

INTRODUCTION TO INFORMATION OPERATIONS

Last Updated: 28 April 2016

The purpose of [information operations](#) (IO) is to affect adversary and potential adversary decision making with the intent to ultimately affect their behavior in ways that help achieve friendly objectives. Information operations is defined as “the integrated employment, during military operations, of information-related capabilities [IRCs] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.”¹ Deliberate targeting of an adversary’s decision making process is enabled by understanding the cognitive factors related to that process, the information that they use, and how they receive and send information. IO is an integrating function, which means that it incorporates capabilities to plan, execute, and assess the information used by adversary decision makers, with the intent of influencing, disrupting, corrupting, or usurping that process. This is not the same as integrating non-lethal capabilities and activities, which may or may not have a behavior-related objective as their primary purpose.

The decision-making process can be modeled with a cycle of steps referred to as the observe, orient, decide, act (OODA) loop.² The steps of this model occur within the information environment and consist of three targetable dimensions: 1) informational, 2) physical, and 3) cognitive.

The information dimension represents the content of the information used by the decision maker. Once someone applies meaning to any data element, the data element is transduced into information. This distinction is subtle; but the impact is profound.

Not all data is transmitted by electronic means. A handwritten note or the sound of an explosion conveys data, but the predetermined meaning applied to either the data on the note, or acoustical data will cause the recipient to act or not to act.

The cognitive dimension is where the decision maker transforms the data from the physical dimension into meaningful information. While we can’t directly target the adversary’s cognitive processes, we can indirectly target them through the information

¹ Joint Publication (JP) 3-13, [Information Operations](#). ² AFDP 3-0, [Operations and Planning](#).

and physical dimensions. This is accomplished by understanding the adversary's culture, organization, and individual psychology, which enables us to affect the adversary's OODA loop and ultimately their behavior.³

IO is fundamental to the overall military objective of influencing an adversary. IO involves synchronizing effects from all domains during all phases of war through the use of kinetic and non-kinetic actions to produce lethal and non-lethal effects. The planning and execution processes begin with the commander's operational design that guides planners as they coordinate, integrate, and synchronize the IRCs and other lines of operation. IO planning should be integrated into existing planning processes, such as the [joint operation planning process](#) (JOPP). IO planning is not a standalone process. In fact, JP 5-0 clearly identifies IO as a key output resulting from course of action development.

Additionally, IO is complementary to the practices, processes, and end goals of an [effects-based approach to operations](#). IO facilitates targeting development and intelligence requirements, and matches actions with intended messages. Through planning, execution, and assessment processes, IO provides the means to employ the right capabilities (kinetic and non-kinetic) to achieve the desired effects to meet the combatant commander's objectives while supporting the commander's communication synchronization strategy.

INFORMATION OPERATIONS DEFINITIONS AND DESCRIPTIONS

Commander's Communication Synchronization⁴: [Commander's communication synchronization](#) (CCS) is the Department of Defense's primary approach to implementing United States Government (USG) strategic communication guidance as it applies to military operations. The CCS is the joint force commander's (JFC's) approach for integrating all IRCs, in concert with other lines of effort and operation. It synchronizes themes, messages, images, and actions to support the JFC's objectives. Commander's intent should be reflected in every staff product. Air Force component commanders should similarly conduct their own commander's communication synchronization program. This component level communication synchronization coordinates themes, messages, images, and actions to support the commander, Air Force forces' objectives

Information Environment. The [information environment](#) is defined as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."⁵ The information environment is comprised of the physical, informational, and cognitive dimensions. IO primarily focuses on affecting the cognitive dimension, where human decision making occurs, through the physical and information dimensions.

³ JP 3-13, [Information Operations](#).

⁴ Joint Doctrine Note 2-13, [Commander's Communication Synchronization](#).

⁵ JP 3-13, [Information Operations](#).

Information-Related Capabilities. IRCs are defined as “tools, techniques, or activities using data, information, or knowledge to create effects and operationally desirable conditions within the physical, informational, and cognitive dimensions of the information environment.”⁶ IRCs create both lethal and nonlethal effects. When IRCs are employed with the primary purpose of affecting the cognitive dimension, it is typically considered IO. IRCs may also include activities such as counterpropaganda, engagements, and shows-of-force, as well as techniques like having the host nation designated as the lead for night raids or not using dogs to search houses. IRCs can be employed individually or in combination to create lethal and non-lethal effects supporting a wide range of missions and objectives.

Informational Dimension. The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the command and control (C2) of military forces is exercised and where the commander’s intent is conveyed.

Physical Dimension. The physical dimension is composed of C2 systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, and any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries.”

Cognitive Dimension. The cognitive dimension encompasses the minds of those who transmit, receive and respond to, or act on information. These elements are influenced by many factors, including individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies.

Target Audience. A [target audience](#) is defined as “an individual or group selected for influence.”⁷

⁶ JP 3-13, [Information Operations](#).

⁷ JP 3-13, [Information Operations](#).



CURTIS E. LEMAY CENTER

FOR DOCTRINE DEVELOPMENT AND EDUCATION



AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-13 INFORMATION OPERATIONS

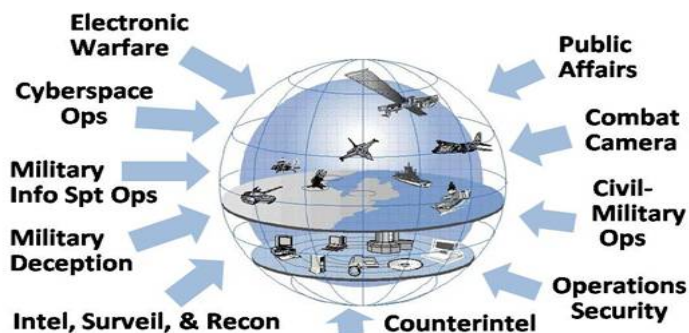
ROLE OF INFORMATION OPERATIONS THROUGHOUT THE RANGE OF MILITARY OPERATIONS AND PHASES OF WAR

Last Reviewed: 28 April 2016




Information operations (IO) presents viable options to combatant commanders (CCDRs) for conducting operations throughout the range of military operations (ROMO) and all phases of war. IO enables forces to achieve objectives and possibly deter aggression. It enables the use of information-related capabilities (IRCs) in restricted, contested, or politically sensitive areas where traditional air, land, and sea operations may not be permitted. Historically, commanders have employed various IRCs to prevent escalation and enable security.

For example during a humanitarian assistance operation, a commander may influence host nation and even regional cooperation through the integration of public affairs (PA) activities and military information support operations (MISO) messaging designed to facilitate safe and orderly humanitarian assistance among the local populace. During a major operation, the commander may influence region-wide perceptions as well as local behavior through integration of electronic warfare (EW), MISO, and cyberspace operations (CO) with other kinetic or non-kinetic missions against key targets. Examples of other IRCs employed across the ROMO can be seen in figure on IO and the ROMO.

IRCs Employed Across the ROMO



IRCs Employed Across the ROMO

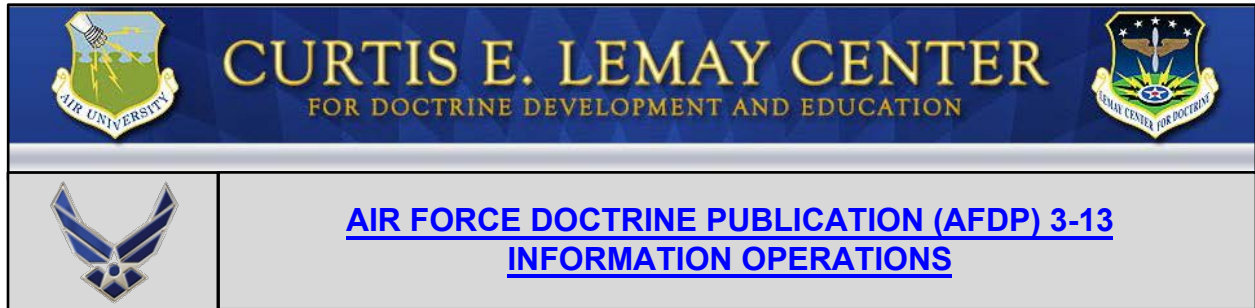
	CURTIS E. LEMAY CENTER FOR DOCTRINE DEVELOPMENT AND EDUCATION	
	<u>AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-13</u> <u>INFORMATION OPERATIONS</u>	

POLICY AND LEGAL CONSIDERATIONS FOR INFORMATION OPERATIONS

Last Updated: 28 April 2016

As in all military operations, the [law of armed conflict](#) applies to information operations (IO). Questions may arise about the legality of [targeting](#) systems with dual-use functionality that support an adversary's military and civilian populace. Likewise, targeting military systems without consideration to collateral effects may result in legally or politically unacceptable indirect effects on the civilian population. Similarly, [rules of engagement](#) (ROE) in a [given area of responsibility](#) may further constrain the integrated employment of IRCs. Commanders, in coordination with legal advisors, should request mission-specific ROE from the appropriate senior authority (e.g., [combatant commanders](#), Secretary of Defense etc.) as required. However, due to the sensitive nature of targeting anything prior to hostilities, commanders may not want to risk inadvertent escalation. Since the operational complexity of applying IRCs is furthered by diverse legal concerns, legal advisors should be included in IO planning.

See AFDP 1-04, [Legal Support to Commanders](#) for additional information.



