AIR FORCE DOCTRINE PUBLICATION 3-13

INFORMATION IN AIR FORCE OPERATIONS



U.S. AIR FORCE

01 May 2026

Air Force Doctrine Publication 3-13, *Information in Air Force Operations*

Table of Contents

Foreword i
Chapter 1: INTRODUCTION TO INFORMATION IN AIR FORCE OPERATIONS 1
- **INFORMATION ENVIRONMENT** 1
- **INFORMATION FUNDAMENTALS** 2
- **OIE ACROSS THE COMPETITION CONTINUUM** 4
- **CAMPAIGNS AND OPERATIONS** 5
- **POLICY AND LEGAL CONSIDERATIONS** 8

Chapter 2: CAPABILITIES, OPERATIONS, AND ACTIVITIES FOR LEVERAGING INFORMATION 9
- **CAPABILITIES** 9
- **OPERATIONS** 10
- **ACTIVITIES** 12

Chapter 3: COMMAND AND CONTROL 17
Chapter 4: INFORMATION PLANNING, EXECUTION, AND ASSESSMENT 21
- **PLANNING** 21
- **EXECUTION** 27
- **ASSESSMENT** 28

References 31

FOREWORD

To deter, compete, and win across the competition continuum, Airmen should advance solutions that enable operations in highly contested environments. Broadly, the joint force's approach to meet this challenge is encapsulated in joint all-domain operations (JADO). Together with combined joint all-domain command and control (CJADC2), JADO provides joint force commanders (JFC) the means to integrate, synchronize, and deconflict the convergence of effects across all domains to achieve operational advantage. The joint force cannot only rely on force. To support achieving the commander's objectives, the joint force should also leverage the joint function of information through activities that inform audiences, influence foreign relevant actors, and attack and exploit information, information networks, and information systems.

AFDP 3-13, *Information in Air Force Operations,* is firmly rooted in the past but also looks to the future, adapting where needed to ensure continued utility and efficacy for the challenges to come. Operations in the Information Environment (OIE) encompass a wide range of informational capabilities that United States Air Force (USAF) information planners can leverage to affect relevant actor perceptions and help achieve JFC objectives, while acknowledging OIE are not independent military actions. Rather, the USAF conducts and supports OIE by planning, integrating, and employing information capabilities to create desired effects and influence relevant actor decisions.

Airmen should be trained to plan operations in a distributed or decentralized manner and execute the mission when isolated from higher echelons in distributed environments. Airmen at all levels should be comfortable making decisions and operating based on the commander's intent and the principles of mission command.

CHAPTER 1: INTRODUCTION TO INFORMATION IN AIR FORCE OPERATIONS

INFORMATION ENVIRONMENT

The information environment (IE) is a complex and ever-present reality, comprising the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that shape how both humans and automated systems derive meaning from and act on information. Joint force operations are increasingly interconnected and conducted within this highly contested environment, where an adversary's manipulation of information can limit friendly freedom of maneuver and erode American influence. The joint force plans and operates in the physical domains of land, maritime, air, and space, as well as in the IE and the electromagnetic spectrum (EMS). Each JFC's operational environment (OE) is defined by the conditions, circumstances, and influences of the physical domains, the IE, and the EMS that affect the employment of military capabilities and influence command decisions.

The air component, through its inherent attributes of speed, range, and flexibility, provides the joint force commander (JFC) with unique capabilities to conduct operations in, through, and from the air to affect the cognitive and physical aspects of the IE. The integrated employment of air component information capabilities with other joint force operations and activities is essential to influencing adversary decision-making, protecting friendly information, and achieving information advantage in any OE.

Cognitive aspects include how information is transmitted, received, understood, and responded to or acted on by members of the joint force. Many factors, including culture, beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies, influence the cognitive dimension, whether the focus is on an individual or a collective.

Physical aspects are comprised of:

- Command and control (C2) systems and facilities, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects.
- People, newspapers, books, microwave towers, computer devices, servers, smart phones, and any other objects that are subject to empirical measurement.
- Diverse military or national systems and processes connected across national, economic, geopolitical, and geographical boundaries.

Information is data in context that a receiver assigns meaning. Receivers include humans and automated systems, each may acquire information in a variety of ways (e.g., spoken, written words, observation, or other sensing mechanisms). Humans use information to understand, make decisions, and communicate. Automated systems use information to support decision-making, control their functions, or control the behavior or functions of other systems. Humans and automated systems share information to establish a common understanding and to inform, influence, or direct others' behavior.

Information (as a joint function) encompasses the management and application of information to support the achievement of objectives; it is the deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired relevant actor behaviors, and to support human and automated decision-making.[1] When this function is applied effectively, the joint force can achieve a distinct operational edge. **Informational power** is the ability to use information to support the achievement of objectives and gain an informational advantage. The essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of objectives. Information advantage is the operational advantage gained through the joint force's use of information for decision-making and its ability to leverage information to create effects on the IE.[2]

The Department of War (DoW), in coordination with other United States Government departments and agencies, supports the informational instrument of national power by using information to influence how humans or systems behave or function.[3]

Operations in the information environment are military actions involving the integrated employment of joint information forces to affect drivers of behavior by forming audiences, influencing relevant foreign actors, attacking and exploiting relevant actor information, information networks, and information systems, and protecting friendly information, information networks, and information systems.[4]

Central to the execution of these operations is understanding who or what to influence, attack, or protect. **Relevant actors** are individuals, groups, populations, or automated systems whose capabilities or behaviors have the potential to affect the success of a campaign, operation, or tactical action[5]. Relevant actors may include:

- ✪ Adversary political leadership, military forces, allies/partners, or general populations.
- ✪ Third parties whose support can significantly affect joint force success.

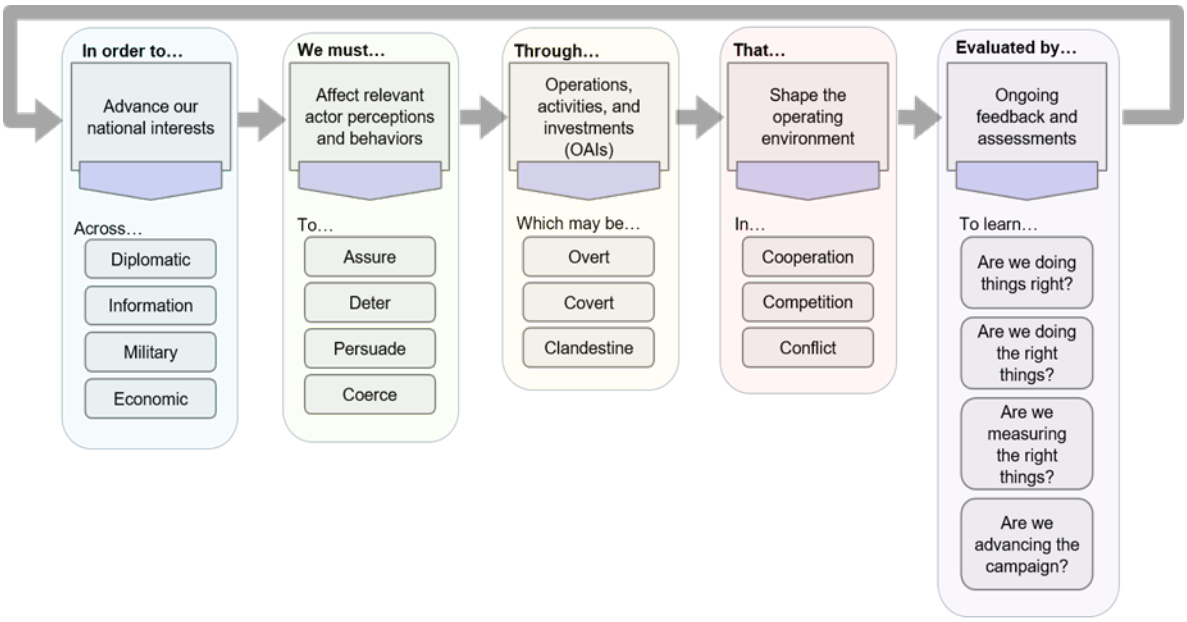
INFORMATION FUNDAMENTALS

Many United States Air Force (USAF) activities, from words and images posted on social media to the presence of an armed aircraft on the ramp can communicate a message or intent leveraged to support the achievement of JFC objectives. Recognizing its criticality in joint operations, the 2018 update to Joint Publication (JP) 3-0, *Joint Operations*, introduced information as the seventh joint function. The information function encompasses the management and application of information, as well as its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors, and to support human and automated

