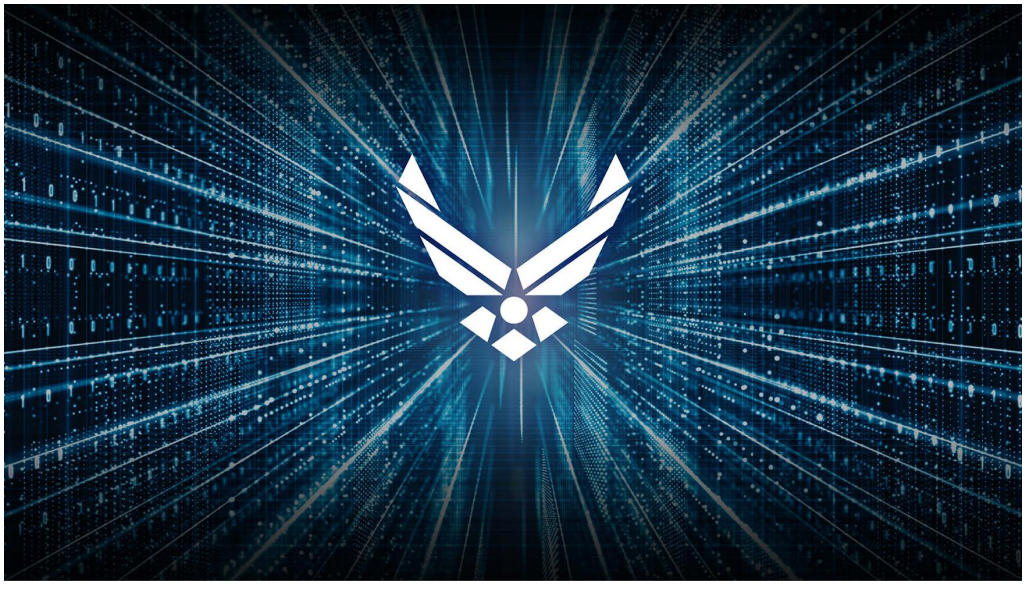
Achieving Convergence in the Information Environment

Revising the Air Component Structure

Brig Gen George M. Reynolds, USAF



Introduction

The Air Force activated Sixteenth Air Force (AF), a numbered air force focused on information warfare (IW) on 11 October 2019. It was a significant step by the service. The Air Force is not the first military organization to make a meaningful commitment to operating in the information environment. In 2017, the chairman of the Joint Chiefs of Staff added *information* as a joint function to Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*.[1] This revision to joint doctrine signaled the importance of information throughout the Department of Defense (DOD).

All four services are reemphasizing information's importance during planning, execution, and assessments. Information has always been critical to achieving military and national objectives. In fact, nation states and nonstate actors are in-

creasingly turning to IW to achieve their objectives, making now the right time for the US to focus on IW. However, creating an organization responsible for IW with its complex relationships, numerous authorities, and global problems requires new thinking about how the Air Force organizes operational staffs for employment by joint force commanders.

What is Information Warfare?

The Air Force describes *information warfare* as "the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and to preserve friendly freedom of action during cooperation, competition, and armed conflict."[2] IW can deny, degrade, disrupt, deceive, discover, disclose, or destroy the use of information and its functions while also defending against those actions. The objective of IW is to influence or change perceptions, actions, and behaviors in a manner that is consistent with US interests. Typical targets are data, systems, and people. This description of actions, objectives, and targets may sound overly broad such that any military operation or capability could qualify, but contemporary IW is much narrower.

Today's IW integrates the capabilities within the disciplines of weather, public affairs, cyberspace operations, electronic warfare, information operations, and intelligence, reconnaissance, and surveillance (ISR). Each of these disciplines are proven and necessary; however, once under a single operational commander, it can form new, integrated IW options for joint force commanders. Integrating IW disciplines under a force provider can accelerate experimentation, tactics development, specialized planning, professional development, focused intelligence, and operational-level innovation. It is also important to point out that the processes and building blocks IW uses are similar to any military exercise or operation. It requires time-tested actions, including education, training, planning, execution, command and control (C2), and assessments (see fig. 1). These actions must be assigned with clear responsibilities, missions, functions, and tasks.