AIRMAN'S PERSPECTIVE ON INFORMATION OPERATIONS

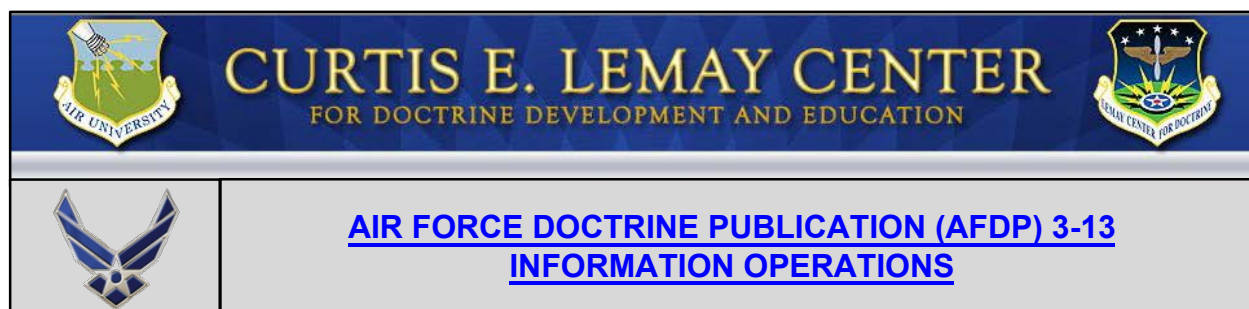
Last Updated: 28 April 2016

Air Force information operations (IO) primarily exists at the air component level as part of the joint IO effort under the [joint force commander \(JFC\)](#) and [combatant commander \(CCDR\)](#). "At the [operational level of war](#), IO ensures synchronized messaging from all IRCs and ensures information-related capabilities (IRCs) complement each other and do not detract from or interfere with any IO-related/messaging objectives. It includes informing and attempting to affect behavior and decision making as it applies to all relevant non-US audiences. IO should not be confused with integrating non-lethal capabilities. IO planners should be aware of capabilities for creating both [lethal and non-lethal effects](#), as well as plans to ensure any cognitive effects they have will enhance and not detract from IO-related/messaging objectives. IO planners work with all other planners and IRC liaisons, using standard planning and execution steps of the [joint operation planning process for air](#), air tasking cycle, and targeting cycle to accomplish commander's objectives. IO-specific by-products include items such as synchronization matrices, coordinated narratives and themes, and target audience analysis. There is no separate IO plan.

The targeting of a select audience's decision-making process is not new for Airmen. In addition to the requisite understanding of the information content and connectivity used by targeted decision makers, the Air Force has developed an analysis capability called [behavioral influence analysis \(BIA\)](#). BIA provides an understanding of the decision makers' behavior to include culture, organization, and individual psychology (e.g., perceptual patterns, cognitive style, reasoning and judgment, and decision selection processes). It is this knowledge, coupled with an Airman's ability to strike information-related targets that is the essence of Air Force IO. The integrated employment of capabilities to affect information content and connectivity of an adversary provides military advantage to friendly forces.

Air Force IO also includes the integrated planning, employment, monitoring, and assessment of themes, messages, and actions (verbal, visual, and symbolic) as part of the commander's communication synchronization (CCS) at the component level. The CCS will include pertinent portions of the joint force commander's or combatant commander's communication strategy, which may include communication synchronization themes and messages as well as any relevant component commander's themes and messages. At the [air component level](#), Air Force IO planners

should ensure these themes, messages, and actions (e.g., IRCs) are integrated across all lines of operation.

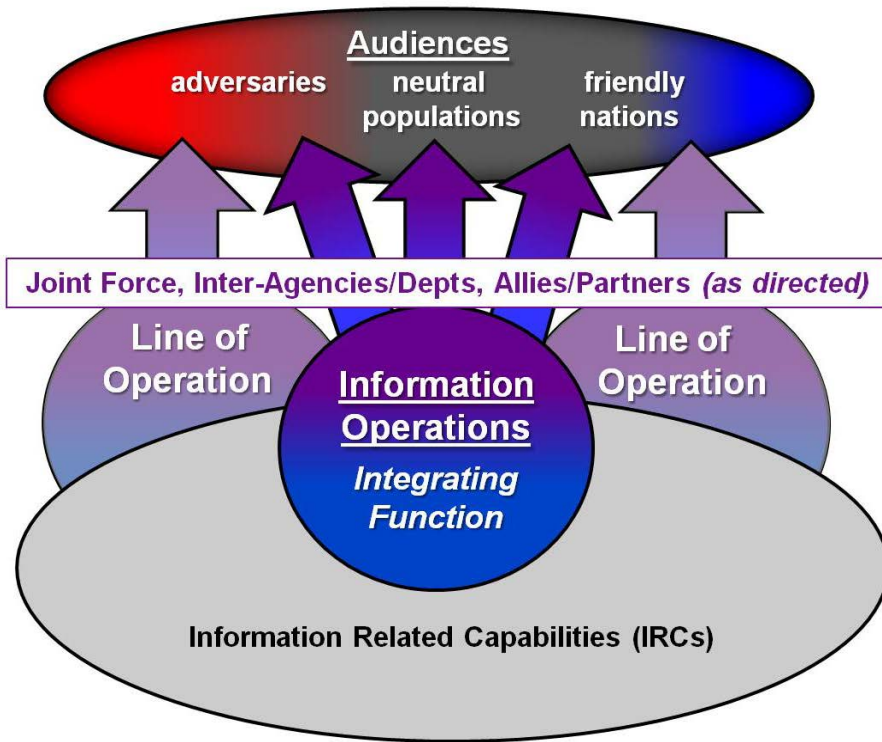


INFORMATION-RELATED CAPABILITIES (IRCs)

Last Updated: 28 April 2016

In 2011, the definition of information operations (IO) was revised to eliminate references to specific capabilities and describe those generically as information-related capabilities (IRCs). As a result, the Air Force no longer distinguishes and categorizes IO capabilities with terms like “core capabilities”, “influence operations,” or “integrated control enablers.” The Air Force now references tools, techniques, and activities when used to affect the information environment.

The distinction of IO’s role as an integrating function merits emphasis. IO is not a capability in and of itself. IO does not “own” individual capabilities but rather plans and integrates the use of IRCs, tools, techniques, and activities in order to create a desired effect—to affect adversary, neutral, and friendly decision making, which contributes towards a specified set of behaviors. IRCs can be employed by themselves or in combination to conduct or support a wide range of missions. For example, IO planners should help ensure [electronic attack \(EA\)](#), offensive [space control](#), air attacks, and cyberspace operations are coordinated and deconflicted from the perspective of cognitive/behavioral effects. The coordination process should also strive to resolve conflict between actions and messages. Individually, IRCs have wider application than IO employment. What unites capabilities as IRCs is a common IO battlespace—the [information environment](#)—whether those capabilities operate in it or affect it. Numerous Air Force capabilities have potential to be employed for IO purposes. See figure on IO Employment of IRCs.



IO Employment of IRCs



CURTIS E. LEMAY CENTER

FOR DOCTRINE DEVELOPMENT AND EDUCATION



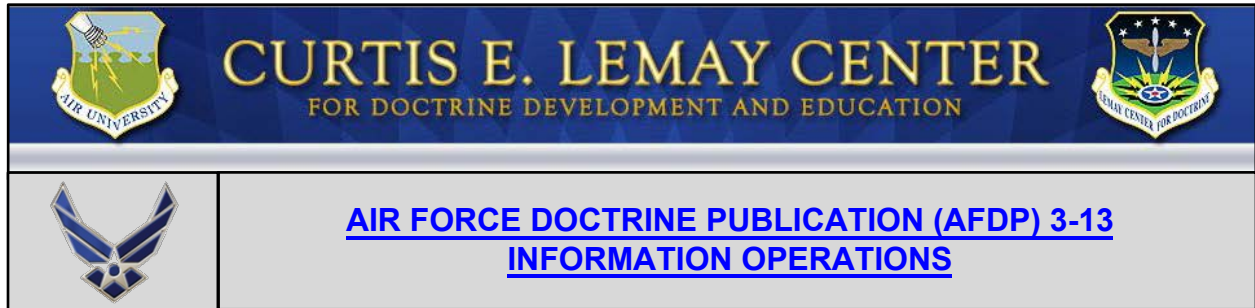
AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-13 INFORMATION OPERATIONS

INFORMATION-RELATED CAPABILITIES: ELECTRONIC WARFARE (EW)

Last Updated: 28 April 2016

Electronic warfare (EW) is defined as “military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum [EMS] or to attack the enemy.”¹ EW consists of three divisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EW contributes to the success of information operations 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 in that spectrum. During combat operations, the commander, Air Force forces (COMAFFOR)/joint force air component commander (JFACC) is usually designated as EW control authority (EWCA) and jamming control authority for the employment of EW assets, associated policy, and processes in the joint operations area. The COMAFFOR/JFACC typically stands up an EW coordination cell to employ EA to negate an adversary’s effective use of the EMS by degrading, neutralizing, or destroying combat capability. To deconflict intended effects, the following activities should be closely coordinated: EA, EP, ES, offensive cyberspace operations, offensive space control, military deception, operations security, and intelligence.

¹ JP 3-13.1, Electronic Warfare.



INFORMATION-RELATED CAPABILITIES: MILITARY INFORMATION SUPPORT OPERATIONS (MISO)

Last Updated: 28 April 2016

Military information support operations (MISO) are defined as “planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives.”¹ MISO may attempt to either induce change in foreign attitudes and behavior or reinforce existing attitudes and behavior. MISO at the combatant command level usually resides in the combatant commander’s (CCDR) J39 directorate or in a military information support task force (MISTF), which includes a MISO planner as a member of the joint IO cell or joint IO staff.

