Vol. 28, July 2021

MITCHELL INSTITUTE
Policy Paper

Key Points

Networks and software are essential to success in modern warfare, and they must rapidly adapt and reconfigure to provide a combat advantage.

Air Force networks are rigid, and software development paradigms take too long to be operationally effective.

The bureaucratic systems that govern how these capabilities are funded and managed are outdated, and they slow down the Air Force's ability to adapt in the battlespace.

The Air Force does not have the right manning, skillsets, and software tools to reconfigure networks and adapt software at a pace that can meet real-time mission demands.

The Air Force should normalize the development, acquisition, management, and modernization of mission integration software tools and fund each as its own program of record.

With mission integration software tools, specially trained officers at the unit level can reprogram software and operational network architectures at the time of need to outpace the adversary.

Speed is Life: Accelerating the Air Force's Ability to Adapt and Win

By Lt Gen David A. Deptula, USAF (Ret.)
Dean, The Mitchell Institute for Aerospace Studies
Heather Penney
Senior Resident Fellow, The Mitchell Institute for Aerospace Studies

Abstract

Future warfare concepts like Mosaic, joint all domain command and control (JADC2), and the Air Force's advanced battle management system (ABMS) will all rely upon information networks and advanced, software-based integration programs as their operational foundation. Success in tomorrow's conflicts will largely depend on how warfighters are able to harness and adapt everything from mission systems on aircraft to sensor packages, networks, and decision aides To prevail in a dynamic and contested battlespace, warfighters must be able to reprogram and reconfigure their weapon systems, sensors, and networks.

Yet the Air Force continues to develop, update, and manage software and architectures in a highly centralized and stove-piped fashion. Data links are fixed and predictable, and they cannot share information across different networks. The bureaucracy of Department of Defense (DOD) funding categories also prevents software tools from being fielded and employed. As a result, warfighters cannot adapt their weapon systems faster than the changing battlespace. This is a recipe for failure given tomorrow's challenges. To put it bluntly, software and networks shouldn't governed by industrial age processes.

Software tools that adapt and integrate operations across different types of weapon systems, languages, and datalinks and facilitate their coordinated execution are urgently needed—as are airmen trained and skilled in programming them. To address the bureaucratic and funding barriers to these mission integration software tools, the Air Force should create a system program office dedicated to developing these software capabilities, funding these tools independently of traditional weapon systems, and creating specialized funding architectures that can keep pace with software development. Furthermore, the Air Force should train unit-level mission integration officers to employ these tools and build operational architectures.

The old adage, "Speed is life" is no longer just about flying—it's about rapidly evolving mission tools to fight and win.

Introduction

Success in future conflict will largely depend on a military's ability to exploit the potential of information networks, machine-to-machine data sharing and teaming, automation, and machine learning. If used to their full potential, advanced networks, technologies, and algorithms can provide key operational advantages such as rapid adaptation, as well as enable complex multi-domain kill webs and decision optionality. These attributes are necessary to disrupt adversary strategies to defeat U.S. and allied operations.

U.S. forces will need the ability to quickly field new capabilities, modiy existing weapon systems, and change weapon system and network configurations to rapidly adapt platform, network, and operational architectures in ways that diminish or even negate adversary advantages. China and other global adversaries have observed U.S. operations and capabilities for decades in a quest to thoroughly understand U.S. systems and employment concepts. By introducing unknowns into their understanding of our weapon systems, U.S. forces can also erode the speed and quality of their decision making in the heat of an operation.

Complex, multi-domain kill webs brought about by new forms of technology can use this adversary uncertainty to provide U.S. and allied forces with time, initiative, and resiliency in a contested environment. These attributes give commanders critical, war-winning decision optionality: that is, they allow commanders to review and undertake multiple and simultaneous courses of action. Adaptability is what will ultimately allow leaders to compose forces, take action, and complete kill chains in a dynamic and contested battlespace.

As part of this vision, future warfare concepts like Mosaic, joint all domain command and control (JADC2), and the Air Force's advanced battle management system (ABMS) will all rely upon information networks and advanced software-based integration programs as their operational foundation. The Air Force, however, is not positioned to quickly develop, mature, fund, field, operate, and employ these mission integration tools. It is stuck in past models of hardware acquisition, development, and management structures. In other words, outdated Air Force bureaucracy is preventing them from fielding adaptive software tools.

Adaptive software programs that integrate operations across different types of weapon systems, languages, and datalinks and facilitate their coordinated execution are urgently needed—as are airmen trained and skilled in programming them. Airmen should also have the ability to adapt and integrate legacy technologies with current and future capabilities. In other words, unlike common standards or planned architectures, adaptive software tools could enable U.S. capabilities to be both backward and forward compatible. This would enable the Air Force to maximize every element of its force design in future operational concepts. Without this adaptability, U.S. operational architectures will remain fixed and predictable—and, therefore, brittle and vulnerable. To step into the future, the Air Force must ensure its acquisition processes, resources, and manning are appropriately structured to facilitate this kind of rapid mission integration.

Value of Networks to U.S. Operations

Combat operations over the last 25 years have clearly demonstrated the value of datalink technologies, and future operational concepts all rely on networks and datalinks to employ combat power. A significant obstacle the Air Force and joint force face today in realizing future information and operational

architectures is the challenge of integrating the vast array of these systems across the U.S. military. Information architectures are the structures that describe how data is exchanged across these networks to support the tactics and procedures of U.S. and coalition forces. Different datalinks cannot share information with each other without the need for gateway "translation" nodes, and this accommodation often drops key message elements or imposes a latency to the data exchange.

The incompatibility of the many different datalinks and information-based systems embedded in major weapon systems across the services, however, presents a significant barrier to realizing this future of seamless, machine-to-machine data exchanges.[1] Even major modernization efforts may not be able to retrofit interoperability and connectivity. When it comes to datalinks, the radio-specific waveforms and message-types and formats are generally immutable—especially in legacy datalinks. The Air Force's long difficulties in connecting the F-22 Intra-Flight Datalink (IFDL) and the F-35's Multifunction Advanced Datalink (MADL) is a case in point.[2]

To enhance interoperability across different systems, defense leadership is looking to migrate the force toward a common set of standards to improve interoperability. While mandating standard interfaces—the protocols that enable diverse systems to interact—could mitigate some of these incompatibilities, better solutions can be pursued through the fielding of mission integration tools. Mission integration tools are software programs that are platform-agnostic and can connect, direct, and synchronize military operations across different weapon systems and datalinks.

Emerging concepts such as Mosaic Warfare, JADC2, and ABMS offer new ways to leverage U.S. operational strengths and complicate any adversary's strategy of systems destruction. JADC2, ABMS, and Mosaic Warfare are not mutually exclusive; they are complementary approaches moving the Department of Defense (DOD) toward the same general warfighting concept. JADC2 seeks to maintain an advantage through sharing data across platforms and domains to offer commanders targeting options in compressed time cycles.[3] Similarly, the Air Force's ABMS is an ambitious architecture that takes an "internet-of-things" technical approach to achieve high-speed, seamlessly coordinated combat operations.[4] Mosaic Warfare is a force design approach to help field and adapt JADC2 and ABMS as continuously evolving, tailorable, and scalable warfighting concepts. Mosaic seeks to help implement JADC2 with technologies to enable a complex, resilient, and scalable structure of functionality that embraces federated networks, links, and platforms composed at time of need as a means to confound adversary targeting and ensure operational effectiveness. As such, efforts around Mosaic Warfare are developing software-based integration tools that can conduct a wide array of functions needed in these future concepts. Military and policy leaders are converging on this vision of complex system warfare—the challenge is getting there.

Open mission systems and universal or common standards are unlikely to solve integration problems. Once a universal standard is defined, it would take years of modernization to retrofit legacy systems. Even more problematic, in order to allow programs to design to a target, any universal standard would have to be fixed and stable. The static nature of such a standard would render U.S. forces unable to take advantage of or out-pace the adversary with state-of-the-art network and datalink techniques.[5] Common standards are useful design criteria

to ease the integration of different systems, but not when they inhibit the development of newer approaches. Future architectures must be flexible and adaptive enough to be backward-compatible while also facilitating the adopting of future standards. Mission integration tools, because they can act like software "shims," can provide this function as one of many of their suite of capabilities.

In realizing this future solution vector, DARPA is developing mission integration tools (MIT) that can seamlessly connect and direct heterogeneous platforms and datalinks well inside traditional modernization cycles. The capabilities of these tools include, but are not limited to:

- Filling the battlespace with a sufficient density of software-defined radios to serve as communication relays between disparate radios without the brittle bottlenecks posed by traditional gateways.
- Autonomously managing networks in a spectrum-contested environment, dynamically routing and shaping data loads to optimize performance for changing environments, and evolving missions regardless of the underlying heterogeneous network fabric.
- Auto-generating data translation software patches to allow data from disparate systems to be used by shared mission applications, such as fusion and targeting.
- Supporting mission commanders with real-time recommendations regarding potential cross-domain kill webs for emerging targets, helping mission commanders to evaluate potential tradeoffs of re-tasking, and navigating the complexities of cross-domain authorities.
- Coordinating the subsystems on a weapon system autonomously with off-board assets, enabling the synchronization of mission effects in a dynamic battlespace.[6]

Fielding these mission integration tools offers the potential to employ legacy platforms in a more surprising and unpredictable manner, and many of these tools are mature enough to transition to the warfighter today. As newer weapons systems and more advanced technologies become operational, MIT will enable forward and backward interoperability across the force. In other words, mission integration tools can accelerate future operational concepts, even with today's legacy systems. Instead of waiting the decades it could take to fully recapitalize the service's force design, current weapon systems can begin operating in future ways. Beyond fielding new capability, mission integration tools give warfighters the potential to tailor a force capability to immediate mission need when the unexpected happens and war plans break. These tools provide commanders the ultimate hedge, as they do not need to wait on next-generation weapon systems in order to knit platforms together and begin executing future operational concepts. MIT have the potential to revolutionize how current and future force designs employ, and they can build that bridge to transition to the future force.

Despite their obvious value, a major challenge these technologies face is the difficulty in transitioning technology from research to operations. There are three main hurdles. The first is the bureaucratic lag in the acquisition and budgeting process. Whether referring to requirements definition, transitioning to a program of record, or establishing funding beyond initial development, current acquisition and management processes are neither well-suited nor fast enough to on-board these technologies at relevant speeds. Secondly, the Air Force's program management structure is ill-fitted to field and support these technologies. As program-agnostic

software, generally speaking, there is no existing program executive office to champion, manage, and sustain mission integration tools. Finally, the Air Force does not have the organizational structures, skill sets, and manning needed to operationally employ these software tools. Maximizing the combat potential of MIT would require specialists embedded in operational units at all levels of warfare.