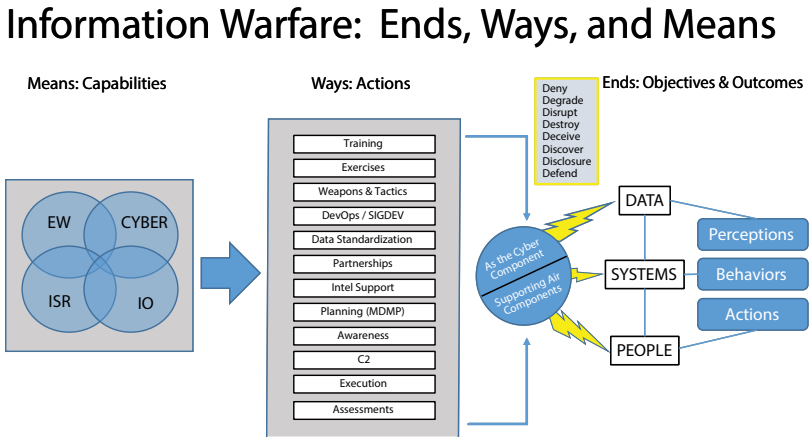


Figure 1. Information warfare ends, ways, and means

Characteristics of Information Warfare

Although IW shares many similar characteristics with other military operations, it possesses some unique challenges and additional complexities. As nations move from competition to conflict in the future, those military organizations that are more agile, adaptive, and able to learn faster can use IW more effectively. A successful organizational design must address four specific operational challenges while also considering process changes to speed up military operations.

IW operations are perishable while coordination takes time. Intelligence preparation, attack access planning, execution, and assessment windows are often perishable and frequently much more so than kinetic operations. Whether a network is no longer accessible, a weapons system changes encryption, or the news cycle moves on to the next event, IW planning and execution requires agility, insights, and the ability to adapt quickly. Conversely, approval processes, tool development, content creation, and other important elements of IW can take significant time and coordination. It is important to note that during counterterror operations, these processes improved, but future complex conflicts will not have the luxury of extended coordination. IW operations will require rapid coordination or even preapproval.

Authorities, forces and capabilities are not centralized. Typically, a single commander or command does not possess all the necessary IW authorities, forces, data access, capabilities, and responsibilities to prosecute an IW mission. Even in those rare cases when a combatant command has most of these assets, the command must coordinate across functional and geographic boundaries to execute a mission.

Achieving integration is challenging. Military operations in and across domains relies on integration. However, achieving IW integration is difficult. Expertise within each IW discipline is specialized, in high demand, and in short supply. IW practitioners may not have experience in integrating their discipline with and across other IW disciplines. There may be limitations with data sharing, clearances, legal concerns with crossing authorities, or simply a lack of opportunities to work with other IW disciplines. Partnerships, exercises, training, mission exposure, and integrated capability development are critical. At its core, IW is an integrated endeavor.

Command and control can be fluid. Supported or supporting relationships can change during a single IW operation and certainly during a campaign. As an example, a single IW operation could:

- Yield insights about adversary capabilities and vulnerabilities for one combatant command
- Create effects for another functional or geographic combatant command
- Provide real-time feedback to an ISR crew supporting yet a third command.

Supported or supporting relationship can change as new information becomes available and mission requirements evolve. The ability of IW forces to support multiple combatant commands and service components fluidly requires partnerships, precoordination, effective delegation of authorities, and clear priorities.

Other military operations can and do share these characteristics, but the design of an effective IW organization must emphasize speed, integration, meaningful partnerships, adaptive processes, and clear lines of responsibility.

Convergence: How Information Warfare is Realized

As outlined in the paper, *16th Air Force and Convergence for the Information War*, "IW convergence is *the integration of capabilities that leverage access to data across separate functions in a way that both improves the effectiveness of each functional capability and creates new information warfare outcomes.*"[3] Convergence occurs during integrated planning and execution in support of combatant commands and their service components, but it also occurs before IW forces are presented. Examples include bringing IW forces together during exercises and training events resulting in new tactics, techniques and procedures (TTP); integrating development operations (DevOps) initiatives creating new, interoperable capabilities; mission rehearsals improving operational integration;[4] implementing data strategies ensuring better access; and experimenting with new and evolving IW concepts leading to improved innovation. Applying the concept of convergence informs how an

operational-level organization can fully leverage IW disciplines that generate meaningful outcomes in support of joint force objectives.