The final approving authority for themes normally resides at the national level but is usually delegated to a geographic CCDR or joint task force commander during times of crisis. At the Air Force component level, MISO planners may be part of the joint force air component commander (JFACC’s) IO team, or may be retained as part of the commander, Air Force forces’ (COMAFFOR’s) staff. It is essential for the MISO planner to represent COMAFFOR/JFACC requirements to MISTF for integration into the joint force commander’s overall plan. Additionally, MISO planners should closely coordinate with military deception, operations security, public affairs, and other information-related capability leads to ensure the integrity and consistency of themes, messages, images, and actions.

¹ JP 3-13.2, Military Information Support Operations.



Capt. Abraham Alvarenga of the 102nd Group Support Battalion, 71st Theater Information Group assigned to Task Force Larimar, visits the Dominican Republic's Barahona province, May 7, 2014. The Military Information Support Operations group interviewed members of the community regarding the general and specialized medical services they received at no cost during the annual bilateral humanitarian exercise known as Beyond the Horizon. Such face-to-face communications are critical to MISO's mission today.



[AIR FORCE DOCTRINE PUBLICATION \(AFDP\) 3-13](#)
[INFORMATION OPERATIONS](#)

**INFORMATION-RELATED CAPABILITIES:
MILITARY DECEPTION**

Last Updated: 28 April 2016

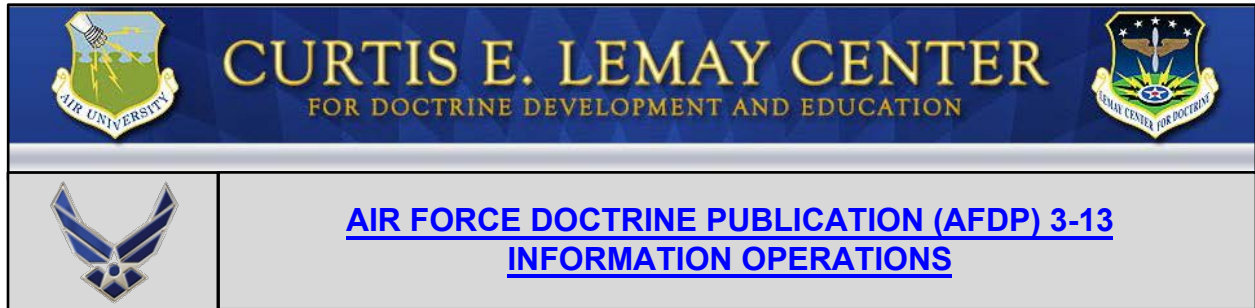
[Military deception](#) (MILDEC) is defined as “actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or fail to take actions) that will contribute to the accomplishment of the friendly mission.”¹ Deception operations can span all levels of war and can include, at the same time, both offensive and defensive components. During planning, MILDEC can be integrated into the early [phases of an operation](#). The MILDEC role during the early phases of an operation will be based on the specific situation of the operation or campaign to help set conditions that will facilitate phases that follow. Deception can distract the adversary from legitimate friendly military operations and can confuse and dissipate adversary forces. MILDEC affects the adversary’s information systems, processes, and capabilities to create desired behavior. MILDEC planners require adversary and potential adversary decision maker analysis for a sufficiently detailed understanding of how the information environment supports the adversary’s decision-making process.

Each [information-related capability](#) (IRC) has a part to play in successful MILDEC credibility over time, so information operations (IO) facilitates close coordination with [military information support operations](#) (MISO), operations security (OPSEC), [public affairs](#) (PA), and [commander's communication synchronization](#) (CCS) personnel within the [joint IO cell](#) or staff. Whereas MISO, 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. Inappropriate media access may compromise deception efforts. Conversely, MILDEC must not intentionally target or mislead the news media, the US public, or Congress. Deception activities potentially visible to the US public should be closely coordinated with PA operations so as to not compromise operational considerations or diminish the credibility of [PA operations](#) in the national media. Due to the sensitive nature of MILDEC plans and objectives, a strict need-to-know policy should be enforced. Additionally, approval authorities for conducting MILDEC actions are typically at the joint force commander-level or above, so the approval action may require sufficient lead time for staffing.

¹ JP 3-13.4, [Military Deception](#).



Army Field Manual 90-2, *"Battlefield Deception,"* (October 1988) revealed that the Army was revitalizing its deception capabilities, leading up to the greatest modern use of tactical deception in 1991 — Operation DESERT STORM. During DESERT STORM, a signal company mimicked traffic for the XVIII and V Corps headquarters to make it appear that they were stationary, when in fact they were moving into position for the "left hook," a flanking maneuver through the western Iraqi desert. The enemy focused on an amphibious training demonstration put on by the Marine Corps, causing Iraqi forces to reinforce the coastline, facing away from the main attack.



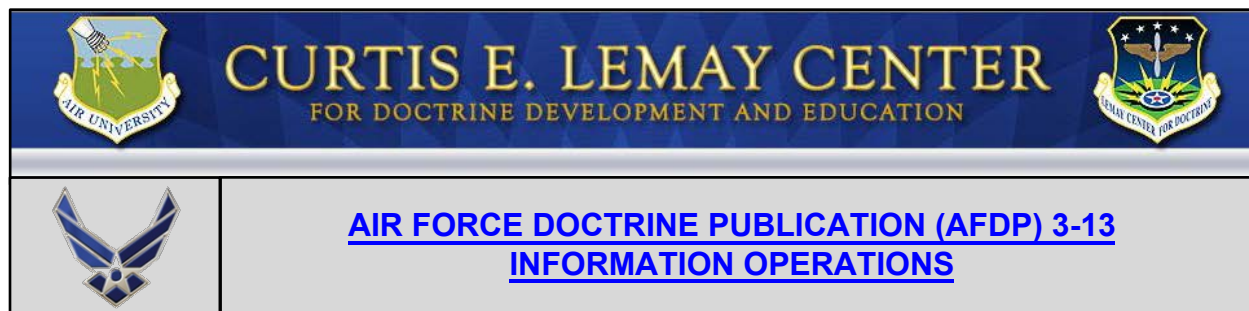
INFORMATION-RELATED CAPABILITIES: OPERATIONS SECURITY

Last Updated: 28 April 2016

[Operations security](#) (OPSEC) is defined as “a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities.”¹ OPSEC denies adversaries critical information and observable indicators about friendly forces and intentions. OPSEC identifies any unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities. A critical information list should be developed and continuously updated in peacetime as well as conflict. The critical information list helps ensure military personnel and media are aware of non-releasable information.

The information operations (IO) team enables the OPSEC planner to maintain situational awareness of friendly information and actions and to assist other [air operations center](#) planners in incorporating OPSEC considerations during the planning process. Once the OPSEC process identifies vulnerabilities, other information-related capabilities (e.g., military deception, military information support operations, [electronic warfare](#), [cyberspace operations](#)) can be used to ensure OPSEC requirements are satisfied.

¹ JP 3-13.3, [Operations Security](#).



INFORMATION-RELATED CAPABILITIES: PUBLIC AFFAIRS

Last Reviewed: 28 April 2016

[Public affairs](#) (PA) provides information operations (IO) with an open and credible means to reach key public audiences. PA consists of public information, command information, and civic engagement activities that are directed toward both the external and internal publics with interest in the DOD.¹ The external public may include allied, neutral, and adversary audiences. Truth is foundational to the credibility of all public affairs operations. [Timely and agile dissemination](#) is essential to help achieve desired information effects. PA plays a significant role throughout the [range of military operations](#), with PA being one of the most prominent [information-related capabilities](#) (IRCs) used prior to the outset of hostilities and during stability operations. While PA cannot provide false or misleading information, it must be aware of the intent of other IRCs such as [military deception](#), [military information support operations](#) (MISO) and [operations security](#) to lessen the chance of compromise. PA integration with other IRCs is vital to ensure the capabilities complement rather than conflict with each other.

Rather than providing an advantage to an adversary, the carefully coordinated release of operational information in some situations can intimidate an adversary, deter conflict, and counter adversary propaganda while also maintaining or building support for military operations.

Counterpropaganda

Counterpropaganda operations involve those efforts to negate, neutralize, diminish the effects of, or gain an advantage from adversary propaganda efforts.² Counterpropaganda operations are normally handled through PA channels; however, several other IRCs can support that activity. In addition to PA activities to refute adversary propaganda, there may be [electronic warfare](#) or [cyberspace operations](#) denying adversary use of propaganda outlets. MISO contributes to counterpropaganda missions by amplifying key themes and messages among specific foreign audiences, some of which may be inaccessible by PA operations. Timing and initiative in the information environment is vital to defeating propaganda, particularly when addressing incidents involving collateral damage or friendly force mistakes. Rapidly providing

¹ JP 3-61, [Public Affairs](#).