U.S., allied, and coalition operations are ever more dependent on networked operations. Understanding how crucial these operational architectures are to modern warfare—and the limitations and vulnerabilities of how these networks are constructed—is key to understanding the full value of mission integration tools.

America's Way of War: Systems-of-Systems Operational Architectures

Rapid adaptation of how America presents its combat forces, conducts command and control, and closes kill chains will require changes to business-as-usual. If the Air Force does not address its barriers to fielding these crucial technologies, it risks never transitioning them to the warfighter. The service already recognizes the unique nature of operational software and is working to adapt software management, development, and sustainment across the enterprise. Institutionalizing mission integration tools across the Air Force can be accomplished by leveraging the momentum of these software maintenance reforms more broadly to encompass funding, organizations, and processes.

The Air Force must consider how to employ these tools at the battlespace edge. The speed of combat will require airmen savvy in combat operations and skilled in how to construct and reconfigure these systems as adversaries seek to collapse these networks and the operations dependent on them. If DOD is to exploit the full advantage of such technologies, it must adapt its policies, processes, and personnel to accelerate the transition, fielding, management, and employment of mission integration tools.

The U.S. military increasingly wields its combat power as a system-of-systems, and these systems do more than just deconfliction and timing. This is implicitly acknowledged in how the Air Force talks about its combat platforms. Although they might be called "fighters," "bombers," and so forth, the Air Force officially refers to its combat platforms as "major weapon systems." Each weapon system, on its own, is an interconnected and interdependent set of sensors, processors, and avionics. As capable as each weapon system is, they share information and collaborate to achieve greater effects than any platform could independently. The broader system is created by the dependencies and interactions between these major weapon systems needed to execute combat operations. These relationships are called an operational architecture.

An operational architecture includes the structure and description of the specific relationships, information flows, datalinks, functions, and weapon systems that comprise the structure of the combat system-of-systems. This structure typically represents a kill chain, an OODA Loop (Observe-Orient-Decide-Act), or another specific mission. A familiar example might be the iconic OV-1 "High-Level Operational Concept Graphic" used in the acquisition process.[7] This graphic describes a mission or scenario as a means to demonstrate how a new or proposed capability fits into the structure of an operational concept and its architecture.[8]

Figure 1, for example, depicts notional datalink connectivity and information flows in a JADC2 operational concept, providing a visual representation of an operational architecture. Here, one can see the various

Figure 1: A Visualization of the JADC2 Vision

Credit: "Joint All-Domain Command and Control (JADC2)," Congressional Research Service.

"nodes" of systems—the satellites, aircraft, ships, and tanks—and the information flows or datalinks that connect them. Given the mission roles and functionality of each node, one can begin to surmise the how the system works together to execute a mission. The satellites along with the MQ-1, E-3, and 5th generation aircraft act as a sensor layer, sharing and cross-cuing with each other and other weapon systems like the C-130 and the B-2. While this graphic does not depict closing the kill chain, picturing how to add that to this operational architecture would not be a stretch.

U.S. operational architectures have become fairly predictable because of how the functional and informational relationships are physically built into each weapon system. When weapon systems are designed, they are engineered to fit into these established architectures. How a weapon system is envisioned to execute its mission and participate as part of the larger system sets its function within and its contribution to the system. These predetermined mission needs define a platform's systems, datalinks, and radios.

For example, original requirements for the F-22 envisioned the aircraft as operating deep in adversary territory. Whereas receiving Link-16 data enhanced F-22 mission performance, maintaining the advantage of stealth meant that the F-22 could not transmit on the datalink. Link-16 is a strong, omni-directional radio, and would act like an early warning siren and homing beacon to adversary forces. But collaboration with other F-22s was important, so the Raptor was designed with a low probability of detection, low probability of intercept (LPD/LPI) intra-flight datalink. These requirements were set nearly three decades ago, and how the F-22 participates in the larger operational architecture has not since changed; the F-22 can still only "talk" to other F-22s.

Modernization upgrades have not substantially altered the F-22's inability to share information. Program offices typically focus their modernization budgets on enhancing traditional combat capability, not communications. Budget pressures force tradeoffs in programs, and communication is not often viewed as a priority when compared to other needs. The Air Force explored adding the F-35's MADL to the F-22 in 2008 as part of

planned Increment 3.2 capabilities, but later removed it due to cost and changing requirements.[9] Instead, F-22 Increments 2, 3.1, 3.2A, and 3.2B focused on advanced air-to-air missiles and air-to-ground attack modes and weapons.[10] Even today, despite tests and experimental demonstrations, the F-22 cannot operationally offboard any of its sensor data to other weapon systems.[11]

The stable nature of U.S. warfighting systems has allowed adversaries to develop strategies to target U.S. operational architectures to negate these advantages. These architectures tend to be rigid and predictable because they are inherent to the mission hardware of weapon systems. Adversaries are familiar with our technologies and our tactics, techniques, procedures, and they intimately understand our way of war. Perhaps most crucially, adversaries understand the relationships and interdependencies between our platforms and are developing the ways and means to counter U.S. operations.

System-of-Systems Denial, Degradation, and Destruction: Defeating U.S. Operational Architectures

China, DOD's "pacing threat," is the nation-state assessed to pose the greatest and most credible threat to America's national security. According to the Military and Security Developments Involving the People's Republic of China 2020 annual report to Congress, "Beijing will seek to develop a military by mid-century that is equal to—or in some cases superior to—the U.S. military."[12] China is aggressively developing their military, and their strategy of systems confrontation and system destruction is specifically designed to counter American operational architectures.[13] While other potential adversaries may not be able to match China's rate of development, they are likely to view China's strategy to deny and defeat U.S. military capabilities as a model to emulate or learn from. At the very least, understanding Chinese strategies can reveal potential vulnerabilities in U.S. operational architectures.

Information superiority is key to China's strategy. Despite aggressive investments in military equipment, Chinese military strategists are acutely aware that the PLA is likely to remain at a disadvantage in terms of military capability against the United States and its allies for some time to come. Unable to compete symmetrically, China's key to seizing the initiative and, therefore, an operational advantage is attacking U.S. operational architectures. China's 2013 edition of the Science of Military Strategy states:

> *Our military force will still face the difficulty of confronting advantageous enemies … One way to reverse that trend is to create conditions which are friendly to us, to seize the war initiative, and to use favorable condition/posture to compensate the inferiority in equipment … control of information is the foundation of seizing initiatives in battle. Without information supremacy, it is difficult to effectively organize fighting for control of air and control of sea.*[14]

Chinese intelligence operations expert Mike Dahm explains the Chinese conception of information superiority as "battlespace awareness and the ability to preserve information for one's own weapon systems while simultaneously denying battlespace information to one's adversary."[15] Kinetic military operations, while important, do not form the foundation of Chinese operational concepts.

China intends to starve U.S. systems of information while maintaining its own battlespace awareness.

In this context, the real strategic purpose of China's air defense systems is to establish information superiority by degrading and destroying opposing systems. In other words, China uses A2/AD systems "to seize the operational initiative and execute offensive operations."[16] To do this, they will employ their ISR network and air defenses to target the U.S. platforms and capabilities that are key to U.S. battlespace awareness and decision making. Advanced air defenses are not simply about denying geography. These A2/AD systems—and other military capabilities—are employed to deny information to U.S. and coalition forces.

China first recognized the fundamental role of information in warfare by studying Operation Desert Storm. Their lessons learned went beyond precision-guided weapons and data processing. Chinese military strategists focused on how the air campaign paralyzed Iraqi military forces by denying information at all operational levels. Whether air defense systems were passively denied information through the stealthy shaping of the F-117 or command nodes disconnected from higher headquarters as a result of broken network lines, information denial made the Iraqi military vulnerable and provided U.S. forces the offensive initiative.

Chinese military documents call this trend "informatization," broadly referring to the "application of information technology to all aspects of military operations."[17] Informatization includes advanced sensors, algorithms, processing, and electronics on weapon systems, as well as, importantly, datalinks. Noted China scholar M. Taylor Fravel observes that China has learned the lessons of American warfare well: "The 'informatization' of weapons makes them more precise and lethal, and, when networked together, enables the unified, simultaneous command of disparate units and forces."[18] Informatization not only makes the employment of individual weapons more effective through precision, it also allows for the composition and execution of a much larger operational system-of-systems. This is why information superiority matters.

The military goal of Chinese operations is to achieve victory through degrading and destroying U.S. information networks and, therefore, operational architectures. RAND analyst Jeffrey Engstrom states, "The PLA has increasingly recognized that war is no longer a contest of annihilation between opposing forces, but rather a clash between opposing operational systems."[19] Electronic warfare and Chinese specialists John Costello and Peter Mattis describe Chinese military force as using "conventional kinetic attempts to destroy critical nodes in an adversary's C4ISR system quality as information operations—a distinction the Chinese military divides as 'hard' and 'soft' kills."[20] The objective of kinetic strikes and other "hard kills" is to collapse U.S. information networks by depriving the system of critical sensors, gateways, and command and control nodes. "Soft kills" attack networks using electronic warfare, jamming, or other cyber operations. Kinetic and non-kinetic attacks work in a synergistic fashion to "paralyze and destroy the enemy's operational system of systems."[21]

Lest one dismiss the threat of systems destruction as uniquely Chinese and therefore improbable, the United States and its allies must anticipate that any adversary in any conflict would also seek to degrade and destroy U.S. information networks. As our military operations become ever-more dependent on networked operations, and these architectures present both

an advantage and a vulnerability. The advantages that combat networks provide are the accelerated initiative of operations while providing resiliency and adaptation through redundant complexity. Increased dependencies on networks, however, poses a potential vulnerability in that the loss of both platforms and networks may cascade through U.S. information architectures and collapse U.S. combat operations.

Any adversary who is successful in disrupting U.S. and coalition information networks will have the opportunity to seize and retain the operational initiative. However, the answer should not be to "harden" American and coalition networks; doing so would not problematize an adversary's targeting calculus, disrupt their decision cycle, or induce confusion and surprise. Whereas hardening certain military assets might make sense, it is neither plausible nor pragmatic to do so for the many dispersed nodes in a kill chain network. Generally speaking, spending more time and resources to kinetically defend current networks does not create a dilemma for those adversaries—it just reinforces on which static targets they should focus to effectively disrupt U.S. information flows.

To achieve the full potential of JADC2, ABMS, and Mosaic Warfare, the DOD and the Air Force should seek to empower the warfighter to rapidly compose federated and tailored operational architectures that are mission-defined, not system-defined. "More kill chains faster" is a good initial goal, but it will not be enough. Unlike today's structures, success in any conflict will require ad hoc information networks, surprising operational architectures, and resiliency through complexity and adaptation. This means that how we acquire, manage, and employ information and operational architectures must change.