Program Guidance Letter Assigned Missions

Sixteenth AF is assigned six specific missions and associated authorities detailed in the Secretary of the Air Force-approved program guidance letter (PGL).[5] These missions include Component-Numbered Air Force (CNAF), Air Force Cyber, Service Cryptologic Component, Defense Intelligence Component Head, Joint Force Headquarters-Cyber Air Force (JFHQ-C (AF)), and responsibility for securing and operating the Air Force Information Network. Each of these missions contain their own responsibilities, authorities, forces, capabilities, access to unique data, and C2 relationships. In most cases, there is natural integration between these missions. Independently, they offer advantages, but together, Sixteenth AF uses each authority distinctly to integrate IW activities that generate options and outcomes for combatant commands and service components.

Command and Control Model and Organizational Description

Before the activation of Sixteenth AF, Twenty-Fourth AF, and Twenty-Fifth AF had organizational structures unique to their assigned authorities and missions. Twenty-Fourth AF was comprised of a C-NAF staff and operations center and also included the JFHQ-C, Air Force. The JFHQ-C followed a traditional joint task force model with the requisite staff components. It had operational control of assigned cyber mission forces from the Air Force, Army, and Navy, as well as responsibilities for planning, C2, and the execution of cyber operations of these assigned forces. This "joint" headquarters structure was mandated by the DOD and manned by Air Force personnel absent a joint-manning document. Likewise, Twenty-Fifth AF consisted of a numbered air force (NAF) staff and operations center; however, it included the Air Force Cryptologic Office, a staff focused on the service cryptologic component mission. Although each NAF's organizational structure shared similarities, blending their unique authorities, missions, and resources into an IW NAF required a new way to think about Air Force operational organizational design. The traditional component NAF structure was insufficient. Luckily, two component major commands had already begun a similar transformation.

Building upon the Pacific Air Forces (PACAF) and US Air Forces in Europe's (USAFE) new air component models, Sixteenth AF was structured to leverage its distinct authorities, responsibilities, relationships, and multiple staffs while in-

formed by IW's unique operational characteristics and the concept of convergence.[6] This transformation occurred through a series of important steps.

First, Sixteenth AF was activated on 11 October 2019 as a "combined" staff and followed the principle of "doing no harm" to each NAF's missions. The A-staff directorates were led by a single director and supported by cyber and ISR deputies. Additionally, the 625th Operations Center (OC) and 624th OC remained in place, executing their assigned missions.

Second, working with Air Combat Command (ACC), specific operational test and evaluation functions were vertically aligned or divested such as elevating Air Force Inspection Program oversight to ACC, and shifting Joint Worldwide Intelligence Communications System operations to the 688th Cyber Wing.

Third, the 624th OC and 625th OC were deactivated, and the 616th OC was activated on 16 March 2020.

Finally, the ACC commander (COMACC) approved the Sixteenth AF full operating capability (FOC) organizational structure on 19 April 2020 and formally accepted FOC on 13 July 2020.

This COMACC-approved design included an A-staff and a unique IW operations staff consisting of a J-staff, 616th OC, and four cyber operations integrated planning elements (CO-IPE) aligned to United States European Command, United States Strategic Command, United States Transportation Command, and United States Space Command. The four CO-IPEs are aligned to specific combatant commands, supported by the broader Sixteenth AF enterprise. The FOC structure also included IW concepts needed to realize Sixteenth AF's full IW potential. These concepts included:

IW cells. ACC and Sixteenth AF recognized that generating IW outcomes required experts with weather, information operations, electronic warfare, ISR, cyber, and public affairs expertise. As detailed in ACC's *IW Cell Concept Paper*, the "16 AF IW Cell will plan, coordinate, synchronize, and present integrated IW support to air components and CCMDs across the spectrum of military operations and throughout the competition continuum in order to gain and maintain an information advantage."[7] These IW cells will be aligned to unit type codes (UTC), making them available to service component commands to provide surge capacity and IW expertise during exercises and operations. Placing IW cells at the operational level and near the joint force commander not only helps with the creation of IW options but emphasizes the integration of operations in the information environment.[8] As detailed in their paper, *Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment*," Gen Mark D. Kelly and Dr. Sandeep S. Mulgund stress the importance of putting OIE at the forefront of component

activities.[9] The IW cell provides the added expertise to do this. But the IW cell members also have the right clearances, read-ins, an understanding of combatant command operational plans, relationships with key players, and experience.

Partnership engagement and the political advisor (POLAD). Connecting organizations that operate in the information environment is critical to IW. This connection includes allies, partners, joint organizations, and the interagency. The POLAD plays an important role in understanding changes within international affairs and linking DOD and interagency efforts. Equally important, Sixteenth AF required a Partnerships and Engagement (J54) branch that connects the IW NAF with aligned combatant command and service component operations, activities, and investments and with broader partnership implementation. Having preexisting relationships and partnerships with multiple players is critical to speeding up coordination and cooperation.