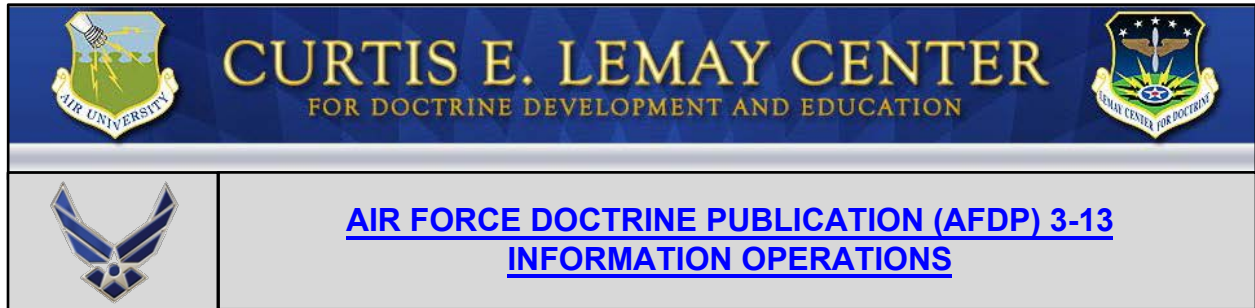
² AFDP 3-61, [Public Affairs Operations](#).

accurate, available information to the public may help disarm adversary attempts to exploit friendly actions for their propaganda value. MISO planners may also assist PA with conducting propaganda analysis.

Combat Camera (COMCAM)

COMCAM is a specialized directed imagery capability in support of strategic, operational, and planning requirements during wartime operations, worldwide crisis, contingencies, joint exercises, humanitarian operations, and other events of significant national interest involving the DOD. COMCAM acquires, processes, and distributes classified and unclassified still and motion imagery. PA typically has oversight responsibility for COMCAM activities, although COMCAM may support other IRC operations. COMCAM teams are uniquely organized, trained (including fully certified/qualified aircrew members) and equipped for rapid global response to provide documentation of air and ground operations and provide visual products for use by IRCs. Commanders use these products for [communication needs](#), [operational planning](#), decision making, [operational assessment](#), and to satisfy requirements for historical documentation of operations. Where rapid global response, aerial imagery, special forces operations, or combat maneuver and capability are not required, traditional visual information resources, not COMCAM, should be used.

See Annex 3-61, [Public Affairs Operations](#), for more information on PA, Counterpropaganda, or COMCAM.



INFORMATION-RELATED CAPABILITIES: AUDIENCE ENGAGEMENTS

Last Reviewed: 28 April 2016

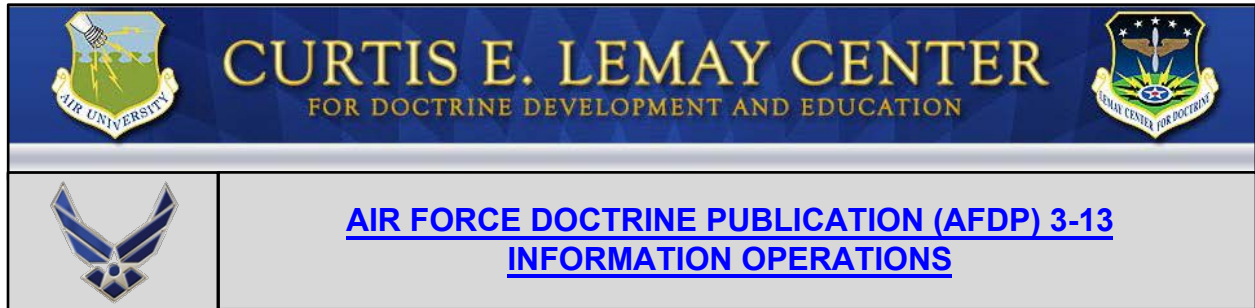
Audience engagements are an important contributor to information operations (IO) because of their ability to convey key messages where they are needed to assist in accomplishing military objectives. Engagements permit interface directly with a specific audience through traditional methods of information exchange. Engagements are broadly described as interactions that take place between military personnel and audiences.¹ Audiences may be key leaders or mass populations, and those audiences may be military or civilian. Engagements may be in person or virtual (e.g., a teleconference), impromptu encounters or planned events, such as during [civil-military operations](#) (CMO).

Civil-Military Operations

CMO are engagement opportunities of particular interest to IO planners. In CMO, military personnel perform functions normally provided by the local government, placing them in direct contact with civilian populations. This level of interface results in CMO having a significant effect on perceptions of the local populace and on relations with the military, as they work with governmental and nongovernmental organizations. CMO principally engage with friendly and neutral populations but may also reach adversaries. While CMO activities occur in conjunction with other military actions, they may present the only engagement opportunity with certain audiences.² Forces involved in engagement opportunities such as [medical](#), [engineering](#), or [security force assistance](#) may not have a habitual working relationship with IO efforts, so IO planners should be pro-active with their coordination. CMO can enable broader IO objectives and ensure consistency with the [commander's communication strategy](#).

¹ JP 3-13, [Information Operations](#).

² JP 3-57, [Civil-Military Operations](#).



INFORMATION-RELATED CAPABILITIES: INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

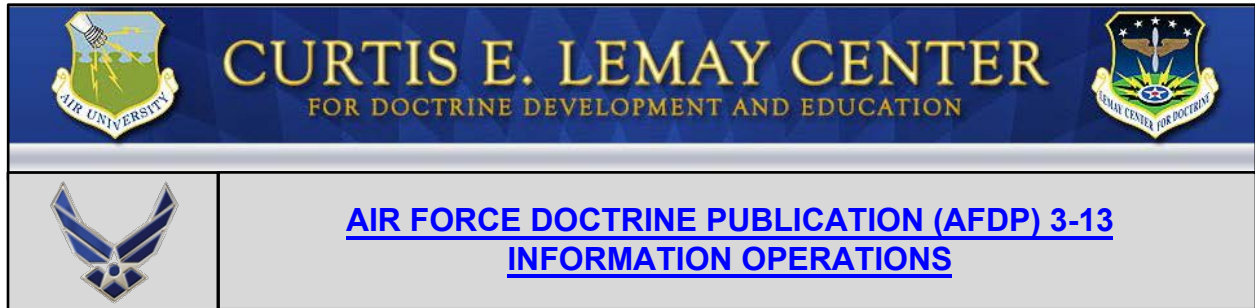
Last Reviewed: 28 April 2016

Information operations (IO) planning, execution, and assessment rely heavily on tailored [intelligence, surveillance, and reconnaissance](#) (ISR). While information-related capabilities (IRCs) separately rely on ISR support for their array of individual application, IO integrated employment of IRCs requires concerted, tailored ISR support in its own right. ISR is defined as “an activity that integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.”¹ The IO team’s affiliation with the Air Force forces (AFFOR) operations directorate and the [combat operations division](#) of the [air operations center](#) (AOC) enables an inherent close coordination for the operations aspect of ISR. Similarly, the IO team maintains habitual coordination with the AFFOR intelligence directorate or AOC [ISR division](#) for the intelligence aspect of ISR. The intelligence directorate or ISR division may opt to establish an [IO intelligence integration](#) (IOII) function to dedicate intelligence support to IO.

Establishment of a dedicated IOII function satisfies IO’s needs, which require advanced and timely coordination to establish baseline characterizations of the information environment, analyze current intelligence for nuanced IO application, develop detailed targeting packages, and conduct complex effects assessments. Furthermore, the IOII element is a conduit for translating and internally coordinating IO’s requirements with the intelligence collection management and production cells.

See AFDP 2-0, [Global Integrated ISR Operations](#), for more information.

¹ JP 2-01, [Joint and National Intelligence Support to Military Operations](#).



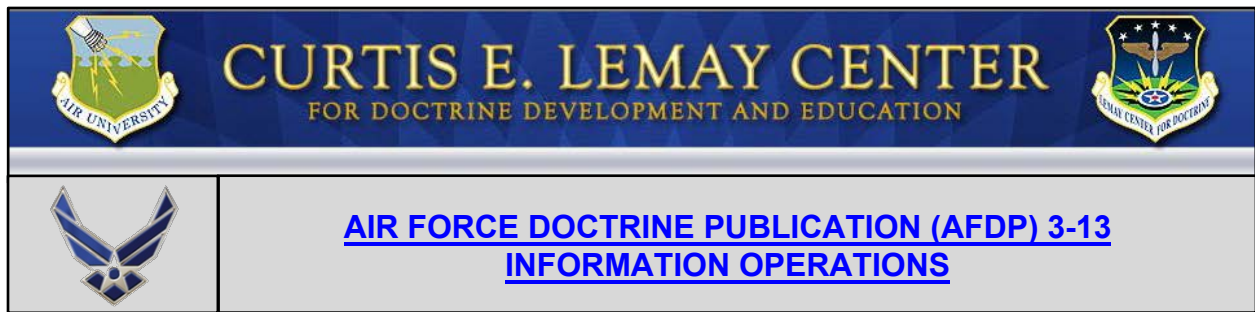
INFORMATION-RELATED CAPABILITIES: COUNTERINTELLIGENCE

Last Updated: 28 April 2016

Counterintelligence (CI) is defined as “information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.”¹ Air Force Office of Special Investigation oversees all Air Force CI activities.

CI support to information operations (IO) includes identifying threats within the information environment through CI collections and analysis and assessing those threats through reactive and proactive means. Threat documentation through intelligence, surveillance, and reconnaissance (ISR) processes and CI products are the primary methods of notifying commanders. CI has the capability to neutralize and exploit threats through investigation and operations. Successful CI and operations security (OPSEC) activities deny adversaries useful information on friendly forces. CI typically has a close working relationship with information-related capabilities (IRCs) such as ISR and OPSEC but may not have the same habitual relationship with other IRCs. IO planners should ensure collaboration with CI professionals to maximize CI integration with other IRCs such as military information support operations, military deception, and cyberspace operations.

¹ JP 2-0, Joint Intelligence.



INFORMATION-RELATED CAPABILITIES: SPACE OPERATIONS




Last Updated: 28 April 2016

Two mission areas of space operations concern the information environment—[global space mission operations](#) and [space control](#).

