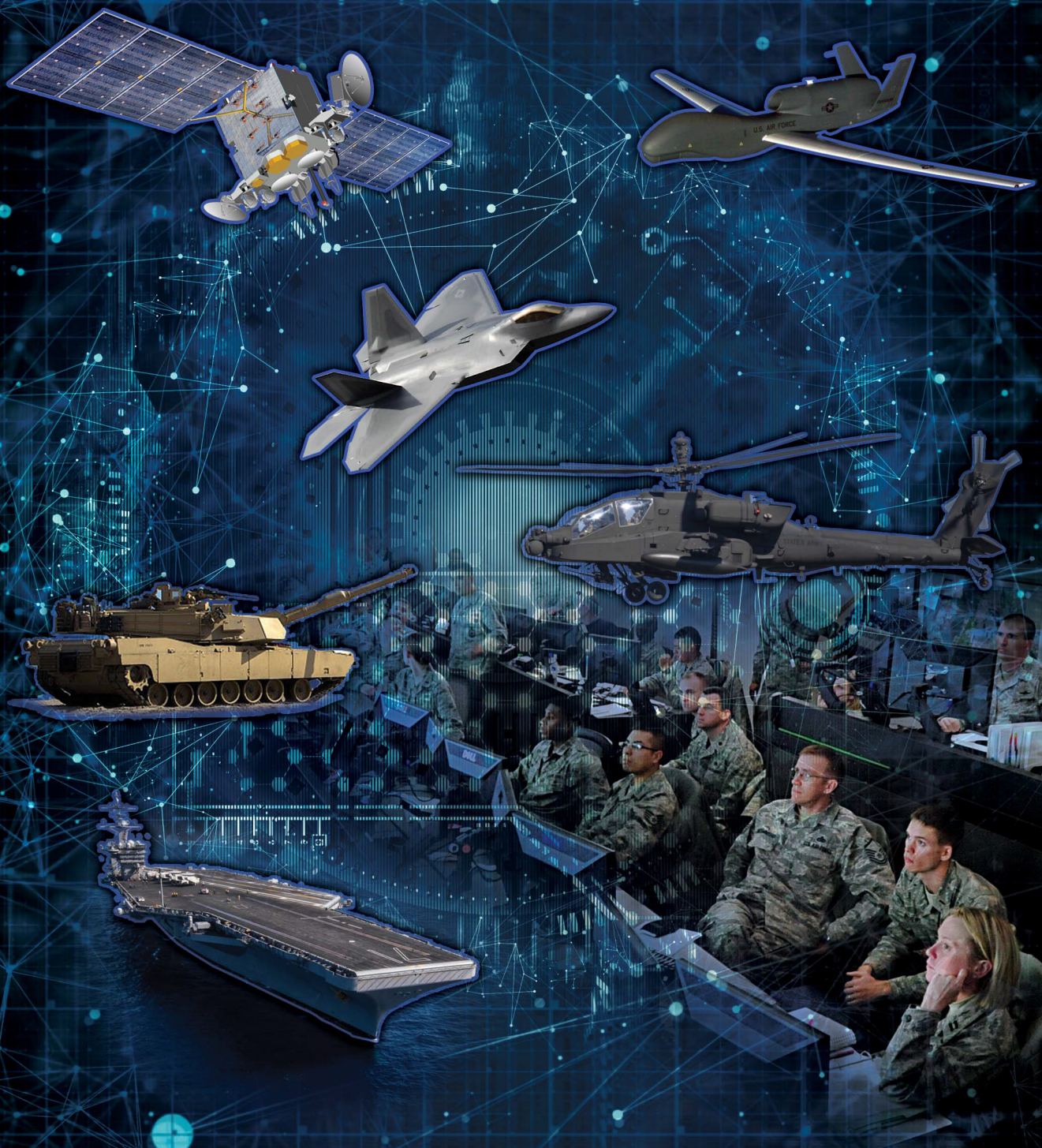
ASPJ

Air & Space Power Journal

JADO Special Edition

Summer 2021



ASPJ Air & Space Power Journal

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

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

https://www.af.mil/ https://www.spaceforce.mil/ https://www.aetc.af.mil/ https://www.airuniversity.af.edu/

FORWARD

ARTICLES

Joint All-Domain Operations

Lt Gen James B. Hecker, USAF

In the struggle for survival, the fittest win out at the expense of their rivals because they succeed in adapting themselves best to their environment.

–Discussion of Charles Darwin's views

Ritchie R. Ward, *The Living Clock*, 1951

The Department of Defense's transition to Joint All-Domain Operations (JADO) as the doctrinal framework for future strategic competition captures and codifies truths about war fighting that may be obvious in the comfort of 20/20 hindsight. The idea that the application of force in one domain may affect outcomes and capabilities in another has been an element of American military thought for more than 240 years, for example the Battle of Yorktown, 1781. B-17s conducting antisubmarine patrols during the Battle of the Atlantic to protect Allied shipping in World War II engaged in multidomain operations: in this case, air assets were used to detect and prosecute German U-boats that harassed merchant convoys delivering supplies and troops to the European theater of operations. Likewise, carrier-based aviation naval and ground-based fighters performing close air support for soldiers and Marines on the ground in Korea and Vietnam delivered firepower in support of land objectives.

In contrast, however, JADO marks a dynamic transition in the conceptualization of maneuver warfare characterized by complexity, speed, and precision. Success in JADO will require sophisticated combinations of synchronized domains far beyond what has been historically demonstrated. Additionally, the rapid technological changes we have recently experienced and the ever-growing dependence on the electromagnetic spectrum will have an unforeseen impact on the effectiveness of military operations in all five recognized domains—air, land, sea, cyber, and space.

Assumptions and practices that guided American military thought from Desert Storm to the wars in Afghanistan, Iraq, and Syria may not be valid in future strategic competition against adversaries using advanced technologies. The notion

that future conflict will resemble Operation Desert Storm, with its months of buildup in regional sanctuaries unchallenged by an isolated regional adversary, has been invalidated by Russia's gray-zone operations in Syria and Ukraine, and in perpetual challenges in the cyber and space domains. Regional access to secure operating locations is no longer a given.

Threats to access in the electromagnetic spectrum, as well as the integrity of data down to the individual bit level, challenge our ability to communicate with and command and control our forces. Ransomware attacks against American commercial and civil targets offer hints about the potential impact of dedicated adversary actions against infrastructure and communications. As we continue to rely on access to information across the space and cyber domains, potential vulnerabilities multiply by the thousands. The decisive actions in future wars may be completed within the first 30 seconds of conflict; the outcome on the battlefield may not manifest until weeks or months later.

The release of Air Force Doctrine Publication 1 earlier this year recognizes the challenges present in contemporary strategic competition in its reframing of how Air Force personnel must consider airpower. The key tenet of Air Force doctrine, dating back to its roots in the Army Air Force, is that airpower's true potential is realized in command relationships of centralized control and decentralized execution. The changing threat environment and the realization the Air Force needs to change to stay relevant, means that we now "execute mission command through centralized command, distributed control, and decentralized execution." The addition of both mission command and distributed control are integral to the service's continued relevance in the Joint all-domain battlespace.

Success in the Joint all-domain environment at the tactical, operational, and strategic levels cannot be guaranteed by massive system investments and recapitalization efforts. Nor is it enough to accept as an article of faith that artificial intelligence will save the day in future conflict. Unmanned aerial vehicle swarms may one day be able to demonstrate new and novel capabilities, but turning these ideas into capabilities that demonstrate value in today and tomorrow's fight is imperative. It is neither easy nor quick to do so. We deliver air and cyberspace capabilities every day for the nation while also learning how to do so in more effective ways. As an organization, the Air Force is unable to take a sabbatical for a decade to figure out the future. This means that research, modernization, and current operations compete for attention, manpower, and money and the emphasis on flexibility and rapidity is precedent in today's era of competitiveness.

The articles in this volume do not solve JADO for the Department of the Air Force. Rather, they capture contemporary thoughts and insights about different aspects of operating and fighting in Joint, multidomain environments. These

practitioners begin to address the deep work required to advance JADO from a conceptual framework to true mission capability for Air Force personnel, Guardians, our Joint partners, and our Allies and partners around the globe. Mission command and distributed control will be inherent components in future military action. Both the Air Force and the Space Force need to define how we will embed these elements into our institutions, structures, and processes. While new hardware and software are essential elements of future operational realities, the thoughts and ideas that accompany them will be just as important in creating relevant and decisive capabilities for the nation.⊛

Lt Gen James B. Hecker, USAF

Commander, President, Air University

Future Command and Control: Closing the Knowledge Gaps

Lt Col Heidi M. Tucholski, USAF, PhD

Future operating environments will require a real time, fully networked command and control (C2) capability; this concept is considered a critical enabler throughout the Department of Defense (DOD), regardless of advocacy for platform compositions or force structure designs. The Air Force Warfighting Integration Capability (AFWIC) identifies C2 as the required core capability to conduct Joint multidomain operations across all types of conflicts.[1] This concept, which calls for a comprehensive sensing grid, has been validated by results from the Futures Wargame and numerous exercises. The vision is highly aspirational but deemed vital for the future operating environment. Contrary to what many advocates of this technology claim, human decision-making decreases in quality as access to information increases, unless human decision-makers have relevant training and knowledge about the environment. The Air Force must consider some immediate implications for organizational strategy and funding to eventually achieve the long-term vision for a future C2 capability.

Definitions

The Joint definition of command and control includes two elements: the authority over forces and the integration and synchronization of actions.[2] This article focuses on the latter element as technology will continue to shape how the military integrates and synchronizes. The Air Force must be prepared organizationally to address this aspect. Technology will continue to compress C2 structures by providing commanders with direct access to lower echelons. While this is an important issue that will continue to create complications from the authority aspect, this article focuses on the closer issue of whether C2 integration and synchronization can even be developed for the future operating environment.

This article adheres to the simple label "C2" with the understanding that any relevant C2 capability in the future will operate within and through every domain—air, land, sea, cyber, and space—by a Joint crossfunctional force. This concept represents any service- or career-field-specific terms such as multidomain C2 or Joint all-domain C2, as they share the same key characteristics. This

comprehensive future concept of C2 includes a significant transition from a platform-centric to a platform-agnostic capability.

The timeline for a future capability varies depending on context. For conceptualization of capabilities and operational environments, the future is often represented by more than 15 years from the present. This long-term perspective provides guidance for desired end states and will be referenced within this article as the AFWIC's future vision. The Air Force examines operating concepts in windows 5-15 years out.[3] This midterm future is critical for technology developers as it provides a realistic timeframe for funding and implementing projects that advance the Air Force toward its long-term vision. The short-term future, less than five years out, is generally already programmed, thus the midrange period is the focus of this article. Currently, the long-term aspirational vision provides sufficient guidance to drive technology development, but as an organization, the Air Force has not yet committed to the necessary incremental steps to achieve this vision.

Some conceptual visions jump straight to fully autonomous decision-making, but that is premature for the midterm timeline of a C2 operating concept. There are three tiers of autonomy: (1) semiautonomous, or human-in-the-loop operations where human action is necessary to continue functioning; (2) supervised autonomous, or human-on-the-loop operations where a human observes and can intervene if desired; and (3) fully autonomous or human-out-of-the-loop operations without any human feedback or communication.[4]

All three tiers fit within the Air Force's doctrinal concept of C2.[5] While eventual artificial intelligence (AI) applications should be kept in mind, a future C2 capability will have humans in the loop, or at least on the loop, for initial spirals.

Background

The Joint Operating Environment 2035 depicts an extremely complex and interactive future environment.[6] The Joint Force requires a C2 capability that can operate within such an environment while maintaining its necessary functions as a critical enabler.[7] Across the spectrum, from conventional warfare to competition below the level of armed conflict, C2 is a necessary component in a complex future. The AFWIC's response envisions strategic dominance through a persistent distributed networked C2 capability that enables global multidomain operations "within seconds and minutes."[8]

This persistent network requires the proliferation of sensing and communications hardware. The early development of such hardware is promising. The Air Force is moving toward its goal of a proliferated geosynchronous and low-earth-orbit integrated architecture with small, persistent satellites from the military

sector through the Air Force Research Laboratory (AFRL) Space Vehicles Directorate (AFRL/RV) and from the civilian sector through commercial partnerships.[9] The proliferation of intelligence, surveillance, and reconnaissance platforms continues to increase alongside operational capabilities that transform the everyday war fighter into a sensor. From an enterprise perspective, the Air Force acquisitions process is emphasizing interoperability with modular components and open-source programming. The initial development of hardware for a proliferated network appears to be on pace.

From a software perspective, the AFRL Sensors Directorate (AFRL/RY) is researching what information and processes will be necessary for implementing real-time distributed coordination across such a large system.[10] Their contributions will help determine the feasibility of the cognitive process for both human-in-the-loop and human-on-the-loop operations while achieving the appropriate workload division for aggregated sensing and data processing. This software and analytics research is critical for the development of a C2 capability, but the timeline for expected results is uncertain. The AFRL/RY is also researching data processing within a trust and mission-assurance context, but that effort is outside the scope of this project.

How well human war fighters and decision-makers will utilize these technologies is not so clear. Empirical evidence suggests more information often has negative effects on decision-making, resulting in inferior outcomes. Humans make poorer or incorrect decisions, compared to what they value, with increasing amounts of information.[11] It follows, then, that unfamiliarity and ambiguousness make Air Force officers worse strategic decision-makers.[12] To prevent information overload, humans employ heuristics to limit the required amount of information processing.[13] Dealing with massive amounts of information will not necessarily make it more difficult or time-consuming for humans to make decisions, but it is more likely that humans will not identify some crucial information, resulting in dysfunctional or less optimal outcomes.[14] The problem becomes even more difficult as humans interface with an increasingly large number of nodes.[15] The processing speed and capacity of systems are quickly improving, but the human interaction effort is still the key problem for improving a human-tech interface.

The vision for a networked C2 capability that enables Joint operations in a complex and information-rich environment is highly aspirational. If the Air Force assumes new technology can transition directly into real-time, distributed C2 without accounting for known issues of information veracity, task saturation, and analysis paralysis, it will never achieve its vision. Operators, decision-makers, and networked systems must be supported by appropriate organizations

and procedures to realize desired effects. The Air Force has clearly established the requirement for this future C2 capability, but will they be prepared to use this capability when it becomes available? What incremental steps must the Air Force take in the next 5-15 years to enable the development and implementation of this capability? Is the Air Force on the right track?

Knowledge Gaps

The organizational processes for training and implementation are vital to a successful spiral development process. The desired end state is not yet defined enough to develop tactics and procedures for future war fighting, but it provides guidance on the general direction for technological development. The next few incremental steps for how the Air Force prepares to organize, train, and equip for this future C2 capability are where the most problematic knowledge gaps still exist.

Challenges and Implications

The intended purpose of a future C2 capability is quicker and better decision-making from the tactical to strategic levels of warfare and policymaking. Even though the concept of turning massive amounts of data into usable information seems intuitive, more data does not necessarily provide a better context for understanding an operating environment or anticipating outcomes to alternative courses of action. In fact, the most likely scenario is that more information will produce worse decisions. New technology, alone, will not provide a comprehensive solution for C2 in a complex operating environment.

An appealing assumption is that a sufficiently advanced technical interface with a data-fused backend will provide decision-makers with an intuitive, decisive aid for making real-time decisions. Unfortunately, that assumption fails to hold up in real-world practice. If a decision-maker is not adequately trained or knowledgeable about the information presented on a system, decision accuracy and quality can decrease within an environment of better information.[16]

The solution cannot be one-sided where technology is developed for humans to use. It must be double-sided where technology is developed alongside training that educates humans to work in an information-centric environment. Even when humans are only on-the-loop and not directly in the C2 process, humans will be required to interact with more information at a faster rate than ever before. To realize this vision of improved decision-making with a networked C2 capability, the Air Force must deliberately and iteratively develop training and build knowledge for the systems and their operating environments.

Fortunately, this problem is not entirely unknown within the Air Force. Multiple organizations have nascent efforts to understand or address elements of the problem. Together these efforts are creating an initial foundation, but they are not yet fully synchronized across organizations or able to assume any organizational staying power in the next few years. The Air Force must consider three major implications in the short term to realize the future vision for C2. Each of these implications is discussed in detail below, but all fall under the broad theme that new technology alone will not enable future C2 without a deliberate effort from the Air Force to organize, train, and equip for this capability throughout its entire development process.

Capability as a Catalyst

The successful adaptation of new operating concepts cannot be forced from the top down. To truly be disruptive, a new technology or capability must act as a catalyst by enabling war fighters to employ fundamentally different approaches to how they operate at all levels of warfare. This tactic may be challenging in an era of low-level, irregular, and proxy warfare as it is difficult for new technologies to prove anything without being used in a major war. Without stark success in application, new technologies are normally assimilated into old doctrine rather than stimulating the desired changes.[17] Even when developed and used appropriately, military organizations have a history of misperceiving benefits or failing to integrate technology properly.[18] If a future C2 capability is not identified by war fighters and decision-makers as essential to survival or success in future conflicts, it will be extremely challenging to integrate the capability into military doctrine or organizations, even if it is successfully developed.

Another adaptation hurdle is whether strategic planning creates temporal mismatches between the requirements of today versus a long-term future. At their worst, strategic visions can turn a desired operating concept, such as the AFWIC's vision for a future C2 capability, into a programmatic demand signal. This development may hinder innovative developments or fenced-off budget investments to ensure consistency with previous justifications.[19] Demand signals for a future C2 capability must not be replaced by programmatic funding signals for specific enabling programs. The C2 requirements the DOD established for the future operating environment must remain the overarching demand signal.