Building Today's System-of-Systems: Engineering Weapon Systems and Datalinks

The range of possible operational architectures is defined by three general factors: the physical properties of the links and connectivity, the data and information standards, and the platforms that host the terminals. Physical properties include the frequencies and waveforms a datalink uses. Standards are the rulesets, message formats, and other defined features that dictate data and information discovery, exchange, and management in the network. Finally, and critically, a network is only as rich and broad as its participants. Although datalinks can modernize to increase their capabilities—enhancing encryption, adding free text and imagery, for example—the mutual dependencies between these three characteristics tend not only to reinforce the overall stability of the network but also its predictability and brittleness. Conversely, decoupling these characteristics as much as possible makes managing them more complex to operate, but it also increases its resiliency and the surprise it can impose upon the adversary.

The Link-16 tactical datalink is a useful example because it is perhaps the most prolific military datalink in the U.S. military and across allied and coalition partners. First developed in 1975, Link-16 transmits and receives in the frequency range of 960-1215 MHz (the L Band of UHF) in a line-of-sight, omni-directional manner.[22] Data is encrypted, and because each Link-16 network hops across 51 frequencies 77,000 times a second, it is considered jam-resistant.[23] The hopping pattern defines a net, allowing for multiple networks to use the same 51 frequencies with minimal interference.

Link-16 uses a "time division multiple access" (TDMA) scheme, in which there are 1536 time slots to each cycle—this is why

Figure 2: Graphical Depiction of Link-16

Credit: ViaSat, Link-16 Tactical Datalink Radios.

Link-16 is often graphically depicted as a circle. Each network cycle is built on sets of time slots called "net participation groups" (NPG).

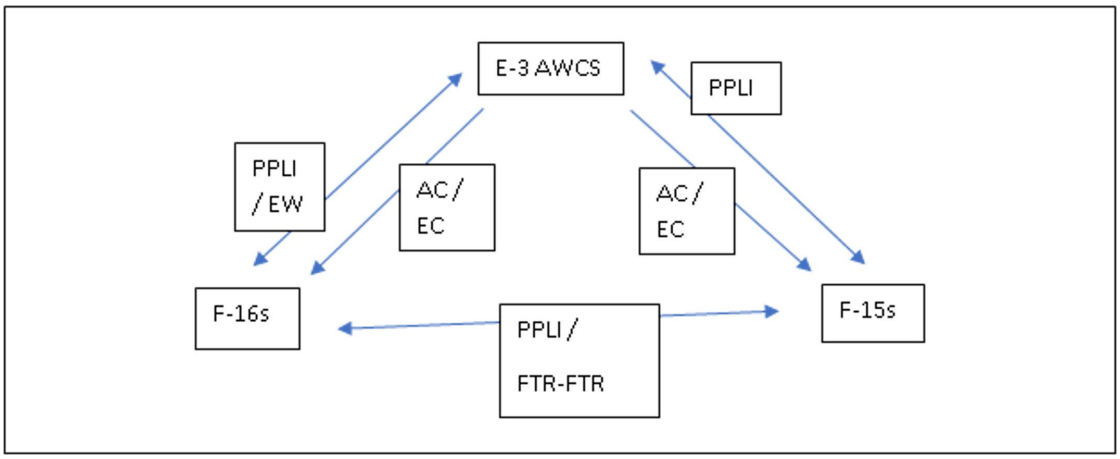
NPGs are organized around mission functions: for example, electronic warfare is NPG 10, fighter-to-fighter is NPG 19, and air control is NPG 9.[24] Message formatting follows Tactical Digital Information Link–Joint (TADIL-J) standards, and the available messages in each NPG are defined by and limited to that NPG's function.

Users are assigned a specific time slot within an NPG to transmit data. They can only transmit during that slot, and must wait for their next time slot to transmit again.[25] Depending on their mission requirements, participants may be members of more than one NPG and therefore have more than one time slot in the cycle.[26] Furthermore, participants could be assigned to an NPG but not be granted transmit status—that is, they would receive only.[27] Finally, each network has net time reference (NTR) that synchronizes everyone for their TDMA window and the net's frequency hopping patterns.

While the above description may sound byzantine, Link-16 relationships, structures, and groups are fairly intuitive. For example, when one considers the mission requirements of an E-3 AWACS, it is clear that it should belong to multiple net participation groups: network management, precise participant location and identification (PPLI), surveillance, mission management, air control, electronic warfare (EW), and engagement coordination. Similarly, an F-16 flight conducting a suppression of enemy air defenses (SEAD) mission would need to participate in PPLI, EW, the fighter-to-fighter net, and would be receive-only on the air control and engagement management NPGs. Because the F-16 flight does not belong to the network management, surveillance, or mission management, it would not transmit or receive any of that message traffic generated by the E-3. An F-15 air superiority mission would similarly be part of the PPLI and fighter-to-fighter net and receive-only on the air control and engagement management NPGs. However, the F-15 would not have any mission requirement

Figure 3: Link-16 Notional Architecture

Credit: Mitchell Institute



to be part of the EW NPG. In this Link-16 architecture, E-3s, F-16s, and F-15s would be able to see each other's PPLI messages; the F-16s and the F-15s would be able to receive the E-3's air control and engagement management messages; the F-16s and E-3s would be able to exchange EW data; and the F-16s and F-15s would be able to share fighter-to-fighter information.

This does not mean that building a Link-16 network architecture is simple or easy. Furthermore, Link-16 is only one of many datalinks in the battlespace. An operational architecture must seek to maximize relevant data exchanges across disparate datalinks, platforms, and domains to be effective. Building this complex system-of-systems does not happen by chance. These networks are not on-demand, as-needed, or opportunity-based. Instead, every datalink in the battlespace is planned, reviewed, and approved—often months in advance—to ensure the interfaces across the many different networks are optimized, gateways are programmed, frequencies are deconflicted, and that the resulting information architecture best supports the joint force commander's desired operational architecture. At the unit level, participants know how to program their datalinks because details of network parameters are assigned through the operational tasking datalink (OPSTASKLINK) section of the air tasking order (ATO). Developing such architectures is difficult and detailed work and requires the dedicated efforts of a highly trained joint interface control officer (JICO).

Builders of the Battlespace: The Joint Interface Control Officer

As datalinks proliferated and became more important to combat operations, the position and specialty of JICO were established to overcome interoperability deficiencies. Link-16 may be the most prolific datalink among U.S. and coalition forces with over 12,000 terminals (and therefore as many potential participants), but other datalinks must be architected, managed, and integrated into operations across domains and joint and coalition forces. These include Link-11, Link-22, MADL, and IFDL, among others. Together, these networks constitute the joint data network (JDN), and that system-of-systems is built by the JICO. JICOs are operational and technical experts who go through a year of extensive training to "manipulate complex link architectures in order to maximize the combat effectiveness of joint and combined forces in dynamic operations."[28]

JICOs work to optimize the joint datalink network to support the operational architecture, but there are limits on what

they can do. An underappreciated challenge they face is how the weapon systems they need to connect can constrain their options to link systems together. Although two different platforms may need to share information, if they do not have compatible datalinks, the key connection is impossible except through a gateway. This is why F-22s and F-35s cannot "talk" to each other. Furthermore, a datalink cannot share just any information from a weapon system. Two different systems might have the same datalink, but if one's data bus has not been configured to share certain information, it cannot be transmitted over the datalink. An F-16CJ and an F-15 might both have Link-16, but if the F-15 has not been programmed to share threat emission data, the F-16CJ has no way of knowing that the F-15 is being targeted. In other words, data exchanged via datalink is a small portion of the relevant information on the platform.

The information available to the datalink is predetermined through the bureaucratic processes of requirements definition and modernization timelines. This requires warfighters to anticipate how the weapon system might integrate into future operational concepts, what other platform or system data needs might be, and how to fund the software upgrades to make that data available to the network. Predictably, this cycle can lag emerging mission needs and often is not representative of the full richness of information available to the pilot or weapon system operator, especially as subsystems are modernized.

Additionally, as previously discussed, weapon system modernization programs prioritize combat capability, which is typically viewed as advanced sensors and weapons. Whatever can increase kinetic or sensor combat effectiveness receives the priority both in terms of funding as well as share of limited processing power in a operational setting. Datalinks have historically been viewed as enhancing communication only—not combat effectiveness or lethality.

More obvious limitations to the joint datalink network are inherent to the very nature of the datalink terminals and antennae. The physical attributes of datalinks, like frequency ranges and waveforms, can be incompatible in part due to their apertures and the firmware elements of the datalink terminal. The frequency that can be emitted and received is directly related to the size of the antenna. Think of the connection between a lock and key—it's a fixed relationship. Antennae and terminals are similar—they only match with a given number of predetermined partners. Older terminals may lack the ability to change if their waveform is hardware-based.

Software-defined radios have not made networks any more adaptive or flexible. Although the software can host more waveforms on a single terminal, the fixed apertures they are connected to physically constrain available frequency ranges. Likewise, the structure and standards of the datalinks they host have remained constant. Link-16, for example, depends on the stable structure of net participation groups, time slots, assignments, and transmissions. Without that fixed structure, any transmission would simply be noise and gibberish. This is why so much attention in the JADC2 effort has been focused on setting common standards. It is the logic, rulesets, and formatting of the datalink and its messages that enable current machine-to-machine data exchange.

But that is outdated thinking. The very stability that makes legacy datalinks functional also makes them predictable and

targetable. Furthermore, they severely limit future capability or even re-assignment of missions and existing capability to different platforms This is what must change. To achieve the resiliency, initiative, and lethality in operational architectures, we must have a way to expand beyond these current standards and structures while maintaining backward compatibility.

The datalinks in service today are likely to remain so for decades to come. It is unreasonable to expect a radical shift away from these valuable networks. But current operational architectures are too predictable due to the nature of datalinks and how platforms are engineered and programmed to participate in the larger system. A major challenge that the DOD and the Air Force face is how to enable the rapid adaptation of operational architectures with the datalinks we have in order to create unpredictability and disrupt adversary decision-making. Mission integration tools offer the potential to do just that.

Mission Integration Tools Enable Future Operational Concepts with Today's Force

Mission integration tools are a set of software programs that enable the fast and flexible composition of operational architectures at the time and place of need. In future conflicts where elements of the force may be disconnected, virtual and actual attrition are a reality, and planned architectures are likely to be disrupted, the need to responsively adapt becomes urgent. On the offensive front, rapidly integrating new capabilities and modifying missions of existing systems and units will require them to receive new types of information in new ways. This can encompass everything from identifying and constructing new kill chains during mission execution, programming subsystems on different platforms to autonomously collaborate, or identifying network degradation and rerouting message traffic in real time.