Global space mission operations capitalize on the information environment to provide force-enhancing capabilities, which include: intelligence, surveillance, and reconnaissance; launch detection; missile tracking; environmental monitoring; satellite communications; and positioning, navigation, and timing.

Space control is defined as “operations to ensure freedom of action in space for the United States and its allies and, when directed, deny an adversary freedom of action in space.” Defensive space control operations are defined as “operations conducted to preserve the ability to exploit space capabilities via active and passive actions, while protecting friendly space capabilities from attack, interference, or unintentional hazards.” Offensive space control is defined as “those operations prevent an adversary’s hostile use of United States/third-party space capabilities and services or negate (deceive, disrupt, degrade, deny, or destroy) an adversary’s efforts to interfere with or attack United States/allied space systems.”

See AFDP 3-14, [Space Operations](#), for more information.

	CURTIS E. LEMAY CENTER FOR DOCTRINE DEVELOPMENT AND EDUCATION	
	<u>AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-13</u> <u>INFORMATION OPERATIONS</u>	

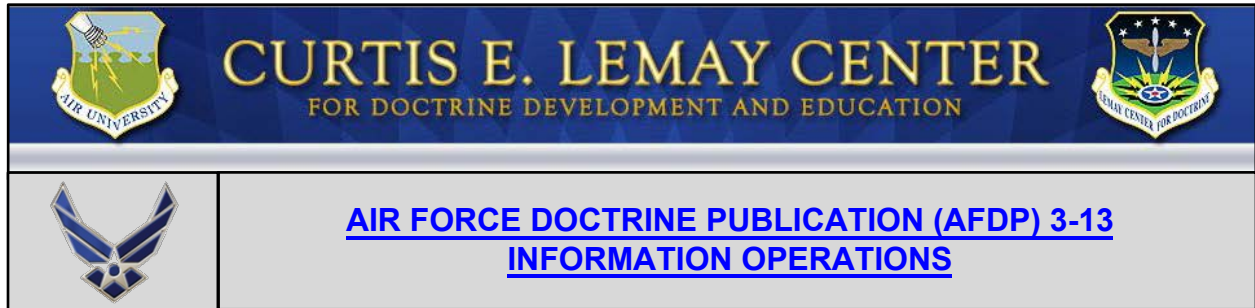
INFORMATION-RELATED CAPABILITIES: CYBERSPACE OPERATIONS

Last Updated: 28 April 2016

Cyberspace operations (CO) are defined as “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”¹ CO use specific cyberspace capabilities to create effects that support operations across all domains. In contrast, information operations (IO) integrates information-related capabilities (IRCs) with its focus on the decision making of adversaries and allies alike. When employed in support of IO, CO include offensive and defensive capabilities exercised through cyberspace, as an integrated aspect of a larger effort to affect the information environment. CO may be employed independently or in conjunction with other IRCs to create effects in the adversary’s battle space and ensure US forces’ freedom of maneuver in the information environment.

See AFDP 3-12, Cyberspace Operations, for more information.

¹ JP 3-0, Joint Operations.



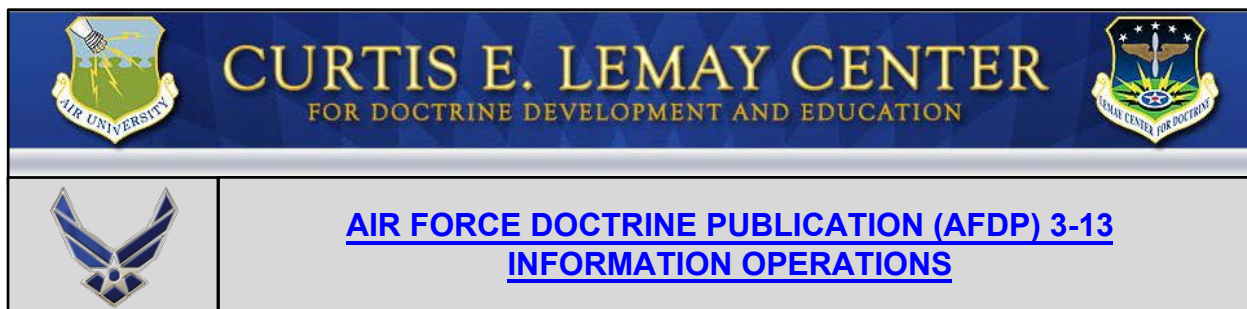
INFORMATION-RELATED CAPABILITIES: SIGNATURE MANAGEMENT

Last Updated: 28 April 2016

Signature management (SM) is a process used to profile day-to-day observable activities and operational trends at wings/installations and at each of their resident or associate units. SM incorporates the analytical methods of [OPSEC](#) creating synergies and resource efficiencies for the wing/installation OPSEC program. These result in identifying details that can be used in efforts to defend or exploit operational advantages at a given military installation and inherent to a unit's operational mission.

When an air component commander's military deception (MILDEC) plan requires Air Force wings and installations to present specified observable activities, the air component commander's MILDEC planner determines the actions required by the supporting unit(s) and communicates those requirements to the wing or installation Signature Management Officer (SMO) or NCO (SMNCO).

Wing and installations do not directly plan or execute MILDEC on their own, but are tasked by the operational MILDEC planner or OPSEC planner to accomplish S M tasks that directly support the operational MILDEC plan. The SMO defines the local operating environment and captures process points that present key signatures, observables, indicators, and profiles with critical information value. This process, known as the base profiling process, is the deliberate effort to identify functional areas and the observables, signatures, and indicators they produce and how they contribute to the overall signature of day-to-day activities and operational trends. Ultimately, this provides the correct presentation of forces when tasked to support the operational MILDEC plan.



OTHER INFORMATION OPERATIONS CAPABILITIES

Last Reviewed: 28 April 2016

Information operations (IO) planners should consider all available options and/or combinations of lethal and non-lethal, kinetic and non-kinetic means in order to achieve the desired lethal and/or non-lethal effects.

Modern military operations require the ability to engage a [target audience](#) with a combination of lethal and non-lethal means, to produce both lethal and non-lethal effects. Non-kinetic and non-lethal means are not reserved only for friendly or neutral audiences. The ability to influence and affect an adversary through non-lethal means may prove to be a better option. For example, well-crafted [military information support operations](#) products may be the best solution to convey the intended message through a variety of print and electronic media to select audiences, which may also free-up conventional, kinetic assets to pursue other objectives.

Lethal actions are those taken through “physical, material means like bombs, bullets, rockets, and other munitions.”¹ Kinetic actions are those designed to produce effects using the forces and energy of moving bodies and directed energy, including physical damage to, alteration of, or destruction of targets. Kinetic actions can have lethal or non-lethal effects.² Non-kinetic and -lethal actions include logical, electromagnetic, or behavioral means, such as gathering intelligence to understand how an adversary’s cyber networks function in order to prioritize targeted nodes or a [public affairs operation](#) to inform friendly, neutral and/or adversarial audiences. Non-lethal options offer the capability to create effects and achieve influence without destroying targets, which may be more advantageous to the overall objectives.

Special Technical Operations

IO planners should maintain close coordination with the special technical operations element to integrate, synchronize, and deconflict operations, as appropriate.

For additional information, see JP 3-13, [Information Operations](#).

¹ AFDP 3-60, [Targeting](#).

² AFDP 3-0, [Operations and Planning](#)



CURTIS E. LEMAY CENTER

FOR DOCTRINE DEVELOPMENT AND EDUCATION



AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-13 INFORMATION OPERATIONS

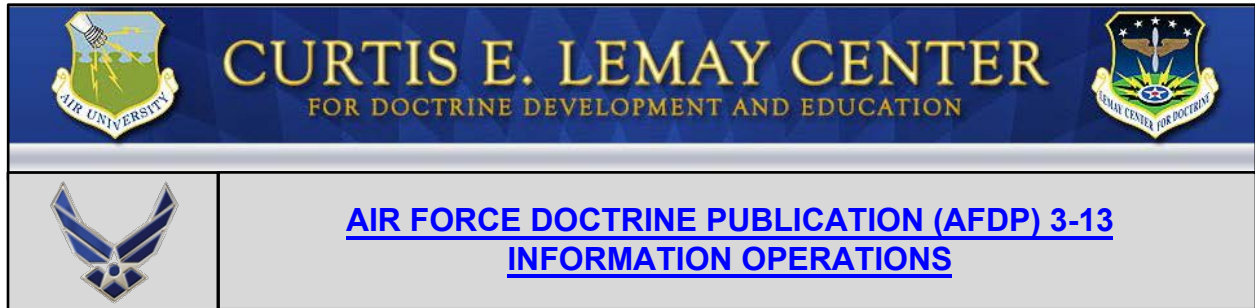
COMMAND AND CONTROL OF INFORMATION OPERATIONS PLANNERS AND INFORMATION-RELATED CAPABILITY FORCES

Last Updated: 28 April 2016

Information-related capability (IRC) forces and information operations (IO) planners are assigned to geographic and functional combatant commands (CCMDs) who employ forces in support of worldwide operations. The functional CCMDs provide IRC support to joint operations in all geographic area of responsibilities (AORs), as required. Thus, the command and control (C2) structure established for integrating IRCs should be robust enough to account for these various operating areas.

The combatant commander (CCDR) develops a theater campaign plan to accomplish ongoing and enduring theater objectives, including those involving IO. The CCDR may establish a joint task force (JTF) commanded by a joint force commander (JFC) to accomplish specific tasks or carry out a particular contingency. The CCDR or subordinate JFC normally designates a joint force IO officer to accomplish broad IO oversight functions. The joint force IO officer heads the JTF IO cell, when designated.