Throughout military history, the pace of a capability's development has been chiefly determined by the extent to which its mission and operational function are known and defined.[20] Even if the potential of an innovative technology is readily apparent, its initial success in tests and application is not inevitable. This separation often comes from an inability to fit the capability within current

tactics, techniques, and procedures rather than embracing the unknown change that might result.[21] But even having an established doctrine is insufficient if the Air Force is not organized to support an innovative capability.[22] The Air Force recently formed a multidomain warfare officer career field to lead operational-level C2. In establishing this career field, the Air Force solicited a broad range of experience and expertise from other career fields,[23] providing an excellent environment for innovative perspectives as the future C2 capability is developed. Common training in this career field provides foundational knowledge, but it remains to be seen whether this specialty limits itself to today's procedures and doctrine or if it permits the capability to act as a catalyst for how war fighters operate in the future.

The Air Force is aware that implementing this new C2 capability necessitates information superiority, but organizational parochialism could easily prevent war fighters from developing approaches for war fighting. To achieve the future vision, C2 must be "agnostic to domain, platform, and service."[24]This shift threatens the Air Force's institutional identity, founded on fielding the most technologically advanced platforms.[25] It is not clear if the Air Force is simply echoing Joint language or if it is prepared for the corresponding shift away from a platform-centric concept of air superiority. Operational concepts that rely on traditional air superiority against technologically capable adversaries are already futile.[26] The growing demand for information superiority has simply been added to the existing operating concept's reliance on air and space superiority, demanding an insatiable requirement for all-domain dominance that is simply not feasible—at least not in a strategically relevant timeframe.[27]

Information has become one of the seven Joint functions, alongside C2, and is recognized as necessary for enabling effective decision-making.[28] It is yet to be determined how the formation of the Space Force within the Department of the Air Force affects this institutional identity, but integration between the Air Force and the Space Force through the information Joint function will be strategically imperative and must not be inhibited by service parochialism. The creation of a new career field and an additional service within the department have created an environment where war fighters can develop new tactics and approaches that fundamentally change how we fight and win wars with information. This environment is ripe for a disruptive catalyst like a future C2 capability, as long as the individual services allow war fighters to develop the capability freely and do not attempt to force adaptation within current doctrines.

Deliberate Human Integration

The DOD recognizes information superiority in the future hinges on systems integration rather than just individual technologies.[29] But while it focuses on the role that technology plays in developing these systems architectures, the Department largely disregards the human integration piece. Wargames incorporate tiers of automation and analytics in future environments without articulating the role of human interaction.[30]

To conduct decision-making at the "speed of relevance," the DOD's vision of C2 requires the capability to "connect, share, and visualize" information across all domains at all levels of warfare.[31] How, or even if, this can be accomplished is a still unanswered question. Enabling technologies that utilize novel information and computing techniques might provide improvements beyond what is possible today, but they will never provide a comprehensive solution that does not require human integration. Enablers, such as AI, machine learning, or cloud computing are still enablers, not decision-makers. Air Force leaders often refer to these technologies as if the technology itself is what will provide a future C2 capability.[32] The Air Force advocates for technological speed and automation without calling for an equal focus on human integration, even though it recognizes the human integration aspect is vital for future effectiveness.[33] These arguments may be necessary to advocate for program funding, but if the Air Force relies on this approach, amazing technology might just sit on the shelf.

Having identified the need for deliberate human integration, the AFRL Airman Systems Directorate within the 711th Human Performance Wing (AFRL/RH) has three main areas of research specifically targeted at this element of a future C2 capability: distributed team performance, human-machine teaming, and training.[34] All three areas are vital for understanding and deliberately developing human integration. The AFRL/RH has identified multiple research streams in each area for initial spiral efforts over the next 5-15 years, but these nascent efforts have yet to gain significant traction within the larger science and technology community or from the AFWIC.[35] The AFRL/RH has established initial proposals and testbeds, but more funding for formal programs is necessary to synchronize these cognitive integration efforts alongside the technology-focused programs.

More developed from the programmatic side is the advanced battle management system (ABMS). The concept for the ABMS essentially expands C2 beyond an individual platform into a comprehensive networked capability with built-in data fusion and decision processes. The problems and delays this program has already encountered early in its development showcase how difficult it is to

develop a capability for a long-term vision without clear guidance for a spiral process. Regardless of whether the ABMS retains its nomenclature or another concept develops for C2, the future operating environment requires an enabling capability that generates, shares, and processes massive amounts of information for decision-makers. To provide an informative common operating picture, a future C2 capability must operationalize data fusion and the prioritization of information successfully. ABMS advocates will continue to argue it provides the answer to C2, but as we saw earlier, human decision-makers are only as good as their training and familiarity with using technological aids.

The Air Force must accept the responsibility for deliberate human integration at an organizational level and direct the training and development of such activities among appropriate stakeholders. The AFRL has recognized the need for deliberate integration of human training and knowledge, but their research proposals have not yet captured the necessary buy-in and funding from the larger Air Force. The ABMS is receiving the necessary programming to continue development, and human integration must be considered early and developed deliberately alongside the technologies. Yet it is often touted as a replacement rather than an integrator for human decision-making, and the Air Force has not coordinated the larger effort that directs the necessary human integration for a future C2 capability.

Iterative Concept Development and Funding

No program or technological advancement can single-handedly provide a panacea for future C2 requirements. It is tempting to believe a single program or effort can bridge the gap from where the Air Force is today to where it needs to be in the future. But a future C2 capability will require numerous iterations of concept development, each significant within their own right, and corresponding iterations of program funding. This requirement will be particularly challenging for such a large-scale C2 capability because prioritization and funding need to be committed in the short term for efforts that cannot yet promise the desired end state. A significant gap exists between current DOD funding and the aspirational vision for C2. The Air Force faces a lengthy development process, and organizations such as the AFRL and the AFWIC will be required to produce multiple iterations of technical advancement and incremental integration to realize the final vision.

While the AFRL is structured to advance scientific research, it is not well-structured to directly develop war-fighting capabilities.[36] Programs that integrate across science and technology lanes early to develop new operational concepts are high risk but necessary for innovative capabilities.[37] Both the AFRL and the

AFWIC have put forth initiatives to establish experimentation events to provide an environment for incremental development and implementation.[38] Recent planning for wargames, such as the Futures and Doolittle games, also emphasizes the need for spiral feedback.

These interactions are instrumental for concept development, and they must be protected. Shared participation may help coordinate internal planning and budgeting activities,[39] but the Air Force must accept the ambiguity of early concept development and protect these high-risk environments, even if a decade of experimentation fails to provide a program capable of producing the final vision in a single budget cycle.

The Air Force and DOD visions for future C2 continue to evolve; this instability can slow down the early programming for scientific research and investment.[40] The AFRL has pushed forward with internal guidance for kickstarting and directing more research on human-centric C2.[41] Even though the demand signal will likely continue to evolve, the AFRL must continue to move forward with incremental efforts.

Investment in a future capability demands balancing the budget between new technologies and legacy systems. The Air Force is underinvesting in the former and overinvesting in the latter; this prevents the long-term development of transformational technologies.[42] Unfortunately, the Air Force has not been able to demonstrate much success with prototype-based spiral development for large programs.[43]

Redirecting funding and effort toward new programs in the hope of finding shortcuts to the final vision slows down necessary progress. The AFWIC's operating concept and force designs provide the strategic vision, but the entire linkage from concept to planning and funding through implementation must be deliberate for a C2 capability that is so fundamentally different from how C2 is executed today.

The commercial sector is often leveraged as a way to attain technological advancement quicker or cheaper than it would be to develop such advancement through organic DOD processes, but this solution fails to overcome the issues that the Air Force would face with a future C2 capability.

Commercial off-the-shelf products can be used by war fighters to identify potential ways technology can be used to develop new capabilities. That is, if the Air Force as an organization can still permit the capability to act as a catalyst in how war fighters develop new approaches rather than forcing adaptation within current tactics and doctrine.Otherwise, commercial products are simply inefficiently or not used in place of existing means. The commercial sector is also facing the same problems as the DOD with developing human integration within

its products and capabilities. Commercially sourced or collaborative efforts might provide quicker or easier access to training that could enable the necessary human integration piece.

But even if these efforts are successful at training and building organizational knowledge of the capability and its environment, the Air Force must still implement the corresponding organizational changes. Without lasting changes that direct ownership and continue to deliberately develop the human integration piece, any advancements in an Air Force capability will not be maintained.

The commercial sector is spiraling with incremental concept development and funding, as well. Commercial products or services are not able to achieve the final vision in a single step.

The Air Force must be able to plan and fight wars organically with a future C2 capability; it cannot rely solely on a contractual arrangement with the commercial sector. All three of these implications for developing a future C2 capability still apply whether it is a wholly Air Force effort, an Air Force-commercial collaboration, or a fully joint-commercial effort.

Conclusion

This effort scoped the implications for the Air Force's way forward. These challenges must be met first and soon, but once the Air Force has closed these knowledge gaps, it must address the larger issue of how the Air Force's concept of a future C2 capability fits within the larger Joint framework—something upon which the Joint community has different perspectives. Regarding the nature of a future C2 capability, the Air Force perspective focuses on enabling global effects whereas an Army perspective originates from the principle of maneuver; future C2 often implies something different between services. Regarding responsibility and authority, some staffs place a future C2 capability within the purview of current and future operations whereas others place it within the communications and information realm; future C2 implies something different between Joint functional areas. Joint integration of the acquisition process will also significantly affect the development process. There is an explicit requirement for Joint operations with a future C2 capability, but the Joint community does not yet share the same perspective. How the Air Force's way forward fits within the larger Joint framework will develop as a question for future research.

The DOD has established the requirement for a real-time networked C2 capability for decision-makers to operate successfully in the future operating environment. This is not a call to change what the Air Force is doing; it is a call to protect what it is doing right. Both the AFRL and AFWIC have nascent yet promising efforts to develop a future C2 capability, but knowledge gaps on how

to continue these efforts persist. This article outlined three implications the Air Force must consider and resolve in the short term for the aspirational vision of future C2 to eventually become a reality. First, the capability must act as a catalyst to drive transformational change; it cannot be forced. Second, technology alone cannot provide the capability; transition requires deliberate human integration. Third, the Air Force as an organization must embrace iterative concept development and funding, even as this advocacy will struggle against shorter-term or more tangible priorities.✪

Lt Col Heidi Tucholski, USAF, PhD

Lieutenant Colonel Tucholski (MA, George Mason University; MA, Air University; PhD, University of California, Irvine) is an assistant professor at the US Air Force Academy. She has worked in personnel policy, weapon evaluations, and Pacific Air Forces strategy, as well as strategic assessments and policy analysis.

Notes

1. Headquarters, US Air Force (HAF), *Building the Air & Space Forces We Need*, Draft Response to the Senate Armed Services Committee, (Washington, DC: HAF, August 2019).
2. Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-0, *Joint Operations*, (Washington, DC: CJCS, October 22, 2018), xiii, https://www.jcs.mil/.
3. Curtis E. LeMay Center for Doctrine Development and Education (Lemay Center), Air Force Doctrine Publication (AFDP) 1, *The Air Force*, (Maxwell AFB, AL: Lemay Center, March 10, 2021), 21, https://www.doctrine.af.mil/.
4. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton, 2018), 28–30.
5. Lemay Center, AFDP-1, 68.
6. CJCS, *The Joint Operating Environment (JOE) 2035: The Joint Force in a Contested and Disordered World*, (Washington, DC: CJCS, July 14, 2016), 36, https://www.jcs.mil/.
7. CJCS, *JOE*, 47.
8. HAF, *Air & Space Forces*.
9. Air Force Research Laboratory (AFRL) Space Vehicles Directorate, discussion with the ACTS 2.0 Research Task Force, October 30, 2019.
10. AFRL Sensors Directorate (AFRL/RY), discussion with the ACTS 2.0 Research Task Force, September 12, 2019.
11. Jacob Jacoby, "Perspectives on Information Overload," *Journal of Consumer Research* 10, no. 4 (March 1984): 433–34.
12. Alex Mintz, "Foreign Policy Decision Making in Familiar and Unfamiliar Settings: An Experimental Study of High-Ranking Military Officers," *Journal of Conflict Resolution* 48, no. 1 (February 2004): 103.
13. Jacoby, "Information Overload," 435.
14. Jacoby, "Information Overload," 435.
15. Dan R. Olsen and Michael A. Goodrich, "Metrics for Evaluating Human-Robot Interactions," Proceedings for Performance Metrics for Intelligent Systems Workshop, 2003.
16. Srinivasan Raghunathan, "Impact of Information Quality and Decision-Maker Quality on Decision Quality: A Theoretical Model and Simulation Analysis," *Decision Support Systems* 26, no. 4 (October 1999).
17. Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 55.
18. Posen, *Military Doctrine*, 56.
19. Robert A. Glecker, "Why War Plans, Really?" *Joint Force Quarterly* 79 (Fourth Quarter 2015): 75.
20. I. B. Holly, Jr., *Ideas and Weapons* (New York: Yale University Press, 1983 repr.), 19.
21. Holly, *Ideas and Weapons*, 14.
22. Holly, *Ideas and Weapons*, 19.
23. Air Force Personnel Center, PSDM 20-20, "Multi-Domain Warfare Officer (13OX) Selection Board Call for Nominations," 26 February 2020.
24. Air Force Warfighting Integration Capability (AFWIC), "Designing the Air Force We Need. . . To Be," keynote speech, Wright Dialogue with Industry, July 17, 2019.
25. Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore: Johns Hopkins University Press, 1989), 23.

26. Christopher M. Dougherty, Why America Needs a New Way of War, Center for a New American Security (CNAS) Report, (Washington, DC: CNAS, June 12, 2019), 35-36, https://www.cnas.org/.
27. Dougherty, New Way of War, 21.
28. CJCS, JP 3-0, III-1, III-17–27.
29. CJCS, *Joint Operating Environment 2035*, 16–7.
30. LeMay Center, Doolittle Series 18: *Multi-Domain Operations*, LeMay Paper 3 (Maxwell AFB, AL: Air University Press, 2019), 20, https://www.airuniversity.af.edu/.
31. US Department of Defense, "JADC2 Operational View," March 3, 2020.
32. Maj Gen Michael Fantini and Lt Col Jake Sotiriadis, "The New Imperative: Connecting the Joint Force with a Digital Advantage," C4ISRnet, March 23, 2020, https://www.c4isrnet.com/.
33. HAF, *Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond* (Washington, DC: HAF, April 2019), 7, https://www.af.mil/.
34. AFRL Airman Systems Directorate, "Review to Scientific Advisory Board: Joint All-Domain Command and Control Research," October 2019.
35. Jeffrey Palumbo (AFRL/RH), interview with the author, January 24, 2020; and Sam Kuper (AFRL/RH), interview with the author, February 12, 2020.
36. HAF, *Science and Technology Strategy*, 4.
37. HAF, *Science and Technology Strategy*, 11.
38. HAF, *Science and Technology Strategy*, 13; and Air Force Warfighting Integration Capability, "Weekly Activity Report," March 27, 2020.
39. HAF, *Science and Technology Strategy*, 13.
40. Palumbo, interview.
41. Kuper, interview.
42. DOD's Role in Competing with China: Testimony before the House Armed Services Committee, 116th Cong. (2020)(statement of Michéle Flournoy).
43. Flournoy, "Competing with China."

Mission Assurance in Joint All-Domain Command and Control

James F. "Frank" Hudson Jr.

Current cybersecurity paradigms are ineffective against most malicious cyber actors. Moreover, the paradigms of old are based on reactive efforts, hardware-based solutions, and paper drills that falsely imply security as the standard. The Department of Defense (DOD) should transition to a more modern framework that implements proactive measures to secure its networks and enables them to operate in a denied, degraded, intermittent, or limited bandwidth (D-DIL) environment, thereby providing mission assurance. The DOD requires a rapid and massive undertaking to revolutionize how cyber defense is planned, executed, and sustained to ensure network availability in the most contested environments and future conflicts. In order to achieve mission assurance and cyber superiority for Joint forces across a multidomain environment, the Department must shift from the current global internet model. Failure to do so will only exacerbate existing problems and create numerous avenues for adversaries to exploit DOD networks to their advantage, leaving these networks ineffective in combat and unable to support the war fighter.

Introduction

One of the most discussed topics within the DOD is the security, or lack thereof, of its networks and the inability to share or protect data. Today the DOD forces the user to conform to an environment of legacy applications and siloed data. Current commercial initiatives in information technology, such as cloud computing and virtualization, render the classic castle-and-moat network security structure obsolete. Technology has advanced past clearly defined perimeters using multiple firewalls to protect data. The DOD continues to acquire weapon systems with stovepiped communications networks and data links that cannot mesh with or talk to other systems to share data. The DOD model of monitor-detect-react enforces a cybersecurity paradigm that is ineffective against most malicious cyber actors and fails to incorporate mission assurance truly.[1]

Security requires more than just building a moat or barrier around networks. The Department has failed to prevent internal and external network threats and

has become a reactive force in protecting its networks and data. The DOD and the commercial industry must strive for a system that delivers mission assurance in the Joint all-domain command and control (JADC2) environment. This article outlines recommendations for the DOD to prioritize and embrace new technology and rethink its current approach to mission assurance.

Today the Department is slowly shifting to a cloud-based model to protect data, one that aligns with the so-called zero-trust model. A zero-trust model involves trusting no one inside or outside the network perimeter—all users must verify their credentials before being granted access to the network and data. Nonetheless, the DOD must move faster in efforts to change how it thinks in terms of technological solutions, adopting the mentality that networks are already compromised and no one can be trusted.[2] The internet was created for efficient information sharing, and security was not an important consideration. The current model does not work in a contested environment; the DOD should move forward with security at the forefront to ensure it achieves mission assurance.[3]

The military has grown accustomed to having an internet connection, and the current model does not adequately consider resiliency or the integrity of information to achieve the mission.[4] The Department operates under a falsehood that the DOD network will always function, but the reality is the network will be ineffective in meeting the requirements for fighting in future highly contested environments. The current DOD strategy falls short. The Department must foster and enforce resiliency and work with private-sector technology development to better align with national security objectives and partners (such as security firms) to eliminate threats.

