Soldiers with the 1st Multi-Domain Effects Battalion (1st MDEB) train 13 February 2023 at Fort Huachuca, Arizona. 1st MDEB demonstrated a wide array of capabilities during the training event, highlighting the 1st Multi-Domain Task Force's progress toward becoming fully operationally capable and contributing to the Army's goal of achieving information advantages. (Photo by Sgt. 1st Class Henrique De Holleben, U.S. Army)

Information Advantage

A Combined Arms Approach

Col. Richard Creed, U.S. Army, Retired

Lt. Col. Michael Flynn, U.S. Army, Retired

Information is central to everything we do—it is the basis of intelligence, a fundamental element of command and control, and the foundation for communicating thoughts, opinions, and ideas.

—Lt. Gen. Milford H. Beagle Jr.,
foreword to ADP 3-13, *Information*

Army doctrine on information changed with the November 2023 publication of Army Doctrine Publication (ADP) 3-13, *Information*. This new doctrine represents an informed consensus about the role information plays during the range of operations Army forces conduct across the competition continuum. It addresses the informational aspects of multidomain operations found in Field Manual (FM) 3-0, *Operations*, by describing a framework for creating and exploiting information advantages to achieve objectives. It provides fundamental considerations for how Army forces use, protect, and attack data and information while affecting the threat's (adversary or enemy) ability to do the same.[1] Most importantly, it makes clear that everyone in the Army plays some role in achieving information advantages relative to our adversaries worldwide.

As a keystone publication, ADP 3-13 links the Army's application of information to all warfighting functions and methods of warfare in ways previous doctrine did not. It represents an evolution in how Army forces think about the military uses of data and information, emphasizing that everything Army forces do, including the information and images it creates, generates effects that contribute to or hinder the achievement of objectives. ADP 3-13 addresses information as a dynamic of combat power and stresses a combined arms approach to creating and exploiting information advantages.

Background

The more you employ stratagems and ruses, the more advantages you will enjoy over the enemy. You must deceive him and induce him to make mistakes in order to take advantage of his faults.

—Frederick the Great[2]

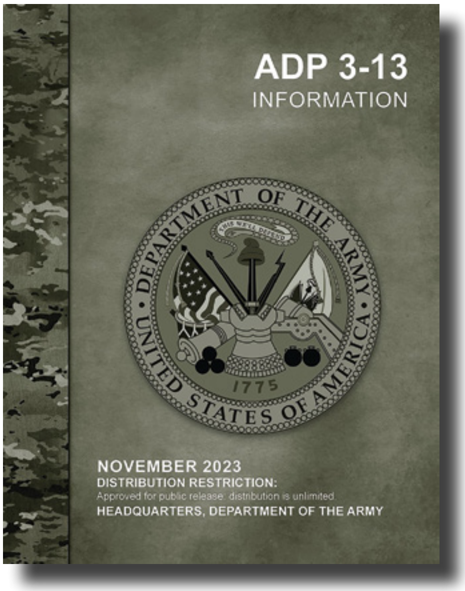
Historically, successful military leaders understood the importance of using information to create and exploit an advantage—a condition that puts a force in a favorable geographical, psychological, or moral position. They understood that knowing more than the enemy and acting effectively on that knowledge faster than their opponent provides an advantage. They understood denying the enemy information or affecting the enemy's ability to communicate enhances friendly chances of success. Successful commanders also understood that using information combined with action or inaction to mislead the enemy creates favorable conditions for the friendly force.

Some of the Army's earliest doctrine finds references of the importance of information to achieve objectives. The Army's first combined arms doctrine, the 1905 *Field Service Regulations*, dedicated a chapter to the "Service of Information," which focused on reconnaissance and communications.[3] Army doctrine throughout World War II, Korea, and Vietnam emphasized security, deception, psychological operations, and electromagnetic warfare to protect friendly intentions, deceive enemy forces, and disrupt enemy command and control (C2). The 1991 Gulf War demonstrated the benefit of employing these elements together in a synchronized fashion to disrupt enemy C2 and to deceive Iraqi leaders about the coalition's plan of attack. Successes in the Gulf War and accelerated growth of information technologies (military and civilian) led to the Army's first comprehensive field manual on information operations, FM 100-6, in 1996.[4]