Primary and supporting components are designated by the JFC. If deemed appropriate, the CCDR or subordinate JFC may choose to use service component assets as part of IO integration into their planning efforts. Air Force IO planners and information-related capabilities are typically presented by the commander, Air Force forces to the CCDR or other JFC through either an Air Force component major command or a component numbered Air Force. In addition to IO support to CCDR objectives and messaging requirements, Air Force forces should also use their capabilities, tools, techniques and activities to support component objectives and leadership's messaging objectives.



COMMAND RELATIONSHIPS AND INFORMATION OPERATIONS

Last Updated: 28 April 2016

When a theater requests [information-related capabilities](#) (IRCs) from organizations with global responsibilities, the Secretary of Defense (SecDef) will specify a command relationship between the [functional combatant commander](#) (FCC) and the [geographic combatant commander](#) (GCC) - normally a [support relationship](#). This will be employed at appropriate levels within both the supporting and supported commands. These support relationships fall into four categories: general, mutual, direct, and close support.¹

For IRCs providing effects via a support relationship, it is important for both [supported and supporting commanders](#) to document their requirements in an “establishing directive.” The establishing directive should specify the purpose of the support relationship, the effect(s) desired, and the scope of the action(s) to be taken. Additional information includes:

- ★ The IRCs allocated to the supporting commander's effort.
- ★ The time, place, level, and duration of the supporting commander's effort.
- ★ The relative priority of the supported commander's effort.
- ★ The degree of authorities exercised by the supported and supporting commanders over the effort, to include processes for reconciling competing requirements and resolving emergency events expeditiously, as required.

To facilitate a support relationship, there should be an appropriate level of coordination between the involved commanders. This facilitates planning the detailed integration of IRCs and their effects with theater operations, and enables theater warfighters to coordinate directly at either the same or differing organizational levels. A [direct liaison authorized](#) relationship² should be established for coordination between the theater and functional IO planners.

¹ JP 1, [Doctrine for the Armed Forces of the United States, Chapter IV, Section 6](#).

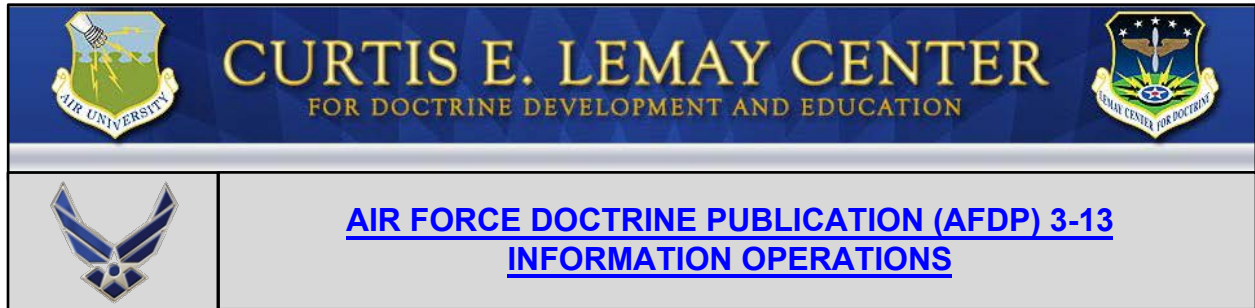
² [DIRLAUTH](#) is explained in JP 1, Chapter V, Section 9c.

If the desired effects produced by IRCs of a functional combatant command are focused primarily on a single area of responsibility, the SecDef may direct the FCC to attach IRC forces to the GCC of that theater. In these situations, the SecDef normally attaches the required forces with specification of [operational control](#) (OPCON)³ to the GCC. An example may be the SecDef directing the Commander, [US Strategic Command](#) to attach space forces to a GCC. The GCC, in turn, normally attaches gained forces to the appropriate Service component commander with specification of OPCON. The theater [commander, Air Force forces](#) (COMAFFOR) is the Service component commander for Air Force IRC forces. The functional component commander for many IRCs is usually the in-theater [joint force air component commander](#).

If the COMAFFOR is formally designated as the supported commander for IRC operations, the JFC normally delegates related coordinating authorities down to the COMAFFOR to coordinate joint IRC operations and integrate theater and global IRCs and their effects. The COMAFFOR is well suited to coordinate many Air Force IRC operations because of the COMAFFOR theater-wide perspective, ability to exercise command and control of IRC forces, and subject-matter expertise on the [AFFOR staff](#) and the [air operations center](#) IO team. Senior IRC or IO advisors on the COMAFFOR's staff may be assigned the responsibilities of executing IRC authorities on behalf of the COMAFFOR. Examples of coordinating authorities include [space coordinating authority](#) and counterintelligence coordinating authority.⁴

³ See [JP 1, Chapter IV, Section 4](#).

⁴ For a description of these coordinating authorities, see Annex 3-14, [Space Operations](#), and JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations*.



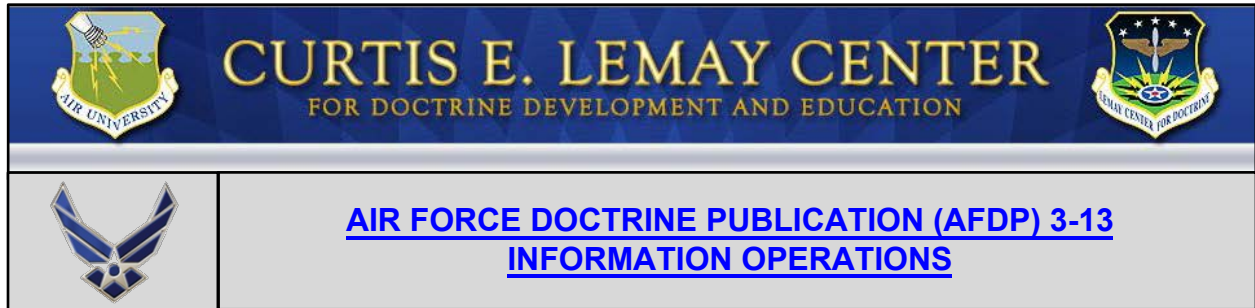
ORGANIZATION OF INFORMATION OPERATIONS

Last Reviewed: 28 April 2016

Air Force [information-related capability](#) (IRC) planners operating in-theater under the [operational control](#) (OPCON) of the [commander, Air Force forces](#) (COMAFFOR) are typically assigned or attached to an [air expeditionary task force](#) (AETF). Within the AETF, IRC forces are normally attached to an air expeditionary wing, group, or squadron. The COMAFFOR normally exercises command and control (C2) of the AETF through an A-staff and an [air operations center](#) (AOC). See AFDP 3-30, *Command and Control*, for further discussion of [C2 mechanisms](#).

The Air Force embeds information operations (IO) and IRC expertise within the AFFOR staff, AOC IO team or the [joint force commander's](#) (JFC's) IO staff or cell to facilitate IRC integration and operations. Component staffs address component objectives and the desired effects required to achieve them. Also, the Air Force may augment other staffs with IO and IRC expertise to assist with tasking IRCs in-theater and integrating global IRCs and effects. IO planning should be coordinated during planning at the JFC and air component level, by AFFOR and AOC staffs. Planners at both levels should coordinate adaptive planning processes with supporting commands for IO.

As an example, US Air Forces Central Command's combined air operations center established a non-lethal effects team and non-lethal effects duty officer, similar to the IO team and IO duty officer. It was organized to focus primarily on integrating [electronic warfare](#), [cyberspace](#), and [space](#) effects into the JFC's operation, as opposed to integrating all non-lethal effects. The processes and organizational constructs by which non-lethal effects are integrated are based on individual commander's requirements and thus vary widely across AOCs.



PRESENTATION OF INFORMATION OPERATIONS PLANNERS AND INFORMATION-RELATED CAPABILITY FORCES

Last Updated: 28 April 2016

When directed, the Air Force presents information operations (IO) planners and information-related capability (IRC) forces to [combatant](#) commanders (CCDRs) to meet national-level and theater-level taskings.

The [IO staff](#) and planning function for a theater component is typically presented as a function within an [air operations center \(AOC\)](#) and on the [commander, Air Force forces'](#) (COMAFFOR's) staff. The AFFOR and AOC IO planners typically serve as a focal point for coordinating requirements for reachback support from IRCs outside of theater and should ensure their plans and support are in line with joint IO across the joint operations area.

An AOC normally includes an IO team that coordinates with all of the AOC divisions and with counterpart IO elements at other commands and task forces. The IO team may be attached to the AOC's strategy division and coordinate with the other AOC divisions, or the IO team may report direct to the AOC commander as a cross-cutting specialty team. Also within the AOC, an IO duty officer is typically assigned to work alongside other specialty duty officers for the senior duty officer or directly for the chief of combat operations.

Service and Functional IO Responsibilities

IO planners and IRC specialists on the Service and functional component staffs fill critical roles needed to successfully integrate IRC tasks and effects into theater operations. AFFOR and AOC specialists share a common effort in support of the commander's objectives and complement each other's responsibilities. The two staffs coordinate regularly to ensure consistency in focus and that their respective responsibilities and external relationships are appropriately deconflicted.