This research explores three critical areas of concern and provides recommendations for achieving mission assurance in a JADC2 environment. The DOD must take immediate action and enact a change from the current way of thinking. To better understand the current state of security practices and technology, the article will focus specifically on current internet development, security incidents, transports, and policies for protecting the network. The unsatisfactory nature of the current state compels a rethinking of how the Department designs networks and implements security.

The article will first analyze the cloud platform, emphasizing data security and integrity. Next, the article will consider transports of data, critical to survival in a degraded environment. In short, the DOD must modernize the transport architecture to make every system a data node. Lastly, the Department should explore ways to achieve mission assurance by placing security first, leading to a network dependable in a D-DIL JADC2 environment. The DOD must strive to develop

new technology and military mission command systems functional in a contested environment to ensure the success of specific missions and achieve victory. They must proactively defend weapon systems and allow the war fighter to communicate in a D-DIL environment. Now is the time for the DOD to truly consider the suggested recommendations and act on them to maintain its competitive edge over adversaries.

Current State

> *The fundamental problem is that security is always difficult, and people always say, "Oh, we can tackle it later," or "We can add it on later." However, you cannot add it on later. You cannot add security to something that was not designed to be secure.*
>
> —Peter G. Neumann, *RISKS Digest*, 1985

The Internet of Things we know today is not the internet developed more than 60 years ago as a US government Cold War weapon. The focus on science and technology ramped up quickly in the US after the launch of Sputnik with the creation of the DOD Advanced Research Projects Agency to further develop weapon and computer systems. The engineers developed ARPAnet, which evolved into what we know today as the internet. The original model never considered security but instead emphasized the openness of the Transmission Control Protocol/Internet Protocol (TCP/IP) Protocol Suite used universally today. The vision of connecting without dedicated circuits created an environment of good intentions and unforeseen bad intentions as the internet evolved.[5] Addressing the innately insecure TCP/IP model requires the US to improve the engine that continues to fuel the modern-day internet more than 30 years after its inception.[6]

The Department's answer to securing an internet is to apply a security layer to the stack; however, this does not protect the other layers from vulnerabilities or attacks. Simply throwing security at a layer can induce other unforeseen flaws within other protocols. Further, this solution reveals the security manager does not have a real grasp of cyber risk to the actual mission and instead is attempting to protect all assets essentially equally.

The DOD continually works hard from within to defend the Department of Defense Information Network (DODIN) and its vulnerabilities, but it is not making gains where truly needed to assure the mission. The US Cyber Command's new vision states, "adversaries exploit our dependencies and vulnerabilities in cyberspace and use our systems, processes, and values against us to weaken our democratic institutions and gain economic, diplomatic, and military advantages." This vision recognizes development of cyber defense lags behind cyberat-

tack capabilities. Preventive defensive measures cannot keep up with malicious programs, viruses, or other attacks against DOD networks.[7] Previous approaches to cleaning up the mess after the spill are ineffective in today's environment.

Philosopher David Hume wrote, "there can be no demonstrative arguments to prove, *that those instances, of which we have had no experience, resemble those, of which we have had an experience*."[8] Hume's unassailable logic implies the Department will never get ahead of the threat based on reactive practices and technology. Known (much less unknown) cyber threats increase every year. The DOD cannot prevent every cyber threat under the current construct, and its current defensive mindset does not come close to mission assurance.

Defenders of DOD networks react to attacks after the attack versus looking for a new solution that guarantees cyber superiority. The Department patches and uses firewalls and intrusion-detection tools, but it does not stop attackers who want to do damage. These tools are add-ons to the network and create a greater surface-attack area. These actions are decidedly tactical, defensive, and reactive. The effectiveness of current defensive tools is questionable and illustrates a much broader phenomenon proving current reactive measures to secure DOD networks do not work and do not enable them to operate in a D-DIL environment. Some abbreviated vignettes illustrate the gravity of the issues.

In 2015, Russian hackers implemented a cyberattack on the Joint Chiefs of Staff. The attack affected 4,000 personnel, and the email system was down for 11 days. The DOD cannot even determine how much sensitive data was collected.[9] Then in 2017, BGPMon identified a "suspicious event where 80 prefixes normally announced by organizations such as Google, Apple, Facebook, Microsoft, Twitch, NTT Communications, and Riot Games were not detected in the global Border Gateway Protocols routing tables with an origin out of Russia."[10]

Lastly, in 2018, an operational assessment conducted by Joint Interoperability Test Command validated the US Air Force's inability to defend against cyberattacks using the Joint Regional Security Stack (JRSS). To add further insult, the JRSS provided little improvement from the operational assessment conducted in 2017.[11]

Clearly, cyber defense has failed DOD networks, and many will argue the Department is one attack away from losing the entire DODIN used for mission command. Former Defense Secretary Leon Panetta stated, "a cyber-attack perpetrated by nation-states or violent extremist groups could be as destructive as the terrorist attack of 9/11."[12] The word *could* is not the right word; instead, such an attack *will* be at the time and place of an adversary's choosing if the DOD does not change its current defensive paradigm. The Department needs to recognize the enemy will inflict harm to win, even if this means forcing the DOD to

"unplug" from the world to achieve its mission. The DOD is sadly mistaken if it believes current defensive cyber operations are sufficient.

Today, the DOD is heavily invested in commercial off-the-shelf equipment (COTS) versus government off-the-shelf equipment. Commercial equipment is here to stay—the DOD will not reverse the course as it is too costly to do so. Guaranteeing COTS supply chain security is unrealistic, however, and a monitor-detect-respond model will not find the security flaws, forcing the Department to use untrusted components—hardware, software, networks, protocols, users, and operators.[13] Using COTS creates many more vulnerabilities within the DODIN that will worsen over the next decade as the DOD lacks the strength to mandate greater security in COTS products.[14]

Huawei, a Chinese telecom company, is quickly becoming a dominant global competitor, and the US can expect more companies from China to emerge in other communication networks. Huawei, currently subject to undue influence by the Chinese government, has signed more than 45 commercial 5G contracts worldwide, including with European countries such as Germany. The company plans to ship more than 100,000 base stations to countries free of cost to gain business.[15]

Equipment vulnerabilities are a part of the equation, but commercial transports carrying the critical information are just as important. In 2008, 14 countries lost access to the internet when two undersea cables were severed.[16] The severed lines caused Egypt to lose almost all internet services, and traffic had to be rerouted through other countries including the US. At first glance, the incident seems unimportant because the network traffic rerouted through other commercial transports. But what if the alternate lines were too congested, or slowing or delaying mission-critical information? In 2006, a 7.0-magnitude earthquake struck off the coast of Taiwan, severing eight cables in multiple places. The damage caused disruptions of information flow to and from China and required 49 days to repair.[17] Most alarming, China Unicom, China Telecom, and China Mobile own a 20 percent and growing share of the market today as the companies recently connected Europe, the Middle East, and Southeast Asia.[18]

Space presents the same concerns posed by ground-base transports but for different reasons. Satellites are susceptible to jamming and targeting. The use of kinetic weapons in space has not occurred outside of testing, but it may be only a matter of time. Even though space debris fields and possibly killer satellites pose threats, DOD continuously protects our nation's most vital assets in space: intelligence surveillance and reconnaissance assets, global positioning satellites, mission command satellites, and the Missile Warning System.[19] China has an edge in hypersonic and space technologies as it launched more satellites than any

other country in 2018 and launched the first quantum communications satellite in 2016.[20] Transports are just as vital as creating a network with security first; developing a sensor-driven transport network in a JADC2 environment is essential to achieving mission assurance.

The Path to Mission Assurance

The DOD Directive 3020.40 defines mission assurance "as a process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DOD mission-essential functions in any operating environment or condition."[21] According to Joint Publication 3-12, cyberspace consists of the interdependent networks of information technology infrastructures and resident data including the internet, telecommunications networks, computer systems, and embedded processors and controllers.[22] If cyberspace remains a critical tenet to achieving military objectives or end states across all war-fighting domains—air, land, sea, cyber, and space—then the DOD cannot rely on the current DODIN defense model or network.

The DODIN is the mission command, but current actions taken to secure the DODIN do not guarantee mission success. These actions fail to protect the integrity of information needed to make timely tactical decisions across all domains. The current cybersecurity paradigm is not reliable and will not allow forces to execute missions in a contested environment. The DOD must engage other means and strategies to deny adversary attempts to access and threaten the DODIN in cyberspace.[23]

Achieving mission assurance in a JADC2 will not happen if the DOD continues to use prescriptive cyber policies enforcing monitor-detect-react constructs on information technology systems.[24] In particular, the desired end state remains war fighting systems that prioritize security, thus ensuring mission success in contested environments and future conflicts. But the DOD must adopt new, commercial-driven technology with a premium on security—an intelligent network that absorbs damage and recovers instantaneously, one that is self-healing. To map the way, the Department can start by developing a secure cloud to provide maximum data access, sensor-driven transports, and a wartime "milnet."

Cloud and Data

No 1960s engineer imagined the military walking around with a COTS handheld device sending information globally. Ensuring the integrity of information

is paramount when traversing COTS systems to carry out military missions. To ensure mission assurance across JADC2, the DOD must embrace the confidentiality, integrity, and availability (otherwise known as the CIA Triad) of information within the commercial cloud. Secured information must flow unimpeded across all transports, or the DOD will fail to achieve national security objectives in peacetime and wartime.

Data resides in various formats on AOC proprietary systems. But navigating through the legacy proprietary systems requires owners agree to merge their data with other AOC systems to create quality data management. The AOC has more than 80 systems, from command and control systems such as Theater Battle Management Core systems, Joint Automated Deep Operations Coordination systems, and the Master Air Attack Planning Toolkit, to Oracle and Microsoft SQL servers.

Each weapon system provides its own proprietary data, making it increasingly harder to unlock and then determine the correct data in a clean state. One approach with legacy systems is using the data as is, but again, in most cases, this does not provide clean, usable data. The DOD must break away from the current proprietary model and move toward a commercial model of open-architecture utilizing apps. To do this, the Department must work hand-in-hand with commercial industry and recognize the commercial world has achieved cloud data integrity.

The DOD has evolved in a defense industry that develops platform-centric systems; instead, industry must design a buffering system or median that can take various data inputs and convert them into an interface understood by all weapon systems and sensors. This buffering system requires a standardized set of entities or data fields where the interface or application correctly accepts the input and creates a common data relationship across the systems, matching and merging all data. The deciphering median is created around a common data standard that allows for cross-utilization among proprietary weapon systems and sensors. This common data standard enhances the DOD's ability to make timely decisions.

It will not be simple, and there is no straightforward solution; however, DOD must identify data as a strategic asset. As the Department builds new weapon systems, it must place interoperability first and identify the right data standard within a modular open system. The DOD needs data; how much is still the unanswered question. Large amounts of useful data are necessary for machine learning and enable the Department to develop a more intelligent network able to heal itself and anticipate the adversary's next attack. Future wars will only become more complicated and complex. Data is a strategic asset in its own right.

The DOD must prioritize interoperability at the start with a metadata standard and a modular open-systems architecture.

The commercial cloud provides the ability to scale and secure both the collection and the analysis of data stored in an enterprise DOD cloud.[25] The cloud provides the operator with the ability to make decisions with the most relevant information. The DOD would no longer maintain a costly data silo infrastructure across commands, and such storage would increase a combatant command's ability to share data enterprise wide. The cloud would eliminate costly proprietary data systems and data silos, making it possible to achieve real-time information and infuse data in a JADC2 environment.

Further, the DOD could increase or decrease the information flow, and cloud computing provides the platform for machine learning (ML) and artificial intelligence (AI). An enterprise cloud has lower upfront costs and reduced legacy infrastructure costs, but most importantly, an enterprise cloud works in every environment, across all military operations—from the tactical edge to the home front—and at all classification levels.[26] A commercial cloud ensures availability and increased security and data protection, and it reduces infrastructure cost, enhancing the DOD's ability to collaborate worldwide. If implemented across the DOD, an enterprise cloud will increase the ability of the Department to operate in a JADC2 environment. Commercial cloud storage will improve tactical effectiveness and efficiency while in a D-DIL environment, allowing war fighters in every JADC2 environment to make data-driven decisions. This capability will also enhance the ability of the DOD to share data with allies and operate as a coalition force.[27]

Transports

Information must flow unimpeded and remain confidential and accurate across all transports, or the DOD will fail to achieve national security objectives in peacetime and wartime. As the Department moves toward AI and ML, many assume the DOD will always have the available bandwidth even in a degraded state. The highly sophisticated and expensive satellites used by the Department will not work in a JADC2 environment. Data availability is vital to achieving national interest in the future crossdomain/multidomain collaboration within a JADC2 environment. High data availability in a degraded environment is the difference between winning and losing. Developing a security-first architecture not only provides confidentiality and information integrity, but it ensures a transport system will overcome power outages, commercial circuit outages, or satellite failures to deliver the right information unimpeded to the right personnel on demand.

To enhance network resiliency, the DOD must increase the number and diversity of transports, thus exponentially increasing the probability of connecting. The DOD is currently at risk because it relies on an aging communication satellite infrastructure augmented by commercial satellites. Overwhelming multiple types of transports also creates greater confusion and costs to the adversary as the DOD can decrease the predictability in data traffic routes. Currently, the Air Force is conducting real-world experiments to achieve this vision as they connected F-35 and F-22 stealth fighters to share data without divulging their location.[28]

Ultimately the DOD must develop a transport-agnostic approach where all systems in every domain become transport nodes to move data, giving the DOD "a seamless battlefield presence crossing the air, land, sea, space and cyber domains where troops and weapon systems are connected 24/7 to ubiquitous sensors and can react almost instantly to put effects on targets."[29]

The DOD's highly sophisticated and powerful communication satellites are costly and take years to launch into space, labeling them a critical center of gravity in a wartime environment. Understanding this critical vulnerability and working with the commercial sector to create cheap minisatellites with the ability to launch instantaneously will help achieve JADC2.[30] Looking ahead, partnering with companies like Amazon and SpaceX is critical. Currently, Amazon plans to launch 3,236 satellites over the next decade and create 12 ground-station facilities.[31] Like Amazon, SpaceX is mass producing and launching thousands of minisatellites within the next five years.[32]

To build the right constellation for communicating in a D-DIL environment, the DOD should consider a new satellite communications enterprise vision that addresses the current aging system and creates a roadmap to a seamless network of military and commercial communications satellites. The Department must designate war-contingency bandwidth reservations across all transports, better understand Wi-Fi signals or low-level cellular, or advance strategies in space through satellites.

Achieving Mission Assurance

Developing a scientific approach with industry forces the DOD to comprehend the utilization or effects of innovation across all domains and how the innovation will attain mission-essential functions in conflict. Driving technological complexity through mission assurance will produce exponential challenges and vulnerabilities to our adversary, causing confusion and overwhelming effects in conflict.[33]

Moreover, mission assurance requires the DOD to conceptualize and focus within a realistic framework considering actual adversaries with realistic capabilities and real strategic objectives.[34] The DOD cannot continue to paper-drill exercises and assume everything will work but instead should introduce real anomalies, incorporate outside the box thinking, and force consideration of worst-case scenarios. Testing aircraft systems' resistance to cyber threats and the ability to operate in a contested environment to achieve mission assurance is a start. Introducing a new type of wargaming to thoroughly exercise networks, computers, satellites, facilities, tanks, aircraft, or ships in a JADC2 environment through nonkinetic and kinetic means allows the DOD to understand where changes are needed to achieve success. Also, this testing is critical for the DOD to implement a smart, self-healing, and proactive defensive network utilizing AI and ML.

As the Department embraces AI and ML fully, the hardest decision for the DOD is how much data it truly needs in a JADC2 environment. Large video files not only take up tremendous bandwidth but are also a hacker's dream as they can easily hide malicious code. Giving up bandwidth-hungry features may not sit well with all stakeholders, especially in today's world where users are accustomed to seeing massive amounts of information with no restrictions. In a time of war, standard peacetime capabilities like PowerPoint and video teleconferences may not be absolutely necessary, but determining the right information needed to make timely decisions is vital.

Just last year, the Air Force began to recognize the importance of data in a JACD2 environment and is now leading the way within the DOD to create a strategy to exchange data between platforms, address data management, and standardize data policies. As the network grows smarter through ML, and the DOD designs a buffering system that takes various inputs from proprietary systems and converts the data into a similar standard for all, bandwidth utilization may continue to be an issue. Bandwidth is critical, and even as a smart network predicts the right path or sensor to transmit data for the highest probability of success, it will require a DOD communications transport strategy to mesh military and commercial transports.

The Air Force Research Lab is developing a network that puts security first, and understanding bandwidth utilization is critical to this effort. This network will provide a user the ability to share necessary data similar to telegraphic transmissions using plain-text data. The lab network uses low-bandwidth transports to access critical mission data segmented across multiple regions worldwide, creating a "milnet" that brings together requested data from the cloud to the user as needed. The critical information is transmitted in multiple data packets across

the JADC2 architecture sensors and assembled again at the next user point, making it virtually impossible to intercept and capture the full data transmission and leaving the adversary with only bits at best. The bottom line: the data is never fully compiled until it reaches the user's point of presence.