[1] See JP 3-0, *Joint Campaigns and Operations*, for additional information.
[2] See JP 3-04, *Information in Joint Operations*, for additional information.
[3] See JP 3-04, *Information in Joint Operations,* for additional information.
[4] See JP 3-0, *Joint Campaigns and Operations,* and JP 3-04, *Information in Joint Operations,* for additional information.
[5] See JP 3-04, *Information in Joint Operations,* for additional information.

decision-making.[6] Therefore, the purpose of Operations in the Information Environment (OIE) is to shape perceptions and behaviors that advance friendly objectives. The USAF leverages the range of information capabilities by:

- Informing, engaging, or involving relevant actors.
- Influencing foreign relevant actors.
- Attacking, exploiting, and denying relevant actor information, information networks, and information systems.
- Protecting friendly information, information networks, and information systems.



Context for Operations in the Information Environment

The Context for OIE figure illustrates the application of information as discussed in this publication. The ability to influence relevant actors' perceptions and behaviors is vital to advancing US national interests through both military operations and whole of government (diplomatic, information, military, and economic [DIME]) efforts. This occurs through operations, activities, and investments (OAIs) that may be overt or covert. The intent of those OAIs is to shape the OE across the competition continuum.[7] These OAIs are evaluated through ongoing feedback and assessment mechanisms that enable the calibration and refinement of future strategic approaches.

OIE integrates kinetic and non-kinetic capabilities across the competition continuum to produce lethal or nonlethal effects. The OIE planning and execution process begins with the commander's operational design, which guides planners as they coordinate, integrate, and synchronize the employment of information capabilities with other

[6] See JP 3-0, *Joint Campaigns and Operations*, for additional information.
[7] See Joint Doctrine Note (JDN) 1-22, *Joint Force in Strategic Competition,* for additional information.

whole-of-government efforts to leverage informational power. OIE planning should not be conducted in isolation or as an afterthought to more “traditional” military operations. Rather, OIE should be integrated into existing air component and joint planning processes to design air component operations directly around its effects.

OIE necessitates target development, drives intelligence requirements, and matches actions with intended messages. Through planning, execution, and assessment processes, OIE provides the means to employ the right capabilities that generate desired effects to achieve combatant commander (CCDR) objectives while supporting the commander’s communication synchronization (CCS) strategy. Through the CCS, JFC's integrate information-focused activities with other lines of effort and operations. It synchronizes themes, messages, images, and actions to support JFC objectives. Similarly, the air component commander should conduct their own CCS program to ensure alignment across the staff and assigned or attached units. Commander's intent should be reflected in every staff product.

The USAF embeds OIE expertise within the air component commander’s staff, or the JFC’s staff, to facilitate information capability integration and synchronize the effects of informational OAIs. This expertise is needed to address component objectives and properly apply information capabilities to achieve desired effects. Similarly, the USAF may augment other staffs with OIE expertise to assist in tasking information capabilities in theater and integrating global capabilities and effects. USAF information planners operating in theater are assigned or attached to the air component commander and are typically placed on the commander’s staff or an air expeditionary task force (AETF). Within an AETF, information forces are normally assigned to an air expeditionary wing, group, or squadron.

OIE ACROSS THE COMPETITION CONTINUUM

Crises can occur in many forms across the continuum. OIE plays a key role across the entire continuum to support the creation, maintenance, and exploitation of overall joint force advantage. The OIE Across the Competition Continuum figure presents examples of OIE activities across the competition continuum that can be used to achieve and leverage information advantage through integrated and coordinated campaign activities. Employed in coordination and concert with operations across all warfighting domains, leveraging information through OIE can support and enhance operations, and may be required to achieve operational objectives in restricted, contested, or politically sensitive areas where destructive physical force is constrained or insufficient.

For example, a commander conducting humanitarian assistance airdrop operations may aim to secure host nation or regional cooperation by integrating civil military operations (CMO), public affairs (PA) activities, and information activities to coordinate drop zones and facilitate safe distribution of food and medicine among the local populace. Similarly, a commander may direct information forces to conduct OIE during a major combat operation to influence regional perceptions by integrating electromagnetic spectrum operations (EMSO) and cyberspace operations with other capabilities to achieve effects against key targets.



OIE Across the Competition Continuum

–Dr. Sandeep S. Mulgund. and Gen Mark D. Kelly*, Air & Space Power Journal,* "Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment."

CAMPAIGNS AND OPERATIONS

A key to shaping relevant actor perceptions and behaviors across the competition continuum is tied to the execution of deliberate, long-term combatant command (CCMD) campaigns. Campaigns are planned and designed to comprehensively and coherently link steady-state activities and contingency operations within a unifying framework consisting of a series of related OAIs. Campaign activities focus on a CCMD's day-to-day activities to create effects through the conduct of operations, military engagement, security cooperation (SC), deterrence, and other shaping or preventive activities.[8] The Campaign-level Informational Ends, Ways, and Means table lists campaign ends, ways, and means from an informational perspective.

[8] See JP 5-0, *Joint Planning,* for additional information.

Campaign-level Informational Ends, Ways, and Means	
Informational ends should shape the operational environment to advance JFC campaign objectives across the competition continuum by leveraging information to affect relevant actor perceptions and behaviors.	
Informational Ends	✪ Increased understanding and trust with domestic and international audiences in the purpose of and approach to component activities. ✪ Erosion of adversary confidence in their capabilities, strategies, and relationships. ✪ Diminished enemy ability to observe, orient, decide, and act effectively.
Informational ways should prioritize and synchronize the execution of OAIs that integrate the use of information with other instruments of military power for strategic gain.	
Informational Ways	✪ Establish overall component narrative and key themes and allocate resources in accordance with and in support of them. ✪ Nest with support for CCMD, DoW, and DOS narratives and themes. ✪ Synchronize efforts across components and areas of responsibility with allies and mission partners. ✪ Continually reinforce the component narrative through sustained presence and engagement in the IE, proactively and in response to emergent events across the competition continuum. ✪ Assess effects in support of JFC campaign objectives and refine campaign approach.
Informational means are OAIs executed using responsive force packages that integrate informational capabilities, operations, and activities to synchronize and leverage the informational aspects of joint force capabilities and operations.	

PLANNING OPERATIONS IN THE INFORMATION ENVIRONMENT

Information planners should nest component operations within the JFC's overall campaign planning to leverage the inherent informational aspects of joint force capabilities, optimize employment of informational capabilities, and achieve informational and operational advantage. Information planners work alongside, and in coordination with, other component and functional planners through the Joint Planning Process for Air (JPPA), air tasking cycle, and other joint planning processes to achieve operational objectives. OIE planning products can include items such as synchronization matrices, PA guidance, coordinated narratives and themes, and relevant actor analyses. There is no separate OIE plan or annex within these products.