Weapons and tactics. As outlined in the PGL, tactics development is critical to IW, but it is about more than the final tactic. The process of creating TTPs strengthens partnership, improves capabilities, integrates IW disciplines, trains and educates the IW force, and fosters agile innovation. Additionally, resource decisions are informed by these experiences, leading to improvements within DevOps, data sharing, and the convergence of IW disciplines.

IW Operations Staff: Revising the Air Component Structure

Similar to the PACAF and USAFE A3-centric approach, Sixteenth AF focused on the air component structure by creating the IW Operations Staff. It uses the strengths of both an Air Force air operations center (AOC) and Joint Task Force staff. Led by a one-star deputy commander, this IW Operations Staff is responsible for component operations and IW convergence for Sixteenth AF. This staff uses its joint task force staff and AF AOC structures to plan, execute, and assess operations.

To avoid duplicative responsibilities and planning gaps, the IW Operations Staff segmented the joint planning process along a linear time horizon. The AOC is responsible for real-time planning, execution, and assessments, as well as the C2 of assigned forces, including those executing DOD Information Network operations. It also coordinates IW convergence activities with other AOCs during execution. The 616th OC's unique relationships with other AOCs allows for greater awareness, changes to supported and supporting relationships during mission execution, and convergence on emerging problems. The J33 is focused on current operations, the J35 on future operations, and the J5 on long-term planning. The CO-IPEs provide their aligned combatant commands a collocated planning staff. These responsibilities are also detailed in General Kelly and Dr. Mulgund's C2OIE Conceptual Framework. The result is an integrated IW operational staff

that not only supports combatant commands and service components but a structure that they can understand—an IW component with a J-staff and an operations center. The transition along the joint planning process from the J-staff to the 616th OC is the strength of the IW operations staff.

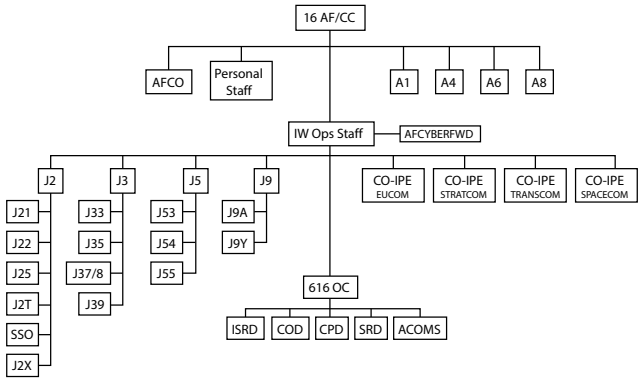


Figure 2. Sixteenth Air Force structure

IW Operations Staff also includes a J2, J5, and J9 under the direction of the IW Operations Staff deputy commander. This alignment not only brings these functions closer to operations and planning but helps eliminate friction points between a staff, AOC, and an empowered A3. The J2 supports the J-staff and cyber mission force's operational-level requirements while staying closely connected to the 616th OC's ISRD. The J5 is responsible for the joint planning group, linking Sixteenth AF to combatant command operational plans and strengthening partnerships through the strategic partnership and engagement division. The J9 conducts assessments, analysis, and lessons learned while working with the assessments team within the 616th OC's Strategy Division. These processes and relationships are critical to IW and require thoughtful coordination between each staff organization. In fact, concept of operations (CONOPS) for planning, intelligence support, assessments, DevOps, a crisis action team, information technology support, and exercises were created to deconflict, then integrate staff missions, functions, and tasks.

These CONOPS are also supported by traditional planning processes and convergence activities. The J3 is responsible for operational planning through an Operations Planning Group, while the J5 leads the Joint Planning Group focused on long-term planning. The J37/8 combines component fires with traditional NAF responsibilities of standardization and evaluation, training, exercises, DevOps, and weapons and tactics. This division's focus is converging IW capabilities through exercises, TTP development, and leading an IW Weapons and Tactics Conference—ultimately, making convergence a reality before forces are presented. The J39

is responsible for integrating information operations, military information support operations, electronic warfare, special technical operations, space, and special programs into IW. Along with the J35, J2, and J54, the J39 provides specialized personnel who support the service component command-aligned IW cell UTCs.