Another unique feature of this network allows the user to carry a dongle as their computer to connect to the internet of things globally, while the data itself does not reside on any local computer or laptop used to connect to the cloud. It affords the DOD the ability to access data at all classification levels and places security first. This innovation may force the DOD to rethink command and control to support forces using applications with less bandwidth like multiple miniaturized versions of combined air and space operations centers within a theater; however, this article cannot go into the possible new C2 support.[35]

Finally, as the DOD moves forward to achieve mission assurance in a JADC2 environment, it must develop a culture of change. Many organizations, especially the DOD, do not accept change well and are unwilling to accept the resulting risk. Program managers have focused on the system life cycle and now need to focus not only on the system but on the data, too. Current DOD leadership backs multidomain communications using a mission assurance model, but this effort will require a significant culture change within the DOD. Shifting from a reactionary defensive posture to virtualization, fob technology, zero-trust, or consolidating data across all security platforms introduces new ways of thinking. Promulgating these new ways of thinking means focusing on mission assurance, which takes time and requires personnel to work outside their comfort zone.

Transformational change is a long-term investment and introduces two anxieties—transparency and inclusivity—into organization personnel, survival, and learning.[36] People hate change but will follow if adequately informed and coopted from the beginning and educated about where their mission fits into the change. Transparency and inclusivity are crucial tenets to achieving change and avoiding resistance. Leadership must know how to reinforce transparency and inclusivity within a military organization. Resistance to change can be a struggle to overcome. But with a clear focus on goals, reinforcing the desired end state at all levels, transparency, and recognizing that risk and mistakes are acceptable, the DOD will achieve this new implementation of technology, thus gaining mission assurance across all domains.

Conclusion

As the DOD goes through the transformation to proactive security, security first, and mission assurance, it should become creative in testing and evaluating mission command across war-fighting domains. If the DOD's goal is to present

exponential challenges to adversaries, expose their vulnerabilities, and cause them confusion, it should understand the adversaries are trying to do the same. The Department cannot continue to carry multiple systems in war fighting to access different classifications of information. Military members need simple ways to access data at the right time and place. To achieve this, the DOD must shift from defending the current internet to creating a new internet with COTS products built on solid security principles embracing data protection through global cloud storage. The new internet thinking places emphasis on mission assurance across multiple domains and pulls the DOD away from reactive defense of its networks.

Now is the time for the DOD to act and quickly move away from a monitor-detect-react model to one that delivers mission assurance in the JADC2 environment by implementing the following recommendations:

1. Develop a sensor-driven transport network.
2. Develop a secure cloud to provide maximum data access, sensor-driven transports, and a wartime "milnet."
3. Move to a commercial model of open-architecture utilizing apps.
4. Increase the number and diversity of transports.
5. Partner with commercial companies to create cheap minisatellites that can launch instantaneously.
6. Test all aircraft systems' resistance to cyber threats and the ability to operate in a contested environment.

These recommendations will remedy the DOD's current strategy that falls short in adequately addressing security first and mission assurance in a JADC2 environment. Undeniably, cyberspace networks are the center of gravity to deliver mission command in a future JADC2 architecture. Understanding DOD vulnerabilities before they are exploited and identifying new ways of defending a network gets the Department closer to cross-functional success in all domains. The need for immediate changes in network defense in an ever-changing environment can only happen if the DOD fully understands the need for out-thinking the adversary.

The US Cyber Command vision emphasizes the utilization of cross-research and advancements by academic communities, government, and commercial sectors that understand the need for a more robust way of thinking in terms of cyber superiority in a highly contested environment.[37] The network may not be a new internet, but the solution must guarantee security first to accomplish mission-essential functions within a JADC2 environment. In the words of former Secretary of Defense Mark Esper, "You've got to be able to take some risk, and you've got to be able to accept some failure."[38] ✪

James F. "Frank" Hudson Jr.

Mr. Hudson (MBA, Touro University; MSS, Air War College) is currently assigned as the Chief Technology Officer and Chief Data Officer, Headquarters Pacific Air Forces, Joint Base Pearl Harbor-Hickam, Hawaii. He has over 30 years of commercial, government service, and Air Force officer leadership experience.

Notes

1. Dr. Kamal Jabbour, "The Post-GIG Era: From Network Security to Mission Assurance," Air Force Research Laboratory, Secretary of the Air Force Public Affairs, *Cyber Defense Review*, November 15, 2019, https://cyberdefensereview.army.mil/.
2. C. Todd Lopez, "Assume Networks Are Compromised, DOD Official Urges," defense.gov, September 24, 2019, https://www.defense.gov/.
3. Jabbour, "Post-GIG Era."
4. Jabbour, "Post-GIG Era."
5. History.com, "The Invention of the Internet," October 28, 2019, https://www.history.com/.
6. Jeff Hussey, "The Fundamental Flaw in TCP/IP: Connecting Everything," May 17, 2019, https://www.darkreading.com/.
7. US Cyber Command (USCYBERCOM), *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade, MD: USCYBERCOM), March 1, 2018, https://www.cybercom.mil/.
8. David Hume, *A Treatise on Human Nature: Being an Attempt to Introduce the Experimental Method of Reasoning into Moral Subjects and Dialogues Concerning Natural Religion* (London: Longmans Green, and Co., 1878), 390 (emphasis in original).
9. Will Robinson, "Russia Hacked Joint Chiefs of Staff and Have Shut Down the Email System of 4,000 Pentagon Employees for ELEVEN DAYS. . . and Counting," August 7, 2015, https://www.dailymail.co.uk/.
10. Richard Chirgwin, "Suspicious BGP Event Routed Big Traffic Sites through Russia, December 13, 2017, https://www.theregister.co.uk/.
11. Office of the Director, Operational Test and Evaluation (DOT&E), *Director, Operational Test and Evaluation: FY 2018 Annual Report* (Washington, DC: DOT&E, 2018).
12. Jim Garamone, "Panetta Spells Out DOD Roles in Cyberdefense," October 15, 2012, https://www.army.mil/.
13. Jabbour, "Post-GIG Era."
14. Robert H. Anderson and Richard Hundley, *The Implications of COTS Vulnerabilities for the DoD and Critical U.S. Infrastructures* (Santa Monica, CA: RAND Corporation, 1998) 1–15, https://www.rand.org/.
15. Michael Nienaber, "Germany Could Still Ban Huawei from 5G Build-Out: Defense Minister," Reuters, November 5, 2019, https://www.reuters.com/.
16. Kim Zetter, "Undersea Cables Cut; 14 Countries Lose Web Updated," December 19, 2008, https://www.wired.com/.
17. Douglas Main, "Undersea Cables Transport 99 Percent of International Data," *Newsweek*, April 2, 2015, https://www.newsweek.com/.
18. Stacia Lee, "The Cybersecurity Implications of Chinese Undersea Cable Investment," East Asia Center, University of Washington, February 6, 2017, https://jsis.washington.edu/.
19. Todd Harrison, "Space Threat Assessment 2019," Center for Strategic and International Studies, April 4, 2019, https://www.csis.org/.
20. David Vergun, "Chinese Set Sights on High-Tech Production," Department of Defense (DOD), 29 October 2019, https://www.defense.gov/.
21. Office of the Under Secretary of Defense for Policy, DOD Directive 3020.40, *Mission Assurance*, https://fas.org/.

22. Office of the Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: CJCS, June 8, 2018), https://www.jcs.mil/.

23. North American Electric Reliability Corporation and US Department of Energy, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," June 2, 2010, https://www.energy.gov/.

24. Jabbour, "Post-GIG Era."

25. John Curran, "DoD Publishes Cloud Strategy With Eye on Modernization," MeriTalk, February 5, 2019, https://www.meritalk.com/.

26. Curran, "Cloud Strategy."

27. Tom Keelan, "The Pentagon's JEDI Cloud Strategy is Ambitious, But Can It Work?," March 21, 2019, C4ISR Net, https://www.c4isrnet.com/.

28. Sydney Freedberg Jr., "F-35 To F-22: Can We Talk? Finally, the Answer Is Yes," World Defense, November 7, 2019, https://world-defense.com/.

29. Theresa Hitchens, "Breaking D's 2019 Top Five: From Multi-Domain Ops to Killer Robots," Breaking Defense, December 27, 2019, https://breakingdefense.com/.

30. Sydney J. Freedberg Jr., "Build Bare-Bones Network & Small Satellites for Multi-Domain Battle," Breaking Defense, July 31, 2017, https://breakingdefense.com/.

31. Michael Sheetz, "Amazon Cloud Business Reaches into Space With Satellite Connection Service," CNBC, November 27, 2018, https://www.cnbc.com/.

32. Eric Ralph, "SpaceX's Starlink Eyed by US Military as Co. Raises $500-750M for Development," Teslarati, December 21, 2018. https://www.teslarati.com/.

33. US Air Force (USAF), *USAF 2030 Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond*, April 1, 2019, https://www.af.mil/.

34. Williamson Murray and Allan Millett, *Military Innovation in the Interwar Period* (New York: Cambridge, 1998).

35. Colin Clark, "MDC2: Air Force Works on Huge Command, Control System; Allies Key," Breaking Defense, March 7, 2017, https://breakingdefense.com/

36. Edgar H. Schein, *Organizational Culture and Leadership* (Hoboken, NJ: Wiley & Sons).

37. US Cyber Command, "Achieve and Maintain Cyberspace Superiority."

38. Brian W. Everstine, "Esper: Culture Change in DOD Needed to Improve Acquisition

Cloud Conundrum

Maj William Giannetti, USAFR

Last September, "Russian" cruise missiles were streaking toward the continental United States. Sophisticated cyber attacks against US interests overseas and laser-dazzling of reconnaissance satellites preceded the launch. At Joint Base Andrews, Maryland, the tracking data poured in real time, and operators across the country stood ready. It was the second in a series of on-ramps (or testbeds) for the Advanced Battle Management System (ABMS), a military Internet of Things that rapidly links data to decision-makers and provides commanders a menu of shooters.

BQM-167 target drones played the incoming cruise missiles, and the commanders made their selections. Over Creech Air Force Base (AFB), Nevada, an MQ-9 Reaper shot down one BQM-167 with an AIM-9X missile. An M-109 Paladin shattered another "cruise missile" in seconds at White Sands, New Mexico, with an experimental hypervelocity shell.[1] For the Joint Force, the display of firepower was a technological coup. "Tanks shooting down cruise missiles is awesome—video game, sci-fi awesome," said former Air Force acquisitions chief Dr. William Roper.[2]

Behind the scenes, classically stovepiped command-and-control data flowed at 5G speed. The Department of Defense's (DOD) array of "ONE" products supported mainly by public cloud mega-brokers Amazon Web Services (AWS) and Microsoft Azure made the linkages possible. OmniaONE, fed by dataONE's Unified Data Library, provided the on-ramp's "space to mud" common operating picture. For secure cloud applications, cloudONE provided remote data storage, and for war fighters, edgeONE did the same.[3] The on-ramp evidenced some impressive benefits, yet what are the risks of this military partnership with the public sector? History provides an answer.

The Cloud: A Brief History

According to the National Institute of Standards and Technology, a cloud is a ubiquitous, shared pool of configurable computing resources "that can be rapidly provisioned and released with minimal management effort or service provider interaction."[4] In short, a person uses someone else's computer—for a fee—to run their apps, process their data, and store their work. For almost a decade, AWS and Microsoft have dominated the public cloud market. Their storied competition for

the Joint Defense Enterprise Infrastructure (JEDI)—a "one cloud to rule them all"—has played out in court. They rent shared computing resources to customers inside their standard data centers, and there is extraordinarily little for the individual user to do. Patches and updates are done remotely, and interruptions are seldom.

Private clouds, on the other hand, are tailored for customers who have industry-specific or regulatory needs. Insurance companies, health management organizations, and investment firms typically use this type of cloud. The Defense Information Services Agency (DISA) offers private clouds to military customers with sensitive projects. The infrastructure is supervised inside the workplace or overseen off-premises inside a secure location. Like AWS and Azure, DISA offers an enterprise cloud, which is just a more expansive grouping of servers, routers, and switches. If a cyberattack happens in smaller, private clouds, defenders have less to focus on and more time to fight off a problem before it spreads.

But where did the cloud originate? Its founding concept precedes the internet as we know it. In the 1950s and 1960s, IBM's reel-to-reel mainframes employed a time-share model that allowed multiple users to use one computer. About this time, "mad" Major John Boyd, USAF, experimented with an IBM-704, testing an idea that influences combat aircraft's design and performance today—the energy-maneuverability theory.[5] The 1980s wave of computer resources' decentralization swept the old mainframes into the dustbin. Local ethernets codesigned by Bob Metcalfe linked single points of presence to businesses and industry.

Then, in 1996, two advertising men from Compaq—Sean O'Sullivan and George Favaloro—had an idea. Compaq servers were known for their reliability, and analysts projected $2 billion in sales to fledgling internet service providers like AOL. The duo looked at network engineering drawings, the wiring diagrams within them, and how a cloud signifies distant connections. A slogan was necessary—something that would make the company's products synonymous with the newly expanding internet. "Cloud computing" was born, though it did not become a household name until 2006. Google and Amazon began using the phrase to describe a new paradigm when people were accessing their software and computing power, not with their desktops but via the Web.[6]

The Value Proposition

A public cloud's value proposition is what buyers find most attractive. In essence, like any utility—water, electricity—you only pay for what you need. The mid-2000s saw growing interconnections between individuals and organizations that together made cloud computing economically attractive.[7]

The cloud industrialization push by AWS and Azure implies economies of scale, where average production cost falls as output volume increases.[8] At the dawn of the American Industrial Age, scale meant more electric power stations for more factories, followed by more railroads and more public schools for primary, secondary, trade, and university education. All these things combined promised better goods and services, with everyone sharing some slice of the burden. Similarly, as the theory went, more computing power concentrated inside data centers meant lower customer costs.

According to the Government Accountability Office (GAO), cost-cutting is vital because the federal government's bill for information technology overhead is $67 billion a year.[9] As part of the 2019 Federal Cloud Computing Strategy, the DOD has made some reductions by shrinking its brick-and-mortar presence and consolidating cloud management into fewer, higher functioning facilities.[10] While the GAO says the consolidation's results are unclear, it could translate into cost savings for taxpayers. The savings mean more cash for artificial intelligence (AI) research and development, small-business grants, or newer Next Generation Air Dominance fighters on the tarmac.

The Intelligence Community began its move to the cloud in 2013. Then Director of National Intelligence James Clapper led the effort to virtualize all 16 agencies' standalone computers into one network called the Intelligence Community Information Technology Effort (IC ITE), better known as "Eyesight." At an Association of Old Crows meeting in Washington that year, Clapper touted the windfall: "If we're going to make big savings in the Intelligence Community it will have to be in our IT enterprise."[11] That savings came from cost reductions in heating, ventilation, and cooling for the older machines, as well as similar reductions in electricity and maintenance bills.

At the time, the Intelligence Community was still reeling from former Central Intelligence Agency contractor Edward Snowden's revelations and how much damage one insider can do to national security. Snowden held sole superuser rights to many National Security Agency databases, too, a fact that slipped past Fort Meade, Maryland's security. If there was a way to track people's access to classified information by keystroke logs or metadata identity tagging, Clapper was for it. "The bumper-sticker mantra for IC ITE is 'tag the data, tag the people'. . . . So that if we tag the data, then we have the assurance as to the bona fides of the handlers, and can audit that, [it] would go a long way to promoting security."[12]

"Goldfinger"

A cloud's potential benefit—to be a formidable pool of data and machinery—also happens to be its primary potential vulnerability. Since Snowden, the re-

sponse of the Defense Department and the Intelligence Community has been to recentralize and pack the cloud into select "Fort Knox" data centers. Then the defenders erect virtual ramparts with redundant firewalls, routers, and proxy servers or put public cloud providers on contract to do it for them. "Fort Knox," said Harvard professor Jonathan Zittrain in 2010, "represents the ideal of security through centralization—gunships, tanks, and 30,000 soldiers surround a vault containing over $700 billion in American government gold."[13]

And that gold—the command-and-control data for the on-ramps—is very precious, indeed. Moving it rapidly to the people that need it is key to the success of ABMS. To hoard it all away from malign actors under one roof (or within one system of systems) seems logical.

But commingling data from every service could pose some thorny policy and security problems. Cybercriminals are lurking. The antivirus company McAfee estimates the global cost of cybercrime is about $600 billion annually.[14] A 2020 Price Waterhouse Coopers survey ranks cybercrime as the government and public sectors' most disruptive event with an estimated $42 billion in losses in the last two years alone.[15] Like the eponymous 1964 James Bond movie *Goldfinger*, seizing a target with an impregnable appearance could be an irresistible prize to criminals that carries very real—and potentially devastating—consequences.[16]

This scenario certainly paints a tantalizing picture, though an unforced human error could be just as damaging. Along the outskirts of Northern Virginia is Amazon's most extensive data hub for Simple Storage Service (S3). On February 27, 2017, administrators detected a bug inside S3's billing system. Once the problem was isolated to a specific subnet, they hastily followed a standard procedure to resolve it. But A miskeyed script removed a large group of the massive network's index servers. The East Coast operations of AWS momentarily froze. S3 could neither accept new virtual machines, retrieve location information, nor process requests until the problem was corrected five hours later.[17]

Nature's fury plays a part, too. Ten regional hubs host Azure's software development tools. They must be kept cool to operate at peak efficiency. But when a severe lightning storm lashed South Central Texas on September 4, 2018, power spikes jolted a nearby Microsoft data center's air conditioning. As temperatures inside rose, an automated, step-by-step shutdown process went into effect to reduce equipment damage and prevent data loss. After 21 hours, normal service was restored, followed by a public inquiry citing "cross-dependencies" that caused a cascading series of outages worldwide.[18]

"Don't Be Evil"

A public cloud's democratic appeal has also contributed to a phenomenon known in the industry as multitenancy. Private DOD clouds are reserved for DOD members who undergo a strict security background check before starting their work. They have some assurance of the soldiers or sailors neighboring them and work (mostly) without any political or social factors to disturb them. But experts say external tenants—outside the Department and the federal government—warrant a watchful eye. Private citizens, foreign countries, and other rogue entities inhabit the for-profit public cloud, too.[19] In one notable example, AWS suspended Parler's account following the January 6, 2021 insurrection on Capitol Hill.[20] The social media outlet is a favored alternative for alternative-right users who violate Facebook and Twitter's codes of conduct regarding hate speech.

