–43, http://www.dtic.mil/docs/citations/ADA598234; and L. Richard Moore Jr., "Cognitive Model Exploration and Optimization: A New Challenge for Computational Science," conference paper (Mesa, AZ: Lockheed Martin Systems Management, Air Force Research Laboratory, Warfighter Readiness Research Laboratory, 24 March 2010), 160, http://www.dtic.mil/docs/citations/ADA553672.

23. Lt Col Shane H. Connary, USAF, "Computer Network Operations Command and Control: A New Perspective," final report (Monterey, CA: *Naval War College*, 22 October 2009), 1–3, http://www.dtic.mil/docs/citations/ADA513948.

24. Matthew Presley, "Beyond Data Services: Cloud Processing for Net-Centric Information Distribution," *High Frontier* 6, no. 4, August 2010: 57–61, http://www.dtic.mil/docs/citations/ADA549792; Andrew Miller and Rob Jansen, "Shadow-Bitcoin: Scalable Simulation via Direct Execution of Multi-threaded Applications," research report (Monterey, CA: Naval Research Laboratory, 10 August 2015), 6, https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/15-1231-1593.pdf; and Rodney Van Meter, "Security of Quantum Repeater Network Operation," final report (Fujsawa, Japan: Keio University, 3 October 2016), 3–5, http://www.dtic.mil/docs/citations/AD1019872.

25. Lt Gen Charles Croom, USAF, Retired, "The Cyber Kill Chain: A Foundation for a New Cyber Security Strategy," *High Frontier* 6, no. 4 (August 2010): 52–56, http://www.dtic.mil/docs/citations/ADA549792.

26. Barry R. Schneider, "Asymmetric Rivals: The Enemy Next Time," *The War Next Time: Countering Rogue States and Terrorist Armed with Chemical and Biological Weapons, 2nd edition,* ed. Schneider and Jim A. Davis (Maxwell AFB, AL: USAF Counterproliferation Center, April 2004), 1, https://www.hsdl.org/?view&did=446550.

27. Lt Col Patrick J. Obruba, USAF, "Breaking Stovepipes: Bridging Gaps in Air Force Industrial Control Systems Management to Enable Multi-Domain Mission Assurance," technical report (Maxwell AFB, AL: Air War College, 16 February 2016), iv–1, http://www.dtic.mil/docs/citations/AD1037194.

28. Michael J. McNerney, "Department of Defense and Security Cooperation: Improving Prioritization, Authorities, and Evaluations," technical report (Santa Monica, CA: RAND Office of External Affairs, 9 March 2016), 3–4, http://www.dtic.mil/docs/citations/AD1014435.

29. Maj Michael D. Pritchett, USAF, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment" (master's thesis, Wright Patterson AFB, OH: Air Force Institute of Technology, 14 June 2012), 39–41, http://www.dtic.mil/docs/citations/ADA563712.

Capt Keith B. Nordquist, USAF

Captain Nordquist (BA, USAFA; MA, Embry-Riddle Aeronautical University) earned his commission in 2008 as a distinguished graduate. He is a strategic initiatives officer with the Commander's Action Group, US Transportation Command at Scott AFB, Illinois. Before his current position, he completed two assignments as a C-5 instructor aircraft commander and served in training, safety, inspection, flight command, and executive officer positions at squadron, wing, and major command levels.

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

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

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

One of the most fascinating early chapters in the book (chap. 2) discusses deterrence theory and its application by emerging nuclear states. This (deterrence theory) is the foundation that formalizes strategy, and it quickly becomes apparent to the reader that a myriad of subjects need to be analyzed. Having challenged Clausewitz, the editors substantiate their claims that "more is better" with a broadening discussion on several factors that affect the resultant strategy and political status quo. No reader is left doubting that nuclear strategy is a complicated, devious, and fully expansive subject. Those of us who thought we had a good understanding of it will find additional gems of knowledge to admire.