Regardless of how good CONOPS, processes, and relationships are between staff members, the key is an integrated IW operations staff responsible for the prioritization and execution of IW on behalf of the Sixteenth AF commander. The IW operations staff can leverage the assigned authorities, forces, and capabilities to drive staff agility, rapid reprioritization, and IW convergence within an integrated staff.

Way Forward

Creating processes and revising the air component structure are necessary, but organizations need reps and sets to hone their skills, and Sixteenth AF is no exception. Organizational changes will accelerate TTP development, improve training, and create new capabilities. However, planning, executing, and assessing IW repeatedly is how Sixteenth AF, combatant commands, service components, and joint forces will improve their IW game. More broadly, these same steps are necessary if the DOD is going to compete with adversaries by leveraging operations in the information environment.

As nation-states and nonstate actors increasingly turn to IW, the US's comparative advantage is not guaranteed. Refocusing on IW now provides meaningful options to counter malign influence activities during competition, deescalate crises, and enable success in conflict. Achieving this requires an IW force that can adapt, experiment, take measured risk, and develop clever professionals. This process includes creating an organization that can use IW authorities to integrate activities and generate outcomes for combatant commands and their service components.

The demand for military-based IW options is on the rise. Now is the right time for the Air Force to focus on and integrate IW disciplines to solve military problems, provide commanders additional options for our nation, and change how we organize at the operational level. This focus on complex problems, partnerships, and integrating IW requires a new organizational structure designed for competition and conflict—and one that integrates a staff and operations center as an air component operating at the speed of relevance. ✪

Brig Gen George M. Reynolds, USAF

Brigadier General Reynolds (MS, Gonzaga University; MS, George Washington University; MS, Air Force Institute of Technology) is the vice commander, United States Air Force Warfare Center. His previous assignments include deputy commander, Information Warfare Operations Staff, Sixteenth Air Force (Air Forces Cyber); vice commander, Twenty-Fifth Air Force; and the Air Force Military Fellow, Council on Foreign Relations, New York.

Notes

1. Joint Publication 1, *Doctrine for the Armed Forces of the United States,* 12 July 2017, I-19, https://www.jcs.mil/.

2. *Information Warfare*. According to Draft HAF/A3 Terms of Reference: "The Air Force describes IW as the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and to preserve friendly freedom of action during cooperation, competition, and armed conflict. It is distinguished from [operations in the information environment] (OIE) by an increase in the intensity, type, and purpose of activities. Information warfare is an adversary-focused expression of OIE—a subset of circumstances, not a subset of capabilities. Information warfare may be the military purpose of an organization, but the professional competencies and capabilities necessary to conduct it will be equally suited to conducting OIE. Currently, the principal USAF capabilities for IW are CO, EMSO, Information Operations (IO), Intelligence, Surveillance, and Reconnaissance (ISR), and Weather. Critical enablers include, but are not limited to, PA, the Office of Special Investigations (OSI), and the Judge Advocate (JA)."

3. Lt Gen Timothy D. Haugh, Lt Col Nick Hall, and Maj Eugene Fan, USAF, "16th Air Force and Convergence for the Information War," *Cyber Defense Review* 5, no. 2 (Summer 2020), https://cyberdefensereview.army.mil/.

4. DevOps: "Practices which seek to more closely bring together software *dev*elopers and *op*erations staff to work on the same project in a more collaborative manner," https://opensource.com/.

5. Headquarters United States Air Force, Program Guidance Letter 19-05, *Establishment of the Information Warfare (IW) Component Numbered Air Force (C-NAF) under Air Combatant Command*, 6 September 2019, 5.

6. Lt Gen Charles Q. Brown Jr. and Lt Col Rick Fournier, USAF, "No Longer the Outlier: Updating the Air Component Structure," *Air & Space Power Journal* (*ASPJ*) 30, no. 1 (May–June 2016), https://www.airuniversity.af.edu/ASPJ/; and Gen Jeffrey L. Harrigian, Maj Gen Charles S. Corcoran, Col Edward T. Spinelli, and Col John C. McClung, USAF, *Unfinished Business: Refining the Air Component Structure*, *ASPJ* 33, no. 4 (Winter 2019), https://www.airuniversity.af.edu/ASPJ/.

7. Air Combat Command and Sixteenth AF (AFCYBER), "Information Warfare Cell Concept Paper," 28 April 2020.

8. Dr. Sandeep S. Mulgund and Gen Mark D. Kelly, USAF, *Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment, ASPJ* 34, no. 3 (Winter 2020), https://www.airuniversity.af.edu/ASPJ/.

9. Kelly and Mulgund, *Command and Control of Operations.*