More complications between the tech industry and the military have arisen. Though Google's AI engineers are responsible for creating some of the most advanced software for image recognition on the market today, the Silicon Valley giant began to have ethical doubts about its contract with the DOD's Project Maven in 2018. Maven's algorithms sift through thousands of hours of reconnaissance drone footage, pinpointing buildings, people, and vehicles that human analysts tag. In an open letter to Chief Executive Officer Sundar Pichai, thousands of Googlers said the relationship violated their "Don't be evil" motto.[21] Pichai found their argument had merit and approved the agreement's termination. It bowed out of consideration for the Joint Defense Enterprise Infrastructure, saying the contract's sole sourcing also violated its corporate principles. The head of Google's Open Research group, Meredith Whittaker, praised the end of the controversial alliance over Twitter: "I am incredibly happy about this decision, and have a deep respect for the people who worked and risked to make it happen. Google should not be in the business of war."[22]

Former Deputy Secretary of Defense Robert O. Work is an early founder of Project Maven who chaired a recent government commission on AI's strategic importance. He reacted, saying Pichai's call was "motivated by an assumption that any use of artificial intelligence in support for the Pentagon is a bad thing. But what about using artificial intelligence to power robots that defuse bombs or improvised explosive devices? Or using AI to prevent cyberattacks on our electrical grid?" The parting of ways marked the end of a dark chapter in Silicon Valley's history of innovative partnerships with Washington and the military. "Not being able to tap into the immense talent at Google to help DOD employ AI in ethical and moral ways is very sad for our society and country," he added. "It will make it

more difficult to compete with countries that have no moral or ethical governors on AI in the national security space."[23]

The Hybrid Option

Private and public clouds aside, a third option is a hybrid cloud. Hybrid clouds combine a private cloud's security and customization with a public cloud's high-speed computer processing. They are ideal for organizations that do not want to deal with a commercial cloud's baggage and the unanticipated cost. Google and Amazon have been industry leaders in selling customers on a preset menu of tools to use on their public platforms. Microsoft and IBM have been more flexible by comparison, allowing users to deploy their cloud tools on their existing on-premises networks. Due to the computer code's iterative nature, all companies charge per second, use, and gigabyte.[24] One struggling IC program that could not be named due to its work's sensitivity accrued $1.5 million in AWS charges in one year. Researchers with finite budgets and periods of performance try to find their way around these challenges, and it is not easy.

One solution is a private, hybrid cloud owned by the government and operated by cleared defense contractors. It could provide a haven for ABMS ideas to "fail-fast" Silicon Valley-style or win quickly. This way, a project's financiers can see what works, renegotiate contracts, and move on, if necessary. Also, both major public competitors—AWS and Azure—can process secret-level information. Disturbingly, only Amazon is accredited to process top-secret data, and Microsoft is likely to follow suit.[25] A previous edition of *Air & Space Power Journal*, however, made a case for Technology for Innovation and Testing on Accredited Networks (TITAN).[26] That system is a good example of a private, hybrid cloud overseen by Headquarters Air Force that can process all the same information for a flat fee. Such an arrangement could likely help the government avoid an uncomfortable vendor lock-in situation in the future.

Without question, like any monumental task, shooting down cruise missiles with data has its risks. Choosing the right kind of cloud should not be one of them. The Air Force's partnership with private industry has helped counter US adversaries abroad for generations. Keeping that partnership healthy and alive will be critical to growing cutting-edge ABMS ideas inside a hybrid cloud that is safe, affordable, and secure.

Maj William Giannetti, USAFR
Major Giannetti (MS, St. Joseph's University) is the 62nd Airlift Wing's reserve senior intelligence officer and TITAN's former director of operations.

Notes

1. David Axe, "One Battle System to Rule Them All," *Combat Aircraft Journal* (December 2020): 96.
2. Theresa Hitchens, "ABMS Demo Proves AI Chops for C2," Breaking Defense, September 3, 2020, https://breakingdefense.com/.
3. Theresa Hitchens, "Roper Pushes Moving Project Maven to Air Force," Breaking Defense, June 11, 2020, https://breakingdefense.com/.
4. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," US Department of National Institute of Standards and Technology (NIST), special publication 800-145 (Gaithersburg, MD: NIST, September 2011), https://csrc.nist.gov/.
5. Robert Coram, Boyd: *The Fighter Pilot Who Changed the Art of War* (Boston: Little, Brown, 2002).
6. Antonio Regalado, "Who Coined 'Cloud Computing'?" *MIT Technology Review*, October 31, 2011, https://www.technologyreview.com/.
7. Tim Maurer and Garrett Hinck, *Cloud Security: A Primer for Policymakers* (Washington DC: Carnegie Endowment for Peace, 2020), https://carnegieendowment.org/.
8. "Economies of Scale and Scope," *Economist*, October 20, 2008, https://www.economist.com/.
9. US Government Accountability Office (GAO), *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Need to Be Better Tracked* (Washington, DC: GAO, April 2019), https://www.gao.gov.
10. Office of the Federal Chief Information Officer (CIO), *Federal Cloud Computing Strategy: From Cloud First to Cloud Smart* (Washington, DC: CIO, 2019), https://cloud.cio.gov/.
11. Jordana Mishory, "DNI Clapper Pegs IT Enterprise Effort as Best Way to Save Money," *Inside the Pentagon* 29, no. 44 (October 31, 2013), https://www.jstor.org/.
12. Mishory, "Clapper Pegs IT."
13. Jonathan Zittrain, "The Internet's Fort Knox Problem," Future of the Internet and How to Stop It (blog) June 3, 2010, https://blogs.harvard.edu/.
14. McAfee, *The Economic Impact of Cybercrime: No Slowing Down* (Santa Clara, CA: McAfee, December 2017), https://www.mcafee.com/.
15. Kristin Rivera et al., "2020: Fighting Fraud: A Never-Ending Battle: PwC's Global Economic Crime and Fraud Survey," Price-Waterhouse-Coopers, 2020, https://www.pwc.com/.
16. Maurer and Hinck, *Cloud Security*.
17. Amazon Web Services, "Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region," https://aws.amazon.com/.
18. Buck Hodges, "Postmortem: VSTS 4 September 2018," Microsoft Azure DevOps Service (blog) September 10, 2018, https://devblogs.microsoft.com/.
19. Maj Steven C. Dudash, *The Department of Defense and the Power of Cloud Computing* (Maxwell AFB, AL: Air University Press, 2016).
20. John Paczkowski and Ryan Mac, "Amazon Will Suspend Hosting for Pro-Trump Social Network Parler," BuzzFeed, January 9, 2021, https://www.buzzfeednews.com/.
21. Drew Harwell, "Google to Drop Pentagon AI Contract after Employee Objections to the 'Business of War,'" *Washington Post*, June 1, 2018, https://www.washingtonpost.com/; and Lucy Suchman et al, "Open Letter in Support of Google Employees and Tech Workers," International Committee for Robot Arms Control (blog) June 2018, https://www.icrac.net/.

22. Meredith Whittaker, "I am incredibly happy. . ." Twitter, 1 June 2018, 3:28 p.m., June 1, 2018, https://twitter.com/.

23. Harwell, "Google to Drop Pentagon."

24. Maj Noah Hassler et al., "Bullet Background Paper on Commercial Cloud Usage in the Intelligence, Surveillance and Reconnaissance Enterprise," ISR-300 background paper, November 2019, 1.

25. Aaron Gregg, "With a $10 Billion Cloud-Computing Deal Snarled in Court, the Pentagon May Move Forward without It," *Washington Post*, February 10, 2021, https://www.washingtonpost.com/.

26. Maj William Giannetti, "Quiet Giant: The TITAN Cloud and the Future of DOD Artificial Intelligence," *Air & Space Power Journal* 34, no. 1 (Spring 2020): 54-58, https://www.airuniversity.af.edu/.

The Future of Artificial Intelligence in ISR Operations

Col Brendan Cook, RCAF, MSM, CD

Every day, Canada and its allies conduct intelligence, surveillance, and reconnaissance (ISR) operations of one type or another. Despite many successes, operators and analysts have a daily mountain to climb—one which grows with each subsequent mission. That mountain is the result of the continual influx of ISR "big data" that needs to be processed, exploited, and disseminated to end users to ensure the maximum advantage is gained from each mission. Many nations now concede current systems cannot properly analyze and fuse multisensor data. Moreover, these systems cannot provide analysts and operators real-time cues to important information they may be missing. Despite the best efforts to rationalize and realign resources, the mountain of ISR big data grows along with the sense that important intelligence revelations buried in that mountain are being missed.

As with any mountain, there are many paths one can take to the summit. This article aims to chart one path. It will define the ISR community's big data problem as a way to understand the terrain, explore the potential of artificial intelligence (AI) to address the challenges posed by that terrain, and seek to understand the legal and ethical pitfalls posed by AI. With these factors in mind, this article will present recommendations on how best to develop artificial intelligence, revealing a clear path to the summit of the ISR mountain.

Background

Put simply, AI is a sophisticated decision-making method that enables machines to think and learn on their own.[1] Artificial intelligence differs from autonomy, a broader term referring to "the ability for a machine to perform a task or function on its own."[2] Autonomy does not necessarily require AI. In less complex environments, autonomy can be achieved by simple, preprogrammed rules. But more complex, autonomous tasks in open and varying environments do not lend themselves to preprogrammed responses. These tasks require decision-making bordering on cognition—the realm of AI.

Lethal autonomous weapon systems combine autonomy and lethality, may have a human in the loop, on the loop, or human out of the loop, and may or may not possess some form of AI—a feature which often sparks concerns. This article will not address the full breadth of complex problems associated with using these weapon systems. Instead, it will focus on the use of AI in semiautonomous (human-in-the-loop), supervised autonomous (human-on-the-loop), and AI-enabled ISR systems in ISR processes spanning data collection, analysis, and decision-making up to the point of target nomination to a human. In this way, the article will examine what is often considered a less contentious use of AI to determine if some problems and pitfalls remain, even with this limited use.[3]

Intelligence, surveillance, and reconnaissance is the process by which operators and decision-makers learn about an environment at the tactical, operational, and strategic levels.[4] Disciples of the revolution in military affairs once preached that the ubiquity of sensing and communications systems would lead to a "powerful synergy" and deliver dominant battlespace knowledge, near-perfect mission assignment, and immediate and complete battlespace assessment.[5] In an attempt to achieve this vision, militaries worldwide have made significant investments in the ISR enterprise. The Department of Defense (DOD), for example, increased expenditures in ISR systems six-fold from 2001–12.[6] Similarly, Canada's latest defence policy leveraged previous commitments and prioritized joint ISR investments to anticipate and better understand potential threats to Canadian interests.[7] Through these investments, the ISR enterprise now can access data from every domain: air, land, sea, surface, subsurface, space, and cyberspace. [8] Moreover, the enterprise can draw upon open-source and multilevel classified data.

But the exponential increase in data collection has not led to commensurate improvements in intelligence. As early as 2008, the United States Intelligence Science Board acknowledged that the volume of ISR data exceeded the capacity of the existing analyst community and that much of the data was never reviewed.[9] In 2014, the RAND Corporation estimated analysts had access to as little as 5 percent of total ISR data.[10] The result for commanders is that fewer intelligence needs are being met.[11]

To address this deficiency, organizations have improved processes and manning structures, centralizing key functions to maximize manpower, yielding minor improvements in some areas. But the big data problem is only getting worse. Robert Cardillo, director of the National Geospatial-Intelligence Agency since 2014, has noted despite recent improvements, with the current architecture the agency would need 8 million new analysts using current processes to analyze the glut of full-motion video data expected to be collected in the next 20 years.[12] This is but one data source and does not account for the myriad other ISR data sources—

signals, acoustic, radar, and electronic support measures, to name a few—that require analysis to be of any decision-making value.

Challenges

While there is no recognized definition of big data, two recurrent themes emerge: the size and the utility of the dataset. First, big data comprises those datasets "whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze."[13] Second, big data consists of information assets whose utility to the organization "demand cost-effective, innovative forms of information processing for enhanced insight and decision making."[14] These themes are also descriptive. Big data comes from multiple platforms, sensors, systems, and sources that exceed the ability of current database software tools. While highly useful, big data must be given to the right person, at the right time, and in the correct format, to enable decision-making. An analysis of the characteristics of big data sheds further light on why it makes sense to think in terms of ISR big data.

The understanding of the characteristics of big data has evolved. In 2001, Doug Laney proposed the three Ds (data volume, data velocity, and data variety) when analyzing data in e-commerce.[15] A 2014 RAND Corporation study for the US Navy concluded the four Vs can best characterize big data: volume, velocity, variety, and veracity.[16] More recently, other researchers have stressed the importance of adding another V, namely value, to big-data characteristics.[17] These five Vs directly relate to ISR big data.

Intelligence, surveillance, and reconnaissance data is collected in large volumes with a wide variety of formats, sources, and types, and arrives at a high velocity (frequency)—a requirement for delivery to end users.[18] The variety of ISR big data further complicates matters. It may be both open source or classified and, as a result, must be managed across multiple, mutually exclusive security domains.[19] Moreover, ISR big data contains inherent ambiguity, incompleteness, and uncertainty as some data sources are higher quality than others. As such, the veracity of ISR big data must always be challenged and considered when integrating it with other data and information. Lastly, the value of ISR big data is directly related to its role in generating situational awareness and its ability to inform decision-making by being delivered to the right person at the right time and in the correct format.

Opportunities

Having defined and characterized the terrain of the ISR big data mountain, the article will evaluate the promise AI offers to address the five Vs of these data. Since its inception six decades ago, the AI field has alternated between the highs and lows of expectations and actual performance. Setbacks and disappointments have followed periods of great promise.[20] The promise has stemmed from the development of AI systems that have progressively challenged humans in gameplay. In 1997, Deep Blue famously beat world chess champion Garry Kasparov, who observed "glimpses of true intelligence and creativity in some of the computer's moves."[21]

Advancements since Deep Blue showed promise until recent AI system designs required human intervention to train the systems and necessitated learning from vast amounts of data. Further, these developments demonstrated only a narrow application to gameplay. However, AlphaGo and its successor AlphaGo Zero heralded a new era of AI by demonstrating the ability to play the game of Go, considered the most challenging of human games, at the highest level. AlphaGo was the first AI algorithm to beat human Go champions—the European Champion Fan Hui in October 2015 and Lee Sedol, the winner of 18 international titles, in March 2016.[22] In 2017, AlphaGo Zero went one step further, achieving the long-standing goal of learning tabula rasa without human intervention. The algorithm learned to play Go through the process, "reinforcement learning, without human data, guidance or domain knowledge," playing itself in more than 25,000 games. [23] In doing so, the algorithm learned Go from scratch and beat its earlier version 100-0 after only 36 hours of learning.[24]

While the algorithm's ability was confined to a narrow task, this experiment demonstrated the potential for AI systems to learn unsupervised. This discovery has opened the way toward artificial general intelligence (AGI), a single system that can learn multiple tasks and employ the knowledge gained in one task to positively transfer over to other tasks—sometimes called meta learning.[25] The makers of AlphaGo Zero, DeepMind, announced their subsequent algorithm, Impala, could learn 30 different challenging tasks involving learning, memory, and navigation.[26] With AI now on the cusp of AGI, it is poised to provide solutions that will address ISR's big-data problem.

Artificial intelligence technologies have already been commercialized to address the volume, velocity, and variety of data in multiple fields. The AI employed by John Paul, Amazon, and Netflix have demonstrated the ability to review vast volumes of data regarding customer preferences and available products to provide recommendations for travel needs, online purchases, and entertainment, respec-

tively. Each of these systems analyzes billions of records to suggest products and services based on the previous reactions and choices of users.[27]

In addition to addressing the volume challenge, economists have turned to AI to address issues of data velocity. Artificial intelligence is being used to create novel data sets from unstructured information, enabling economists to answer questions in real time that previously required months of study. Google has developed systems to analyze search queries to predict changes in unemployment, and Yelp predicts local business patterns, both doing so in real time.[28]

The ability to process large volumes of data arriving at high velocity is particularly valuable when coupled with AI's ability to analyze many varieties of data such as imagery, speech, language, and electronic signals. Google and Facebook have already deployed face- and image-recognition AI widely in search engines and social media platforms. Project Maven, a DOD initiative, is working with multiple companies to develop image-analysis algorithms to analyze full-motion video data acquired from unmanned aerial vehicles to identify people, vehicles, buildings, and other objects of military value.[29] Siri, Alexa, and other personal-assistant AI technologies can already recognize, decode, and translate language.[30] The Israeli HARPY missile and US AGM-88 HARM can analyze the radar spectrum, identify enemy radar signatures, and home to targets.[31]

Artificial intelligence architectures have also been proposed and successfully tested to analyze radio signals for a wide variety of applications.[32] Each of these specialized capabilities is individually important. A common critique of having specialized AI for each task, however, is that this specialization "inevitably lead[s] to too many network models, increasing the storage complexity."[33] Recent research demonstrated a single AI model constructed from several AI building blocks across multiple domains could be trained concurrently on many data types and tasks.[34] Similarly, DeepMind's Impala has demonstrated the capability to conduct many tasks through reinforcement learning. Consequently, AI is already capable of analyzing ISR big data to translate languages, recognize patterns in images and data, find linkages and causation between data, and extract meaning.[35] Thus, rather than analysts and operators sifting through raw data, they can now be given the higher-level task of responding to cues, alerts, and conclusions presented to them by an AI-enabled ISR system.[36]

By fusing and cross-referencing data, these approaches go beyond simply addressing the characteristics of volume, velocity, and variety; they provide mechanisms to address the veracity and value of ISR big data. By overlaying multiple perspectives on each target, the five Vs of ISR big data are satisfied, which improves confidence in the resultant conclusions on target identity, location, motion, and other characteristics. When this process yields conflicting observations, AI

could identify these inconsistencies to operators indicating additional scrutiny is required. Moreover, by providing multiple perspectives on a single target, various low-level features can be extracted and selected from each perspective, and these features can then be compared to identify new, higher-level features in the data.[37] Researchers demonstrated this capability by employing a heterogenous, adaptive team of autonomous air and ground robots to monitor a small village; search for, localize, and identify human targets; and simultaneously conduct three-dimensional mapping in an urban setting.[38] In these ways, AI systems can be used to ensure the veracity of data while also adding value to it.