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

Nine of twelve chapters focus on individual nation-states, and because each is a stand-alone essay, they can be read in any order. Nevertheless, their selection for inclusion is interesting in itself. China is one of the official nuclear states, having detonated a device in 1964 and thus meeting the conditions laid out in Article IX of the Nuclear Non-Proliferation Treaty. At the other end of the spectrum, Japan also warrants an essay even though it is not

a nuclear state. Yoshihara and Holmes include Japan because it does have a robust deterrence policy, linked closely to its relationship with the United States. Developing a nuclear weapon capability, however, is not on Japan's near-political horizon. South Africa is featured as well, having developed a covert nuclear program that it subsequently relinquished. The nuclear and conventional impasse between India and Pakistan ensures that these two nuclear nations receive similar yet contradictory essays. The ambiguity of Iran is discussed. The motivations, policies, and strategies of North Korea come under the microscope. Since the book was published, North Korea has continued to develop and improve its nuclear technology. In hindsight, the essay offers fascinating insight into how the rationality of new nuclear states is difficult to predict with any degree of certainty. The contributors offer many surprises, and I have deliberately not expanded on the details. All I will say is that to gain full benefit, readers should question—really question—the balance of argument.

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

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

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

Strategy: Context and Adaptation from Archidamus to Airpower edited and authored by Richard J. Bailey Jr., James W. Forsyth Jr., and Mark O. Yeisley. Naval Institute Press (http://www.usni.org/navalinstitutepress), 291 Wood Road, Annapolis, Maryland 21402, 2016, 288 pages, $39.95 (hardcover), ISBN 978-1-68247-003-9.

As one might expect of a book with the word "context" in its title, what *Strategy: Context and Adaptation from Archidamus to Airpower* gives its reader is heavily context-dependent. This collection of essays by instructors at the School of Advanced Air and Space Studies (SAASS) is a must for past and future SAASS students seeking to appreciate and revisit the perspectives of that institution's renowned faculty. For readers with recent experience anywhere on Maxwell Air Force Base's Academic Circle, many of the essays will be useful amplifications of familiar themes from curricula that have been heavily influenced by proximity to SAASS. Readers interested in how the faculty of the American military's most strategically oriented school approaches the task of training the nation's future military strategists will find much to appreciate. In short, the context of *Strategy* is SAASS and its approach to making and teaching strategy. This is not to say that as a collection of essays about strategy, *Strategy* lacks but to say that these pieces by leading strategic thinkers provide a much clearer editorial position on the building of strategists than they do on the building of strategy.

Although the book's subtext is consistent throughout, the topics covered are broad and the methods varied. As intimated in the title, the essays range from Socratic dialogue to

meditations on the development of strategy in air, space, and cyberspace. The first four essays are essentially philosophical, trending respectively from theory toward practice. Everett Carl Dolman, who literally wrote the book on *Pure Strategy*, begins the series by contemplating the meaning of the word "strategy," setting the pace for the remainder of the book by ruthlessly defining terms and questioning easy answers. Harold Winton's exploration of the utility of military theory evokes Heisenberg and cites Jomini en route to describing the importance of theory and the flaws inherent in any theory about the conduct of war. Winton's warning on theory sets the stage well for James Forsyth's essay on application of the realist theory of geopolitics to the creation of strategy. Forsyth explains a theory that is famous for putting practical considerations above all others and then demonstrates the moral imperative necessary for its function. James Tucci follows with a fun Socratic dialogue that makes a strong case for the study of the classics, as well as for the Socratic method itself.

