



# Resilient Command and Control

## The Need for Distributed Control

By Gilmary Michael Hostage III and Larry R. Broadwell, Jr.

A guiding principle that has long underpinned the projection of dominant U.S. Air Force airpower is the tenet of *centralized control and decentralized execution*. This foundational concept is deeply rooted in Air Force history and remains a cornerstone of its doctrine. It informs how we organize and train for combat and helps prioritize the weapons systems and technologies we pursue. It has proved integral to every successful contemporary air campaign by synergizing a single commander capable of balancing tactical needs with strategic requirements with tactical operators capable of fostering initiative and flexibility.

---

General Gilmary Michael "Mike" Hostage III, USAF, is Commander of Air Combat Command. Lieutenant Colonel Larry R. Broadwell, Jr., USAF, is Executive Officer to the Commander of Air Combat Command.

While the relevance of this simple, elegant tenet is unquestionable, the simplicity of centralized control and decentralized execution renders it incomplete when applied to modern contested and denied operations. This insufficiency has not and will not be evidenced by our experiences in Iraq, Afghanistan, or Libya as the resiliency of our networks, datalinks, and communications went unchallenged. However, in antiaccess/area-denial (A2/AD) environments, the resiliency of our networks, datalinks, and communications will almost certainly be contested. It is during these moments that distributed control, not centralized control, will provide the continued orchestration of combat airpower. Stated more completely, resilient command and control (C2) in an A2/AD environment will require *centralized command, distributed control, and decentralized execution*.

We have grown accustomed to the benefit of an unfettered network-enabled battlespace where our networks, datalinks, and communications operate without interruption. Since the advent of such capabilities, U.S. and allied forces have enjoyed an exclusive advantage. Consequently, it is preposterous to believe any sophisticated future adversary would not possess at least the desire and, likely, the capability to disrupt our C2 architecture. Therefore, we must be prepared to synchronize and project combat airpower through distributed control during periods when our C2 architecture is strained by asymmetric challenges or saturated with intense air activity. If the Combined Forces Air Component Commander (CFACC) becomes isolated, the concept of distributed control empowers subordinate commanders, organizations, operations centers, and battle management command and

control (BMC2) platforms to amalgamate otherwise disconnected units into teams of synchronized combat airpower. Stated explicitly, the power of distributed control is its ability to join otherwise disconnected and independent units, thus increasing the resilience of our overall airpower projection.

A resilient C2 architecture is essential to executing the full range of military operations in an A2/AD environment. Resilient C2 is also foundational to the conduct of parallel operations and reinforces the elements of operational design—simultaneity, depth, timing, and tempo. While the resilience of our C2 architecture has gone untested for decades, we cannot assume this will hold true in the future. Inevitably, our ability to conduct distributed control in the absence of or degradation in centralized control will prove essential to providing continued dominant combat airpower for U.S. and allied warfighters.

## Distributed Control

*Distributed control* can be defined as the conditional, adaptive delegation or assumption of control activities through orders or protocols to synchronize operations, maintain initiative, and achieve commander's intent. Distributed control could occur explicitly or implicitly; the CFACC could delegate some control authority to a subordinate unit, or the subordinate unit could assume a particular level of control authority by following predetermined lost-communication protocols. Distributed control occurs largely at the operational and tactical levels of warfare. At the operational level, the CFACC might choose to implement distributed control to focus his attention on areas of more intense combat or, perhaps, reduce demands on limited Air Operations Center (AOC) bandwidth. Just below the AOC, subordinate operations centers and BMC2 platforms are both uniquely capable of executing distributed control. Either could be delegated additional authorities by the CFACC to control operations in an area experiencing a modest level of activity, thus allowing the AOC to focus control on

areas of more intense fighting. Through the use of established protocols, BMC2 platforms such as the E-2, E-3, E-8, or a Control and Reporting Center could assume additional control activities from the AOC after being cut off for a predetermined period of time. Finally at the tactical level, flight leads and mission commanders regularly exercise distributed control by redirecting to alternate targets or rerolling to a secondary mission. They do this based on their knowledge of the commander's intent and tactical circumstances.