EFFECTS ON RELEVANT ACTOR BEHAVIOR

Relevant actors may be either **adversaries** or **non-adversaries**. Non-adversaries include a broad range of actors, who may be allies, partners, or neutral third parties. The

threat of using military forces and capabilities may help reinforce existing behaviors or convince an actor to modify or change the direction of their behavior. These categories combine to describe the four strategic uses of military force and capabilities to affect relevant actor behavior in support of campaign-level ends:

- **Assure** is using the military instrument of national power to demonstrate commitment and support to allies and partners. Assuring often takes the form of SC, combined exercises, and forward stationing of United States (US) forces.
- **Deter** is the prevention of undesired action by the existence of a credible threat of unacceptable counteraction or the belief that the costs of action outweigh the perceived benefits.
- **Compel** is the more complicated form of coercion since it requires precise signaling and communication through actions. It is even more dependent on an accurate assessment of the adversary's will than deterrence is. The US often compels the threat for limited ends or objectives achievable without sustained violence, occupation, or regime change.
- **Force** is using pure military strength to achieve the objective directly by subduing the enemy and imposing the will of the US. Force does not depend on the enemy's decision not to comply; rather, the enemy's choice of noncompliance is what distinguishes forcible action from coercion.[9]

OIE CONDUCTED THROUGH LEVERAGING OPERATIONS, ACTIVITIES, AND INVESTMENTS

Campaigns are executed by CCMDs through a series of OAIs that span day-to-day operations to crisis response. Commanders and planners select and design OAIs to shape the OE and advance component or CCMD objectives. Informational capabilities, operations, and activities can provide the primary means to target, shape, and influence an adversary, or be used to enable or complement other military operations by:

- Creating conditions for success (e.g., EMSO activities, offensive cyberspace operations).
- Imposing costs by concealing and obscuring the nature of joint force actions (e.g., signature management).
- Influencing relevant actor behavior through overt/covert messaging (e.g., CO, PA).
- Driving a relevant actor to expend additional resources by exposing malign activities (e.g., PA, cyberspace-enabled OIE).

Synchronizing OIE with operations and activities within individual OAIs creates reinforcing effects by optimizing the timing, tempo, scope, and purpose of each action, thereby maximizing informational and operational advantage for the joint force. The following

[9] For additional information on the strategic uses of military force, see JP 3-0, *Joint Campaigns and Operations*.

example OAIs contain inherent informational aspects that can be shaped and leveraged to assure, deter, persuade, or coerce relevant actors. OIE related OAIs may include: exercises, force posture, audience engagements, foreign military sales, SC, dynamic force employment, flexible deterrent options, show of force, crisis response, and operation plan (OPLAN) execution.

During military operations, OIE can be employed to demonstrate the intent and will behind a message. Similarly, post-employment, OIE can shape relevant actor's perceptions or interpretations of events, thereby conditioning the anticipation of subsequent action. Such a coordinated approach enables JFCs to take the initiative in the IE, rather than being reactive to adversary actions.

Such combined actions require both integration and synchronization—integration in planning and synchronization in execution, predicated on an accurate understanding of the OE. For effective integration, planners should seek complementary combinations of informational and physical effects that drive desired behavior. Synchronization in execution seeks to converge these effects with sufficient timing, tempo, scope, and intensity to achieve the desired objective. Importantly, OAIs may vary according to the relative degree and weight of combined informational and physical actions. For example, military engagement or SC activities focused purely on exposing and countering malign influence or disinformation may not require the application of physical force but rely principally on information capabilities instead.

POLICY AND LEGAL CONSIDERATIONS

As in all military operations, operational law, including the law of war, applies to OIE. Actions against military systems without consideration of collateral effects may result in legally or politically unacceptable effects on the civilian population. Similarly, rules of engagement (ROE) in an area of responsibility (AOR) may further constrain the integrated employment of information capabilities. Commanders, in coordination with staff judge advocates, should request mission-specific ROE from the appropriate senior authority (e.g., CCDRs, Secretary of War [SecWar]) as required. Since the operational complexity of applying information capabilities may involve multiple approval authorities and complex laws, principles, and policies, legal advisors should be included early in OIE planning.[10]

[10] See AFDP 3-84, *Legal Support,* for additional information.

CHAPTER 2: CAPABILITIES, OPERATIONS, AND ACTIVITIES FOR LEVERAGING INFORMATION

OIE encompasses a wide range of capabilities, operations, and activities that information planners can use to leverage information to affect relevant actor perceptions and achieve JFC objectives. These military actions are not conducted independently; rather, they are integrated to create desired effects and influence the decisions of relevant actors.



CAPABILITIES

OIE are driven by a range of integrated capabilities designed to leverage information to influence adversary perceptions, reduce their effectiveness, and ultimately degrade their ability to achieve objectives.

UNITED STATES AIR FORCE INFORMATION FORCES

USAF information forces are specifically trained to apply social science principles and fundamentals to shape the perceptions and behavior of relevant actors. Understanding the cognitive factors related to adversary decision-making, the information they use, and how they receive and send information enables targeting relevant actor perceptions, attitudes, and behaviors. To this end, USAF information forces conduct behavioral influence analysis, leveraging the principles of psychological operations (PSYOPS), operations security (OPSEC), and military deception (MILDEC) to influence relevant actors and gain an understanding of decision-maker behavior.

INTELLIGENCE SUPPORT

OIE planning, execution, and assessment rely heavily on tailored intelligence to validate measures of effectiveness (MOE) and answer a commander's critical information requirements (CCIR). Each information capability relies on intelligence support for independent operations. To enable integrated employment, commanders and planners should anticipate additional intelligence requirements and resources. Interaction between information planners, the air component commander's operations directorate, and the air operations center's (AOC's) combat operations division enables detailed coordination of intelligence and intelligence, surveillance, and reconnaissance (ISR). Similarly, information planners continually coordinate with the air component commander's

intelligence directorate or the AOC's ISR division (ISRD) for the intelligence aspect of ISR operations.

OIE requires the timely coordination of intelligence to establish baseline characterizations of the IE, analyze current intelligence for nuanced OIE application, develop detailed targeting packages, conduct complex effects assessments, and aid relevant actor/target audience analysis. To meet such requirements, the air component commander should establish a dedicated intelligence integration element. In addition to the functions listed, the integration element serves as a conduit for translating and internally coordinating OIE's requirements with collection management and production cells within the ISRD.[11]

SPACE SUPPORT

One of the core competencies of military space power in the United States Space Force (USSF) is information mobility. According to the USSF, information mobility is the timely, rapid, and reliable collection and transmission of data across the range of military operations in support of tactical, operational, and strategic decision-making. Within the IE, information mobility includes point-to-point communications, broadcast communications, long-haul communication links, protected strategic communications, machine-to-machine interfaces, position, navigation, and timing (PNT), nuclear detonation detection, missile warning, and intelligence, surveillance, and reconnaissance. Information mobility is highly dependent on the IE to support specific capabilities.

To project airpower globally, the USAF requires information collection and data transportation capabilities USSF is uniquely postured to deliver. Information mobility extends lines of communication into the most remote areas. Among other military users, the USAF capitalizes on the ability to share information beyond line of sight to synchronize power projection on a global scale across all warfighting domains.[12]

OPERATIONS

To achieve overarching objectives, a variety of operations are executed to influence the IE and the decisions of relevant actors. These operations include Civil-Military Operations, cyberspace operations, EMSO, information support operations, and weather operations. Each of these operations, whether conducted independently or in concert, contributes to the broader military effort.

CIVIL-MILITARY OPERATIONS

During CMO, military personnel may perform functions normally provided by the local government, placing them in direct contact with civilian populations. Because of this level of interaction, the CMO significantly affects the local populace's perceptions and relations with the military, as they work with governmental and non-governmental organizations. CMO personnel engage primarily with friendly and neutral populations but may also be used to influence adversaries.

[11] See AFDP 2-0, *Intelligence,* for additional information.
[12] See Space Capstone Publication, *Spacepower: Doctrine for Space Forces*, for additional information.

CMOs are of particular interest to information planners. They may enable broader OIE objectives and can ensure consistency with the CCS. Target audience engagements conducted during CMO are an important contributor to OIE and aid the accomplishment of military objectives by conveying key messages where they are needed. Engagements permit direct interface with specific audiences through traditional methods of information exchange. Generally, these operations involve military personnel and key leaders, as well as larger populations, both military and civilian. CMO engagements may be in person or virtual (e.g., via teleconference), impromptu encounters (e.g., during disaster relief), or planned events (e.g., military exercises).