Artificial intelligence could also increase the value of ISR big data by alerting analysts and operators to key data and intelligence relating to an area of interest. Siri, Alexa, Google, Amazon, and Netflix AI engines can already monitor user searches and preferences to recommend products and services that anticipate the user's needs.[39] Artificial intelligence could monitor the searches and preferences of analysts and recommend data intelligence products to meet their needs. Moreover, as it learns the analyst's requirements, AI could then search through historical data sets to look for patterns of behavior, detect changes, or search for newly assigned priority targets.

For ISR operators, AI algorithms could compare data collected in real time to historical data to ensure sensor operators are alerted to changes from previous observations. Alternatively, as new data from neighboring ISR platforms is collected, it could provide automated cuing regarding observations that may impact the area of operations. These applications would ensure the value of ISR big data is maximized for both analysts and operators, and that less data is lost under the mountain of ISR big data.

A final method AI could use to address the ISR big-data problem is to employ its emerging capacity for creativity, one AlphaGo demonstrated during its second match against Lee Sedol. Midway through this match, AlphaGo made a move that was so unexpected, Sedol paused the game and left the room for 15 minutes to regain his composure. Observers classified the probability that a human would have played that move as 1 in 10,000 and commented that the move displayed "improvisation, creativity, even a kind of grace."[40] With this level of creativity now possible, AI could be tasked to generate hypotheses about the data it has analyzed. It could then search out data sets to prove or disprove its hypotheses or make recommendations for further ISR data collections. In this way, AI would enable more efficient and focused collections by suggesting collections to prove or disprove its theories, improving the data veracity.

Limitations

Despite the many advantages of employing AI to optimize ISR big data, a question of risk remains. The International Committee of the Red Cross, European Parliament, United Kingdom, the DOD,[41] and others have all considered the implications of employing lethal autonomous weapon systems in warfare. Few have focused on the narrower problem using AI-enabled ISR systems in semiautonomous (human-in-the-loop) or supervised autonomous (human-on-the-loop) modes. But the analysis to date regarding these systems and the work of Nick Bostrom and Paul Scharre regarding risk reduction in autonomous systems, suggest future AI-enabled ISR systems must address the following obstacles: the proper application of the principles of distinction and proportionality; the concerns rising from the "black box" dilemma; the potential for AI systems to mislearn; and the requirement to ensure accountability under the rule of law.[42]

Under International Humanitarian Law (IHL), the principle of distinction requires attacks only be directed against legitimate military targets. Noncombatants including civilians, children, medical staff, and those combatants considered d'hors combat, should be immune from attack, as should civilian objects of no military value.[43] To adhere to IHL, an AI system must be able to distinguish between military and civilian targets, a challenge compounded by the fact that no clear criteria exist to make this distinction. It is difficult to instruct or, in the case of AI, to teach a system to avoid targeting civilians and civilian objects when there is no precise specification for "civilianess."[44]

Neither the 1949 Geneva Convention nor the 1977 Protocol 1 define civilian in a negative sense (for example, anyone who is not a combatant) requiring the application of common sense in the determination.[45] The presence of nonuniformed combatants on the battlefield, particularly in dense urban environments, further complicates matters. Ultimately, an AI system would require a "human understanding of other people's intentions and their likely behavior" based on subtle cues that may not be easily detectable by sensors or big-data analytics.[46] In 2013, the Directorate-General for External Policies concluded in its report to the European Parliament that no autonomous system currently exists that can "reliably distinguish between legitimate military targets and civilian persons and objects, [and] take precautions to avoid erroneous targeting."[47]

More recently, scholarship on the subject concluded that while it may be possible to distinguish cooperative targets that emit known signatures in a controlled environment, accomplishing the same task in an environment with clutter is much more difficult. Moreover, distinguishing an uncooperative target in a cluttered environment is presently beyond the capability of current systems, and "no such

technology is on the horizon."[48] Until this challenge can be surmounted, human intervention will be required to ensure the principle of distinction is correctly applied to any targeting decisions.

The principle of proportionality presents another significant challenge for AI systems. This principle requires the expected military advantage to be gained by engaging a target must not be outweighed by the expected civilian collateral damage. While many automated systems can calculate expected civilian collateral damage, there is no objective method to calculate the direct military advantage to be gained.[49] Absent a method to either program or teach this calculation, there is virtually no way an AI system can comply with this principle on its own. Experts have proposed that human-in-the-loop and on-the-loop autonomous systems do not need to make these judgments on their own to ensure compliance with IHL. By pairing AI systems with humans, the AI system can identify potential military targets and then calculate the potential collateral damage, leaving the human to make the moral judgment.[50]

Beyond the challenges of distinction and proportionality, AI poses a "black box" dilemma. The black box dilemma arises when the complexity in a system increases to the point that a human cannot reasonably understand the process. The human can see the input and output to the system, but the system function is effectively opaque to the user. The principal concern of the black box dilemma is that if a human cannot easily comprehend why and how an AI system is arriving at its conclusions, it is almost impossible for the human to detect when the system fails.

Researchers demonstrated the limitations of the human understanding of AI in a 2013 study of the unexpected outcomes of AI-enabled image identification systems. They studied deep neural networks, a form of AI used in image recognition that had generated counterintuitive conclusions. They found by introducing imperceptible perturbations to images, they could arbitrarily change the AI's classification of the image. In one experiment, they started with a simple picture of a puppy that was correctly classified by the system. They then made an imperceptible change to the image, only noticeable to the human eye at 10x magnification, and the system then classified the image as an ostrich.[51]

Another study investigated this phenomenon from the opposite perspective. The research team trained an AI system to recognize baseballs and then asked it to draw a picture of a baseball. The resulting image was "completely unrecognizable garbage" to a human, but other AI systems agreed with their test system, interpreting the image as a baseball.[52] Researchers call images that can trick AI systems into misidentifying *adversarial images*. Further work has shown that image recognition software has a widespread vulnerability to adversarial images.[53]

Consequently, as AI systems develop, humans may not be able to comprehend easily why and how a system arrives at its conclusions.

The difficulties of the black box dilemma can be compounded by the vulnerability of AI systems to mislearn. In March 2016, Microsoft launched Tay on the internet, an AI system designed to exhibit age-appropriate behavior for a teenage girl and to learn through interactions on Twitter.[54] Microsoft expected Tay to learn millennial slang and start chatting about pop stars. It was instead bombarded with controversial messages from online trolls and within 24 hours was tweeting pro-Nazi messages, denying the Holocaust, and advocating for genocide. Microsoft promptly took Tay offline and issued a formal apology.[55] This stark example demonstrated the vulnerability of AI systems to mislearn.

The 2016 US election provides a second example where an adversary exploited the use of AI leading to the widespread dissemination of disinformation. As noted in the report to the US Senate, there is compelling evidence that suspected Russian-backed, highly automated, or fake social media accounts were used to sow misinformation and discord in the United States to influence the outcome of the 2016 election.[56] They achieved this influence by leveraging Facebook, Twitter, Instagram, and YouTube, which each use AI to target users based on interests and behaviors.[57] In effect, the AI inherent in these social media platforms was exploited to deliver misinformation to American voters on a massive scale. An ISR AI employed to comb through open-source data and classified data in order to deliver useful intelligence to analysts and operators according to their individual preferences could potentially be exploited by an adversary using similar methods.

The vulnerability of AI to mislearn highlights the need to understand AI decision-making with sufficient confidence to ensure accountability under the rule of law. States are obligated under IHL to conduct investigations into the lawfulness of the use of force by their agents.[58] When incidental civilian death, injury, and/or destruction occurs, or the lawfulness of an attack is in question, an immediate, exhaustive, and impartial investigation must be conducted.[59] This requirement means information and actions must be traceable in the decision-making process. But if an AI system is effectively a black box—making connections and determinations too complex for any human to comprehend—this becomes problematic, particularly if the AI system cannot be made to explain its reasoning. Therefore, some consideration must be made to ensure some level of transparency exists in an AI-enabled decision-making process to permit detection of failures, prevent mislearning, and for traceability.

Better design, development, testing, and training can minimize the risks of failure in an AI system, but accidents can and will happen with AI-enabled decision-making, just as they do with human decision-making using current

technologies. The accidental shooting down of Iran Air Flight 655 in 1988 by the USS *Vincennes*, and the multiple fratricides by US Patriot missile batteries during the 2003 Iraq War are two examples in which automated systems provided threat indications to operators, who then took what they believed to be an appropriate action.[60] An AI-enabled system will inevitably result in some failures. Human decision-makers must remain vigilant and closely monitor AI results, with the understanding that this effort may prove difficult on the battlefield.

Experts argue as confidence grows in the use of AI, there is a risk humans will learn to simply trust a system, effectively cease trying to detect failures, and hence become morally disengaged from an AI-enabled decision-making process.[61] There are four known reasons why relying on humans to make decisions based on the assistance of automation can be problematic, each of which played some role in the Iran Air and Patriot missile incidents.

First, reliance on automation leads humans to neglect ambiguity and suppress doubt. Human supervisors then jump to conclusions and cease searching for alternative interpretations to resolve uncertainty.[62] Second, humans tend to infer and invent causes and intentions by linking fragments of available information through the process of assimilation bias.[63] Third, humans are biased to believe and confirm by uncritically accepting suggestions from computers, also known as confirmation or automation bias.[64] Lastly, a reliance on automation focuses humans on existing evidence and leads them to ignore absent evidence. This phenomenon is often termed "What You See Is All There Is" and "facilitates the feeling of coherence that makes us confident to accept information as true."[65] While these factors are all currently at play with existing weapon systems, the black-box nature of AI may magnify these effects, raising the risk humans will cease questioning their "expert AI systems."

If a human decides on a military action based on the faulty reasoning of an AI system, who is to be held accountable for the decision? There is no easy solution to address this apparent "accountability gap." Some experts recommend developers pay attention to the human-machine interface design and operator training to ensure that the human-in-the-loop or human-on-the-loop has the capacity and mindset to be responsible for the decisions they make.[66] Furthermore, AI systems must be designed to allow greater insight into how they arrive at their conclusions and recommendations. Absent these actions, the introduction of AI systems could accelerate existing trends and result in the eventual cessation of effective human supervision.

Recommendations

To summarize, artificial intelligence offers solutions to address the ISR big-data challenge. Well-suited to address the characteristics of ISR big data, the emerging ability of AI to learn without human intervention makes it conducive to manage the myriad of ISR analytical tasks. But the difficulty of providing precise definitions for the principles of distinction and proportionality under IHL will establish an upper limit on what AI can be expected to do. The complexity of AI can render its operation effectively opaque to humans. Adversaries could also leverage the algorithms themselves to disseminate misinformation on a massive scale. The technology is vulnerable to mislearning through the corruption of the data and perverse incentives in algorithms. Moreover, humans are usually predisposed to believe automated systems. All these factors create the risk that humans could become ineffective supervisors of future AI-enabled ISR systems.

To realize the great potential of artificial intelligence and mitigate problems and pitfalls, AI development should be vigorously pursued with four key considerations in mind. First, due to the challenges of defining the principles of distinction and proportionality, there is a limit to the ability of AI technologies to provide highly accurate assessments under realistic combat conditions. Development should be tempered with the expectation that human-machine pairing is both necessary and desirable to ensure compliance with IHL.

Second, the reliance of an AI system on any one source of data to arrive at conclusions may expose these systems to a greater potential to either mislearn or to be manipulated by adversaries. The focus of development should be on building the capacity of AI systems to leverage the volume, velocity, and variety of ISR big data to compare and fuse across multiple data sets. This action will enable the veracity of collected data to be confirmed while simultaneously increasing the value of data and reducing the amount of ISR data left unprocessed and unexploited.

Third, AI algorithms and their associated human-machine interfaces must be designed so that humans can effectively monitor alerts, cues, determinations, and recommendations while also enabling some insight into how AI systems arrive at them. This design would enable humans to detect failures, counter AI's vulnerability to mislearn, and provide transparency during investigations.

Lastly, analysts and operators will require considerable training on AI systems and their employment. This training will need to provide a sufficient understanding of the algorithms to permit the operator to best leverage the potential of AI; methods for the detection of failures and mislearning; an understanding of the potential pitfalls of relying too much on AI and automation in decision-making;

and a recognition of the potential for moral disengagement in AI-enabled decision-making.

With these factors in mind, the potential risks can be reduced and the path AI may offer up the ISR mountain is clearer. The opportunity to choose a better way lies before us. As with all innovations, the implementation of an effective AI-enabled ISR system will take courage, determination, training, and perseverance. Fortunately, these are the same traits that define the modern soldier, sailor, airman, marine, and guardian. The summit is in sight—it is the perfect moment to crest the mountain. ✪

Col Brendan Cook, RCAF, MSM, CD

Colonel Cook (MSc, Royal Military College of Canada; MS, Air University) is the commander of 14 Wing, Greenwood, Nova Scotia, Canada. He is an air combat systems officer on the CP-140 Aurora (a P-3 derivative) with 30 years of flying experience and an extensive background in underwater acoustic research and air test and evaluation.

Notes

1. Jafar Alzubi, Anand Nayyar, and Akshi Kumar, "Machine Learning from Theory to Algorithms: An Overview," *Journal of Physics* Conference Series 1142, no. 1 (December 5, 2018): 1, https://iopscience.iop.org/.
2. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton, 2018), 27.
3. "Who Decides: Man or Machine?," *Armed Forces Journal*, http://armedforcesjournal.com/.
4. B-GA-401-002/FP-001, *Royal Canadian Air Force Doctrine: Intelligence, Surveillance and Reconnaissance* (Trenton, ON: Royal Canadian Air Force Aerospace Warfare Centre, November 2017), http://www.rcaf-arc.forces.gc.ca/.
5. Adm Bill Owens, *Lifting the Fog of War* (Baltimore: Johns Hopkins University Press, 2001), 100.
6. Brig Gen Timothy D. Haugh and Lt Col Douglas W. Leonard, "Improving Outcomes: Intelligence, Surveillance, and Reconnaissance Assessment," *Air & Space Power Journal* 31, no. 4 (Winter 2017): 4, https://www.airuniversity.af.edu/.
7. Department of National Defence, *Strong Secure Engaged: Canada's Defence Policy* (Ottawa, ON: Department of National Defence, 2017), https://www.canada.ca/.
8. Isaac R. Porche et al., eds., *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information* (Santa Monica, CA: RAND Corporation, 2014), http://www.jstor.org/.
9. Porche et al., *Data Flood*, 1.
10. Porche et al., *Data Flood*, 14.
11. Haugh and Leonard, "Improving Outcomes," 4.
12. Stew Magnuson, "DoD Making Push to Catch Up on Artificial Intelligence," *National Defense*, June 13, 2017, 22, https://www.nationaldefensemagazine.org/.
13. Zhaohao Sun, Kenneth David Strang, and Rongping Li, "Big Data with Ten Big Characteristics," Researchgate, October 2018, 2, https://www.researchgate.net/.
14. Porche et al., *Data Flood*, 2.
15. Sun, Strang, and Li, "Big Data."
16. Porche et al., *Data Flood*, 2.'
17. Samuel Fosso Wamba et al., "How 'Big Data' Can Make Big Impact: Findings from a Systematic Review and a Longitudinal Case Study," *International Journal of Production Economics* 165 (July 2015): 234–46, https://www.sciencedirect.com/; and Shilian Zheng et al., "Big Data Processing Architecture for Radio Signals Empowered by Deep Learning: Concept, Experiment, Applications and Challenges," *IEEE Access* 6, 2018, 55907-22, https://ieeexplore.ieee.org/.
18. Porche et al., *Data Flood*, 2.
19. Porche et al., *Data Flood*, 18.
20. Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford: Oxford University Press, 2014), 5.
21. Bostrom, *Superintelligence*, 12.
22. David Silver et al., "Mastering the Game of Go without Human Knowledge," *Nature* 550 (October 2017): 354, https://www.nature.com/.
23. Silver et al., "Mastering the Game of Go."
24. Silver et al., "Mastering the Game of Go."
25. Aaron Krumins, "Artificial General Intelligence Is Here, and Impala Is Its Name," ExtremeTech, August 21, 2018, https://www.extremetech.com/.