Distributed control is the process (or the *how*) of transitioning control authority from one entity to another. Distributed control absolutely does not delegate *command* authorities or *command* responsibilities from the CFACC or a subordinate commander to another. Neither the Combined Forces Commander nor the Commander of Air Force Forces (COMAFFOR) would relinquish their command authorities under distributed control. Subordinate units, operations centers, or BMC2 platforms would be delegated or assume additional control activities dependent upon their individual capacity to control and when specified triggering events have occurred. Distributed control could occur over short (minutes to hours) or long (days to weeks) periods. For brief C2 disruptions, subordinate BMC2 platforms would simply assume control activities normally performed by the CFACC and continue to execute using the guidance provided in the Air Tasking Order (ATO) and Air Operations Directive. For disruptions lasting longer than a day, BMC2 platforms, in conjunction with lower echelons of command, could also begin executing a series of preplanned ATOs covering several days. It is even possible, if isolated for many days to weeks, for subordinate units to self-organize into larger, more comprehensive units using distributed control.

Self-organization would only occur in the direst of circumstances and does not include modifications to the chain of command, leaving prehostility command authorities and responsibilities intact. Furthermore, any self-organization

would remain under the command of the CFACC and should evolve as expressed in his mission intent orders about extended periods of lost communications. These new organizations could become as robust as an Air Expeditionary Task Force (AETF), thus husbanding resources from otherwise isolated units—fighters, bombers, tankers, and intelligence, surveillance, and reconnaissance (ISR) aircraft—into a composite fighting force. Again, a distributed control construct does not necessitate the transfer of additional command authority from the COMAFFOR, or the CFACC, to the AETF commander. The commander of the ad hoc AETF would retain all previous command authorities, perhaps as a numbered Air Force or wing commander, while also gaining responsibility for the tactical control activities of his newly federated forces. COMAFFOR command authorities would continue to be retained by the CFACC. The AETF commander would be expected to advance the scope and complexity of operations following the CFACC's intent and utilizing distributed control, all the while attempting to reestablish normal C2 links.

## The Critical Element

In addition to doctrine, organization, and technology, our Airmen are critical to executing distributed control. Airmen are the ultimate source of our combat capability. They possess the knowledge, creativity, and drive to overcome highly complex and dynamic challenges whenever and wherever the Nation asks. They are possessed of a unique air-mindedness. They are creative, highly adaptive, and capable of rapidly making bold decisions. They are our most precious resource and *the* critical element of successful distributed control. The trust shared by Airmen underpins the process of distributed control; without trust, distributed control fails. Trusted autonomy allows Airmen to act with initiative knowing the decisions they make and the actions they take will be supported by the commanders who have placed their trust in them. The expectation that



Crew chief marshals F-16 Fighting Falcon from hardened aircraft shelter in Germany in support of Operation *Odyssey Dawn* (U.S. Air Force/Benjamin Wilson)

Airmen are empowered to operate with trusted autonomy is who we are and how we fight.

During my first operational assignment, I flew one of the earliest versions of the F-16. The avionics aboard that Viper were archaic in comparison to the F-16 of today, never mind our most advanced fighters, the F-22 Raptor and F-35 Lightning II. The Block 10 Viper's radar could only acquire and track targets just beyond what could be seen by the naked eye. It did not carry a beyond-visual-range missile and was limited to six primitive AIM-9 infrared missiles. It had no advanced communication equipment, and it could not import data from outside airborne or ground-based platforms; datalinks had yet to be incorporated into

the F-16. There was no all-seeing AOC Link 16, which is the backbone of our modern tactical C2 architecture. The real-time, unblinking eye provided by our modern ISR platforms could only be found in the imaginations of George Orwell and H.G. Wells.