While CMO activities occur in conjunction with other military actions, they may present the only engagement opportunity with certain audiences. Forces involved in engagement opportunities, such as medical, engineering, or security assistance, may not have a habitual working relationship with OIE efforts. As such, information planners should proactively coordinate with CMO activities.[13]

CYBERSPACE OPERATIONS

Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. During joint operations, information planners may recommend using specific cyberspace capabilities to create integrated effects across all domains. When employed in support of OIE, cyberspace operations include offensive and defensive capabilities exercised through cyberspace, as an integrated aspect of a larger effort to affect the IE. Cyberspace operations may be employed independently or in conjunction with other capabilities to create effects in the adversary's battle space and ensure freedom of maneuver in the IE.[14]

ELECTROMAGNETIC SPECTRUM OPERATIONS

EMSO contributes to the success of OIE by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EMS while protecting friendly freedom of action. During combat operations, the air component commander may be designated as electromagnetic attack control authority and jamming control authority for the employment of electronic warfare (EW) assets and establishment of associated policies and processes in the joint operations area. To negate an adversary's effective use of the EMS, the air component commander will typically stand up a non-kinetic team employing electronic attack (EA) to degrade, neutralize, or destroy the adversary's combat capability. To ensure EMSO and information capabilities complement one another, information planners should coordinate with the non-kinetic duty officer.[15] [16]

---

[13] See JP 3-57, *Civil-Military Operations,* for additional information.
[14] See AFDP 3-12, *Cyberspace Operations,* for additional information.
[15] For additional information on cyberspace-enabled EMSO, see JP 3-12, *Joint Cyberspace Operations*.
[16] See JP 3-85, *Joint Electromagnetic Spectrum Operations,* and AFDP 3-85*, Electromagnetic Spectrum Operations* for additional information.

PSYCHOLOGICAL OPERATIONS

PSYOPS aim to impact foreign governments, organizations, groups, and individuals in a manner favorable to operational objectives by conveying selected information and messages to foreign audiences to influence their emotions, motives, thought processes, and reasoning. Information support operations are one of the principal activities conducted by information forces assigned to a CCMD or an Air Component Command. They may involve counterpropaganda to delegitimize the adversary OIE, thereby reinforcing or, conversely, inducing change in foreign attitudes and behavior. Information support operations at the CCMD-level usually reside in the CCMD J39 directorate or in a military information support task force (MISTF), which includes an information planner as a member of the joint information cell or joint information staff.

The final approval authority for information support themes typically resides at the national level but is normally delegated to a CCDR or JFC during times of crisis. At the component level, information planners may be part of the joint force air component commander's (JFACC) staff or may be retained as part of the COMAFFOR's staff. AFFOR information planners should represent air component commander requirements to the JFC's information planning staff. Additionally, for target audience engagements, information planners should closely coordinate with MILDEC, OPSEC, PA, and other information capability representatives and liaisons to ensure the integrity and consistency of themes, messages, images, and actions.[17]

WEATHER OPERATIONS

Weather operations identify opportunities for maneuver space in the IE by providing actionable information on the current and future state of the environment. Weather personnel, either through reachback or by being embedded with operational units, C2 facilities, and intelligence centers, use tailored weather information to advise decision makers on how to preserve friendly freedom of action, predict adversary behavior based on environmental conditions, and influence adversary behavior through support to MILDEC activities.[18]

ACTIVITIES

A range of activities are undertaken to control information and shape perceptions within the IE. These activities include MILDEC, OPSEC, and PA together. These coordinated activities are essential for achieving mission objectives while protecting friendly forces and maintaining credibility.

MILITARY DECEPTION

MILDEC is an action deliberately executed to mislead adversary military, paramilitary, or violent extremist organization decision-makers, thereby causing the adversary to take specific actions (or fail to take actions) that will contribute to the accomplishment of the

[17] See JP 3-53, *Joint Military Information Support Operations,* for additional information.
[18] See JP 3-04, *Information in Joint Operations*, and JP 3-59*, Meteorological and Oceanographic Operations,* for additional information.

friendly mission.[19] MILDEC is one of the principal activities conducted by USAF information forces. Deception activities can span all levels of war and can simultaneously include both offensive and defensive components. To maximize the potential for achieving positions of relative advantage, planning for MILDEC should be integrated into the early phases of an operation. MILDEC can impede an adversary's use of time, combat power, or the IE.

Effects related to use of time may include:

- Decreased effectiveness and timeliness of adversary decisions by causing a state of "analysis paralysis."
- Increased friendly decision advantage by causing an adversary to perceive that time available to make a decision is compressed.
- Increased adversary costs and resource consumption by driving an adversary to waste time pursuing unproductive ends.

Effects related to use of combat power may include:

- Reduced combat effectiveness caused by errant dispersal or concentration of adversary forces.
- Increased friendly freedom of action through effective concealment of joint force intent and plans.

In the IE, MILDEC can disrupt an adversary's pre-planned narrative or disinformation related to joint force activities.

A particular adversary may leverage the IE in various ways. To drive desired behavior by affecting an adversary's information systems, processes, and capabilities, MILDEC planners require specific analysis to generate a sufficiently detailed understanding of how the IE supports decision makers and decision processes. The Military Deception Process figure shows a simplified representation of the MILDEC planning process. It begins with defining how a deception activity will materially contribute to mission accomplishment. The deception objective establishes desired adversary behaviors or responses that contribute to those goals. From there, the deception story, required perceptions, and deception events establish the desired observables and friendly force actions that should shape adversary behavior as intended.

[19] For additional information on current policy, responsibilities, and direction for conducting deception activities to include joint MILDEC, see JP 3-54, *Joint Doctrine for Military Deception,* and (U) DoDI S-3604.01, *DoD Deception Activities (Classified)*, 18 September 2019.

Deception goal	• How deception activity contributes to accomplishment of the mission
Deception objective *"do"*	• What the deception will cause the adversary to do or not do • Expressed in terms of adversary action or inaction
Deception story	• Friendly force actions to be portrayed to depict what we want the adversary to believe so as to act in the desired manner • Should read like adversary's own intelligence estimate concerning friendly commander's intentions and actions
Required perceptions *"think"*	• Conclusions, official estimates, and assumptions the deception target uses in his assessment and decision-making • What friendly commander wants adversary to believe based on their observations or receipt of information about friendly forces
Deception events *"see"*	• Activities or actions executed by friendly or controlled elements to create what the deceiver wants to the adversary to see • Requires determining what to hide ("dissimulate") and what to show ("simulate")

MILITARY DECEPTION PROCESS

–Derived from JP 3-54, *Joint Doctrine for Military Deception*

Each information capability plays a part in successful MILDEC credibility over time. As such, information planners facilitate close coordination with information support activities, OPSEC, PA, and CCS personnel within the joint information cell or staff. Importantly, though information support activities, PA, and CCS activities may share a common specific audience with MILDEC, only MILDEC actions are designed to mislead. There is a delicate balance between successful deception efforts and media access to ongoing operations. Though necessary as part of an overall OIE strategy, media access may compromise deception efforts if not properly planned and coordinated. Conversely, MILDEC must not intentionally target or mislead the US public. When deception activities are potentially visible to the US public, they should be closely coordinated with PA operations to ensure they do not compromise operational considerations or diminish US credibility. Due to the sensitive nature of MILDEC plans and objectives, a strict need-to-know policy is essential. Additionally, approval authorities for conducting MILDEC actions are typically at the JFC-level or above. Staffing actions for approval may require sufficient lead time.