Developing operational architectures today requires months of advance planning. While JICOs can respond to changes in-theater, they are ill-equipped to face the dynamic environment of peer competition. Attrition, dispersion, new capabilities, and novel operational plans are likely to occur at too fast a pace for a JICO to optimize the joint datalink network. They simply do not have the right enablers. Mission integration tools, however, would empower these skilled airmen to integrate previously incompatible systems and networks, create innovative new systems, and ensure the resiliency of U.S. and coalition systems in combat at operationally relevant scales and speeds.

Cross-domain, cross-service mission compositions are already difficult to coordinate in the current 72-hour air tasking mission planning cycle. Creating and executing on ad hoc, cross-service, cross-domain kill chains in real time face even greater hurdles. Two mission integration tools have already demonstrated their ability to transform old paradigms through their performance in ABMS on-ramps. DARPA's Adapting Cross-Domain Kill Webs (ACK) and System-of-Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) were two tools used by the Air Force to create novel kill chains in real time across previously incompatible networks.[29]

ACK is a decision aide that creates and analyzes thousands of potential kill chains across the range of available platforms, systems, and weapons. Optional kill chains are evaluated based on availability, quality of network service, mission authorities, and even against meaningful tradeoffs against the "value" or "cost" of supporting new missions when assets might be pulled off previously planned objectives.[30] ACK then

offers prioritized solutions as options for a mission commander to select and execute. Furthermore, ACK enables the collection of crucial intelligence, surveillance, and reconnaissance from non-traditional and tangential (not dedicated) assets.[31] In future combat environments, where the adversary will deliberately seek to blind U.S. command and control, non-traditional and under-utilized sensors may prove critical to maintaining decision cycles and operational tempos.

STITCHES is a mission composition suite that expands and facilitates the novel integration of diverse and traditionally incompatible systems and subsystems. A major limitation in the current force paradigm is the fixed connectivity and functionality of systems. Like the previous Link-16 example, only platforms using the same datalink can exchange fixed messages, and available datalinks are determined by the platform type. STITCHES facilitates message translation across different systems without changing message formatting or losing data. The STITCHES toolchain does not require a universal standard. Instead, it uses a library of prior translations and a technician-usable software tool to auto-generate software patches. These patches enable data exchange between existing systems and functions that use different languages and coding. It is software that writes translation software.[32]

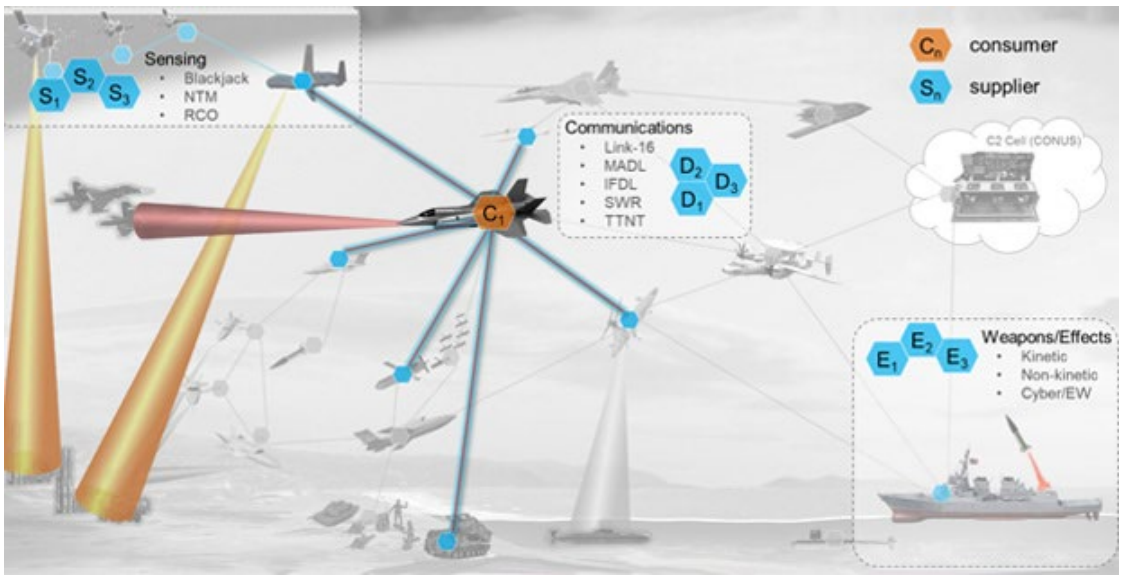
The bespoke software patches generated by the STITCHES toolchain are lightweight code that can be inserted in-line with other types of code with indiscernible latency to create functionality within existing systems. It also does this without disrupting the original programming or operational flight program. In this way, the toolchain presents the opportunity to expand the number of participants in the operational architecture because it does not treat a weapon system as a single entity. STITCHES coding can virtually disaggregate a weapon system into its subsystems; it can make data from any subsystem, from a radar warning receiver to a targeting pod, a participant. These subsystems can then be programmed to collaborate autonomously. For example, the location data from one platform could be used to automatically cue another platform to share threat data or execute threat jamming. In this example, STITCHES facilitates operational collaboration at the component level. Simply put, the suite of STITCHES capabilities enables different systems with different languages and software to understand each other and to dynamically work together at a machine-to-machine level.[33]

ABMS on-ramp 2 employed both ACK and STITCHES to provide the mission commander decision superiority by rapidly providing novel cross-domain solutions to counter threats to the U.S. homeland. While the four-day exercise tested many ABMS technologies, ACK and STITCHES specifically were key to successfully conducting the air defense scenario of "shooting down a cruise missile surrogate with a hypervelocity weapon."[34]

According to program manager Lt Col Dan Javorsek, "The ACK decision aid software analyzed thousands of options to form cross-domain kill webs and recommended the assets for the kill chain and the best command-and-control 'play' to the mission commander."[35] Surveying all of the available capabilities in the battlespace, ACK was able to use non-traditional assets to build a resilient operating picture and provide the mission commander prioritized kill chain options. These courses of action took into consideration cross-service authorities and the interdependencies of how each of the suggested kill chains

Figure 4: Depiction of ACK cross-domain kill webs

Credit: DARPA illustration



might impact other and ongoing missions. Understanding near-term and downstream consequences on operations is critical to superior decision making. Some of the thorniest problems in the JADC2 concept include navigating across organizational and command boundaries and understanding operational tradeoffs. ACK includes these factors in its kill chain construction and makes them visible for the mission commander's decision process.

The STITCHES toolchain was key to enabling the machine-to-machine data exchanges that made such battlespace awareness and kill chain options possible. By providing extremely low latency high throughput machine-to-machine data exchanges across previously incompatible platforms and sub-systems, STITCHES was essential to the functionality of ACK.[36] Gen Mark Kelly, commander of Air Combat Command, said that one of the key takeaways from of the ABMS demo was the need for speed and connectivity, "which really comes down to decision superiority."[37]

DARPA further demonstrated the capabilities of its mission integration suite through a field test of the DyNAMO (Dynamic Network Adaptation for Mission Optimization) tool. This test, conducted by the Air Force Research Laboratory (AFRL), used DyNAMO to share information across disparate and incompatible tactical datalinks in a spectrum-contested environment. DyNAMO automatically routes data to the user who needs it at that moment in a mission. It also manages the flow and prioritization of data, so that lower-priority data does not create a traffic jam for higher-priority data. This is especially important when there is a large variation in performance of the underlying datalinks or links are jammed.

Datalinks in the AFRL test included Link-16, Tactical Targeting Network Technology (TTNT), Common Datalink (CDL), and Wi-Fi networks. To simulate a contested environment, engineers disabled the TTNT network while data was being transmitted. DyNAMO automatically detected the degradation and autonomously transferred the messages to Link-16. Users at each node were unable to detect any operational impact. The DyNAMO program manager shared the warfighter's perspective that "from a user's point of view, they don't care if the data is coming to them from LINK 16 or TTNT or CDL; all they care about is whether they can send and receive a message."[38]

It is important to note that while these software mission integration tools are automated programs that provide machine-to-machine data exchange and processing speeds, they still require skilled individuals to operate the toolkits, configure the software, and install the code. This is distinctly different than what Air Force software detachments such as Kessel Run are doing, as those directly support very specific programs of record. Instead, skilled airmen would use these mission integration toolkits to plan, configure, and compose tailored-to-need mission packages that work across different weapon systems and networks; implement different command priorities; negotiate organizational boundaries; build novel kill chains; and create innovative cross-platform functionality. Software does what it is programmed or trained to do. Having airmen skilled in the operational art of war and who understand systems, software, and code will be crucial to creating unpredictable architectures and functionality at the unit level.

The ABMS on-ramp and DyNAMO demos provide a small insight into the potential of how these mission integration tools can enable the construction of surprising and optimized operational architectures engineered to create the desired effects in any given scenario. Creating the ability of aircraft subsystems to autonomously communicate, collaborate, and synchronize actions through adaptive networks and across different and unrelated weapon systems is a crucial step toward creating the operational architectures that future warfare will demand. As just three tools of a much larger mission integration suite, ACK, STITCHES, and DyNAMO provide powerful demonstrations of the potential these mission integration tools present. Employed creatively, they have the ability to break the current force out of the predictable architectures vulnerable to China's system-of-systems warfare strategy. The application of these mission integration tools to today's force structure can transform how they integrate, collaborate, and operate—but only if the Air Force changes its acquisition approach to developing, procuring, fielding, managing, and sustaining these unique capabilities.

Interoperability and Integration Does Not Require Commonality—The Value of Diversity

Under current network paradigms, the only way to enable ubiquitous connectivity and interoperability across the force is through common standards, waveforms, message formats, and architectures. With each service pursuing its own architecture and interoperability programs, a true "convergence" is highly unlikely and may not even be optimal. Instead, mission integration tools can enable diverse standards and networks to share information across the joint force in a federated manner, enabling constantly changing and adapting information and operational architectures.

What is lost in many discussions of JADC2 or ABMS is that it is not necessary for the services to arrive at commonality. In fact, diversity of standards, networks, waveforms, and even architectures may provide significant operational value so long as information can be shared. Whereas mission integration tools make it possible for many different networks, waveforms, messages, and standards to facilitate integrated operations, maintaining this diversity within the network offers numerous operational advantages. Diverse standards enable the rapid fielding of state-of-the-art technologies and facilitate the evolutionary advancement of data exchange. Diverse networks, waveforms, and datalinks provide the force resiliency through redundancy—

when one fails or is attacked, others can still operate. Diverse architectures, both information and operational, give U.S. and coalition forces optionality, optimize service operations, and complicate the adversary's targeting problem. Diversity as a force attribute creates uncertainty for the adversary, especially in a system-of-systems strategy. Diversity, not commonality, should be an objective when considering future information and operational architectures. Mission integration tools can facilitate integration and interoperability across different standards, systems, and structures.