The second section of the book is arguably more focused on the practical application of theory to current problems. Stephen Chiabotti's discussion of the symbiotic and cyclic relationship between strategy and technology makes the historical case for strategic innovation informed by morality and context. Richard Muller's essay on airpower history for the education of strategists is the most overtly SAASS-focused essay, and its direct discussion of the pedagogy of strategy is a unique contribution of this book. Jeffrey Smith's insightful chapter on the relationship among theory, strategy, context, and technology in the development of future airpower strategy connects the dots between many of the other essays in the collection. Similarly, M. V. Smith's essay on space power and strategy demonstrates the importance of theory and context in application to a domain that will unquestionably grow in importance to military operations in the future. Richard Bailey's chapter on cyberspace reaches back to Dolman on the need for foundational definitions and struggles impressively with fundamental questions of liberty and interstate cooperation. Mark Yeisley considers the perspective of classical military theorists on irregular warfare and the effectiveness of airpower in what is a growing dimension of conflict, concluding that Airmen deserve greater education and training for the problems of irregular war. Finally, Stephen Wright examines the role differences and inevitable disconnects between strategists and planners, laying out the differences in necessary mind-set and the problems of shepherding the right people through military careers to arrive intact as strategists. This chapter is a perfect bookend to the collection, as it struggles with the first problem of defining strategists relative to similar types and with the problem of making strategists.

Bailey, Forsyth, and Yeisley have created a book about strategy that explores the topic from its foundation to its frontiers with depth and precision. Importantly, it both describes and demonstrates a method of teaching strategists as it progresses from definition to theory and then application by alumni. By the end of the book, the reader has a much better understanding of how the world's foremost instructors of strategy see the topic and how they see that it should be taught.

Maj Andrew L. Brown, USAF
Headquarters Air Force, Pentagon

Scales on War: The Future of America's Military at Risk by Maj Gen Bob Scales, USA, Retired. Naval Institute Press (http://www.usni.org/navalinstitutepress), 291 Wood Road, Annapolis, Maryland 21402, 2016, 248 pages, $29.95 (hardcover), ISBN 978-1-68247-102-9.

The general public and government alike believe that the US Medal of Honor is one of the most prestigious awards a military service member can receive. However, Maj Gen Bob

Scales, USA, retired, would argue that medals like these are the result of *unnecessary heroism* (p. 1). The author uses *Scales on War* as a rallying cry, alerting readers to the past, present, and future ills facing personnel assigned to infantry units in the Army and Marine Corps. Evident in the book are the general's extensive combat background and refreshing candor in proposing arguments for revamping and renewing the way the US comprehends and executes intimate combat.

The work begins with interesting—sometimes counterintuitive—observations about the nature of war itself. After a brief examination of the military genius of World War II–era Japanese colonel Hiromichi Yahara, Major General Scales concludes that, on Yahara's advice, perhaps the US *should* fight the next war like it did the last one (p. 25). He follows with narrative that, at its essence, suggests that war is not as complicated as proponents of technological advancement would have one believe: "Non-Western militaries are increasingly internalizing the lessons of war against technologically superior enemies" (p. 35). The author has an innate ability to drive home his point by including relevant facts and figures, stating, for instance, that most of the recent deaths in close combat (52 percent) occurred during searches for the enemy (p. 58).

In instances like these, Scales shows his discontent concerning the lack of proper equipment that these Soldiers and Marines receive. Interestingly, he mentions that the use of simple off-the-shelf body-camera technology could give small units an edge, even preventing some ambushes altogether. The author thus brings into question the seemingly skewed priorities of acquisitions processes and decisions (e.g., purchasing a bright-and-shiny state-of-the-art fighter jet over new rifles and machine guns for infantry).