A lot has changed since the publication of the Army's first information operations manual. Today, military operations are influenced by the exponential growth of information technologies that accelerate and expand the ability of the joint force to collect, process, analyze, store, and communicate data and information at a scale previously unimaginable. A proliferation of satellites, advanced computing and automated

Col. Richard Creed, U.S. Army, retired, is the director of the Combined Arms Doctrine Directorate at Fort Leavenworth, Kansas, and one of the authors and editors of Army Doctrine Publication 3-13, *Information*. He holds a BS from the U.S. Military Academy, an MS from the School of Advanced Military Studies, and an MS from the Army War College. His previous assignments include G-3 of the 2nd Infantry Division, and he has completed tours in Germany, Korea, Bosnia, Iraq, and Afghanistan. He commanded at company, battalion, and brigade levels.

Lt. Col. Michael Flynn, U.S. Army, retired, is a doctrine author and analyst in the Combined Arms Doctrine Directorate and one of the authors of Army Doctrine Publication 3-13, *Information*. As a veteran doctrine writer, he has helped shape Army operations, command and control, and planning doctrine for over twenty years. He served in multiple infantry and staff assignments to include service in Germany, Kuwait, and Afghanistan. He has a master's degree from the School of Advanced Military Studies.



ADP 3-13

INFORMATION

NOVEMBER 2023

DISTRIBUTION RESTRICTION:

Approved for public release: distribution is unlimited

HEADQUARTERS, DEPARTMENT OF THE ARMY

Army Doctrine Publication 3-13, *Information*, can be found online via the Army Publishing Directorate at https://www.armypubs.army.mil/.

systems, mobile networks, and social media are some of the technologies affecting how forces use and employ data and information to achieve objectives. Our primary adversaries now have the same capabilities as the United States. These adversaries can degrade joint force information advantages we may have held in the past, so it is time to start thinking differently.

Multidomain Operations and Information Advantage

The 2022 revision of FM 3-0 is driving change to how Army forces train and fight. The most significant update is the introduction of multidomain operations as the Army's operational concept. Multidomain operations, as defined in FM 3-0, are "the combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders."[5] Multidomain operations are the way Army forces employ ground-based Army capabilities with capabilities from air, sea, space, and cyberspace in mutually supporting ways to create and exploit relative advantages. Information is central to the idea of relative advantage.