26. Krumins, "Artificial General Intelligence."
27. R. L. Adams, "10 Powerful Examples of Artificial Intelligence in Use Today," *Forbes*, January 10, 2017, https://www.forbes.com/.
28. Matthew Harding and Jonathan Hersh, "Big Data in Economics," *IZA World of Labor*, (September 2018): 2, https://wol.iza.org/.
29. Jon Harper, "Artificial Intelligence to Sort through ISR Data Glut," *National Defense*, January 16, 2018, 34, https://www.l3harrisgeospatial.com/.
30. Adams, "Artificial Intelligence."
31. Scharre, *Army of None*, 46-48.
32. Zheng et al., "Big Data Processing Architecture."
33. Zheng et al., "Big Data Processing Architecture."
34. Lukasz Kaiser et al., "One Model to Learn Them All," Cornell University, ArXiv:1706.05137 [Cs, Stat], June 16, 2017, http://arxiv.org/.
35. Ethem Alpaydin, *Machine Learning: The New AI,* The MIT Press Essential Knowledge Series (Cambridge, MA: MIT Press, 2016), 55–84.
36. Harper, "Artificial Intelligence," 34.
37. Alpaydin, *Machine Learning*, 74–76.
38. M. Ani Hsieh et al., "Adaptive Teams of Autonomous Aerial and Ground Robots for Situational Awareness," *Journal of Field Robotics* 24, no. 11–12 (November-December 2007), https://onlinelibrary.wiley.com/.
39. Adams, "Artificial Intelligence."
40. Joi Ito and Jeff Howe, *Whiplash* (New York: Grand Central, 2016), 240.
41. Noel Sharkey, "Guidelines for the Human Control of Weapons Systems," (International Committee for Robot Arms Control, April 2018), https://www.icrac.net/; Nils Melzer, "Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare," European Parliament Think Tank, May 3, 2013, http://www.europarl.europa.eu/; Group of Government Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed To Be Excessively Injurious or To Have Indiscriminate Effects, "Human Machine Touchpoints: The United Kingdom's Perspective on Human Control over Weapon Development and Targeting Cycles," August 8, 2018; and Department of Defense (DOD) Directive, *Autonomy in Weapon Systems* (Washington, DC: DOD, May 8, 2017), http://www.esd.whs.mil/.
42. Bostrom, *Superintelligence*; and Scharre, *Army of None*.
43. Noel Sharkey, "Saying 'No!' to Lethal Autonomous Targeting," *Journal of Military Ethics* 9, no. 4 (December 2010): 378, https://www.tandfonline.com/.
44. Sharkey, "Saying 'No!'," 379.
45. Sharkey, "Saying 'No!'," 379.
46. Sharkey, "Saying 'No!'," 379.
47. Sharkey, "Saying 'No!'," 380.
48. Scharre, *Army of None*, 252–55.
49. Sharkey, "Saying 'No!'," 380.
50. Scharre, *Army of None*, 256–57.
51. Christian Szegedy et al., "Intriguing Properties of Neural Networks," Cornell University, ArXiv: 1312.6199 [Cs], February 19, 2014, http://arxiv.org/.
52. Scharre, *Army of None*, 182.

53. Scharre, *Army of None*, 180–83.
54. Luke Dormehl, *Thinking Machines: The Quest for Artificial Intelligence and Where It's Taking Us Next* (New York: TarcherPerigee, 2017), 95–96.
55. Dormehl, *Thinking Machines*.
56. Philip N. Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018," Computational Propaganda Resesarch Project, University of Oxford, October 2018, 3, https://digitalcommons.unl.edu/.
57. Mike Kaput, "How Facebook Uses Artificial Intelligence and What It Means for Marketers," Marketing Artificial Intelligence Institute, February 7, 2017, https://www.marketingaiinstitute.com/; and Bernard Marr, "The Amazing Ways Google Uses Deep Learning AI," *Forbes*, August 8, 2017, https://www.forbes.com/.
58. Melzer, "Human Rights Implications," 40–41.
59. Melzer, "Human Rights Implications," 40.
60. Scharre, Army of None, 137–43, 169–70.
61. Sharkey, "Saying 'No!'," 381.
62. Sharkey, "Human Control."
63. Sharkey, "Human Control."
64. Sharkey, "Human Control."
65. Sharkey, "Human Control," 3.
66. Scharre, *Army of None*, 261.

Aerial Composite Employment Wings in Joint All-Domain Operations

Capt Kyle Rasmussen, USAF

Since the Gulf War, the United States has seen itself as the world's sole superpower—militarily, economically, and diplomatically. Political pressures at home and the Global War on Terror, however, have stagnated the development and training of the US military to execute major contested operations. During this time, the People's Republic of China (PRC) has used the military atrophy of the US to its advantage, developing massive arsenals of anti-access/area-denial (A2/AD) weapons comprised of advanced surface-to-air missiles and surface-to-surface missiles.

Additionally, the People's Liberation Army (PLA) has achieved major milestones in cyber warfare, antisatellite capabilities, and nuclear delivery platforms that present significant challenges to the United States on the high seas, in the air, in space, and in cyberspace.[1] These advancements pose existential dangers to the current paradigm that the US Air Force uses to fight. The current system consists of air operation centers (AOCs) that provide air tasking orders and higher-echelon intelligence down to air expeditionary wings (AEWs). These wings are comprised of squadrons not normally stationed together, and they do not make major operational military decisions but rely on air tasking orders from the AOCs. This system is heavily reliant upon a center of command that requires uncontested dominance in communication, space, and cyberspace while giving AEWs little operational and command autonomy.

The United States is not historically unfamiliar with conflict in the Indo-Pacific theater, but the geography of the region requires a strong logistics and communication network to sustain modern combat operations. The capabilities of the PLA in a 2030 scenario present a massive threat to the current US logistical and command and control (C2) paradigm. This paradigm is best exemplified in a potential military conflict in the Formosa Straits in a clash between the United States and China over the independence of Taiwan (Republic of China), an American partner.

The distance between Taiwan and the United States is more than 5,600 miles, while the distance between the PRC and Taiwan is a mere 100 miles. In between Taiwan and the United States lies the world's largest ocean with a smattering of

small atolls and islands, requiring a strong naval and air presence to create interior lines.[2] The Chinese have no need for vast, long-distance naval and aerial logistical capabilities as they would be fighting on their "home turf." They have leveraged what was historically considered a geographic advantage to the United States—isolation—and turned it on its head.

By creating an arsenal of newly developed A2/AD weapons, China could deny any external logistical resupply required for sustained US military operations and even isolate combat forces themselves. Combined with rapid advancements in cyber, electronic-magnetic spectrum, and space warfare, the Chinese could likely interrupt or destroy any traditional, long-range communication ability from war-fighting units to higher commands. All these factors render the current combat construct of AOC-to-AEW organization in the Air Force obsolete and incapable of fighting a war in the Indo-Pacific theater as well as anywhere else the US faces an advanced adversary across an ocean. Thus the Air Force requires, in addition to technological advances, a new organizational model to win in the Indo-Pacific and around the world—a model that can operate in isolation and independently, both logistically and with regard to C2, for short to intermediate periods of time.

The Solution

As argued in "JADC2 in Distributed Operations," the solution to the aforementioned problem resides in organization at the wing level.[3] Wing commanders must be enabled to make decisions isolated from the AOC. This capability requires self-sufficient staff programs to develop, target, and prosecute objectives at the wing level that interpret the Joint Forces air component commander's intent for days at a time rather than rely solely on orders from the AOC.[4]

Where this article will direct its focus, however, is in the actual renovation of the wing construct. Such an organizational overhaul cannot be implemented overnight and carries significant financial, political, and organizational implications. The Air Force must create standalone wings that are organic AEWs—self-contained and able to execute full missions independently. These wings can no longer afford to be separated by mission type or singular platform—fighter, bomber, cyber, airlift, and so forth—for their purpose will be to execute the missions independently across Joint all-domain operations (JADO).

These standalone wings would be comprised of multiple squadrons of each type—fighters, bombers, tankers, electronic warfare, cyber operations, and any other capability needed to win indigenously. This new reorganization would harken to the legacy of composite wings in the Air Force but would facilitate the new doctrine of Agile Combat Employment, and as such, this article proposes these independent wings be called aerial composite employment wings (ACE) Wings.

A crucial element of success in JADO is integration—the ability to work in concert across all the domains, maximizing the effects of each platform and mission to achieve the desired effects.[5] Integration success requires two elements: the interaction of parties and practice.

The Air Force is comprised of lethal professionals who train to be excellent at their tradecraft, but currently, most war fighters operate in a vacuum day-to-day. Fighter pilots typically fly sorties with their similar type of aircraft, cyber officers operate at bases with no kinetic or tactical aircraft, and tankers often fulfill taskings with no regard to a bigger mission or identity with the airframes they refuel. These interactions happen daily at only one base in the US—Nellis Air Force Base (AFB), Nevada, at the weapons instructor course. Additionally, Nellis AFB hosts the infamous Red Flag large force exercise (LFE), which occurs three times a year and lasts for two to three weeks. Eielson AFB, Alaska, also hosts a similar Red Flag-style LFE for a few occurrences during the year.

These exercises include select units and result in each combat air force (CAF) squadron, on average, attending one such LFE once a year. Thus, most CAF war fighters may only spend two to three weeks truly interacting with different platforms and understanding their counterparts' capabilities, tactical concerns, and the difficulty and/or necessity of successful integration to modern war fighting. This paradigm presents a massive problem in a modern war where integration is crucial to victory. It places a few weapons instructor course graduates (one or two per squadron) as subject matter experts in integration and gives the remaining officers, potentially, only three or four sorties annually focused on integration.

Aerial composite employment wings would put integration at the core of a unit's identity. It would enable daily LFEs as a part of routine training, and each sortie would facilitate face-to-face interactions and foster professional relationships, invaluable to the Air Force and military as a whole. The integration would enable the tactical development of integration to begin as a grassroots movement from multiple bases, instead of solely at Nellis AFB.

These wings would create environments ripe for innovation, and their quantity would force any foreign intelligence agency to monitor multiple locations simultaneously to collect on American tactical development, making effective collection very difficult. Wing agencies would train to create and perfect the intelligence and air, space, and information operations functions required of a wing isolated from the AOC in a distributed JADO-contested fight.[6] Wing commander intelligence requirements would inherently focus on multidomain problems and associated solutions. Wing commanders would be given constant practice at leading and managing different platforms and warfare across all domains.

In addition to the clear benefits of integration in these composite wings, there are also intangible second- and third-order positive effects. The most beneficial of these would be esprit de corps: a wing's identity would no longer rely, solely, on one part of the mission, but rather the whole. This identity would produce air-minded officers and Airmen across every Air Force specialty code who understand their role and importance in JADO by witnessing integration on a regular basis.

Current AEWs are a collective of various squadrons and platforms assembled from bases across the nation that require months of external major command and combatant command planning. Commanders are typically operators from one of the platforms in the AEW but not typically from a base where one of the expeditionary squadrons originated. This situation leaves the AEW with no real attachment or rapport with their commander and little experience for the wing commander leading various platforms incorporated into the wing until actual deployment.

The logistical capability is all external; a combat air force AEW has no indigenous airlift or tanker assets. To get any localized logistical support, a unit within the AEW must go all the way up to the AOC or interact through a major command or combatant command, a process opposite of being decentralized. To fulfill taskings in the Pacific or any other theater where the adversary possesses long-range strike ordnance, tankers will be required. Currently, without contact to the AOC, any combat air force AEW cannot requisition tankers.

An ACE wing would be completely self-sufficient for short-to-intermediate periods of time. Wing commanders would be able to use their composite capabilities to their advantage should external logistical and communication lines be cut off. Using the last known standing orders and Joint Force commander's intent regarding a geographic area, ACE wings could operate like a submarine in the Pacific in World War II, pursuing the enemy and achieving objectives with autonomy and little support for days to weeks on end. This capability would be practiced and refined so that the loss of communication with higher command would almost be a negligible factor, countering the enemy's capabilities.

Wing commanders would have the ability to approve the use of indigenous logistical assets such as a squadron of KC-135s assigned to the ACE wing to achieve mission success without ever having to request authority from high command. In addition to these tactical and operational advantages, these ACE wings would be an ideal strategic tool as deployable quick-reaction forces for use by the national command authority to handle rapidly developing situations.[7] These units could be deployed with minimal external support to prepositioned forward arming and refueling points or forward operating bases.[8] These wings would be the Air Force's answer to units such as Naval fleets, Marine expeditionary units, or

Army combat brigade teams—cohesive units able to respond and deploy as one team to achieve JADO effects.

The Challenges

While the ACE wing concept is filled with inherent advantages, apparent and otherwise, there are arguments that detractors have used to defeat the composite wing concept in the past. The most obvious of these complexities, particularly in an ever-political environment, is the cost. ACE wings will require vast base infrastructure revision and creation, not to mention logistical issues concerning moving units to bases. This is, ultimately, why the last experiment with a composite wing in Mountain Home AFB, Idaho, during the 1990s was disbanded. According to then USAF Chief of Staff General Merrill McPeak, "the reason we haven't done such a thing [formed composite wings] over the years is that we have been afraid of costs. . . . It is expensive, especially if you create intermediate-level maintenance organizations on each base where you have a composite wing so organized."[9]

The cost estimated to create such a composite wing at Moody AFB, Georgia, in 1993, was $34 million, which is approximately $64 million in 2020, accounting for inflation. The estimates vary from base to base. For example, Pope AFB, North Carolina, needed $43.3 million for the composite wing initially, but an additional $45.6 million was required to rebase the C-130s originally residing there. Meanwhile, Mountain Home AFB's composite wing cost estimate was only $26.9 million in 1993 but had no requirement to dislocate groups or wings initially stationed there.[10]

This situation means the average cost for setting up a composite wing, accounting for 2020 inflation, would be about $56.2 million. This estimate assumes not dislocating a platform like the model of Pope AFB, which would increase costs drastically to $160 million. This initial price tag is seemingly costly; however, it must be taken in context. Currently, a single F-35 will cost the US government $81.4 million.[11] A more convincing comparison is the Department of Defense (DOD) fiscal year (FY) 2020 budget, which allocated $622.4 million in LFEs across the entire military for just one year.[12] With that amount of money, the Air Force could create up to 11 ACE wings that would then use normal FY operational and maintenance funding to fly daily LFEs and achieve all the benefits previously described.

Although cost is the most common and the greatest obstacle facing the establishment of ACE wings, logistics and capacity present their own challenges. Nellis AFB and Eielson AFB can perform massive LFEs due to their access to vast training ranges and airspace such as the Nevada Test and Training Range. Nellis

AFB also boasts proximity to the Joint training centers of Fort Irwin, California, and the Navy's test centers in Naval Air Station China Lake, California. This proximity to other bases enables further Joint integration training.

Any base for consideration would need to be in a location that has relatively close access to similar range complexes. The following range areas might suffice: White Sands Missile Range, Barry Goldwater Range, Mountain Home Range Complex, Utah Test and Training Complex, as well as any of the warning areas located off the US coast. These areas limit base locations to coastal areas or the Western desert areas of the United States.

Additionally, a political challenge is selecting bases that do not currently have fighter jets, as residents of major populated areas are known to complain about the noise produced by afterburning jets. This fact further complicates the limited selection, as does the fact that many of the training wings producing America's newest fighter pilots also require significant range access and occupy some of those optimal bases, competing with any unit jockeying for air and ramp space.

These are just the flying concerns, as JADO also requires space and cyber assets be included and integral to these ACE wings. The infrastructure required to create tactical and operational cyber squadrons is likely highly classified and expensive. An additional second-order effect stemming from the logistics challenges of the ACE wing construct is the professional development and cultural ramifications to Airmen and officers. Air expeditionary wing commanders have typically been fighter pilots, and it is not illogical to see that as a potential route of cultural inertia, particularly in the initial years. This trend could give the political appearance of a "glass ceiling" to other career fields or favoritism by the wing commanders for fighter pilots over other Airmen, potentially limiting career opportunities and positions such as school and command.

While this may be a perception, it should be noted that in previous examples of composite force bases such as Seymour Johnson AFB, North Carolina, tanker pilots felt the fighter wing commander "[made] selections without regard to tankers or fighters. He pick[ed] the best person."[13] Success in this department depends on strong and fair leadership to ensure a meritocracy independent of career field, as does the whole of the Air Force.

The Implementation

The challenges presented by the creation of ACE wings must be viewed in the context of the challenge presented by the threat of near-peer adversaries far from the shores of the United States in 2030. Failure to change our paradigm due to cost or to political or cultural challenges presents the very real opportunity to lose a major war in the Pacific or elsewhere, with serious ramifications for the Ameri-

can way of life. The solution needs to be based in reality and balanced with the drawbacks.

One solution would be to create four ACE wings by syphoning funds from LFEs during the course of four years. The ideal location to start could be Mountain Home AFB, Idaho, as it has historical significance being the previous location of composite wing formation, ease of access to the Mountain Home Range Complex, and reasonable distance from Joint partners at Whidbey Island Naval Air Station and the I Corps at Fort Lewis, both in neighboring Washington State.

Ideally, it would be comprised of at least one squadron of each of the following platforms: F-15E, F-35, B-1, KC-135, MQ-9, and C-130. In its operations group, it would contain a cyber operations squadron and an air control squadron fully integrated and working regularly with the operational aviators. The wing would contain a staff structure much like that of an AOC, ultimately being led by a brigadier general as the commander. This concept could be instituted additionally at bases such as Shaw AFB, South Carolina, Tyndall AFB, Florida, and Hill AFB, Utah, among others due to their similar strengths.

To minimize cost, bases should be selected that currently have an airframe that is desired to be integrated within the specific ACE construct to avoid a Pope AFB-style relocation cost. Vicinity to Joint units is also necessary; to be successful in JADO, these wings must be able to train and integrate on a routine basis with naval and land forces. The self-sufficiency of these units enables commanders to interact directly with their local service counterparts to create Joint training exercises and build strong relationships across the different services.

Conclusion

Modern warfare against a near-peer adversary such as China will require integration and decentralization. The ACE wing model presents a possible solution to the organizational challenges posed as the US military prepares for a possible conflict requiring JADO in 2030. The proposal maximizes deployment ability, training, integration, and autonomy. It is not without drawbacks; cost and logistics are a major factor in the challenges and opposition such a concept would face. But the existential threat the country may face in the future requires monetary and organizational investment, and the cost to build four ACE wings varies from potentially less than the price of four F-35s to as much as the DOD spends on LFEs across the force in a single year.