Next, Scales tackles the intangibles of war fighting such as human factors of intuition, narratives, and intentions. He most certainly advocates that decision makers have a strong understanding that today's wars are not simply fought by faster jets, better bullets, or bigger tanks. Even at the small-unit level, body cameras and more advanced rifles do not negate the fact that the narrative of the war must be kept in check. Encapsulated in "the narrative" are audiences and their perceptions that the US is trying to strategically control. For instance, the author mentions that Gen David Petraeus had to consider four audiences during his time in command: "the Iraqis, the enemy, the Arab community, and the American people" (p. 87). Shaping these perceptions, he argues, is imperative. Additionally, the general points out that cultural awareness is not to be relegated to a 30-minute computer-based training module that is easily glossed over. He makes observations about intuitive leadership that would facilitate better understanding of cultures and the abstractions associated with asymmetric warfare. Scales maintains that not everyone is necessarily fit to be a good close-combat warrior, thus making an often-overlooked point. Specifically, a certain level of intelligence is required to make on-the-spot decisions during firefights. Compellingly, he notes that this intelligence must be coupled with a personality that is able to act "under pressure in the presence of uncertainty and ambiguity" (p. 114).

Further, the author lauds relatively simple technologies. A case in point is the drone. Here, however, any well-versed Air Force operator might find fault with his arguments. Up to this point, Scales has demonstrated thorough comprehension of the battlespace and inherent obstacles, but his discussion of the manner in which the Air Force employs its Predators and Reapers is an oversimplification. That is, he believes that drones are lifesavers, providing the "unblinking eye's" video feed to decision makers back at command posts. Although the general obviously knows that the Air Force is task-saturated with requests for drones to support squadron-level operations, he misses the impact that consistent sorties have on a minuscule, "less-with-more" contingent of remotely piloted aircraft pilots. This situation does not occur due to a singular Air Force command-level decision (where this

work focuses the brunt of frustration). Budget woes and congressional decisions, of course, are factors as well.

Nonetheless, Scales wastes no time returning to his infantry-based wheelhouse, offering a thorough explanation of the poor land-based troop carriers in use today. One notes a pattern in the development of makeshift equipment in his analyses. The infantry often seems to get the veritable short end of the stick. At this point in the book, the reader has been fully exposed to one of the author's major areas of concentration: the death toll of American troops. His evident concern and desire to begin engaging in "unfair fights"—in the US's favor, of course—make this work an engaging read, reminding members of the audience that there are a number of leaders "still on their side." Happily, branching out into hyperpoliticized topics like women in combat and reinstitution of the draft is not taboo in this book either. Not once does the general stifle blatant responses to very controversial and unpopular subjects.

Overall, this very straightforward and "readable" work is a must for individuals who desire a firsthand account of what infantry personnel are experiencing. *Scales on War* walks the reader through the fog and friction of land-based warfare, placing special and timely attention on the oft-forgotten "boots on the ground." Both lawmakers and military leaders would do well to heed the author's observations. After all, the US does not need any more *unnecessary heroes*.

Capt Haley Shea B. Hicks, USAF
Mountain Home AFB, Idaho

Practise to Deceive: Learning Curves of Military Deception Planners by Barton Whaley, edited by Susan Stratton Aykroyd. Naval Institute Press (http://www.usni.org/navalinstitutepress), 291 Wood Road, Annapolis, Maryland 21402, 2016, 256 pages, $39.95 (hardcover), ISBN 978-1-61251-982-1.

Written by the US intelligence community's foremost expert on denial and deception, *Practise to Deceive* is as deceptive as the subject it claims to describe. Although Mr. Barton Whaley's credentials are indisputable and his knowledge of the material presented in this book is encyclopedic, it offers very little to either the professional military operator or intelligence analyst. One might best think of the study as a sourcebook for further research.

Practise to Deceive holds great promise. The introduction by Dr. A. Dennis Clift, president emeritus of the National Intelligence University, describes Mr. Whaley's military, government, and academic credentials, establishing him as the intelligence community expert on denial and deception. The reader should take note that the author died in 2013 and that his book was published in 2016. It reads like (and most likely was) the working notebook of a subject-matter expert. The study opens with the premise that it intends to discover peculiar learning patterns among military deception experts through history but quickly digresses into a series of interesting historical vignettes. The conclusions offered afterwards, though engaging and possibly useful, are not presented in sufficient depth to recommend this text for serious military study.