The proliferation of networks over the last twenty years caused the Air Force to develop gateways and gateway platforms to conduct information exchange across these many different datalinks. Common standards and common architectures are helpful, but not necessary, to share data. Aircraft like the Battlefield Airborne Communications Node (BACN) have acted as translators for the joint force, "distribut[ing] imagery, voice and tactical data from disparate elements—enhancing situational awareness communications for joint warfighters operating across space, air, land, and sea."[39] Lt Gen Clinton Hinote, Air Force Deputy Chief of Staff for Strategy, Integration, and Requirements, is pragmatic when it comes to enforcing a single, unitary standard or architecture for JADC2:

> *We're going to be able to see their [other services'] data, they're going to be able to see our data. And as much as we can, we will come up with common standards. But even if we can't come up with common standards, we realize that translators are going to be something that will be with us for a long time, and we will build the translators necessary to make sure we can share.*[40]

Common standards may make data exchange easier, but committing to a single or a set of common standards has several drawbacks. For one, standards evolve. If the entire joint force were to adopt a single, common standard, they would essentially be locking their data in the past. Long modernization and budget cycles, coupled with the sheer size of the DOD, mean that it takes years to synchronize the entire force to a single configuration. Continuous, periodic upgrades to more advanced standards would only induce configuration chaos. Given the many thousands of DOD systems ranging from major weapon systems, pods, jammers, and sensors, it might not be possible to update all systems before a new, updated standard was required. To reap any benefit, DOD would have to maintain standard stability well past its relevance. But some legacy systems might not even be capable of updating to more modern standards. Backward compatibility will still require managing and integrating multiple standards.

The mission integration tool STITCHES provides an alternative to a common standard. Instead of forcing every system to a single or a set of common standards, STITCHES enables interoperability across different platforms and standards. This allows more capable standards to be fielded opportunistically, with user communities upgrading as relevant and required. As a software-based tool, STITCHES-generated patches can be embedded within systems to provide internal "translation services" across different data standards and without system upgrades.[41] So long as a system is cataloged in the STITCHES library, the STITCHES toolkit can auto-generate a translator to allow the system's data and messaging to be understood and processed by any other system in the library. While

there is a value to commonality, employing STITCHES across the force can facilitate the rapid integration of new standards, new platforms, and new architectures that might be infeasible if a common standard were enforced as the solution of choice.

Just as common standards may not be the best solution for future warfare, a common network, datalink, or architecture is not ideal. Having diversity across the force can provide resiliency to the force through redundancy. Simply put, multiple datalinks in the battlespace provide options when one is lost. Other networks can continue to share information, and, with STITCHES or a gateway like BACN, information can additionally be shared across heterogeneous networks. The challenge that traditional gateway nodes like BACN pose is that they present lucrative targets to an adversary seeking to disrupt U.S. information systems. Suddenly all gateways that have proven exceptional benefits over the last twenty years of permissive operations become prime targets in systems warfare.

The benefit of gateways to diverse networks can still be accomplished without the same kind of vulnerability presented by major gateway nodes like the BACN aircraft. The recent DyNAMO test demonstrated the ability to distribute gateway services across any multi-network platform. During the test, networks integrated Link-16, TTNT, CDL, and several Wi-Fi networks. When TTNT was disabled, participants were still able to seamlessly receive information through alternate datalinks because DyNAMO autonomously reconfigured the radios and re-routed the data. Had this been an operational scenario, combat execution could still have occurred. Traditional gateways simply translate—if a datalink is degraded, the information is simply lost. But as a mission integration tool, DyNAMO was able to detect the health of the TTNT network, recognize the disruption, and re-route the data seamlessly. In systems warfare conflict, the adversary will aggressively attack U.S. networks and degrade the ability to exploit the spectrum. Mission integration tools like DyNAMO can enable diverse and redundant networks to work as desired and provide resilient data exchange to support combat operations.

The significance of these information architectures is that they support the operational architectures; the information architecture is the structure of how data moves to support combat employment and close kill chains. The information and operational architecture should mirror each other. This is one of the challenges of defining an all-encompassing, joint architecture. Traditional systems architecture processes, like what JICOs use, must anticipate all the potential kill chain information exchanges, understand all the organizational and command boundaries and limitations, and then pre-define the systems architecture. This does not happen in real time. It is complex engineering work that can take months to accomplish in a specialized facility with a dedicated team. Pre-defined network/system architectures like this are difficult to change in the heat of battle, and they remain highly predictable through the duration of the conflict. Creating a structure that transcends traditional service boundaries and incorporates all platforms and capabilities would likely be even more complicated and require significant negotiation among service equities to pre-determine certain outcomes.

Traditional information architectures and systems engineering simply cannot construct flexible and novel kill chains on demand. Current examples of cross-domain operational architectures are relatively fixed, like the Navy Integrated Fire Control-

Counter Air (NIFC-CA) architecture. This preconstruction has been necessary to ensure that the network, waveforms, and data are compatible and appropriate and that operational and command considerations have been addressed. Incorporating additional platforms, sensors, and weapons requires additional system engineering. Navy leaders today realize that such predetermined architectures, as capable as they are, are not adaptive enough to provide a combat advantage. Vice Adm Jeffrey Trussler, the Deputy Chief of Naval Operations for Information Warfare, stated that the Navy's Project Overmatch is "trying to link sensors, platforms, shooters, across the service—agnostic of the paths to get there, agnostic to the platforms and source."[42] But with diverse networks, platforms, and standards, the problem may be too complex for a traditional system engineering approach.

Assembling surprising and multi-domain kill chains in real time will require a mission integration tool like Adapting Cross-domain Kill Webs. Humans do not have the ability to identify and evaluate all the potential kill chains for a single target, much less do so at scale and in a dynamic battlespace. ACK can autonomously construct and adjudicate the thousands of potential kill web solutions to identify the best solutions. ACK may not be a tool directly associated with connectivity and interoperability, but its kill chain composition is crucial to identifying the operational architectures that need to be assembled in order to achieve combat outcomes. Together with STITCHES and DyNAMO, these kill chains can be created across different datalinks, and standards, even in a spectrum contested environment. Mission integration tools are not simply about datalinks—they are the connective tissues that span the functionality of combat operations.

These are just three examples of tools from the mission integration suite that DARPA has and continues to develop, and their individual and collective potential to transform the current force toward future operational concepts is clear and urgent. Future warfare will require more than just a common architecture or standard. In a peer conflict where the adversary is aggressively attacking U.S. and coalition information systems, networks, and architectures, cross-domain operations will not provide any advantage if they are predictable and static. Surprise, novelty, and complexity are necessary attributes if U.S. forces are to introduce uncertainty into an adversary's decision calculus. Likewise, real-time adaptation and resilience are necessary architecture attributes if U.S. forces are to operate through an adversary's information warfare operations. Mission integration tools are the key to enabling these kinds of architectures, and it will take the ingenuity and creativity of skilled airmen to fully realize the potential of these powerful capabilities. In combination, both will enable legacy and future forces to employ in ways that confound adversaries like China and weaken their ability to understand the battlespace, predict U.S. actions, and meaningfully degrade U.S. and coalition operations.

The Challenge of Funding and Managing Mission Integration Tools

The Air Force procurement system—or the DOD's, for that matter—is not structured to develop, acquire, field, or sustain combat software tools like ACK, STITCHES, DyNAMO, or the many technologies that will comprise the advanced battle management system. The importance of software in mission effectiveness is recognized by the Air Force, but it struggles to procure, sustain, and modernize software in management and bureaucratic systems

that are structured to support hardware.[43] Mission integration software will be the foundation of JADC2, ABMS, and Mosaic warfare, but unless current funding and management structures are changed, the development and fielding of these crucial and cross-cutting, enterprise-wide mission integration capabilities will falter.

The experience of ABMS is illustrative of the problems faced by software and hardware programs that cut across traditional stovepipes, in regards to the funding and management of their development, procurement, and modernization. ABMS does not neatly fit into any established acquisition process, nor does it clearly belong to a single program executive office (PEO). Dr. Will Roper, former Air Force head of acquisition, acknowledged this misfit when he designated the Air Force Rapid Capabilities Office (RCO) to act as the "integrating" program executive office for ABMS: "This will be something new, and something … like ABMS probably needs a new construct for how we manage and execute."[44]

Historically, DOD has relied upon major weapon systems to fund the development, acquisition, and sustainment of integration capabilities. Datalinks such as IFDL, MADL, and others have all relied upon "sponsor" programs for their funding. While attitudes may be changing, a major problem this structure poses is that these integration tools are often ranked as lower in priority that other, more traditional combat capabilities. As a result, these datalinks have often fallen below the cutline when it comes time to make modernization funding decisions.

The F-22 and F-35 are a case in point. IFDL and MADL are platform-unique datalinks that rely solely on the program funding and management of their respective platforms. These highly advanced LPI/LPD datalinks are proprietary datalinks that were specifically designed for each fighter jet. Although the F-22 and F-35 are the only two 5th generation fighters in the Air Force inventory, they cannot share information with each other machine-to-machine because IFDL and MADL are incompatible waveforms. Because the F-35's MADL was developed ten years after IFDL, it uses a different, more modern waveform and message set that is incompatible with the F-22 datalink.[45]

The Air Force has acknowledged the need for these fighters to achieve interoperability. Since 2008, shortly after the F-22 achieved initial operating capability, the Air Force began experimenting with how to share the vast wealth of information that the F-22 gathers with other fighters and key intelligence capabilities.[46] Although the F-22 was planned to upgrade to MADL, the cost of the retrofit lost out to other, more traditional combat modernization priorities.[47] This is the challenge that integration software often faces: when dependent on a sponsor program's modernization funding, capabilities that increase connectivity are often perceived as not directly contributing to mission imperatives and lethality. Today, the F-22 and F-35 fleet still cannot exchange information without the aid of an externally hosted gateway, one which is still in the experimentation and demonstration phase.[48]

GatewayONE, also referred to as the "Airborne Edge Node," is the latest of many efforts to create an IFDL-MADL gateway and is not subject to either the F-22 or F-35 for sponsorship. As part of the Air Force's ABMS family, gatewayONE is now managed by the RCO within the broader ABMS portfolio. ABMS is often described by service officials as a "military internet of things," a suite of technologies

that will form a data network to connect weapon systems, sensors, and command and control nodes across the Department of Air Force and the joint force.[49] This move appears promising. Instead of depending on a sponsor program and competing against other modernization priorities, gatewayONE can now be managed as part of a focused acquisition capability within the ABMS family of systems.[50] This move to a dedicated PEO and funding line will increase the probability that this datalink will be developed, procured, and fielded.