OPERATIONS SECURITY

The OPSEC process is a systematic method used to identify, control, and protect critical information and subsequently analyze friendly actions associated with military operations and other activities.[20] Within the USAF, OPSEC is one of the principal activities conducted by information operations forces. OPSEC denies adversaries critical information and observable indicators about friendly forces and intentions. OPSEC identifies any

[20] See JP 3-55, *Joint Operations Security,* for additional information.

unclassified activity or information that, when analyzed with other activities and information, may reveal protected friendly operations, information, or activities. To ensure military personnel and media are aware of non-releasable information, a critical information and indicators list (CIIL) should be developed and continuously updated in peacetime and in conflict.

Information planners maintain situational awareness of friendly information and actions to assist other AOC planners with incorporating OPSEC considerations during the planning process. When vulnerabilities are identified, other information capabilities can be used to ensure OPSEC requirements are satisfied.

SIGNATURE MANAGEMENT

Signature management is a process used to profile an installation's (including tenant and associate units) day-to-day observable activities and operational trends. Though wings and installations do not directly plan or execute MILDEC on their own, they may be tasked to support an operational OPSEC or MILDEC plan. Accordingly, the installation's signature management officer (SMO) should have a solid grasp of the installation's signatures gained through the base profiling process, a deliberate effort to identify functional areas, their associated observables, signatures, and indicators, and how they contribute to the installation's overall signature profile. When an air component commander's MILDEC plan requires USAF wings and installations to present specific observable activities, the air component commander's MILDEC planner should determine the actions required by the supporting unit(s) and communicate those requirements to the wing or installation SMO.

PUBLIC AFFAIRS

PA, defined as communication activities with external and internal audiences, is the USAF's primary public communication capability. PA provides the air component commander with an open and credible means to reach key allied, neutral, and adversary public audiences through the carefully coordinated release of truthful and appropriately contextualized information and targeted public engagement activities. Truth is foundational to the credibility of all PA operations, as is adherence to the DoW principles of information of "maximum disclosure, minimum delay". As such, timely and agile dissemination is essential to achieve desired information effects. Likewise, the rapid declassification of relevant operational information can be used to deter adversaries, shape their perceptions, assure allies, and build and sustain public support.

PA plays a significant role across the competition continuum and is often one of the most prominent information capabilities employed during stability operations and operations preceding crisis or conflict. PA is a fundamental aspect of the entire planning process. Through the intentional and coordinated release of operational information, PA can foster or enhance support for military operations, deter an adversary, shape their perceptions and behavior, avoid conflict, and counter adversary propaganda and disinformation. Though PA activities cannot provide false or misleading information, PA operations should be coordinated with the employment of other information capabilities to lessen the chance of compromise.

Counterpropaganda. Counterpropaganda operations involve efforts to negate, neutralize, or diminish the effects of, or gain an advantage from, adversary propaganda. Timing and initiative in the IE are vital to defeating propaganda, particularly when addressing incidents involving collateral damage or friendly force mistakes. Rapidly providing accurate, available information to the public may thwart adversary attempts to exploit friendly actions for propaganda purposes.

Counterpropaganda operations are normally conducted through PA channels. However, several other information capabilities can support that activity. Intelligence professionals can provide information or imagery for rapid declassification to refute adversary claims. EW or cyberspace operations can deny adversary use of propaganda outlets. Information support operations can amplify key themes and messages among specific foreign audiences, some of which may be inaccessible by PA operations. Operations Research analysts and information planners may also assist PA by conducting propaganda analysis.

Combat Camera. Combat Camera (COMCAM) is a specialized visual documentation capability for support of strategic and operational objectives during combat operations, crises, contingencies, joint exercises, humanitarian operations, and other DoW involved events of significant national interest. COMCAM acquires, processes, and distributes classified and unclassified still and motion imagery. Although COMCAM may support other operations, PA is responsible for oversight of COMCAM activities. COMCAM teams (including fully certified/qualified aircrew members) are uniquely organized, trained, and equipped for rapid global response to document air and ground operations and provide visual products for use by information planners. Commanders use these products for communication needs, operational planning, decision-making, operational assessment, and to satisfy requirements for historical documentation of operations. COMCAM is intended for use in situations involving rapid global response, aerial imagery, special operations forces, or combat maneuver and capability. For situations that do not meet these criteria, or where COMCAM capacity is insufficient, traditional visual information resources may be used instead.[21]

[21] For additional information on PA, Counterpropaganda, or COMCAM, see AFDP 3-61, *Public Affairs Operations*.

CHAPTER 3: COMMAND AND CONTROL

Joint information forces and capabilities for OIE are assigned to CCDRs for employment in support of worldwide operations. Commonly, joint information forces conduct OIE through support relationships between CCMDs to aid joint operations across geographic AORs. Supporting C2 structures established to integrate joint information forces and capabilities should be robust enough to account for varied command relationships and operational areas.

When a theater requests information capabilities from organizations with global responsibilities, the SecWar may specify a command relationship between CCDRs, normally a support relationship. These support relationships fall into four categories: general, mutual, direct, and close support. For information capabilities providing effects via a support relationship, it is important that both supported and supporting commanders' requirements be documented by the establishing directive. The establishing directive should specify the purpose of the support relationship, the desired effect(s), and the scope of the action(s) to be taken. Additional information includes:

- Information capabilities allocated to the supporting commander's effort.
- Time, place, level, and duration of the supporting commander's effort.
- Relative priority of the supported commander's effort.
- Degree of authorities exercised by the supported and supporting commanders over the effort, to include processes for reconciling competing requirements and expeditiously resolving emergency events, as required.

To facilitate a support relationship, there should be an appropriate level of coordination between the involved commanders. This facilitates planning for the detailed integration of information capabilities and their effects with theater operations and enables theater warfighters to coordinate directly at either the same or differing organizational levels. Where appropriate, a direct liaison authorization (DIRLAUTH) relationship should be established to enable coordination between theater and supporting information planners.

If the information effects produced by a CCMD without an AOR[22] are focused primarily on or within another CCDR's AOR, the SecWar may, through the global force management process, direct the attachment of joint information forces to the CCDR for that theater. The CCDR, in turn, normally attaches gained forces to the appropriate Service component commander. The theater air component commander is the Service component commander for USAF information forces in theater. Similarly, the JFACC can also be tasked as the functional component commander for a number of in theater information capabilities. Normally, the air component commander exercises only those OIE authorities delegated by the respective CCDR or JFC.

[22] The terms geographic (GCC) and functional (FCC) CCMDs are no longer used in joint doctrine. These terms have been replaced by either CCMDs with an AOR, or CCMDs without an AOR.

At the theater-level, the JFC designates supported and supporting components. If deemed appropriate, the CCDR or subordinate JFC may use Service component assets to integrate OIE into their planning efforts. The CCDR or subordinate JFC may designate a joint force information officer to accomplish broad OIE oversight functions. When designated, the joint force information officer heads the joint task force (JTF) information staff. USAF information planners and supporting capabilities are typically presented by the commander, Air Force forces to the CCDR. In addition to OIE support to CCDR objectives and messaging requirements, Air Force forces should also use their capabilities, tools, techniques, and activities to support component operational and informational objectives.

Coordinating Authorities

If the JFC designates the air component commander as the supported commander for OIE, the JFC may also delegate any related coordinating authorities to enable better integration of theater and global information capabilities and their effects. Because of their theater-wide perspective, ability to exercise C2 of joint information forces, and the subject-matter expertise of information planners on the AOC staff, the air component commander is well suited to coordinate operations involving numerous CCDR information capabilities. Senior information advisors on the air component commander's staff may be assigned responsibilities to coordinate or execute any delegated information authorities. Examples of current coordinating authorities include space coordinating authority, cyber coordinating authority, and counterintelligence coordinating authority.

PRESENTATION OF AIR FORCE INFORMATION FORCES

When directed, the USAF presents information planners and information forces to CCDRs to support national and theater-level OIE tasks. The information planning function for a theater air component is typically presented as a function within an AOC and/or on the air component commander's staff. USAF information planners should serve as a focal point for coordinating requirements for reachback support from information capabilities outside the theater to ensure their plans and support are integrated with joint OIE.