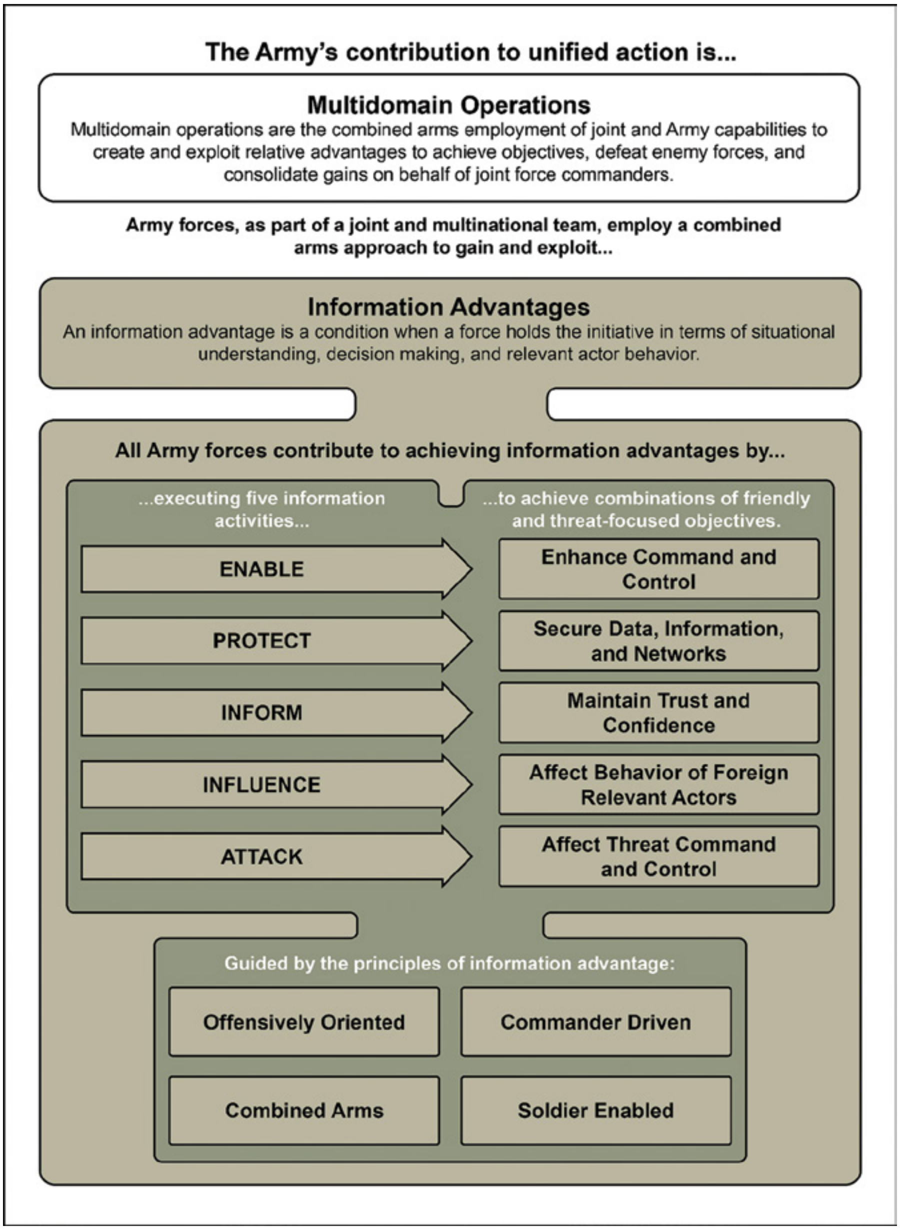
FM 3-0 defines a *relative advantage* as "a location or condition, in any domain, relative to an adversary or enemy that provides an opportunity to progress towards or achieve an objective."[6] Relative advantages are characterized as human, information, or physical. They complement each other. Physical actions, particularly involving the use of force, create information and generate psychological effects. When exploited, these effects can lead to information advantages as friendly forces use information to influence enemy behavior. When combined over time, these physical and information advantages can lead to a collapse of the enemy's morale and will—a human advantage.

This phenomenon was once well understood by military professionals across our Army, but we increasingly made information considerations the purview of specialists and specific staff sections over time. The unintended consequence was intellectual atrophy among many noninformation specialists who planned and led the operations Army forces conducted. ADP 3-13 supports FM 3-0 by ensuring we all adequately consider the desirable cognitive effects we want our operations to achieve. Linking interrelated advantages in the physical, information, and human dimensions addresses that shortcoming since they apply to every echelon, warfighting function, branch, and occupational specialty.

Expanding on relative advantages, ADP 3-13 defines information advantage and describes how creating and exploiting information advantages contribute to achieving objectives.[7] When describing information advantage, ADP 3-13 emphasizes three points. The first is the importance of understanding informational considerations of an operational environment as a precursor to developing effective ways to create and exploit advantages. Informational considerations are those aspects of the human, information, and physical dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information.[8] ADP 3-13 describes how leaders analyze informational considerations from friendly, threat, and neutral perspectives to aid them in developing ways to use, protect, and attack data, information, and capabilities. This analysis enhances several aspects of planning, including the selection of targets and objectives, approaches to influence threats and other foreign relevant actors, and identification of force protection measures.

The second point is the recognition that there are many forms of information advantage—not just a single overarching condition relating to all things information.[9] For example, a force that collects, processes, analyzes, and uses information to understand, decide, and act more effectively than an opponent has an advantage. However, that same force may be at an information disadvantage because the opposing force effectively uses information to influence relevant actor behavior in opposition to friendly-force objectives.

A third point of emphasis is the temporary and relative nature of an information advantage.[10] Like physical and human advantages, information advantages are often temporary and vary over time relative to an adaptive opponent and changes in an operational environment. While friendly forces seek information advantages, threat forces are doing the same. An information advantage is something to gain, protect, and exploit below and above the threshold of armed conflict.