In general, the AFFOR IO staff coordinates planning actions at the [joint force commander](#) or CCDR level. In addition to internal AFFOR coordination, the AFFOR IO staff coordinates with the AOC IO team, component MAJCOM and NAF staffs, the joint staff, and functional and geographic combatant command staffs to:

- ✦ Request IRC forces and IO support (e.g., request for forces).
- ✦ Establish supporting-supported command relationships and authorities for IO planning and IRC tasking (e.g., [direct liaison authorized](#) [DIRLAUTH], electronic warfare coordinating authority).
- ✦ Facilitate deployment, beddown, and redeployment of unit-level IRC forces (e.g., deployment order, time-phased force and deployment data).
- ✦ Provide IO and IRC input on strategic/campaign-level operation planning documents (e.g., [theater campaign plans](#), [concept plans](#), [operation orders](#)).

In contrast, the AOC IO staff coordinates planning and tasking actions at the joint task force (JTF)-level. In addition to internal AOC coordination, the AOC IO team coordinates with IRC contacts on [air expeditionary task force](#) (AETF) staffs, IO contacts on JTF staffs, and IO contacts on other theater component staffs to:

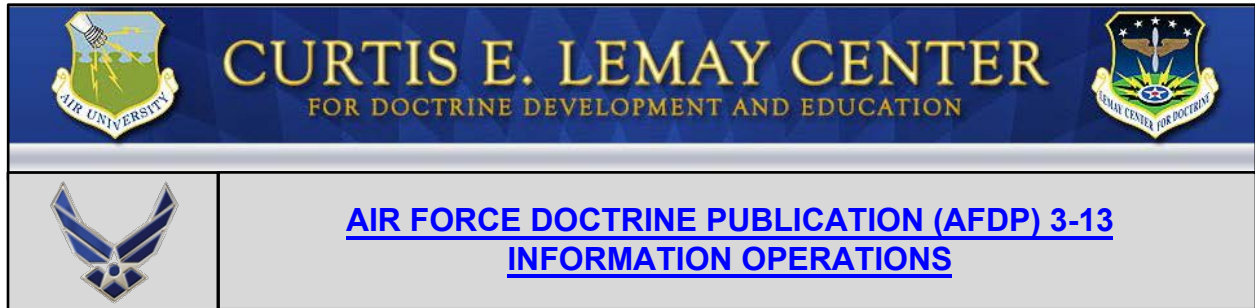
- ✦ Provide input on operation planning documents (e.g., annexes/appendices, [joint air operations plan](#), air operations directive).
- ✦ Coordinate themes, messages, and actions, approvals (e.g., [rules of engagement](#), airspace control order), tasking orders (e.g., air/space/cyber tasking order),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

Example forums (or mechanisms) for coordination and commander's updates may be the joint targeting coordination board, joint collection management board, and battlestaff update brief.

Reachback and Federated Support for IO

Commanders and their staffs should consider leveraging other resources and capabilities available through reachback and federation to support theater IO and IRC activities. There are many Service, joint, Department of Defense, interagency, and national organizations referenced in this publication that can provide additional support to theater IO efforts. For instance, the [National Air and Space Intelligence Center](#) and the [363d Intelligence Surveillance Reconnaissance Group](#) may be able to provide behavioral analysis and targeting products to meet IRC operational requirements. The AOC combat plans, strategy, and ISR divisions should be the main organizations in-theater requesting additional support. The need to establish command relationships for requesting reachback support may vary depending on the purpose and extent of support. If any formal relationship is needed for developing plans, DIRLAUTH is usually appropriate. Command relationships for executing operations may range from nothing formal required (i.e., standard tasking processes are sufficient) to formal establishment

of tactical control (i.e., for dedicated, responsive support). Support established by formal agreement is termed “federated.”



PLANNING AND INFORMATION OPERATIONS

Last Updated: 28 April 2016

Properly integrated employment of information-related capabilities (IRCs) can create desired effects that accomplish objectives at tactical, operational, and strategic levels. Information operations (IO) is a critical military function because it presents viable options to commanders for conducting operations across the range of military operations (ROMO), not just during hostilities. IRCs can be used in restricted, contested, or politically sensitive areas where traditional air, land, and sea operations may not be permitted. The employment and phasing of IRCs may vary based on mission or availability, but the function of IO has broad application and effects. IO should be incorporated seamlessly and early throughout the [operation planning, execution, and assessment processes](#), because of its broad application and effects and also because of its inherent challenges. The large number of potential IRCs that may be applied and the complexity of integration require extensive coordination. While IO requires early and extensive planning, there should not be a separate IO planning process or IO plan from the standard [joint operation planning process](#) (JOPP) and products. IO planners should provide appropriate inputs during each step of the JOPP for air (JOPPA) and the air tasking cycle.

Multiple IRCs can be integrated into planning across the ROMO. IO integration of IRCs is planned within the framework of the JOPP. IO planning should be integrated into the [joint force commander's](#) (JFC's) [deliberate and crisis action planning](#). Moreover, IRCs should be integrated throughout the plans, then developed and executed by all supporting commands. Supporting component planning should be consistent with [campaign plans](#), [operation plans](#) (OPLANs) and [operation orders](#) (OPORDs) developed by the JFC.

Multiple annexes in operation planning products contain IO contributions to the overall effort and should be reviewed by the IO planner. Development of these annexes is the supported commander's responsibility but requires coordinated effort between the JFC, supporting combatant commands, and component level staffs.¹

Deliberate Planning

During [deliberate planning](#), theater planners normally incorporate IO planning into theater campaign plans (TCPs) and OPLANs. However, IO requirements should be

¹ JP 5-0, [Joint Operation Planning](#), provides a list of joint operation planning products.

considered as part of the overall campaign or operational plan, and thought should be given to use of IO during operational design; such requirements should not simply be limited to a single appendix or single phase of an OPLAN. IO planning should be embedded throughout the planning process so that IRCs are appropriately integrated into every phase of the commander's plan. The majority of deliberate planning occurs within the Air Force Service component, AFFOR; consequently, IO and IRC planners should be embedded throughout the [AFFOR staff, especially the A-3 and A-5](#). Planners should ensure IO is thoroughly addressed in a campaign support or contingency support plan's primary annex, Annex C, Operations (Appendix 3), and should coordinate closely with other lead planners to ensure IO is tied into all relevant annexes.

Reachback support

Reachback support may be requested to provide IRC-specific expertise or information to augment theater planning. This cooperation facilitates a comprehensive and realistic development of force requirements in support of theater OPLANs. Likewise, IRC requirements and IO planning considerations should be included in [functional combatant commander's](#) plans supporting theater operations. Planners should also ensure deployable IRCs are included in the time phased force and deployment data. Integration of IRCs is the responsibility of the [geographic combatant commander](#) and the [commander, Air Force forces \(COMAFFOR\)](#). The need to establish formal command relationships for reachback, or federated, support may vary depending on the purpose and extent of support.

Crisis Action Planning

Because of the time-sensitive nature of [crisis action planning](#), it may be challenging to address IRC requirements if not previously identified. Certain IRCs may need substantial lead time for coordination up to the Secretary of Defense (SecDef)-level due to their political sensitivity or because they are controlled by other organizations such as national agencies, civil organizations, or even commercial enterprises. The end result of crisis action planning produces [OPORDs](#) and fragmentary orders that can be executed to satisfy SecDef direction.

Again, commanders should consider IO options throughout operational design and planning, and IRCs should be fully integrated into the development of all [courses of action \(COAs\)](#). During COA development, IO planners should identify tasks for IRCs in support of theater objectives and examine the role and contributions of IRCs in the various phases of the OPLAN. Knowledge of global and theater IRCs will enable the commander to make an informed decision. IO planners should also be embedded in red teams during COA wargaming.

Plan Development

Theater planning can help integrate IRCs and effects throughout the JFC's TCP or OPLAN. For OPLANs, this is normally accomplished through the JOPPA, which combines the mission activities and desired effects into a coherent plan to support the

JFC's overall plan.² The result is the joint air operations plan (JAOP). Again, there is no separate IO planning process or plan. The JAOP should include the integration of all allocated and assigned theater IRCs and all requests for theater support from global-mission IRCs. Theater IRCs, and effects derived from deployed and organic theater IRCs under the COMAFFOR's control, should be integrated into day-to-day operations through the air tasking order. The majority of JAOP development occurs within the air operations center (AOC); consequently, IO planning and IRC expertise should be embedded throughout the AOC. Finally, IO and IRC planners may coordinate with functional operations centers to synchronize and deconflict the development of their planning products such as the joint space operations plan and the space operations directive.

Planning Factors

As an integrating function, the IO planner is typically not responsible for the specific employment planning of the provided IRC. For instance, the electronic warfare (EW) coordination cell plans and employs EW capabilities, the [intelligence, surveillance, and reconnaissance](#) (ISR) collection manager and platform liaison plans and employs ISR capabilities, and the AFFOR A6 is responsible for planning theater communications. Some IRC 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 information environment, resources may not always be available for use.

Global-Theater Integration

Many IRCs have global requirements for national defense, requests from multiple theaters, and are continuously employed or executing tasking orders. This requires timely deconfliction and integration with other elements of the theater operation. Integrating various IRCs is accomplished through deliberate coordination processes between the theater AOCs and functional operations centers. The employment of IRCs at the operational level is accomplished through tasking orders that deconflict and integrate the full range of capabilities with theater operations. Theater IO and IRC planners should coordinate with functional operations centers to synchronize and deconflict the ATO with functional tasking orders, such as the joint space tasking order and cyber tasking order.

Joint Intelligence Preparation of the Operational Environment (JIPOE)

[JIPOE](#) provides commanders at all levels with knowledge of the information environment to effectively conduct planning. Knowledge of the information environment enables commanders to anticipate future conditions, establish priorities, and exploit emerging opportunities. JIPOE is a continuous analytical process to describe the operational environment, evaluate the adversary and other actors, and help determine adversary COAs. IO and IRC planners especially require detailed analysis of the information environment, including:

² See [JP 3-30, Command and Control for Joint Air Operations](#), and [AFDP 3-0, Operations and Planning](#), for more information on the JOPPA and products such as the JAOP and air operations directive.