The book is divided into five broad sections: an executive summary, which introduces the ideas of deception; an introduction, which gives an overview of the deceiver; the case studies themselves— basically a lengthy literature review; the conclusion; and a series of appendices. The executive summary and conclusion reveal Whaley's philosophy of deception. The heart of the book is the series of 88 case studies. Although some are fascinating, especially those pertaining to the Second World War, nearly a quarter of them are essentially long footnotes. Two paragraphs or less, they merely direct the reader to other, more authoritative, sources. Many of the latter are the author's own works: of the bibliography's 86 entries, 8 are Whaley's

studies, and his recollections of conversations are frequently cited in footnotes throughout the book. *Practise to Deceive* offers little research that the author has not presented elsewhere.

Besides the lack of substance, the book contains so many typos and mistakes that it almost seems to be a rough draft. On average, most pages have between two and three typos or editorial errors. Some of these are as simple as forgetting a space between words or reversing letters. Others are as serious as using the wrong name for an individual. Regardless, these flaws are distracting and degrade the author's overall message.

Practise to Deceive is certainly an absorbing, even entertaining, read. By focusing on individual deception planners, it provides an engrossing, personality-based view of history unlike most other military descriptions. The brief sketches of good traits for a military deception planner outlined in the conclusion could prove useful on their own as an introductory paper for new military operations planners or commanders. In general, though, better resources are available to military and intelligence professionals.

The cover of the book describes it as a "handbook for military and intelligence professionals." Yet, after finishing this study, readers are little more prepared to execute denial-and-deception campaigns than before they opened the cover. *Practise to Deceive* is too superficial to be more than a series of intriguing historical footnotes. The last 30 pages are the most useful, offering a short summary of advice on how to establish and run a deception organization. Yet, even this part is too brief to be authoritative. The reader would do better simply to consult Mr. Whaley's other works (amply cited throughout this one) than spend time on these glosses.

Maj J. Alexander Ippoliti, USAF
US Pacific Command

Father of the Tuskegee Airmen, John C. Robinson by Philip Thomas Tucker. Potomac Books (http://www.nebraskapress.unl.edu/pages/PotomacBooks.aspx), 1111 Lincoln Mall, Lincoln, Nebraska 68588-0630, 2012, 352 pages, $29.95 (hardcover), ISBN 978-1-59797-487-5.

During the 1930s and 1940s, many Americans—especially African-Americans—knew about John C. Robinson, perhaps the foremost black aviator of that period. One of a handful of African-American pilots of the interwar years, he became known as the "Black Lindbergh" for his establishment of the first flight school for African-Americans and the first US airport managed by blacks, among many other achievements. As commander of the Imperial Ethiopian Air Force during the Second Italo-Ethiopian War, April 1935–May 1936, Robinson earned the sobriquet "Brown Condor of Ethiopia." During World War II, he served as an aircraft maintenance instructor for the US Army Air Forces in the United States and for the Ethiopian Air Force in Ethiopia after its liberation from Italy.

Unfortunately, Robinson died in 1954 at the young age of 50 from injuries sustained in a plane crash in Ethiopia where he remains buried in a relatively obscure cemetery near the capital of Addis Ababa. However, soon after the war ended, he was forgotten, not only by Americans at large, but also by African-Americans. Ironically, more Americans today know about Eugene Bullard, the first black combat pilot, who flew for the French Air Service during World War I—but for only two months and probably without scoring any enemy kills—than about Robinson, although the latter's aviation record far outweighs Bullard's in many respects.

Despite my 27 years in the Air Force and formal studies in American and military history in general (and Air Force history in particular), I did not know that Robinson existed, much less anything about his civilian and military achievements, until I read this biography. In

this generally outstanding work, Dr. Tucker—a graduate of St. Louis University; the author or editor of more than 20 books on various aspects of African-American, Civil War, Irish, and women's history; and a historian for the US Air Force—has done wonderfully in resurrecting Robinson from obscurity for a new generation of African-Americans.