The Army's contribution to unified action is...
Multidomain Operations
Multidomain operations are the combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders.
Army forces, as part of a joint and multinational team, employ a combined arms approach to gain and exploit...
Information Advantages
An information advantage is a condition when a force holds the initiative in terms of situational understanding, decision making, and relevant actor behavior.
All Army forces contribute to achieving information advantages by...
...executing five information activities...
...to achieve combinations of friendly and threat-focused objectives.
ENABLE
Enhance Command and Control
PROTECT
Secure Data, Information, and Networks
INFORM
Maintain Trust and Confidence
INFLUENCE
Affect Behavior of Foreign Relevant Actors
ATTACK
Affect Threat Command and Control
Guided by the principles of information advantage:
Offensively Oriented
Commander Driven
Combined Arms
Soldier Enabled

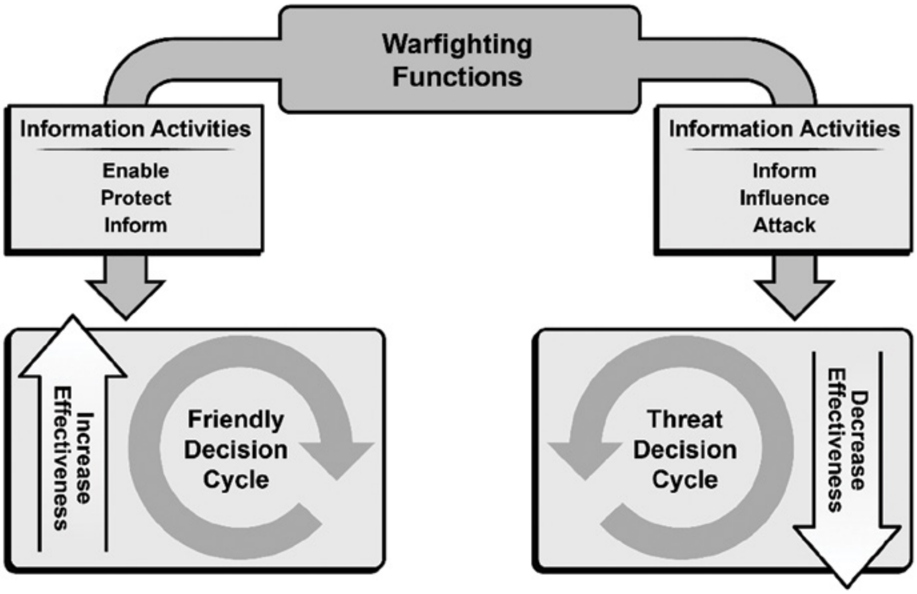
(Figure from Army Doctrine Publication 3-13, *Information*)

Figure 1. Information Advantage Logic Chart

Information Advantage Framework

ADP 3-13 provides an organizational framework to assist commanders and staffs with integrating capabilities and synchronizing actions to create and exploit information advantages. As shown in figure 1, the framework describes how Army forces integrate all relevant military capabilities by executing five information activities (enable, protect, inform, influence, attack).[11] Each information activity incorporates several tasks and subtasks from the warfighting functions to achieve various friendly and threat-based objectives. Guided by the principles of information advantage, Army leaders plan, prepare, execute, and assess information activities as part of the operations process.

The *enable* information activity includes tasks to enhance situational understanding, decision-making, and communications. The *protect* information activity includes tasks that deny threat access to friendly data and information while preserving friendly communications capabilities. The *inform* information activity includes tasks that foster informed perceptions of military operations and activities among various audiences. This activity focuses on maintaining the trust and confidence of internal (members of U.S. Army, Department of the



(Figure from Army Doctrine Publication 3-13, *Information*)

Figure 2. Information Activities Contributions to Agility

Army civilians, contractors, and family members) and external audiences (U.S. domestic and international audiences). The *influence* information activity includes tasks that affect the thinking and, ultimately, the behavior of threats and other foreign audiences. This activity focuses on reinforcing or changing how individuals and groups think, feel, and act in support of objectives. The attack information activity includes tasks that affect the threat's ability to exercise C2. This activity focuses on affecting threat data and their physical capabilities used to communicate and conduct information warfare. This includes the data and communications between automated systems, such as the communications among radars, fire control systems, and firing systems.

Information activities are interdependent. For example, the protect and inform information activities help defend the force against malign influence. The influence and attack information activities affect the threat's ability to C2 but employ different means. Synchronizing military information support operations (an influence means) to enhance the effects of a cyberspace attack (an attack means) represents a combined arms approach to degrading threat C2.