Within the AOC, information planners use the Air Force Planning Process (AFPP) to coordinate with OIE elements at other components, commands, and task forces. Information planners *may* be attached to the AOC's strategy division to coordinate with other AOC divisions. Alternatively, information planners *may* report directly to the AOC commander as part of a cross-cutting specialty team. In either case, such arrangements should be made deliberately and tailored to fit the particular needs of the organization or mission.

16TH AIR FORCE (16 AF)

16 AF develops, prepares, generates, and presents information forces. 16 AF provides multisource ISR, CO, EW, and information capabilities across the competition continuum. 16 AF is the principal USAF organization tasked with providing forces to conduct OIE; numerous other organizations are also tasked to do the same.

SERVICE AND FUNCTIONAL OIE RESPONSIBILITIES

Information planners and information forces on Service and functional component staffs fill critical roles needed to successfully integrate information tasks and effects into theater operations. Air component command staff and AOC staff share a common effort to support the commander's objectives and complement each other's responsibilities. The two staffs coordinate regularly to ensure consistency in focus and to deconflict their respective responsibilities and external relationships.

In general, the Service component staff coordinates planning actions at the JFC or CCDR level. In addition to internal coordination, the Service component staff coordinates with their AOC counterpart(s), component major command (MAJCOM) and numbered Air Force (NAF) staffs, other component equivalents, other CCMD staffs, and the joint staff to:

- Request joint information forces and OIE support (e.g., request for forces).
- Establish support relationships and authorities for OIE planning and information capability tasking (e.g., DIRLAUTH, EW coordinating authority).
- Facilitate deployment, bed-down, and redeployment of information forces (e.g., deployment order, time-phased force deployment data (TPFDD).
- Provide OIE inputs to strategic/campaign-level operation planning documents (e.g., campaign plans, contingency plans, OPLANs.

In contrast, the functional component (AOC or operations center [OC]) staff coordinates information planning and tasking at the JTF-level. In addition to internal AOC coordination, the staff coordinates with contacts on AETF staffs, JTF staffs, and other theater component staffs to:

- Provide input on operational planning documents (e.g., annexes/appendices, joint air operations plan [JAOP], air operations directive).
- Coordinate themes and messages with actions approvals (e.g., ROE, airspace control order), tasking orders (e.g., air/space/cyber tasking order), and targeting lists (e.g., joint integrated prioritized target list, restricted target list, no-strike list).
- Submit requirements for analytical needs (e.g., telecom studies, patterns of life).
- Develop assessment criteria (e.g., measures of performance [MOP], and MOE).

Pacific Air Force's Strategic Messaging Process

Pacific Air Force (PACAF) OIE forces are spread across multiple directorates but benefit from a deliberate process known as the **PACAF strategic message synchronization process (SMSP)**. This directs information planners to create a baseline operational messaging framework—before developing the concept of operations—using a four-step process:

1. Create messaging themes aligned with and supporting commander's intent and objectives.

2. Identify key perceptions through information and cognitive based mission analysis.

3. Synchronize activities with perceptions-led guidance and campaigns to effectively inform and influence all relevant actors.

4. Tailor message plans to maintain positive control of OAI narratives within the information environment.

Once the messaging framework is developed, a multi-disciplinary team called the **strategic messaging working group (SMWG)** refines it into a finalized plan. The SMSP is effectively controlled through the SMWG (which is co-chaired by the A5S Strategic Competition Division), PACAF/Public Affairs, and PACAF/A3/9/5 (Information Operations Team). This construct draws expertise from a wide range of AFSCs, bringing essential knowledge and capabilities to the OIE planning effort that might otherwise be lost in a more traditional process**.**

FEDERATED SUPPORT FOR OIE

Commanders and their staffs should consider leveraging other resources and capabilities available through reachback and federation to support theater OIE activities. There are many services, joint, DoW, interagency, and national organizations referenced in this publication that can provide additional support to theater OIE efforts. Though the nature of support may vary in purpose or extent, command relationships should be established and tailored to ensure support provided is sufficient and optimized to meet operational needs and objectives. Command relationships may range from nothing formal required (e.g., standard processes are sufficient) to a formal "federated" agreement. If a formal relationship is required for the purposes of planning, DIRLAUTH is usually appropriate.

CHAPTER 4: INFORMATION PLANNING, EXECUTION, AND ASSESSMENT

OIE should be incorporated throughout operational planning, execution, and assessment processes. The significant array of capabilities that can be applied along with the inherent complexity involved with integrating them necessitates extensive coordination. Though OIE requires early and extensive planning, there is no separate OIE planning process or plan within the joint planning process. Information planners should provide appropriate inputs during each step of the JPPA and the air tasking cycle, while acknowledging OIE timelines may be substantially longer than traditional operations.

PLANNING

Theater planning can help integrate specialized capabilities and effects throughout the JFC's theater campaign plan or OPLAN. For OPLANs, this is normally accomplished through the JPPA, which combines the mission activities and desired effects into a coherent plan. The result is the JAOP. The JAOP should include the integration of all allocated and assigned theater capabilities and all requests for theater support from global mission capabilities. Theater capabilities and effects derived from deployed and organic theater capabilities under the air component commander's control should be integrated into day-to-day operations through the air tasking order (ATO). The majority of JAOP development occurs within the AOC; consequently, OIE expertise should be embedded throughout the AOC. Information planners use AFPP to coordinate with functional OC to synchronize and de-conflict the development of their planning products.

Importantly, OIE is not addressed in a dedicated planning product annex. Rather, it is embedded in numerous annexes and integrated throughout. Information planners should be involved throughout product development process to ensure OIE and related informational requirements are adequately addressed.[23]

PLANNING CONSIDERATIONS

Global-Theater Integration. Many capabilities support global defense requirements and requests from multiple theaters. This requires timely de-confliction and integration with other theater operational elements. Integrating various capabilities is accomplished through deliberate coordination processes between the theater AOCs and functional OC. The employment of informational capabilities at the operational level is accomplished through tasking orders that de-conflict and integrate the full range of capabilities with theater operations. Theater planners should coordinate with functional OC to synchronize and de-conflict the ATO with functional tasking orders, such as the joint space tasking order and cyber tasking order.

Reachback Support. Reachback support may be requested to provide specific expertise or information to augment theater planning. This cooperation facilitates a comprehensive and realistic development of force requirements in support of theater plans. Likewise, OIE

[23] For additional information on the JPPA and products such as the JAOP and air operations directive, see JP 3-30, *Joint Air Operations*, and AFDP 5-0, *Planning*.

requirements should be included in CCDR's plans that support other AOR operations. Planners should also ensure deployable capabilities are included in the command's TPFDD. Integration of information capabilities is the responsibility of the supported CCDR and the respective air component commander.

Contingency vs Crisis Planning. During contingency planning, theater planners normally incorporate OIE into theater campaign plans and OPLANs. However, OIE requirements should be considered part of the overall campaign or operational plan; such requirements should not be limited to a single appendix or phase of an OPLAN. OIE planning should be embedded throughout the process to ensure enabling capabilities are appropriately integrated. Planners should ensure OIE is thoroughly addressed in a campaign support or contingency support plan's primary annex, Annex C, Operations (Appendix 3), and should coordinate with other lead planners to ensure that OIE is tied into all relevant annexes.

The time-sensitive nature of crisis planning may make it challenging to address emergent OIE requirements. Certain capabilities may need substantial lead time for coordination up to the SecWar due to their political sensitivity or because they are controlled by other national agencies, civil organizations, or even commercial entities.

Operations in the Information Environment in Phased Operations. Although OIE occurs across the entire competition continuum, understanding the sequence of operations over time is critical to effective planning. Commanders and planners often use phasing to arrange and conduct a complex operation in manageable parts. The main purpose of phasing is to integrate and synchronize related activities, thereby enhancing flexibility and unity of effort during execution. The commander determines the number and actual phases of an operation. Phases in a plan are sequential, but during execution, activities within the phases often run in parallel and overlap

During shaping or deterrence activities, OIE is often the primary means by which the JFC can deter aggression and prevent escalation of hostilities. The objective is often to convince adversaries that the likely costs of planned or potential courses of action (COAs) that threaten the US's vital interests outweigh potential benefits. While doing so, the JFC and information planners should posture OIE for potential hostilities. Once combat operations commence, OIE efforts may still focus on garnering support and establishing conditions conducive to political solutions.