While some mission integration tools such as STITCHES and ACK have participated in ABMS on-ramps, it is not clear whether they will be folded into the ABMS portfolio. Many of these capabilities are ready to transition out of DARPA and are even mature enough to be operationally fielded to the warfighter. Air Force budget documents, however, do not describe these software tools in the ABMS budget documentation.[51] Due to the unique and enterprise nature of mission integration tools, depending on a sponsor weapon system will not be a viable transition path. Still, ABMS may not be quite the right fit. It is crucial that the Air Force look to transition these software tools as their own individual programs of record and designate a program executive office to oversee and manage them.

Even with a dedicated PEO that is able to fund software as its own program of record, funding categories will remain a challenge to software tools and slow down their ability to get to the warfighter. Software programs can go from good idea to a viable product well within the traditional developmental timelines that budget categories reflect. Budget activities (BA) in research, development, test, and evaluation (RDT&E) are intended to describe and restrict the character of work being done on a program. There are seven categories to cover the stages of development, from basic research and advanced technology programs to operational systems development, and these roughly correspond to technology risk levels.[52] These BA categories provide Congress crucial oversight into research and development activities. The presumption is that a new program would linearly sequence through each budget activity per year at its fastest, giving Congress the ability to monitor a program's progress and performance. However, software is often developed faster than traditional programs, and conforming to these timelines risks making these software programs irrelevant or, worse, dysfunctional.

A new eighth BA was approved in 2020 to cover software and digital technology pilot programs. This category is intended to accommodate the speed and activities of software development, procurement, production, and modification.[53] Unfortunately, as a new category, it only covers pilot programs and is not widely applied to all software programs that might be eligible. In FY22, the Air Force submitted three programs under BA 8: the Strategic Mission Planning and Execution System, the Air & Space Operations Center (AOC), and the Defense Enterprise Accounting and Management System (DEAMS).[54]

The disconnect between this new funding category is that despite the speed at which the BA 8 is intended to move, this new category is very limited in its application. Many DARPA and AFRL programs are funded through broad area announcements (BAA), standing requirements defined more by problems than tightly scoped specifications and key performance parameters. This is deliberate, as it increases the creativity and innovation that companies can bring to solutions.[55] BAAs are traditionally used to help the

DOD to understand potential solutions and technical challenges future programs may face. In fact, defense federal acquisition regulation (FAR) 35.016 (a) specifically describes BAAs as applying to "basic and applied research and that part development not related to the development of a specific system or hardware procurement."[56] As a result, DOD legal interpretations threaten to limit BAA funding to RDT&E budget activities 1 through 4: basic research, applied research, advanced technology development, and advanced component development and prototypes. BA 8 would not be eligible to fund BAA activities.[57]

This means that software pilot programs in BA 8 are constrained by the joint capability integration and development system (JCIDS) process. JCIDS is instruction series that directs how the DOD decides what capability gaps exist, what they need to buy to fill those gaps, and what the requirements and program performance metrics will be, and it then provides guidance for how programs progress along their developmental milestones. The JCIDS is a byzantine and bureaucratic process that often takes years to plod through. While that might be appropriate for such massive efforts as the Strategic Mission Planning and Execution System, the AOC, and the DEAMS, the requirement for BA 8 pilot programs to have been processed through JCIDS is clearly a mismatch for smaller, go-fast software programs like mission integration tools.

Software programs like mission integration tools often progress from problem statement to viable product well within the span of a year. Software programs in DARPA or AFRL are still limited by the annual nature of BA 1 through 4 funding. Broadly speaking, these colors of money are still organized to support hardware timelines. Once a program "graduates" past the prototype phase, a program office or fielded organization has to openly recompete the program. For software, where specific coding techniques may constitute the special sauce of the program, recompeting risks source selection that did not participate in the prototyping phases. If the end-user seeks a sole-source award, the process of justification often takes just as long as competition.[58] Despite the potential value of BA 8 to accelerate software development to the warfighter, the potential of this category is extremely limited by legal interpretations of broad area announcement applicability and the JIDCS process.

If the Air Force wants to achieve a more integrated and agile force, software programs are essential to creating the networked operational architectures and adaptive systems that modern warfare will require. Current management and funding paradigms simply do not make sense for mission integration software tools. The future is clear: connectivity and interoperability are a combat advantage; constant adaptation and change unbalance the adversary; unpredictable and surprising operational architectures disrupt adversary tactics and strategies. These management and funding schemas, from software program development to fielding and employment, must be changed to achieve these attributes.

People are Key to Employing the Full Range of Mission Integration at the Battlespace Edge

Skilled and experienced architects—officers knowledgeable in combat operations, systems engineering, and software—are needed at the forward edge of the battlespace to employ mission integration tools. Operational architectures are not simply kill chains, but distributed lethality appears to be the primary, if

not sole, focus of JADC2 and service efforts. Instead, operational architectures should be understood as describing and encompassing all of the information exchanges, interactions, dependencies, and functions in the battlespace. These relationships and structures facilitate all mission sets, not just kinetic attacks, and mission integration tools enable the construction, collaboration, and functionality of these architectures. Trained officers will be needed at the unit level to exploit the power of mission integration tools to optimize and adapt potential operational architectures.

Data exchange and networks are critical to the kind of distributed operations that future warfare will require, and achieving that vision will demand innovative cross-domain and cross-service functionality. The mission integration tools that can facilitate just that do not program themselves. Moreover, it is the element of human creativity that can provide crucial insight, introduce an element of uncertainty, and deliberately impose uncertainty on the adversary in orchestrating the autonomous collaboration of systems. It is one thing to simply share information and another entirely for machines to take action based on the information shared. Putting airmen who have a strong understanding of operational architectures and who have been trained in using mission integration tools can provide a crucial combat advantage to U.S. forces.

There are too few operational examples today that demonstrate this kind of "edge adaptation." Combat adaptation today occurs primarily through platform modernization programs developed at the enterprise level. This is to ensure high-quality work on advanced subsystems, standard configurations, and interoperable systems. The centralization of capability adaptation is not limited to modernization programs; electronic warfare is highly centralized and tightly controlled for similar reasons. Given how important these electronic signals are to modern and future warfare, electronic warfare is an area of competition that can provide insight regarding the pace of adaptation in the battlespace—and demonstrate the essential value that mission integration officers can bring to combat operations. While electronic warfare (EW) systems in the future will most likely rely on cognitive EW techniques, the following operational example is illustrative of why mission integration tools and skilled officers empowered to employ them are needed at the battlespace edge.

The electromagnetic spectrum has become essential to both U.S. and adversary combat capabilities. In response, the Air Force has collected and curated a large library of electronic signatures. These libraries are called mission data files (MDFs). Identifying a threat system through their electronic signals is very much like voice recognition. If one is familiar with another person, they can be identified simply by the sound of their voice. Their voice and tonal inflections indicate their emotional state or intentions, such as when they are angry, excited, sad, or happy. Similarly, every threat system's electronic signatures have unique and specific characteristics, such as frequency, polarization, or pulse repetition frequency, that can be used to identify the threat. And just as a person changes their voice inflections based on circumstance and intention, the signal characteristics of a system change based on the system's operational phase, like search, target, track, guide. All of these details, including those for friendly systems, are located in the MDF library. When electronic signals are detected, they can be matched against the MDF library to positively identify the emitting system.

These electronic characteristics are also used to develop electronic countermeasures. Electronic warfare officers use collected signals to develop and program countermeasures like jamming or deception techniques. When a threat signal and its operational phase are detected and identified through the MDF, the MDF can match specifically programmed countermeasures that have been tested and validated. Unclassified signals—signals that have no match in the MDF—are simply returned as "unknown." Unclassified signals could be insignificant noise from modern life, represent a previously undetected adversary modification to a known system, or be a wholly new development. When an "unknown" is determined to be of interest, a deliberate collection effort is made to record the signals against the new threat. The exploitation of these signals is accomplished at the enterprise level by specialists in the Air Force ISR Agency, now in the 16th Air Force.[59] The Air Force centralizes signals analysis both to protect means and methods and to provide the highest quality analysis and greatest certainty for warfighters. This process can take weeks or months. Until then, any new signal remains "unknown" and without countermeasures. Whether identifying a threat or selecting the appropriate countermeasure technique, keeping these MDFs up to date is crucial for warfighters.

The pace of future warfare will not allow for the time this enterprise process takes. A recent example from an electronic combat officer (ECO) deployed to the Middle East on an E-3 demonstrates why speed matters and how response cycles between the edge and enterprise differ. In this situation, an adversary air defense team had incorrectly assembled their surface-to-air missile system. The system was still functional, but the system's electronic signals were inadvertently changed and no longer matched the theater's MDF. According to the ECO, "because it no longer matched any of the libraries [MDF], no one in theater had the ability to identify this threat—it simply showed up as an 'unknown'."[60] But the E-3 had an older electronic warfare system that provided the ECO organic signals for analysis. Furthermore, he had the ability to reprogram the aircraft MDF library in real time.

The ECO was able to positively identify the threat and correlate it to the signal, allowing him to validate his collected emissions and add the altered threat signal to the E-3 threat library. Because this database was "native" to the E-3 and not part of the larger theater MDF, the E-3 was the only aircraft that could identify this threat, share its location through datalinks, and support combat operations within range of this particular threat. The ECO was able to validate and make these changes over the course of a single mission. This kind of rapid adaptation was only possible because the ECO could reprogram his system at the edge—he did not have to wait on the enterprise. For those who did, it took over a month for their MDF to be updated and disseminated to the rest of the theater.

Adaptation at the unit level entails a different approach to risk. Consider the modifications that the ECO in the above example made to the E-3 electronic warfare system. In this case, his training and intuition got it right—but what if it hadn't? Other concerns might include configuration control and interoperability. In peer conflict, however, the calculus for risk acceptance changes. Consider the risk of business-as-usual when facing adversary war reserve modes—electronic signals that are held in reserve for war. Unlike the above example, which was a result of construction error, war reserve modes are held in secret, employed only in combat to side-step adversary countermeasures and be more

effective than standard modes. These modes are not likely to be in the MDF because they may not have been collected. Without the ability to adapt at the unit level, war reserve modes would leave warfighters in the battlespace exposed for as long as it took the broader enterprise to respond. It is reasonable to conclude that leadership would be willing to accept the risk of edge adaptation.