This initial investment is worth the benefits. The ACE wing model would foster tactical and operational innovation from the squadron up across multiple nodes by having daily exercises equivalent to major, semiannual LFEs across all

domains. These wings would create and foster relationships across career fields in all domains, engendering awareness of counterparts' strengths, concerns, and weaknesses. Additionally, this construct would create effective commanders able to deploy their units and operate on a moment's notice with the capability and experience to lead in JADO. Notably, in the history of airpower, there is not a single example of a composite wing that was unable to meet its mission objectives or operate below the standard expected of it.[14] This reorganization would put the war-fighting capability directly back into the hands of those who have innovated and won throughout the history of American airpower—the squadrons, groups, and wings.

Capt Kyle Rasmussen, USAF

Captain Rasmussen is a flight commander in the 510th Fighter Squadron, 31st Fighter Wing, US Air Forces in Europe, Aviano Air Base, Italy. He is an F-16 instructor pilot who has flown combat sorties in Operation Inherent Resolve and served as the "Wild Weasel" liaison officer to the Combined Air Operations Center, Air Forces Central Command.

Notes

1. Miranda Priebe et al., *Distributed Operations in a Contested Environment*, RR2959 (Santa Monica, CA: RAND Corporation, 2019), 9, https://www.rand.org/.
2. David Brunnstrom, "U.S. Warns China against Taiwan Attack, Stresses U.S. 'Ambiguity,'" Reuters, October 8, 2020, https://www.reuters.com/.
3. Capt Kyle Fitle, *JADC2 in Distributed Operations*, August 6, 2020, 2, https://apps.dtic.mil/.
4. Fitle, *JADC2*, 2.
5. Priebe et al., *Distributed Operations*, 47.
6. Fitle, *JADC2*, 2.
7. Maj James E. Moschgat, *The Composite Wing: Back to the Future!* (Maxwell AFB, AL: School of Advanced Airpower Studies, May 12, 1992), 75, https://apps.dtic.mil/.
8. Priebe et al., *Distributed Operations*, 7.
9. Tyler Rogoway, "Remembering When The 366th Wing Was An Experimental Rapid Response 'Air Force In A Box,'" Warzone (blog), July 27, 2018, https://www.thedrive.com/.
10. US General Accounting Office (GAO), GAO/NSIAD-93-183R, *Cost of Composite Wing* (Washington, DC: GAO, May 13, 1993), 1.
11. Mike Stone, "Pentagon Announces F-35 Jet Prices for Next Three Years," Reuters, October 29, 2019, https://www.reuters.com/.
12. Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2020 Budget Request* (Washington, DC: DOD, March 2019), 3-12.
13. Moschgat, "The Composite Wing," 71.
14. Moschgat, "The Composite Wing," 68.

Optimizing Joint All-Domain C2 in the Indo-Pacific

Capt Stefan Morell, USAF

In a discussion in early 2018 about the new national defense strategy, then Secretary of Defense James N. Mattis emphasized, "[the military] cannot expect success fighting tomorrow's conflicts with yesterday's weapons or equipment."[1] This statement is especially true regarding the current command and control (C2) structure supporting low-observable (LO) strike assets. Considering the most widely employed C2 tactical datalink (Link 16) was initially created in 1975, the "iron triad" C2 platforms averaged only 60–66 percent mission-capable rates in fiscal year 2018,[2] and with the development of advanced adversary weapons such as the CH-AA-10 and CH-AA-X-12, airborne C2 assets are being pushed farther and farther from the fight.

Today's Joint C2 assets and infrastructure would be hard-pressed to help LO strike assets win yesterday's fight against a modernized Indo-Pacific peer threat. Using an analysis of the limitations of the current centralized control C2 structure and doctrine in a peer-level fight and an application of the Agile Combat Employment (ACE) fundamentals to Joint C2, this article argues that to support LO strike assets against threat nations with anti-access and area-denial weapons in the Indo-Pacific, Joint C2 must be restructured to enable distributed, decentralized control. It then outlines requirements for the next-generation tactical datalink to support this decentralized C2 of low-observable strike assets.

Assumptions

This article assumes the reader has past exposure to Indo-Pacific threat capabilities. It also assumes the reader has knowledge of current Joint C2 technology and understands the information flow from a Joint/combined air operations center (AOC) to an airborne asset. This article defines an LO strike asset as a part of a generic Joint strike package comprised of B-2s, B-21s, next-generation air dominance, F-22s, F-35s, EA-18Gs, and RQ-170s that might be tasked to someday penetrate robust Chinese integrated air defense systems. Finally, this article assumes the reader understands the strengths and weaknesses of the Joint Tactical Information Distribution System utilized by current Joint assets.

Limitations of Centralized Control

Since the failures of decentralized control of airpower during the Battle of Kasserine Pass in World War II, the Joint C2 structure has been modeled on the idea of centralized control of air assets. In a best-case scenario, a single air component commander exercising centralized control could provide the "broad, strategic perspective necessary to balance and prioritize the use of a powerful, highly desired yet limited force."[3] The strengths of this doctrine are evident in the success of Operation Desert Storm and current air campaigns in US Central Command that have permissive air environments.

One key limitation of centralized control, however, is "continuous centralized control from [an] AOC requires assured communication to forward forces and bases."[4] The vast amount of data that the current Joint C2 structure in an uncontested environment can feed to an AOC also can lead to the temptation of senior AOC leadership to remove authorities and initiative from tactical decision-makers. The abuse of centralized control can lead to forward-based tactical decision-makers facing an "inability to act in the face of adversary tactics that may . . . cut off communication with the . . . AOC."[5]

If hostilities were to commence against China in the US Indo-Pacific Command (USINDOPACOM) area of responsibility (AOR), several new threat considerations invalidate assumptions required to execute centralized control of an LO strike package. First, the currently fielded Joint tactical C2 assets typically part of a strike package (E-3, E-8, RC-135, or E-2) would have to be placed much farther from the fight than component commanders saw in previous wars.

With the imminent proliferation of J-20 stealth aircraft and other advanced Chinese fighters carrying CH-AA-X-12 and CH-AA-10 weapons and advanced surface-to-air threats such as the CSA-X-18, airborne Joint C2 assets will likely have to be placed so far from threats that their usefulness in supporting LO assets, and both seeing and relaying the battlespace to an AOC, would be negated. The assumption that the frontline battlespace picture would be available to the AOC, due to the vast geography of the Indo-Pacific and the advances in threat capabilities, is no longer assured. Joint Force air component commanders (JFACCs) are unlikely to have the information necessary in AOCs to successfully conduct centralized control without a newer datalink that would allow frontline assets to share the battlespace picture with the AOC.

Additionally, the infrastructure that centralized control is built on has never faced a nation-state threat that can substantially deny communications. The ability of certain threats to deny, jam, or spoof GPS, datalink, and other communications equipment that the current Joint C2 enterprise uses is beyond the classifica-

tion of this article. But one can imagine that if a combatant commander is unable to see the battlespace picture, to pass mission amends to airborne assets, or to receive the results of a mission in a timely fashion, instead of executing centralized control they will be providing no control.

This author experienced the firsthand effects of degraded communications impacting centralized control in the permissive air environment over Syria in 2017–19. On numerous occasions, this author could not establish both voice and digital communications with the AOC due to Joint C2 equipment degradation and could not pass information or receive data from the AOC such as the commander's intent for a new tactical situation. When, for example, one is flying on a low-illumination night while within the visual range of Russian fighters over Syria, and one is unable to pass mission-critical information to an AOC or receive authorization to execute certain tactics to lower risk, it is an extremely uncomfortable feeling. The Joint C2 enterprise needs a newer, more robust datalink and to be restructured away from the centralized control of air assets.

The final problem in the USINDOPACOM AOR that challenges the doctrine of centralized control is that previous AOCs have never faced a robust anti-access/area-denial (A2/AD) threat that has the credibility to destroy an AOC or other central C2 nodes. Whether China chooses to target an AOC or centralized control node kinetically or nonkinetically, it can significantly disrupt an air campaign if it can isolate assets from their controlling agency. For example, a cyberattack on an AOC that prevents it from passing mission amends could lead to extreme risk to other Joint partners. Imagine an airborne strike package that needs to be retasked to perform defensive counterair against an impending Chinese attack, yet the AOC might be unable to pass the change in mission.

Additionally, if China uses nuclear or conventional standoff weapons against an AOC, the subsequent air campaign could be in jeopardy, as the supported assets reliant on centralized control would have nowhere to turn to for subsequent guidance. The infrastructure supporting centralized control clearly is not safe in this AOR.

Benefits of Decentralized C2

Considering the limitations of centralized control in the Indo-Pacific region, C2 in a Joint air campaign will need to embrace the speed and lethality of maneuver warfare to help LO strike assets achieve objectives. This doctrine of maneuver warfare "seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope."[6] The service that best embraces maneuver warfare in their C2 philosophy is the US Marine Corps, which is fitting con-

sidering their relevant history of island-hopping campaigns in World War II in the same region. Marine Corps doctrine further emphasizes, "to best cope with the uncertainty, disorder, and fluidity of combat, C2 must be decentralized."[7]

The importance of maneuver warfare is also emphasized in the *Summary of the 2018 United States National Defense Strategy*: that asserts we need to be "strategically predictable, but operationally unpredictable" to "frustrate [the enemy's] efforts."[8] Applied to Joint C2 in the USINDOPACOM AOR, this strategy means C2 should be structured to support a rapid operations tempo that allows for assets to execute a mission, land at an austere airfield, refuel and rearm at a forward arming and refueling point, and then launch for a subsequent mission before the enemy completing the kill-chain for their A2/AD weapons on allied airfields. Decentralized control is best suited to support this philosophy, and the doctrine of Agile Combat Employment translates this philosophy into guidance for the Joint C2 structure in the AOR.

Agile Combat Employment "focuses on the ability to disperse, recover, and rapidly resume operations in a contested or austere environment" and asserts "decentralized control and decentralized execution [are] required to enable an effective campaign."[9] Whereas centralized control would have difficultly controlling "thousands of sorties per day . . . at more than one hundred airfields," a Joint C2 structure optimized for decentralized control of the combatant commander's centralized vision could allow for the speed and redundancy required to win in a robust A2/AD environment.[10]

To implement a decentralized control doctrine, the structure of Joint C2 in the USINDOPACOM AOR should be modeled around the concept of a distributed group. A similar concept was effectively utilized in Operation Desert Storm, where the "7440th Composite Wing, operating from Turkey, received only objectives and a target list from the JFACC."[11] The group would contain the minimum number of multiairframe assets necessary to form and support a basic LO strike package (for example, 4–8x F-22s or NGAD, 8–12x F-35s, 2–4x B-21s or B-2s, 2–4x EA-18Gs, 1–2x RQ-170, multiple tanker aircraft, etc.).

Additionally, the group would have the maintenance and logistical assets required to support the assets (such as a forward arming and refueling flight), be distributed to multiple contingency bases or airfields, and be able to conduct the C2 of operations within its sector of influence. All higher structures would support the distributed group administratively, trusting unit-level personnel to plan, control, and execute the combatant commander's intent. A redundancy of communications such as mobile satellite communications, local fiber networks, encrypted radios, other line-of-sight communications, and others would allow flexibility for the group to command and control operations, trusting unit-level

intelligence troops and targeteers to perform duties traditionally performed by AOCs.

The Joint C2 structure would be built on the assumption that communications with distributed wings, AOCs, the JFACC, and the Joint Force commander would be degraded. Supporting organizations would limit C2 communications to deconflicting lines of effort, the reposturing of distributed groups, or sharing data affecting multiple distributed groups. While this concept carries a higher support burden and demands more of unit-level commanders, it offers a fighting structure less "reliant on vulnerable communications," and the "greater distribution reduces [LO strike package] vulnerability to air, missile, or ground attack" from threat A2/AD weapons.[12]

Datalink Requirement

One of the lofty objectives for the new concept of Joint all-domain command and control (JADC2) is creating "all-sensors, all-shooters" connectivity across domains, essentially a "military version of Uber."[13] An extreme example that highlights the best-case application of this concept might include a submarine-launched ballistic missile launched against a target where a Space Force satellite provides the target track, an Army clandestine special operations unit provides the target identification, nearby Air Force and Marine Corps fighter assets provide sensor data to the weapon regarding current enemy integrated air defense system activity in order to increase weapon survivability, and the AOC is thousands of miles away seeing the sensor and shooter data near real time.

This capability is an extremely challenging goal that "will require significant resources and institutional effort, including senior leader attention and interventions."[14] To be sure, in achieving such commonality across all domains, there is significant potential that tradeoffs and compromises to achieve commonality would decrease technical functionality and lethality for frontline assets.

To best suit the war fighter, the "all-sensors, all-shooters" philosophy means the data link should be engineered around supporting frontline Joint assets and the distributed groups as the primary customers, not the AOC.

To support Joint C2 of an LO strike package, signature management and emissions control are of paramount importance to these assets for survival. Thus, sacrifices for low probability of intercept (LPI) and low probability of exploitation (LPE) must not be made for the sake of commonality. To achieve LPI/LPE, the datalink signal strength must be scalable, must transmit in narrow and specific beams (not omnidirectional), must have robust encryption, and will likely need to be at a much higher frequency than currently employed datalinks to support the rapid transmission and reception of gigabytes of sensory data.

Also, due to different classification levels of sensory data provided by Joint and coalition assets, aspects of the information shared over the data link should be mission-planning programmable and operator selectable. Finally, the tactical datalink should be integrated with sensor fusion software to tag varying confidence levels of sensory data and adjust that sensor's priority within the network. The physics of a network capable of meeting these requirements significantly reduce the effective range and alone are unlikely to meet the "all-domain" philosophy of JADC2.

Thus to facilitate decentralized C2 at the distributed group and keep distributed wings and higher Joint component commanders informed, the datalink would also need several bands and multiple relays to share select data from C2 centers to and from frontline assets. A key aspect would be a redundancy to enable kinetic and nonkinetic network resilience and sustainability. Supporting Joint assets with standoff capabilities would be the best candidates to serve as central network nodes and relays from distributed groups. These candidates might include naval vessels, Patriot batteries, RQ-170's, or other land- or sea-based mobile relay stations. Additionally, LO strike assets able to receive low-fidelity datalink information from satellites and multiple low bands would allow for rear C2 units to pass significant mission changes promptly.

Conclusion

With the right vision and the right leadership, there is significant potential for JADC2 to remedy an antiquated C2 structure containing weaknesses that have not yet been exploited by a capable enemy. Air Force Chief of Staff General Charles Q. Brown Jr. has made JADC2 his number one priority; the time to shape JADC2 to enable future victories against modernized peer threats is now.[15] The right leadership is in place and the momentum for change is strong. Military professionals must continue to advocate for a frontline-focused C2 structure, fighting for JADC2 to embrace maneuver warfare and redundancy in all domains to support the war fighter in a robust A2/AD threat environment.

By modeling JADC2 around the concept of distributed, decentralized control, the Joint Force could sustain operations in the likely scenario of an AOC in the Indo-Pacific region becoming kinetically or nonkinetically disrupted. Additionally, designing the "all-sensors, all-shooters" datalink around the philosophy of decentralized C2 and a war-fighter-first multidomain mentality would exponentially increase the lethality of Joint assets facing a modernized Chinese peer threat. In conclusion, war fighters cannot afford to squander this opportunity and must realize JADC2 development "must be tended to carefully if it is to achieve its objectives."[16]

Capt Stefan Morell, USAF

Captain Morell is the aircrew flight equipment flight commander, 1st Operations Support Squadron, Joint Base (JB) Langley-Eustis, Virginia. He is an F-22 instructor pilot who has flown combat missions in Operation Inherent Resolve and Operation Spartan Shield. Captain Morell previously served as the chief of training for the 27th Fighter Squadron, JB Langley-Eustis.

Notes

1. James N. Mattis, "Remarks on the National Defense Strategy," address, Johns Hopkins School of Advanced International Studies, Washington, DC, January 19, 2018.
2. Myron Hura et al., *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, CA: RAND Corporation, 2000), 108; and Stephen Losey, "Aircraft Mission-Capable Rates Hit New Low in Air Force, Despite Efforts to Improve," *Air Force Times*, July 26, 2019, https://www.airforcetimes.com/.
3. Curtis E. LeMay Center for Doctrine Development and Education (LeMay Center), Air Force Doctrine Publication (AFDP) 1, *The Air Force* (Maxwell AFB, AL: LeMay Center, March 10, 2021), 67, https://www.doctrine.af.mil/.
4. J. P. Clark et al., *Command in Joint All-Domain Operations*, Research Report (Carlisle, PA: US Army War College, July 22, 2020), 14.
5. LeMay Center, AFDP-1, 68.
6. Headquarters, US Marine Corps (USMC), Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations* (Washington, DC: Headquarters, USMC, July 26, 2017), Glossary-21, https://www.marines.mil/.
7. Clark, *Joint All-Domain Operations*, 33.
8. James N. Mattis, *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, January 2018), 7, https://dod.defense.gov/.
9. Maj Gen Brian M. Killough, "The Complicated Combat Future of the U.S. Air Force," *National Interest*, February 9, 2020, https://www.yahoo.com/.
10. Killough, "Complicated Combat Future."
11. Miranda Priebe et al., *Distributed Operations in a Contested Environment*, RR2959 (Santa Monica, CA: RAND Corporation, 2019), 55.
12. Priebe et al., *Distributed Operations*.
13. Clark, *Joint All-Domain Operations*, 38.
14. Clark, *Joint All-Domain Operations*, 38.
15. Amy McCullough, "The Next CSAF Lays Out Top Priorities," *Air Force Magazine*, June 1, 2020, https://www.airforcemag.com/article/the-next-csaf-lays-out-top-priorities/.
16. Clark, *Joint All-Domain Operations*, 38.

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