During early phases of major combat operations, OIE planning will likely focus on developing advantages across the IE to facilitate execution of component missions. During combat phases, OIE centers on support to objectives aimed at eroding the enemy's will, reducing casualties and collateral damage, and hastening and smoothing the transition to post-conflict operations.

In later phases focused on stability operations, OIE may again become the main effort. The objective is to shape perceptions and behaviors favorably towards US and allied objectives, support peacetime elements of friendly policy, and aid the transfer of regional authority to a legitimate civil entity. During phases devoted to legitimizing civil authority, OIE should help influence the attitudes of relevant populations to regard friendly civil authority objectives favorably.

PLANNING FOR EFFECTS

The information planner's focus is not just on the integrated employment of specialized capabilities but also creating effects to achieve military objectives. Effects may be planned at the tactical, operational, and strategic levels. Information planners should be mindful that any tactical action can result in strategic effects.

Indirect Effects. Information planners should consider the indirect effects (e.g., secondary or tertiary effects) that may arise through the employment of information capabilities. Likewise, beyond the employment of OIE, information effects may often result from the intended, indirect effects of other planned military action. Though indirect effects may impact adversary behavior with wider reach and greater significance than direct effects, they take time to manifest and are more difficult to assess. Because of this, information planners should coordinate requirements and planning early and prepare commanders to anticipate the additional time required for approval and for results to materialize.

Unintended Effects. Whether caused by error, inadequate planning, or unforeseen circumstances, all actions can create unintended effects. Unintended effects may be direct or indirect. To identify potential risks, information planners should deepen their understanding of indirect behavioral effects and should proactively coordinate efforts with other stakeholders. Early consultation with political and legal advisors, CCS representatives, and targeteers ensures planners have the most current information regarding ROE and prohibited/restricted targets lists.[24]

JOINT INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

Joint intelligence preparation of the operational environment (JIPOE) provides commanders, planners, analysts, and targeteers at all levels with the IE awareness necessary to anticipate future conditions, establish priorities, and exploit emerging opportunities. [25] JIPOE is a continuous analytical process that describes the OE, evaluates adversaries and other actors, and helps to determine potential COAs. JIPOE can be leveraged to provide information planners with detailed understanding of:

- C2 networks, organizations, and infrastructure.

[24] For additional information on effects, see AFDP 5-0, *Planning*.
[25] See Joint Guide for Joint Intelligence Preparation of the Operational Environment (JIPOE), for additional information.

- Media infrastructure and the organizations and individuals conducting mass communication.
- Cultural demographics.
- Key leadership behaviors, decision-making processes, and relationships.
- Adversary reliance on cyberspace and use of information.
- Baseline perceptions and attitudes of relevant actors.

Given the long lead times often required to produce intelligence about the IE, intelligence requirements should be identified as early as possible in the planning process and updated throughout the JIPOE process. A well-established intelligence support relationship will foster a better understanding of available types of information and help leaders specify requirements more accurately. Timely and specific feedback and assessment of intelligence collection are vital to optimize JIPOE and drive continued production of useful and actionable intelligence.

MISSION ANALYSIS

Mission analysis enables the air component commander and staff to understand problems facing the JFC and other components, conditions desired by the JFC and national leaders, and component force contributions. The overall focus of this step is to frame the problem and develop viable approaches.

Within information planning, certain factors can be identified and known **(facts):**

- Relevant actors within the context of the commander's objectives.
- Relevant actors outside the AOR who may present opportunities for secondary/tertiary influence, or otherwise affect component efforts.

Though attained through informed insight, certain factors must be assumed **(assumptions):**

- Thresholds for relevant actor physical and informational escalation.
- Relevant actor equities, interests, and decision-making processes.
- Authoritative information sources and channels (e.g., media outlets, government agencies) used by relevant actors.
- Potential methods or paths available to introduce credible information into relevant channels.

Additionally, potential information-related operational limitations **(constraints or restraints)** should be identified. Examples include:

- Required information-related authorities and permissions, the time required to secure them, and additional authorities or permissions that may be needed.

- Potential second and third order effects or effects beyond the intended audience. Since information and its effects may not be contained geographically or limited only to intended audiences, limitations may be necessary for certain relevant actors, the use of certain capabilities, or for specific themes and messages.
- Partner nation operational constraints and restraints (e.g., attribution).

COURSE OF ACTION DEVELOPMENT

COA development establishes the broad actions the force will take to achieve desired future states. It centers on designing an operational approach and potential options for attaining and maintaining conditions that enable achievement of JFC intent. Informational considerations to incorporate into COA development include:

- Available means for informing domestic, international, and internal audiences and relevant actors.
- Available means to affect information, information networks, and systems.
- Possible pathways for effective information and influence activities, to include allies, partners, and other third parties.
- Identification and accessibility of forces required to support OIE actions, to include those from joint, coalition, and interagency partners.
- Determination of COA narratives, key themes, messages, and the OIE capabilities they require.
- Determining relative timing, tempo, intensity, and scope of informational actions and their linkages to other military actions for reinforcing effects.
- Possible adversary OIE approaches and options to counter their efforts.
- Determining, evaluating, and assessing MOE indicators (MOEI) for relevant actor behaviors to validate operational objectives.
- Developing a layered plan to assess changes in relevant actor behaviors and their impacts on operational or informational advantage.

COURSE OF ACTION ANALYSIS AND WARGAMING

COA analysis and wargaming provide an opportunity to test the proposed set of actions against relevant actor responses. Information planners should proactively pre-plan appropriate responses capable of countering anticipated adversary actions. As an example, anticipating that an enemy may publicize false or misleading images of battle-damaged areas, information planners may request ISR support to collect post-attack imagery to provide accurate data, should the need arise. Such action could enable effective counterpropaganda efforts and deny the adversary's pursuit of information advantage.

Wargaming can also be used to determine pertinent MOE and the feasibility of their collection with the timeliness required to enable effective decision-making regarding follow-on actions. During COA analysis and wargaming information planners should:

- Predict how relevant actors may react to each COA.
- Identify potentially relevant actor cognitive biases and predict how they may affect reactions.
- Address possible confirmation bias in planning or developing COAs.
- Anticipate how relevant actors might exploit publicly available information.
- Identify additional relevant actors that could emerge because of the COA, within or outside the AOR.
- Evaluate the ability to gather MOEI of relevant actor behavior changes within operationally relevant timeframes.

DETAILED PLANNING

Detailed planning focuses on translating an overall COA into executable actions by specific forces and capabilities. The emphasis from an OIE perspective is to establish how to affect relevant actor behavior, perceptions, and attitudes through the integration of OIE with other capabilities and activities using assigned, attached, and supporting forces. OIE-related detailed planning actions include:

- Incorporating information-related objectives into existing targeting processes.
- Conducting judge advocate review of proposed informational effects.
- Developing and promulgating OIE-related ROE.
- Drafting collection plans for OIE-related MOEI observation.
- Developing integrated force package options to create desired effects.
- Identifying and resolving capability and capacity shortfalls.
- Developing an integrated plan to leverage information and synchronize OIE with other military operations and force applications.

Generally, information planners are not responsible for planning the employment of specific capabilities. For instance, the EW coordination cell plans and employs EW capabilities, and the ISR collection manager and platform liaisons plan ISR operations. Some assets are controlled at the national level due to their global access and multi-mission capabilities, yet they provide tactical effects and capabilities as well. Additionally, because they operate over a vast IE, some high demand—low density information capabilities may not always be available.