Empowering adaptation at the edge is not something that can only occur once the shooting starts. The ECO in the E-3, for example, had been trained for this very situation, and partly due to necessity. The electronic warfare system in the E-3 was a legacy system that was not supported like other assets in the theater. Out of necessity, the E-3 electronic warfare community had to curate and update their own MDF library. Because their system was natively managed, they developed specific risk management procedures to address concerns of adequacy, quality, and processing. The ECO described his process for adaptation:

> *I could modify the MDF, but before I ever loaded it on a jet, I always conducted a beta test. We would put power on an E-3, and I would test the database for functionality—made sure it didn't crash the system and that it did what I had programmed it to do. We would then fly the new MDF on only one aircraft, and we had a backup version of the older MDF loaded too. If I got any errors airborne, I could hit reset and just go back to the previous library. That isolated the other E-3's from the change in case there were any issues. Then, once I had validated it in a mission setting, I shared the new MDF with other aircraft. They would conduct additional evaluations—like quality control, using a backup too—and provide feedback. Sure, there was risk, but we had the processes in place to manage that risk. As a result, we were able to adapt faster than any other system.*[61]

This example demonstrates how edge adaptation, by its very structure, can act as a risk mitigation measure. By adapting a single aircraft—not the entire fleet of E-3s—the processes developed limited risk to any changes. Any problems were, by the very structure, confined to a single jet. If the changes had been developed at the enterprise level, however, any problems would be fleet-wide. This is one reason why getting it perfect is so crucial when adaptation is conducted at the enterprise level—the potential consequences are enormous. But that imposes time that future warfighters will not have.

Risk calculations change when combat commences, but that is not the time to learn how to identify, manage, and mitigate those risks. One fighter pilot recalled an emergency release of a new F-16 operational flight program (OFP) as their squadron was deploying to Iraq for the commencement of combat operations in 2003. "This release gave us enhanced combat capability, enabling us to employ the JDAM [Joint Direct Attack Munition], among other improvements. It was an emergency release because it had not gone through all of the required testing and debugging. There were some quirks that weren't quite right, but we adjusted our tactics and procedures to compensate for those issues. Having this software drop and the other advances made us much more combat effective. This was definitely a case where faster was better than perfect."[62] This emergency software was only provided to

one wing of F-16s with a specialized mission. Other units of the same type did not receive or install the change, effectively making the software drop a unit-level modification. Tactics and procedures were developed by the wing to mitigate the known and discovered issues with the emergency release. The pilots were aware of the limitations and trained to employ workarounds. Hostilities have been shown to change the risk calculation of leadership when it comes to accelerating adaptation. This example provides additional insight on how risk can be managed at the edge—but warfighters should not have to wait until conflict begins to develop these competencies.

Developing the skills, knowledge, and risk management strategies to enable effective rapid adaptation at the edge is something that is best done now—not when it is needed. Reflecting on his experience of modifying his weapon system MDF at the unit level, the E-3 ECO stated, "That's a model you're going to need in future combat, because … what losses are we going to take in the meantime, waiting for weeks or months-long 'big Air Force' processes to catch up and be distributed to theater? I would say that our tactics, techniques, and procedures for these kinds of skills and authorities have languished because we haven't been challenged in time like this before."[63] "Big Air Force" simply cannot facilitate adaptation at the speeds that future warfare will demand—speeds that only skilled airmen at the unit-level can achieve when trained and empowered. Winning the adaptation and time competition are what drive the imperative to train mission integration officers and to embed them at all organizational levels that they will be needed, to include the unit level.

STITCHES provides an excellent example of the combat advantage these officers and tools can offer. STITCHES is more than a translation service. It enables technical support users to virtually disaggregate the subsystems of a platform such that those systems can be programmed to autonomously exchange data, collaborate, and synchronize. This means that planners are not limited to treating weapon systems as unitary platforms. Instead, they can exploit the full functionality of a platform's subsystems in an operational architecture. For example, the radar warning system from one aircraft could be programmed to autonomously collaborate with the electronic warfare system of another. Major weapon systems have many sensors, processors, and functions. Yet very little of that information and functionality is available to offboard or collaborate with other systems. Mission integration officers, however, can reach these subsystems to enable such functionality across the operational architecture.

Because of the unique approach of STITCHES architectures, all this can be done without breaking into the aircraft's operational flight program (OFP), or master code. Lt Col Jimmy Jones, the STITCHES program manager, describes it this way: "The future operational architecture you want shares data among any system, not just fully composed weapon systems."[64] Using lightweight software language, these officers can insert in-line code that unlocks the power of collaboration and functionality at the subsystem level. This kind of virtual "deconstruction" increases the number of potential operational architectures, creates tremendous uncertainty for the adversary, and makes adversary efforts to counter U.S. and allied operations ever more difficult—but is only possible through the efforts of mission integration officers.

Mission integration officers will be essential to adapting U.S. and allied systems. They will be responsible for shaping

information and operational architectures at the battlespace edge. These officers will generate mission software, configuration data files, and update network functionalities as part of mission planning to provide warfighters the advantage they need at the pace they need in an ever-changing battlespace. Because of their significant responsibility and potential impact to combat operations, these individuals should be officers, not contractors or enlisted service members.

While empowering this kind of unit-level adaptation may incur some risk, identifying and addressing the means to manage those risks should be done now—not when hostilities start. Placing that mission integration capability and the skilled and trained airmen that employ those tools and manage associated risks at the unit level is the best way to achieve the speed that can win.

Recommendations and Conclusion

Future warfare will rely upon the unprecedented integration of data as the foundation of combat operations. Operational architectures—the way that different weapon systems work together to complete missions and close kill chains—only continue to increase their reliance on shared data and information. Traditionally, the integration of different weapon systems has been limited by fixed interoperability—did these systems share the same datalink and standards? The development of mission integration tools allows these architectures to be less defined by systems engineering (what can work together) to mission engineering (what do we want to work together). In other words, system engineering limits possible force composition based on fixed interoperability. Mission integration tools allow planners and operators to build the operational and functional relationships they want among the platforms they have based on what they want to do.

Mission integration tools; the officers who will employ them; and the tactics, techniques, and procedures they will use cannot be haphazardly developed. With this in mind, the following insights and recommendations should be considered to accelerate change to current Air Force information and operational architectures:

1. **Resolve the disconnect that prevents research agencies like AFRL and DARPA from appropriately using BA 8 to fund software program efforts initiated under broad area announcements.** The defense federal acquisition regulations (DFAR) limit the ability to apply BA 8 funding to software programs that fall under a broad area announcement. This is problematic, because BAAs are important tools that enable the software teams to creatively solve problems in surprising and innovative ways. If software programs funded under BAAs must follow standard budget activity categories, their development will be slowed due to the annual nature of the funding and program transition. Furthermore, legal constraints against sole-sourcing during transition risk the government losing the very team and unique code that made the program successful. If contract and evaluation teams do not fully understand the software, a low-cost technically acceptable alternative proposal may appear attractive, even if the developer did not participate in the early activities. Furthermore, this budget activity must have a seamless transfer with operational commands. Congress, the DOD, and the Air Force must find a way that enables research agencies to use budget activity 8, a category specifically designed to encompass the unique, dynamic, and

spiral nature of software development to fund and transition software programs initiated by a broad area announcement.

2. **Consolidate development, acquisition, management, and modernization of mission integration tools as individual programs of record within a dedicated program office.** The management of mission integration tools should not be scattered across the acquisition enterprise or tacked on to a "sponsor" program's modernization program. Whether these tools are consolidated in the RCO with ABMS or located in the AFLCMC/XA Architectures and Integration System Program Office (SPO), the development, acquisition, management, and modernization of mission integration tools should be individual programs of record deliberately managed by a dedicated SPO. These tools provide operational benefits across weapon systems and aggregating them under a single SPO will enable the PEO to identify the interdependencies, gaps, and opportunities as they come together as a system. Unlike traditional systems-of-systems, where the architectures are fixed and require the simultaneous maturation of every element, each mission integration tool brings standalone value to the force. As such, the development and fielding of one tool should each be their own program of record. Having an SPO dedicated to mission integration tools provides for a natural transition partner for technologies developed by DARPA and service labs, especially as the PEO will be able to see how emerging capabilities enhance the overall system.
3. **Train and resource JICOs as mission integration officers and embed them at all operational levels—especially at the unit level.** Joint integration control officers already understand how to build network architectures in order to achieve operational integration. They often have operational experience and a background in battle management. These are foundational skills necessary to understand how to align information networks to support innovative new operational architectures and kill webs. JICOs are natural candidates to develop into mission integration officers. These skilled airmen, however, cannot remain isolated to air operations centers or network development centers. To truly provide rapid adaptation of weapon systems and architectures, these mission integration officers will need to be assigned to the point of need. This means posting billets on unit manning documents and associated resources, from physical space and computers to funding. These are not temporary assignments, nor do mission integration officers "parachute in" to install software and then depart. Instead, these positions must be permanent personnel at the unit level and funded just as any other officer would be. In combat operations, these officers will need to be with the units they support in order to coordinate with other units and execute integration and adaptation at the battlespace edge. Mission integration officers should be a crucial component of every mission planning, training sortie, and large force employment—including combat.
4. **Experiment with and develop mission integration tactics, techniques, and procedures for training, employment, and risk management.** Employing mission integration tools will not be like building the semi-static datalink networks that have facilitated combat operations for the past twenty years. To fully realize the combat potential of these tools, the Air Force must develop

tactics, techniques, and procedures (TTPs) for their employment in both training and combat. Experimenting with how mission integration tools can enhance operations is essential to developing TTPs for effective employment. These TTPs will serve as the foundation to standardize the use of mission integration tools and be a point of departure for innovation an improvisation of operations and architectures, creating a constant cycle of evolution and a way to identify and accelerate new capabilities as they become available. Furthermore, TTPs can serve to train these officers in how to identify risk and provide techniques for managing and mitigating risk. Across the Air Force, TTPs serve as best practices that have been validated, tested, and provide for a shared standard and body of knowledge for each weapon system community. Mission integration tools should be no different.