From my time as a young wingman, the expectation that our rudimentary avionics would not compensate for the complexities of aerial combat drove our tactics, techniques, and procedures (TTPs), and also our attitude. More important than being prepared to "chattermark" to a clear radio channel, we were prepared to alter our TTPs or change the plan in real time without guidance or permission from above. Our attitude of bold, calculated initiative was

integral to mission success then as it will be in the future. The battlefields of Iraq and Afghanistan have grown a generation of Airmen accustomed to leveraging a robust, unparalleled C2 architecture: communications, datalinks, navigational systems, and sensors. Because future conflicts are unlikely to afford the same unfettered access, these Airmen must be prepared to deal with a momentary or prolonged interruption of some or all of that C2 architecture. They must be ready to overcome varying levels of isolation or confusion associated with fighting in an A2/AD environment. The incorporation of distributed control into our daily training, TTPs, and exercises will prepare the force to fight through these challenges rather than be relegated to inaction.

Airmen empowered with trusted autonomy are more likely to seize initiative by assuming control authorities implicitly rather than waiting for those authorities to be delegated explicitly. The ability to maintain initiative and act in the throes of combat is key to putting combat airpower over friendly forces or taking it to the enemy. To enable this initiative, the commander must have clearly expressed his intent to subordinate commanders and their units. From this initial direction, subordinate commanders and units are able to intelligently conduct distributed control as well as decentralized execution in support of the commander's principal goals and objectives and in the absence of direct contact. The following examples are provided to further clarify this concept.

### Preparing for Distributed Control

Distributed control exists in the Air Force today to some degree. All flight leads and mission commanders have been trained to think for themselves, know the mission, and make decisions within guidelines to achieve success. However, the past decades of intense counterinsurgency operations, coupled with pervasive networks and high-level command visibility of combat situations, have muted some Airmen's instincts for independent operations. The intensity of peer-adversary conflict will bring challenges that require tactical leaders who can exercise judgment and achieve mission success despite disrupted C2.

In addition to rekindling this concept at the tactical level, the institutionalization of strategic and operational distributed control in our force will require changes in Service doctrine, organization, TTPs, training and exercises, and the technologies we pursue. Evolving the central tenet of centralized control and decentralized execution to centralized command, distributed control, and decentralized execution will likely encounter significant institutional inertia. Doctrine is formed by critical analysis and military experience and evolves through the incorporation of contemporary thinking, new experiences, and cutting-edge



Pilots briefed in support of Operation *Odyssey Dawn* (U.S. Air Force/Benjamin Wilson)

technologies. Because doctrine presents considerations on how to accomplish military objectives, the Nation's rebalance to the Pacific should drive a critical review and adaptation of existing doctrine in a highly contested environment—on scale with the past decade's renewal of counterinsurgency doctrine.

Organizational adaptability is essential to effective operations under distributed control. The ability of an AETF, Air Expeditionary Wing, or Expeditionary Operations Group commander to assume control authority of otherwise independent or isolated forces is fundamental to the concept of distributed control. The gears of distributed control are lubricated by the proper delegation and assumption of control authorities. Fundamental to executing distributed control is a clear expression of commander's intent and the triggers to achieve it. Distributed control requires subordinate commanders to be prepared to initiate or fulfill new control authority relationships—an arduous task that must be codified and exercised well before being put into practice. Every foreign-based or expeditionary unit, operations center, or BMC2 platform should have established distributed control TTPs and routinely practice them. The CFACC should also tailor unit predeployment preparation messages to prioritize distributed control training scenarios. Lastly, while in garrison, units

should be exposed to a variety of training and exercise opportunities that hone and evaluate their capability to conduct distributed control. Air Combat Command has already embarked on just such a program.