ADP 3-13 illustrates how combining and executing all the information activities to achieve both friendly and threat-focus objectives contributes to agility and the ability to understand, decide, and act more effectively than the threat. As shown in figure 2, the enable and protect information activities increase the effectiveness of the friendly decision cycle.[12] The influence and attack information activities decrease the effectiveness of the threat's decision cycle. The inform information activity is used to both enhance friendly C2 and to degrade the threats decision cycle. The combined effects of enhancing the friendly decision cycle while degrading the threats create a significant information advantage for Army forces.

Principles of Information Advantage

To help guide the thinking about the use of information and the employment of capabilities to create information advantages, ADP 3-13 introduces four principles (see figure 3).[13] The first principle—offensively oriented—is focused on initiative. Any information advantage not sought or actively defended is potentially ceded to the threat. Army leaders maintain an offensive mindset and anticipate events in pursuit of various information advantages. The combined arms principle is tied to the idea that all military activities have inherent informational effects and that all military capabilities can be employed for information advantage. Army leaders combine available organic, joint, interagency, and multinational capabilities in complementary and reinforcing ways to enable C2, protect information and networks, inform audiences, influence threats and other relevant actors, and attack threat C2.

The third principle—commander driven—is related to the idea that information is central to all activity Army forces undertake. Therefore, commanders must understand information and thoughtfully integrate it into operations through the command and control, fires, maneuver, protection, and sustainment warfighting functions during planning. Commanders think of information as a resource to achieve situational understanding, a tool to induce ambiguity and uncertainty in the threat, and the primary means to direct Army forces. Commanders direct the use of information and capabilities to penetrate threat decision-making processes, exploit information dependencies, achieve surprise, and disrupt the threat from within.

Finally, all soldiers have a role in gaining and exploiting information advantages, which is the focus of the fourth principle. All soldiers must protect information. Considerations such as operations security, physical security, noise and light discipline, and electromagnetic emissions control apply to everyone in a formation. Every soldier consumes, communicates, and relies on information to accomplish the mission. Soldiers must retain their digital literacy and readiness as they operate various information systems essential to communications. As representatives of the U.S. Army and the United States, soldiers understand that their presence, posture, and actions always communicate a message open to interpretation. High visibility offers great opportunity as well as potential risk. Effective soldiers at all levels understand the impact that their actions and messages communicate—and that all their activities communicate a message to some audience. This requires all soldiers to understand the broader purpose of operations. It also requires practicing operations security and disciplined communication through all forms of media—including personal media accounts—both in operations and while at home station.

Warfighting Function Contributions

A significant difference from past doctrine is the idea that all military capabilities can be employed for an information advantage—not just a select list of information-related capabilities synchronized with each other as part of information operations.[14] The information advantage framework is based on the idea that information is essential to all warfighting functions, and all warfighting functions can contribute to friendly or threat-focused information advantages. Based on this understanding, the Army did not establish an information warfighting function.[15] Additionally, because of the disparate nature of capabilities and multiple tasks used to create information advantages, ADP 3-13 does not assign a single staff section overall responsible for information advantage; rather, it assigns a staff lead for each activity and identifies staff leads for each task within each information activity.[16]

Offensively oriented—seize and exploit the initiative to create, protect, and exploit information advantages in all domains.

Combined arms— integrate all available Army, joint, interagency, and multinational capabilities in pursuit of information advantages.

Commander driven—visualize and describe the deliberate integration of information to create maximum effects.

Soldier enabled—all soldiers have a role in collecting, assessing, processing, communicating, and protecting information.

(Figure by authors; information from Army Doctrine Publication 3-13, *Information*)

Figure 3. Principles of Information Advantage

Information activities organize various tasks and capabilities from the six warfighting functions (C2, intelligence, movement and maneuver, fires, protection, and sustainment). The C2 *warfighting function* directly contributes to the enable information activity. The entire C2 system (people, processes, networks, and command posts) is designed to support commanders in their abilities to understand, visualize, describe, direct, lead, and assess faster and more effectively than their opponents.