In this highly readable and well-researched biography, the author uses Robinson's original letters, newspaper accounts of his achievements, existing biographies of his subject, and other sources to bring Robinson's story to life. Born in Jim Crow Mississippi in 1903, Robinson, over time, literally brought himself up by his "bootstraps" and escaped the despondent life of his peers in a deeply segregated South to become possibly America's most prominent black aviator before the start of World War II. Tucker describes in detail Robinson's persuasive communication abilities, which he used to pursue and obtain his personal and professional goals, despite existing racial barriers. These objectives included training and work as an auto mechanic, the establishment of a prosperous garage, entry into the prestigious and, at the time, all-white Curtiss Aeronautical School in Chicago, the purchase of his first airplane, and the establishment of his own flight school and airport. During his one year in Ethiopia, he displayed extraordinary flying skills in many aerial skirmishes with far more numerous, better armed, and technologically advanced Italian aircraft.

The only real issue I have with the book is its title, which I believe is a bit misleading since Robinson had very little to do with the actual establishment of the 99th Pursuit Squadron, the first African-American combat aviation unit, and with subsequent African-American aviation combat units (the 100th, 301st, and 302nd Pursuit Squadrons, as well as the 332nd Pursuit Group), manned by the Tuskegee Airmen. Of course, as a graduate of Tuskegee Institute, he did pursue the founding of a black flight-training program with his alma mater's administration between 1934 and 1940, thus providing the initial idea for a flight program at that institution. However, disagreements between him and the school's president, Dr. Frederick Douglass Patterson, delayed the emergence of a flight school there until late 1939 when it became reality as part of the federal government's Civilian Pilot Training Program. Unfortunately, at the time, Robinson had another commitment; consequently, Charles Alfred Anderson Sr., another well-known black aviator, became the chief civilian flight instructor at the Tuskegee school and, later, at the US Army flight schools at Tuskegee.

Additionally, Robinson most certainly inspired thousands of African-Americans in the interwar period to become pilots. Once the Army opened its flight schools at Tuskegee, many of these men wanted to become Army pilots, and, by the end of World War II, nearly 1,000 of them had done just that. At least some of these individuals were probably inspired by Robinson's accomplishments and exploits to become combat fliers. However, Tucker makes no or very little reference to the direct impact or influence of his subject on those African-Americans who volunteered for the Army's flight training and eventually became Tuskegee Airmen. If he had established this connection, then perhaps readers would have better understood his reasons for selecting the book's title.

Finally, despite Robinson's tremendous aviation accomplishments in the 1920s and 1930s, his exploits in Ethiopia during the Italo-Ethiopian War, and his service in World War II and later in Ethiopia, the author doesn't really address why this man dropped into obscurity by the early 1950s. Tucker does mention the prevailing racial discrimination in the South and the possible overshadowing of Robinson's achievements by the wartime exploits of the Tuskegee Airmen and their subsequent accolades. However, that appears to be the extent of his commentary on Robinson's "disappearance" from the minds of African-Americans. The

author's assessment of this phenomenon would have been enlightening, especially since the book does resurrect Robinson as a major African-American aviator of the interwar period, stimulate the growing interest of blacks in aviation, and emphasize his indirect influence on African-American military aviation as embodied by the Tuskegee Airmen.

Robert B. Kane, PhD
Maxwell AFB, Alabama

Why Air Forces Fail: The Anatomy of Defeat, revised and expanded edition, edited by Robin Higham and Stephen J. Harris. University Press of Kentucky (http://www.kentuckypress.com), 663 South Limestone Street, Lexington, Kentucky 40508-4008, 2016, 450 pages, $29.95 (softcover), ISBN 978-0-8131-6751-0.