Mission integration tools and the officers who will employ them will have an outsized impact on revolutionizing combat operations. At the battlespace edge, they will provide resiliency to combat operations as they adapt operational architectures to adapt to changing circumstances and enable machine-to-machine data exchange and collaboration. As more unmanned and autonomous systems populate the service's inventory, these tools and skills will become even more critical. The Air Force does not need to wait for the future. By beginning to transition already demonstrated mission integration tools; properly supporting their acquisition and funding; developing mission integration officers and embedding them at the point of need; and developing the tactics, techniques, and procedures to employ these tools, the Air Force can begin to migrate its legacy force structure into a future force design. ✪

Endnotes

1 Joseph Trevithick and Tyler Rogoway, "Master Chart Showing US Military Aircraft And Their Data-Links Includes RQ-170 Sentinal," *The War Zone* blog, The Drive, April 24, 2018.
2 Sydney J. Freedberg Jr., "F-35 to F-22: Can We Talk? Finally, The Answer Is Yes," *Breaking Defense*, November 7, 2019.
3 Congressional Research Service (CRS), "Joint All-Domain Command and Control (JADC2)," October 23, 2020, pp. 1–2.
4 Author interview, Randy Walden, March 2, 2021; and Air Force Research Laboratory, "Palletized Munitions weapon system C2 demonstrated during ABMS Onramp #2," September 30, 2020.
5 Author interview, Lt Col Jim Jones, October 17, 2020.
6 "Programs," DARPA Strategic Technologies Office.
7 "DODAF Architecting: OV-1 High Level Operational Concept Graphic," ACQNotes: Defense Acquisition Made Easy.
8 "OV-1: High Level Operational Concept Graphic," DoDAF Architecture Framework Version 2.02.
9 United States Government Accountability Office (GAO), *Tactical Aircraft: F-22A Modernization Program Faces Cost, Technical, and Sustainment Risks* (Washington, DC: GAO, May 2012), p.8; and Brian W. Everstine, "The F-22 and the F-35 Are Struggling to talk to Each Other … And to the Rest of USAF," *Air Force Magazine*, January 29, 2018.
10 GAO, *F-22 Modernization: Cost and Schedule Transparency Is Improved, Further Visibility into Reliability Efforts Is Needed*, Report to the Subcommittee on Tactical Air and Land Forces, Committee on Armed Services, House of Representatives (Washington, DC: GAO, May 2014), p. 4.
11 Oriana Pawlyk, "After Successful Data Transfer Between F-35 and F-22, Air Force Plans New Tests," *Military.com*, January 22, 2020.
12 Office of the Secretary of Defense (OSD), *Military and Security Developments Involving the People's Republic of China 2020*, Report to Congress (Washington, DC: OSD, 2020), p. i.
13 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: The RAND Corporation, 2018).
14 "Academy of Military Sciences Press, Beijing, The Science of Military Strategy 2013," in Mingda Qiu, *China's Science of Military Strategy: Cross-Domain Concepts in the 2013 Edition* (La Jolla, CA: University of California San Diego, September 2015), p. 20.
15 Michael J. Dahm, "Beyond 'Conventional Wisdom': Evaluating the PLA's South China Sea Bases in Operational Context," *War on the Rocks*, March 17, 2020.
16 Dahm, "Beyond 'Conventional Wisdom'."
17 M. Taylor Fravel, *Active Defense: China's Military Strategy Since 1949* (Princeton, NJ: Princeton University Press, 2019), p. 219.
18 Fravel, *Active Defense*, p. 219.
19 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica, CA: RAND Corporation, 2018), pp. 10–11.
20 John Costello and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," in Joe McReynolds, ed., *China's Evolving Military Strategy* (Washington, DC: The Jamestown Foundation, 2017), p. 174.
21 Costello and Mattis "Electronic Warfare and the Renaissance of Chinese Information Operations,"p. 179.
22 Tonex, "Link-16 Tutorial."
23 Richard Bell, "Maximum Supported Hopping Rate Measurements using the Universal Software Radio Peripheral Software Defined Radio," Proceedings of the 6th GNU Radio Conference, 2016.
24 "TADIL J: Introduction to Tactical Digital Information Link J and Quick Reference Guide," HQ TRADOC, Air Land Sea Application Center, June 2000, pp I-2–I-5.
25 "TADIL J," HQ TRADOC, p. I-1.
26 "TADIL J," HQ TRADOC, p., I-3.
27 Author interview, Maj Alex Wallis, November 12, 2020.
28 "TADIL J," HQ TRADOC, p. III-10.
29 DARPA Public Affairs, "Creating Cross-Domain Kill Webs in Real Time: DARPA decision-aid software, integration tool key to recent Advanced Battle Management System demo," *DARPA News*, September 18, 2020.
30 Daniel Javorsek, "Adapting Cross-Domain Kill-Webs (ACK)," DARPA.
31 Author interview, Lee Olyniec, December 9, 2020.
32 Author interview, Dr. Jimmy Jones, November 20, 2020.
33 Jimmy Jones, "System of Systems Integration Technology and Experimentation (SoSITE)."
34 Charles Pope, "Advanced Battle Management System field test brings Joint Force together across all domains during second onramp," U.S. Air Force, September 3, 2020,
35 DARPA PA, "Creating Cross-Domain Kill Webs in Real Time."
36 DARPA PA, "Creating Cross-Domain Kill Webs in Real Time."
37 Mark Kelly quoted in "Commander highlights ACC priorities at AFA roundtable," *Desert Lightning News*, September 19, 2020.
38 Aaron Kofford quoted in Carlo Munoz, "DARPA's DyNAMO connects incompatible datalinks under electronic attack," *Janes*, December 18, 2020.
39 "NGC's BACN Gateway System Surpasses 200,000 Combat Flight Hours," *Aerospace and Defense News*, December 15, 2020,
40 Valerie Insinna and Jen Judson, "The Army and Air Force are finally on the same page with a plan to connect the military. What happens next?" *C4ISRNET*, October 20, 2020.
41 Nichols Martin, "DARPA provides two support tools for advanced battle mgmt. system demo," *ExecutiveGov*, September 21, 2020.
42 Jeffrey Trussler quoted in Paul Mcleary, "Navy Makes Major JADC2 Push, Linking Sensors & Shooters,"

Breaking Defense, November 16, 2020.

43 National Academies of Sciences, Engineering, and Medicine, *Air Force Software Sustainment and Maintenance of Weapons Systems* (Washington, DC: The National Academies Press, 2020), pp. 6–8.

44 Will Roper quoted in Jared Serbu, "Air Force nearly ready to begin rolling out its 'internet of military things'," *Federal News Network*, November 25, 2020.

45 Brian Everstine, "The F-22 and the F-35 Are Struggling to Talk to Each Other … And to the Rest of USAF," *Air Force Magazine*, January 29, 2018.

46 "F-22 Enters the Network–Linking IFDL, TTNT, Link 16," *Defense Update*, May 28, 2008.

47 Paul Szoldra, "F-22s Can't Talk to F-35s, Because of Course They Can't," *Task & Purpose*, April 3, 2018.

48 Joseph Trevithick and Tyler Rogoway, "F-22 and F-35 Datalinks Finally Talk Freely with Each Other Thanks to a U-2 Flying Translator," *The War Zone* blog, The Drive, April 30, 2021.

49 Author interview, Randy Walden, March 2, 2021.

50 U.S. Air Force, *Department of Defense Fiscal Year (FY) 2022 Budget Estimates, Air Force*, Vol II, *Research, Development, Test & Evaluation, Air Force* (Washington, DC: U.S. Air Force, May 2021), p. 93.

51 U.S. Air Force, *Department of Defense Fiscal Year (FY) 2022 Budget Estimates, Air Force*, Vol II, pp. 93–103.

52 CRS, *Defense Primer: RDT&E* (Washington, DC: CRS, June 14, 2021).

53 David Mortimore, "New DoD RDT&E Appropriation Budget Activity," *America's SLAMR*, October 20, 2020.

54 U.S. Air Force, *Department of Defense Fiscal Year (FY) 2022 Budget Estimates, Air Force*, Vol III part 2, *Research, Development, Test & Evaluation, Air Force* (Washington, DC: U.S. Air Force, May 2021).

55 AcqNotes, "Broad Area Announcement."

56 "FAR 35.016(A)" in AcqNotes, "Broad Area Announcement."

57 Author interview, Dr. Jimmy Jones, July 14, 2021.

58 Author interview, Dr. Jimmy Jones, July 14, 2021.

59 Author interview, Maj Alex Wallis, December 1, 2020.

60 Author interview, Maj Alex Wallis, December 1, 2020.

61 Author interview, MajAlex Wallis, December 1, 2020.

62 Author's own experience, OIF February 2003–June 2003.

63 Author interview, Maj Alex Wallis, December 1, 2020.

64 Author interview, Dr. Jimmy Jones, November 19, 2020.

About The Mitchell Institute

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

Disclaimer: Mitchell Institute for Aerospace Studies would like to recognize that this publication is based upon work supported by the Defense Advanced Research Projects Agency (DARPA). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of DARPA.

About the Series

The Mitchell Institute Policy Papers present new thinking and policy proposals to respond to the emerging security and aerospace power challenges of the 21st century. These papers are written for lawmakers and their staffs, policy professionals, business and industry, academics, journalists, and the informed public. The series aims to provide in-depth policy insights and perspectives based on the experiences of the authors, along with studious supporting research.

For media inquiries, email our publications team at
publications.mitchellaerospacepower@afa.org

Copies of Policy Papers can be downloaded under the publications tab on the Mitchell Institute website at
https://www.mitchellaerospacepower.org

About the Authors

Lt Gen David A. Deptula, USAF (Ret.) is the dean of the Mitchell Institute for Aerospace Studies. He has commanded multiple aerospace operations ranging from humanitarian relief efforts, to small-scale contingencies, to major theater war. Deptula served as the principal attack planner for the Operation Desert Storm air campaign where he introduced the effects-based approach as the basis of those combat operations; he was commander of the Combined Task Force for Operation Northern Watch which executed no-fly zone enforcement operations; he directed the air campaign over Afghanistan as part of the initial wave of combat operations in Operation Enduring Freedom; and he served as the air commander for Operation Unified Assistance, the South Asia tsunami relief effort. He was twice a joint task force commander. He has also served on two congressional commissions charged with outlining America's future defense posture. Deptula has piloted more than 3,000 flying hours (400 in combat) to include multiple command assignments in the F-15. In his last assignment on active duty, as the Air Force's first chief for intelligence, surveillance, and reconnaissance (ISR), he transformed the U.S. military's ISR and remotely piloted aircraft (RPA) enterprises. Deptula holds a B.A. in astronomy and an M.S. in systems engineering—both from the University of Virginia. He also holds an M.S. in national security strategy from the National War College.

Heather R. Penney is a senior resident fellow at the Mitchell Institute, where she conducts research and analysis on defense policy, focusing on the critical advantage of aerospace power. Prior to joining Mitchell Institute, Penney worked in the aerospace and defense industry, leading budget analysis activities, program execution, and campaign management. An Air Force veteran and pilot, Penney served in the Washington, DC Air National Guard flying F-16s and G-100s and has also served in the Air Force Reserve in the National Military Command Center.