- ★ Command and control networks, organizations, and infrastructure.
- ★ Media infrastructure.
- ★ Cultural demographics of the population and subgroups.
- ★ Key decision makers and their behavioral patterns, decision-making processes, and advisors/relationships.
- ★ Adversary exploitation of the information environment.
- ★ Key communicators.

Given the long lead times often required for producing IO-relevant intelligence, requirements should be identified as early as possible in the planning process. An established IO-intelligence relationship will help with understanding types of information available and better defining requirements.

Sequencing and Phasing of IO

Understanding the sequence of operations over time is critical to effective planning. Commanders and planners often use phasing as a way 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 there will often be some simultaneous and overlapping execution of the activities within the phases.

During the shaping and/or deterrence phase(s) (often “phase 0 or phase 1” of an operation in OPLANS³), joint IO is often the main means by which the combatant commander or JFC can deter aggression and prevent escalation of hostilities. Often, the objective is to convince adversaries that planned or potential COAs that threaten the United States’ vital interests are so undesirable that they give up hostile plans and choose COAs more favorable to US objectives. While conducting operations intended to seize the initiative from an adversary, IO efforts may still be focused on garnering support for unified actions and establishing conditions conducive to political solutions to the situation. At the same time, the JFC must prepare IO for potential hostilities, including recognizing and preempting dangers inherent in the information environment.

During portions of an operation devoted to seizing the initiative and dominating an enemy, IO planning will likely involve developing advantages across the information environment to facilitate execution of component missions (such as gaining and maintaining air superiority and other major combat). Normally, the objective in these

³ See JPs 3-0, [Joint Operations](#) and 5-0, [Joint Operation Planning](#) for a discussion of the joint phasing model.

phases is to break the enemy's will for organized resistance, reduce casualties and collateral damage, act as a force multiplier, and hasten and smooth transition to post-conflict operations.

During the stabilization phase(s) of an operation, IO once again may become the main effort. It should be flexible enough to simultaneously support stabilization and combat operations. The objective is to change the perceptions and behaviors towards favoring US and multinational objectives, support the peacetime elements of friendly policy, and assess the impact of current operations on the ability to transfer overall regional authority to a legitimate civil entity. During phases devoted to legitimizing civil authority, IO should help influence the attitudes of local and regional populations to regard friendly civil authority objectives favorably.

Planning for Effects

All planners, including IO and IRC planners, should approach planning problems using an effects-based perspective. The IO planner's focus is not just about the integrated employment of IRCs, but more so on creating desired effects to achieve military objectives. Therefore, an [effects based approach to operations](#) (EBAO) is an ideal approach to IO planning. IO focuses primarily on affecting the cognitive dimension of the information environment. Effects can manifest at the tactical, operational, and strategic levels depending on the message or action, so IO and IRC planners should consider that any tactical action can result in strategic effects.⁴

Direct and Indirect Effects

IO planners should [consider the indirect effects](#) that IRCs may create beyond the direct effects. Indirect effects from IRC actions tend to resonate more with the audience and manifest in desired behavior and decision making. However, they take time to manifest and are more difficult to identify, characterize, and attribute. Because indirect effects take time to manifest and are more difficult to assess, IO planners should coordinate requirements and planning early and manage the commander's expectations for timing of approval and results.

Additionally, IO planners should not overlook the importance of pre-planning certain responses to proactively counter actions an adversary is known to take. For example, if an adversary is known to exploit damaged areas by publishing falsified or misleading images, or providing those images to media outlets, IO planners could account for such actions before the mission is executed, during the targeting process. For any mission occurring in an area known for this type of exploitation, IO planners could request friendly assets in the area collect post-event imagery to ensure an accurate image is available should the need arise. Such a response would serve as a counterpropaganda effort before the adversary's attempts gained any ground.

Unintended Effects

⁴ See AFDP 3-0, [Operations and Planning](#), for a description of effects and EBAO.

All actions have the potential to generate [unintended effects or consequences](#), whether caused by error, inadequate planning, or unforeseen circumstances. Examples of an unintended direct effect may be collateral damage from an air strike or collateral interference from electronic jamming. Examples of unintended indirect effects may be a local village unwilling to provide a safe area for downed airmen or a host nation government denying access to airspace. All planners, including IO planners and IRC planners, should possess a deeper understanding of indirect behavioral effects and should proactively coordinate on plan annexes and target lists to identify potential risks of unintended effects; as well as consult with political and legal advisors, CCS representatives, and targeteers for information regarding [rules of engagement](#) and prohibited/restricted targets lists.

Targeting

Targeting is defined as “the process of selecting and prioritizing targets and matching the appropriate response, considering operational requirements and capabilities.”⁵ Targeting supports the process of linking the desired effects to actions and tasks. The IO and IRC planner should participate in all aspects of the joint targeting cycle, to include developing targets for nomination to the joint force target list.

See AFDP 3-60, [Targeting](#), for further information.

⁵ JP 3-60, [Joint Targeting](#).



CURTIS E. LEMAY CENTER

FOR DOCTRINE DEVELOPMENT AND EDUCATION



AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-13 INFORMATION OPERATIONS

EXECUTION AND INFORMATION OPERATIONS

Last Updated: 28 April 2016

Execution is a dynamic combination of theater and global operational processes requiring timely integrated employment of [information-related capabilities](#) (IRCs) throughout the joint operation plan.

The [commander, Air Force forces](#) (COMAFFOR) tasks IRC forces to execute operations via the tasking process, which is a part of the [joint operation planning process for air](#) (JOPPA). Within the [air operations center](#) (AOC), [information operations](#) (IO) and IRC specialists coordinate integration of IRC forces, mission, targets, and effects into theater operations via the joint air tasking cycle. Depending on the supporting IRC force, owning command, and relationship, the [air tasking order](#) (ATO) alone may constitute all the tasking information and coordination required to task an IRC force. However, tasking an IRC force will likely require IO and IRC specialists to coordinate with other theater operations centers or functional operations centers, which typically generate corresponding tasking orders of their own. Properly generated and coordinated taskings are vital to successful integration of theater and global operations. Not all operations, actions, and activities (OAAs) however, are captured in an ATO (e.g. engagements, exchanges, Red Horse projects, cyberspace operations). IO planners should maintain awareness of OAAs that have cognitive/behavioral impacts and integrate them into planning efforts

For assigned and attached IRC forces in-theater, execution of operations is tasked via the ATO. IO and IRC specialists primarily coordinate with tasking leads in the AOC's combat operations division and situationally advise external points of contact. For theater IRC forces assigned but not attached to the COMAFFOR, IO and IRC specialists coordinate with other theater operations centers to task those theater forces. For assigned IRC forces operating from outside of theater, this involves global IRCs, IO, and IRC specialists coordinating with functional operations centers to task those global forces through their corresponding tasking cycles (e.g., joint space tasking cycle) and tasking orders (e.g., joint space tasking order, cyber tasking order).

See AFDP 3-0, [Operations and Planning](#), for further information.



CURTIS E. LEMAY CENTER FOR DOCTRINE DEVELOPMENT AND EDUCATION



AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-13 INFORMATION OPERATIONS

ASSESSMENT AND INFORMATION OPERATIONS

Last Updated: 28 April 2016

Assessment is the determination of the overall effectiveness of operations and should be an iterative process. Because of the information operations (IO) planner's integrating nature and focus on affecting the cognitive domain, it is challenging to assess the success of IO. Information-related capability (IRC) effects, especially second- and third-order effects, may not manifest themselves until later in time. Consequently, measurements of effectiveness may be absent or incomplete. Additionally, identifying a cause and effect relationship can often be difficult. IO planners should generate valid measures for all desired effects and coordinate with the intelligence community to ensure that measures chosen are observable by the available collection capability. The employment of IRCs should be assessed to determine if they have been effective in achieving the commander's objectives. Assessment should include observable changes in the specific audience, methods of detection, and the relationship between cause and effect. The ambiguities and limitations resident within the information environment require frequent adjustment of operational planning considerations to ensure desired effects are generated while avoiding specifically designated or unintended negative consequences.

The [commander, Air Force forces](#) is normally responsible for evaluating results of IO. There are two primary types of assessments accomplished, operational and tactical. The operational-level assessment is usually executed within the strategy division of the [air operations center](#) (AOC). The tactical assessment is generally performed by the [intelligence, surveillance, and reconnaissance division](#) (ISR/D) of the AOC.

Assessment at the operational level focuses on both performance and effects via [measures of performance](#) (MOPs) and [measures of effectiveness](#) (MOEs), respectively. MOPs and MOEs can both be measured either quantitatively or qualitatively. MOPs are criteria used to assess friendly accomplishment of IRC tasks and mission execution (e.g., if the desired effect is to decrease the number of violent crimes, then the MOP is to increase security or police forces within the target population). They help determine if delivery methods are actually reaching the intended specific audience. In contrast, MOEs are criteria used to assess changes in system behavior, capability, or operational environment to determine whether IO actions being executed are creating 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).

Operational-level planners and analysts should develop an intimate understanding of the linkage between IRCs and the intended effect. This requires direct feedback from those closest to observing the intended effects, such as the IRC specialists executing IO missions or the supported warfighters. IO assessment may also require coordination of collection requirements with the AOC ISRD.