Far too much is written about the winning team. There is no shortage of books, articles, and documentaries that epitomize narratives of the armies, navies, and air forces that emerged victors ex post facto. Particularly in armed conflict, where the stakes could not be higher, it is enticing to focus on studying the victorious force in hope of learning how its actions, technology, and people outlasted those of the adversary. Although analyzing successful wartime players has merit, a more holistic and proper analysis will take even greater account of those forces that did not survive the conflict—the losers. It may seem counterintuitive at first, but in doing so we mitigate the effects of survivorship bias—the logical fallacy of fixating on the people or things that survived a process or event instead of on all the participants. If one wishes to spot truly meaningful trends and draw statistically consistent conclusions, then the sample must be inclusive and not skewed in favor of those who happened to win in the end. *Why Air Forces Fail: The Anatomy of Defeat* is a vital addition to the body of airpower literature because it tackles the difficult task of providing in-depth analysis of understudied air forces that suffered defeat.

The text is a collection of essays edited by Robin Higham, a professor emeritus of military history at Kansas State University, and Stephen J. Harris, chief historian at Defense Headquarters in Ottawa, Canada. The essayists hail from diverse academic and professional backgrounds, all having published numerous works on airpower and military history. Despite the fact that some essays are stylistically better than others, all are backed by extensive research, offering useful end sections that suggest future reading. Furthermore, the contributors stay on task in providing thoughtful investigation of the facts, shying away from opinionated commentary. One recent highlight is that 10 years after the book's publication, the editors have added two chapters and revised previous ones (e.g., by including new reference sources). The new chapters are "American Air Forces in Vietnam" and "RAF Bomber Command," which features particularly useful illustrations.

Organizationally, each essay illustrates one of three categories of defeat identified by the editors. The "dead ducks," those that never had a chance, emphasize certain countries' lack of infrastructure and national resource levels that are necessary to sustain aerial warfare. The "hares" enjoy early success but are ultimately defeated (e.g., the Luftwaffe and Japanese air force in World War II). Finally, the phoenixes suffer early losses but are eventually successful. These categories supply useful signposting for the reader; however, there is little explanation of specific case study selection or any chapter grouping past the initial explanation that all of the featured air forces fall into one of these categories of defeat. Nevertheless, the introduction does explain these categories in greater detail and tells the reader which essays fall into each category.

An overall strength of this study is that the essayists emphasize the deep interconnectedness among a nation's government, industry, and populace necessary to sustain an effective air force during wartime. This stance runs counter to that of a significantly large portion of airpower literature that myopically concentrates on operations and tactics. One of the major themes of *Why Air Forces Fail* is that air forces demand a high level of technological sophistication (both in industry and in trained personnel), logistical support, and physical space for airfields and flying operations. In many of the book's case studies, an air force could be easily defeated because it did not have the national industry needed to sustain operations after initial shocks, despite having modern and well-equipped aircraft. Another recurring theme is the consequence of timing. Naturally, we seek a causal explanation of historical outcomes by pointing to one or a series of factors. However, far too often the value of luck and timing is wrongfully neglected—an omission that this book makes great efforts to avoid.

Because the individual essays are well organized, analytically driven, and relatively short, this text is ideal for enriching academic or professional group engagement and discussion. Although it still comes recommended for more casual airpower enthusiasts, I believe that this collection would truly come into its own in a group setting. The points and arguments presented in specifically targeted cases can be dissected as part of a larger discussion. For the academic instructor, this book could easily complement a case-based syllabus. Even more broadly, because of its focus on airpower's inextricable relationship with national politics, industry, and technology, the essays could add variety to courses in public policy, business administration, or engineering management, among others. Tactically trained airpower professionals could also find this book a great resource for expanding their familiarity with the strategic environment that enables—or hinders—operational effectiveness. In all, *Why Air Forces Fail: The Anatomy of Defeat* is a meaningful work that contributes to the understanding of successful airpower by examining critical elements of defeated air forces.

2nd Lt Scott T. Seidenberger, USAF
Tyndall AFB, Florida