Readiness Program-2 (RP-2) is a comprehensive approach to the ACC ability to conduct operations in an A2/AD environment. The program enhances and normalizes training in a highly contested environment and ensures our Airmen routinely practice how to deal with the momentary or prolonged interruption of unique communication and datalink systems. RP-2 forces operators to practice existing—as well as develop new—TTPs aimed at expanding tactical expertise operating in a contested environment. Reinvigorating this skillset not only prepares the force to operate in an A2/AD environment but also prepares it to operate under distributed control. Building on tactical level efforts, we should expand RP-2 into operational exercises (for example, Red Flag, an advanced aerial combat training exercise hosted at Nellis Air Force Base, Nevada, and Eielson Air Force Base, Alaska) and incorporate distributed control into our practice of peer-adversary air combat. Our adversaries should know that attacks on our C2 architecture will not stop us and that we will continue to bring lethal combat airpower. Our adversary's



U.S. Air Force F-35A Lightning II Joint Strike Fighters fly in formation off right wing of KC-135R Stratotanker following aerial refueling mission along Florida coast (U.S. Air Force/John R. Nimmo, Sr.)

calculus must account for our advancing doctrine, TTPs, skills, and technology. We must aggressively pursue technologies and TTPs that will enable or enhance resilient C2.

While never a panacea, technical solutions can certainly aid in the implementation of distributed control. The concept of a combat cloud is one technical solution that offers much promise. The strength of the combat cloud is in its pervasiveness. The combat cloud would use a federation of airborne and ground-based systems (nodes) that gather, process, store, and disseminate information. As opposed to a hierarchy, the combat cloud is constructed more like a heterarchy, where connected nodes operate independently from any associated ranking. Information imported to the combat cloud from a strategic system, for example, would not necessarily obviate or overwrite information from a tactical system. The combat cloud propagates information discretely without presenting finite, targetable nodes. Because a plethora of contributing nodes port information into the combat cloud, no

vital node or nodes exist, eliminating the single-point weakness of a central repository. As nodes are added or disconnected from the combat cloud, its information steadily builds or gracefully degrades, with the latter being an acute advantage. Graceful degradation allows the combat cloud to propagate dormant information where an information void would otherwise exist. This benefit, however, brings with it the first potential challenge of a combat cloud: data latency. Data distributed by any cloud must include protocols that allow the user, or more accurately, the user's system, to filter or flag data deemed too old. In addition to latency, data authenticity is a concern emblematic of a heterarchic system such as the combat cloud.

The combat cloud's multinodal and amorphous nature makes it susceptible to injections of corrupt or malicious data. In addition to requiring secure and reliable connections between each node, algorithms capable of fusing, updating, and pruning voluminous information offer an effective counter to inauthentic data. Rather than identifying and removing

countless bits of false data, sophisticated algorithms would continuously resolve contrasting data—true, false, or inaccurate—into a comfortable and fused solution. Outlying data, whether contributed by friendly (inaccurate) nodes or enemy (false) nodes, would simply be pruned from the combat cloud—a machine-to-machine wiki-approach to ensuring authenticity of the cloud's data.

### **Explicit Distribution of Control Authorities**

The CFACC, through the AOC, possesses tremendous capacity both in bandwidth and in manpower to provide effective C2 during major combat operations. Yet as the U.S. Central Command CFACC, I established and practiced procedures for operating with constrained bandwidth. We established rules for prioritizing all users, thus ensuring the most critical communication would continue during periods of limited bandwidth. A CFACC could choose to lower excessive C2 bandwidth demands by explicitly distributing control authorities to lower echelon

commanders or control centers. In addition to bandwidth, effective C2 of large-scale, intense combat operations requires substantial manpower. A CFACC might choose to delegate control authorities to commanders or control centers in sectors with lower operations tempo to focus the AOC staff on areas experiencing intense combat. Whether to manage human or computer bandwidth or to focus attention, explicitly distributing control authorities is a viable option in managing C2 demands.