The *intelligence warfighting* function contributes to the integration of all the information activities by providing relevant information and intelligence. It directly contributes to the enable information activity by providing information and intelligence for situational understanding that informs decision-making concerning all aspects of operations. The *movement and maneuver warfighting function* contributes to the enable, protect, influence, and attack information activities. Through reconnaissance, forces gain information on the enemy and terrain facilitating friendly decision-making. Security operations protect friendly information and

C2 nodes. The positioning and maneuver of forces signals intent, demonstrate capability, and drive tempo that influence threats and assure partners. Raids and other attacks contribute to the capture or destruction of enemy C2 systems and infrastructure. The *fires warfighting function* contributes to the protect, influence, and attack information activities. The delivery of fires ranging from surface to surface to cyberspace and electromatic attacks can protect friendly data and information, influence threats, and affect threat C2. Several tasks within the *protection warfighting function* directly contribute to the protect information activity to include survivability, air and missile defense support, electromagnetic protection, operations security, and cybersecurity and defense. The *sustainment warfighting function* contributes to all information activities by ensuring the friendly force is healthy, manned, equipped, maintained, and supplied. Sustainment activities also contribute to the influence information activity. Providing sustainment to relevant actors can reinforce or change their behavior. The position of sustainment forces and their activities can contribute to both deception and the communication of a will to fight.

Way Ahead

In his foreword, Lt. Gen. Milford H. Beagle Jr. writes, "ADP 3-13 provides the intellectual underpinnings that describe how Army forces will gain, protect, and exploit information advantages. But doctrine is only the beginning. The hard work begins when we incorporate these ideas into leader development, education, and training. As leaders, it is our obligation to study, understand, and implement the doctrine in ADP 3-13."[17] The publication of ADP 3-13 is just the start of a sustained education campaign from the Combined Arms Center.

As with FM 3-0, the Combined Arms Doctrine Directorate is developing a series of products to help soldiers understand the new doctrine. Articles, videos, and podcasts devoted to ADP 3-13 are in the works and will be announced via the Combined Arms Doctrine Directorate's social media channels. The team will also work closely with the centers of excellence, Army University, and the combat training centers to ensure this information is incorporated into professional military education and training. Mobile training teams will also visit select installations and organizations to further integrate the ideas outlined in the manual. ■

Notes

Epigraph. Army Doctrine Publication (ADP) 3-13, foreword to *Information* (Washington, DC: U.S. Government Publishing Office [GPO], 2023).

[1] Ibid., 1-1. Data and information are related but are not the same. ADP 3-13 defines data as "any signal or observation from the environment." Information is defined as "data in context that a receiver (human or automated) assigns meaning."

[2] Jay Luvaas, ed. and trans., *Frederick the Great on the Art of War* (Boston: Da Capo Press, 1999), 334.

[3] General Staff, Chief of Staff of the U.S. Army, *Field Service Regulations* (Washington, DC: U.S. Government Printing Office, 1905), 38–48.

[4] Field Manual (FM) 100-6, *Information Operations* (Washington, DC: U.S. Government Printing Office, 1996), iii–vi.

[5] FM 3-0, *Operations* (Washington, DC: U.S. GPO, 2022), 3-1. The 2022 edition of FM 3-0 formally established multidomain operations as the Army's operational concept. It describes the tenets and imperatives that guide Army forces in competition below armed conflict, crisis, and armed conflict.

[6] Ibid., 1-3.

[7] ADP 3-13, *Information*, 2-3.

[8] Ibid., 1-8.

[9] Ibid., 2-3.

[10] Ibid.

[11] Ibid., viii.

[12] Ibid., 2-12.

[13] Ibid., 2-14–2-15.

[14] Based on changes to joint information doctrine, Army doctrine no longer use the terms information operations, information-related capabilities, or information superiority.

[15] Change 1 to Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: U.S. GPO, 2017), added information to the joint functions (command and control, intelligence, fires, movement and maneuver, protection, and sustainment) in 2017. JP 3-04, *Information in Joint Operations* (Washington, DC: U.S. GPO, 2022), expands doctrine on the joint information function. JP 3-04 describes the joint information function as the management and application of information to change or maintain perceptions, attitudes, and other drivers of behavior, and to support human and automated decision-making. Combined with the other joint functions the information joint function helps joint force commanders and staffs effectively use information to create information advantages and achieve objectives.

[16] ADP 3-13 highlights both the chief of staff (executive officer) and G-3 (S-3) as having responsibilities for overall integration and synchronization of information activities. The chief of staff ensures staff integration where the G-3, as operations officer, ensures information activities are integrated and synchronized into the concept of operations in accordance with the commander's intent and guidance.

[17] ADP 3-13, *Information*, foreword.