OTHER CONSIDERATIONS

Special Technical Operations. Information planners should maintain close coordination with the Special Technical Operations (STO) element to integrate, synchronize, and de-conflict operations as appropriate.

Targeting. Targeting is the process of selecting and prioritizing targets and matching the appropriate response, considering operational requirements, capabilities, and damage estimates.[26] Targeting supports linking the desired effects to actions and tasks. To ensure information effects are integrated and synchronized, information planners should participate in all aspects of the joint targeting cycle.

EXECUTION

In execution, OIE activities focus on carrying out plans and tasking orders with assigned, attached, and supporting forces and capabilities, characterized by a dynamic combination of theater and global operational processes that requires timely integration. Changes in the OE and the results of ongoing operations may result in adjustments to taskings, as needed.

In the AOC, the air component commander directs information planners to plan, coordinate, and task OIE through the AFPP, JPPA, and the joint air tasking cycle, integrating information capabilities, operations, missions, and effects into theater operations. Depending on the supporting information force, and associated command relationships, the ATO alone may constitute all the tasking information and coordination required to task information forces. Conversely, information staff may be required to coordinate with other theater or functional OCs. Other theater and functional OCs may generate corresponding task orders of their own. Properly generated and coordinated taskings are vital to successful integration of theater and global operations. However, not all OIE are captured in an ATO. Information planners should remain aware of OIE that have cognitive/behavioral impacts and integrate them into planning efforts. Examples may be key leader engagements, exchanges, civil engineering projects, or cyberspace operations.

Within the AOC, information planners coordinate with tasking leads in the AOC's combat operations division and situationally advise external points of contact. For theater information forces assigned to the JFC, but not attached to the air component commander, information planners coordinate with other theater OCs to task needed forces. For supporting information forces and capabilities operating from outside of the theater, information planners coordinate with functional OCs to task those forces through their corresponding tasking cycles (e.g., joint space tasking cycle) and tasking orders (e.g., joint space tasking order, cyber tasking order).

[26] See JP 3-60, *Joint Targeting,* for additional information.

During execution, information planners should:

- Recognize and reconcile planning assumptions that are no longer valid or have been overcome by events, and adjust the plan as required.
- Monitor how component activities resonate through the IE.
- Collect MOEI and maintain and understand the IE.
- Synchronize execution of OIE with other component activities (e.g., application of physical force).
- Identify and resolve conflicting OIE approaches with mission partners (joint, interagency, and partner nations).
- Detect and counter emergent adversary disinformation and other OIE of concern.
- Identify new/emerging relevant actors.

ASSESSMENT

Assessment is an iterative process for determining the overall effectiveness of operations.[27] The air component commander is normally responsible for evaluating the results of OIE tasked to them. There are two primary types of assessments: operational and environmental. The operational level assessment is usually executed within the AOC's strategy division. The environmental assessment is generally performed by the AOC's ISRD.

Assessment at the operational level focuses on both performance and effects via MOPs and MOEs, respectively. MOPs and MOEs can both be measured either quantitatively or qualitatively. MOPs are criteria used to assess friendly accomplishment of tasks and mission execution. They help determine if delivery methods are reaching the intended audience. MOPs center on evaluating the execution of OIE and synchronization of informational actions with traditional force application. MOP analysis can be used to:

- Determine if informational and physical actions were sequenced and executed as intended.
- Identify capability shortfalls and resource issues that impeded effectiveness.
- Identify gaps in authorities/permissions that impeded effectiveness.
- Identify coordination (technical or human) issues that impeded effectiveness.

In contrast, MOEs are criteria used to assess changes in system behavior, capability, or OE to determine whether OIE actions have created desired effects, thereby accomplishing the commander's objectives (e.g., the number of weapons caches voluntarily turned over, increase in the number of cooperative projects between the military and the civil population, or decreased number of violent crimes). Planners

[27] See JP 3-0, *Joint Campaigns and Operations,* for additional information.

evaluate MOEI that suggest changes in relevant actor perceptions, attitudes, beliefs, and behaviors, such as:

- Echoing of the air component or joint force messaging by relevant actors.
- Reinforcement of joint force narrative and messages by allies and partners.
- Characterization of public, media, or senior leader dialogue related to joint force narrative and actions by allies, adversaries, or other relevant actors.
- Effects on adversary alliances and partnerships, beneficial or detrimental to US interests.
- Diversion of resources by adversaries attributable to joint force actions.
- Changes in adversary force posture, exercises, or doctrine.

Information planners and analysts, including operations analysts, should develop an intimate understanding of the linkage between OIE and their intended effects. This requires direct feedback from those closest to observing the intended effects, such as the joint information forces executing OIE missions or the supported warfighters. OIE assessment may also require coordination of collection requirements with the AOC ISRD.

ASSESSMENT CHALLENGES

Because OIE simultaneously employs and integrates numerous capabilities and focuses on cognitive aspects, assessing effects can be challenging. OIE effects should be assessed to determine their impacts towards the achievement of objectives. Assessment should include observable changes in relevant actor behaviors, the effectiveness of detection methods, and an examination of cause and effect. Further, the ambiguities and limitations resident within the IE require frequent adjustment to operational planning considerations, ensuring desired effects are generated while avoiding specifically designated or unintended negative consequences.

Information planners should generate valid MOP/MOE and coordinate with intelligence to ensure the measures chosen are observable by available collection capabilities. OIE outcomes, especially second and third order effects, may not manifest themselves until well after actions have concluded. Importantly, information related MOEI may not be easily observed, readily apparent, or the development timeline may exceed operational tempo constraints. Consequently, MOEs may be absent, incomplete, or not yet mature. Though they may be necessary, if a selected COA lacks sufficient MOEI, information planners should account for anticipated difficulties in analysis, subsequent execution, and the overall OIE effort. In some instances, planners may need to consider adjusting the OIE approach based on MOEI available.

Likewise, rushing to gather and evaluate MOEs can result in significant, consequential errors. Further, because of the numerous variables that factor into human behavior and decision-making, cause-and-effect relationships can often be difficult to determine. It is entirely possible to achieve desired effects that result apart from, or despite OIE aimed at

producing them. Objective and continual assessment is key to avoiding errors when attributing observed effects to specific actions.[28]

[28] For additional information on operational assessment, see JP 5-0, *Joint Planning,* JP 3-04, *Information in Joint Operations*, and AFDP 5-0, *Planning*.

REFERENCES

All websites accessed 27 Apr 2026.

Doctrine can be accessed through links provided at: https://www.doctrine.af.mil/

US AIR FORCE DOCTRINE

- AFDP 2-0, *Intelligence*
- AFDP 3-12, *Cyberspace Operations*
- AFDP 3-61, *Public Affairs*
- AFDP 3-84, *Legal Support*
- AFDP 3-85, *Electromagnetic Spectrum Operations*
- AFDP 5-0, *Planning*

JOINT DOCTRINE

- JP 2-0 Appendix C, *Counterintelligence and Human Intelligence/Department of Defense Cover* (Classified)
- JP 3-0, *Joint Campaigns and Operations*
- JP 3-04, *Information in Joint Operations*
- JP 3-12, *Joint Cyberspace Operations*
- JP 3-30, *Joint Air Operations*
- JP 3-53, *Joint Military Information Support Operations*
- JP 3-54, *Joint Doctrine for Military Deception*
- JP 3-55, *Joint Operations Security*
- JP 3-57, *Joint Civil-Military Operations*
- JP 3-59, *Meteorological and Oceanographic Operations*
- JP 3-60, *Joint Targeting*
- JP 3-85, *Joint Electromagnetic Spectrum Operations*
- JP 5-0, *Joint Planning*
- JDN 1-22, *Joint Force in Strategic Competition*
- *Joint Guide for Intelligence Preparation of the Operational Environment*

DOCTRINE FROM OTHER SERVICES

- *https://my.spaceforce.mil/landing-page/spaceforcedoctrine*
- *Space Force Doctrine Document 1: The Space Force*