### Implicit Assumption of Control Authorities

BMC2 platforms and operations centers provide a critical linkage between the CFACC and tactical airpower in combat. Because of their significant C2 capacity, they are delegated sufficient control authorities to allow them to manage portions of the ATO. They are uniquely capable of providing timely, dynamic direction to tactical airpower to assist with attacking complex problems and better achieving the CFACC's intent. Despite this delegation, the CFACC retains needed control authorities under normal operating conditions. In a near-peer fight, it is possible for the AOC, and therefore the CFACC, to be cut off abruptly from subordinate elements of the C2 architecture before having an opportunity to delegate control authorities explicitly (as in the previous vignette). Under these circumstances, BMC2 platforms and operations centers have to be ready to implicitly assume control authorities. Without doing so, combat airpower will rapidly lose the initiative and slowly devolve into disparate, isolated units trying to defend themselves. In contrast, a BMC2 platform or operations center could continue to synchronize airpower regionally by assuming control activities normally executed by the CFACC—given that the CFACC had provided suitable commander's intent and a standing set of protocols for such an assumption. With designated authorities, a BMC2 platform or operations center would have the ability to con-

tinue to orchestrate regional air operations until the CFACC regained C2 connectivity at the AOC or, potentially, relocated to an alternate control center. Again, the key to this process is establishing and practicing detailed protocols for when and how to assume control authorities as well as clear guidance as to commander's intent. Without such direction, subordinates would be forced to wait for direction from the CFACC.

### Control Authorities at the Tactical Level

Tactical operators must have a clear understanding of the authorities they possess as well as the CFACC's intent before flying their missions. The clear expression and understanding of these authorities and intent would promote mission success and save lives. A strike package commander flying an F-35 must understand authorities to induce or forestall major combat operations. If the sparring between two belligerent nations has made combat inevitable, the strike package commander would likely launch with authorities delegated by the CFACC to initiate combat operations. Well before reaching prestrike orbit, the strike package commander would have internalized the CFACC's intent and objectives, the master air attack plan, the ATO, special instructions, and rules of engagement. She understands her role in the strategic picture and becomes a tactical extension of the CFACC. She does not require an explicit "go" command; she is entrusted with employing her flight of F-35s as the situation unfolds and without necessarily being told when or how. Sometimes, however, the road to combat operations follows a less predictable path—a narrow one shrouded in uncertainty where the stakes are high and authorities are retained at the highest levels.

The Air Force's tremendous capability to hold any worldwide target at risk affords our nation's leaders unique options to deal with national security threats. Global precision attack capabilities are continuously enhanced through acquiring advanced technologies and by conducting scenario-based integrated

exercises. Sophisticated platforms have the ability to attack targets previously thought to be too complex, elusive, or well defended. Tremendous political sensitivities and risk surround these types of operations; therefore, the authority to initiate them is seldom delegated from the most senior civilian leaders. The F-35 package commander would do much of the same preparation for this type of mission. In addition, she would likely receive additional training (simulations and exercises) focused on the orchestration and integration of a specialized tactical problem. In stark contrast to the previous example, she would most likely not be authorized to conduct the mission absent the go call. She would marshal her forces airborne in preparation for combat, anticipating the command to execute at a predetermined time. She would know that a go command is required to conduct offensive strike operations regardless of the presentation of enemy forces. She would be prepared, however, to retrograde if attacked, reserving the use of deadly force to defend herself, her flight, and other friendly forces. As the CFACC, I placed tremendous trust in Airmen operating at the tactical level. I was confident in their ability to use the training and authorities they were given to achieve their mission and drive toward my intent whether a go command was needed or not.

The mantra of *centralized command, distributed control, and decentralized execution* is not a change from our past, but a healthy adaptation to the realities of contemporary warfare. The keys to effective use of distributed control are the clear articulation of intent and standing directions for when and how to assume this action. However, the linchpin of success in any fight will be the ingenuity, aggressiveness, and fighting spirit of our Airmen. Execution of distributed control, whether intentional or as a result of enemy activity, hinges on a force that is conditioned to deal with contested environments and empowered with doctrine that ensures that America's Airmen will not be deterred by asymmetric attacks on our command and control architecture or leadership nodes. JFQ