Chapter 1

Information Operations Overview

1-1. Conflict is fundamentally a contest of wills. Winning this contest requires commanders to employ combat power to execute decisive action across the range of military operations. *Combat power* is the total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time (ADRP 3-0). Combat power is comprised of eight elements, the last six of which are warfighting functions: leadership, information, mission command, movement and maneuver, intelligence, fires, sustainment, and protection.

1-2. Information operations (IO) creates effects in and through the information environment. IO optimizes the information element of combat power and supports and enhances all other elements in order to gain an operational advantage over an enemy or adversary. These effects are intended to influence, disrupt, corrupt or usurp enemy or adversary decision making and everything that enables it, while enabling and protecting friendly decision making. Because IO's central focus is affecting decision making and, by extension, the will to fight, commanders personally ensure IO is integrated into operations from the start.

SECTION I –OPERATIONAL AND INFORMATION ENVIRONMENTS

1-3. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). It encompasses physical areas and factors of the air, land, maritime, space, and cyberspace domains, and the information environment, which includes cyberspace. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). Although an operational environment and information environment are defined separately, they are interdependent and integral to the other.

OPERATIONAL ENVIRONMENT

1-4. Several characteristics of the operational environment have a significant impact on land force operations. Each of these characteristics has a significant information aspect. They are:

- Speed and diffusion of information.
- Information asymmetry.
- Proliferation of cyberspace and space capabilities.
- Operations among populations.

1-5. Across the globe, information is increasingly available in near-real time. The ability to access this information, from anywhere, at any time, broadens and accelerates human interaction, across multiple levels (person to person, person to organization, person to government, government to government). Social media, in particular, enables the swift mobilization of people and resources around ideas and causes, even before they are fully understood. Disinformation and propaganda create malign narratives that can propagate quickly and instill an array of emotions and behaviors from anarchy to focused violence. From a military standpoint, information enables decision making, leadership, and combat power; it is also critical to seizing, gaining and retaining the initiative, and consolidating gains in the operational environment.

1-6. Threats, large and small, increasingly operate in an indeterminate zone between peace and war. They seek to avoid U.S. strengths and, instead take advantage of U.S. laws and policies regarding the use of information and cyber capabilities. Coupled with the nation's initial reluctance to engage in major combat operations, they achieve incremental gains that advance their agenda and narrative. They use a range of techniques including non-attribution, innuendo, propaganda, disinformation, and misinformation to sway global opinion favorable to their aims.

1-7. States and non-states are rapidly expanding their investment in cyberspace and space capabilities and forces. They recognize the leveling effect these domains, especially cyberspace, offer in terms of achieving parity or overmatch at minimum relative cost. A significant portion of the threat's information asymmetry comes from its growing capacity in space and cyberspace.

1-8. Threats operate among populations with whom they often share cultural or ethnic identity, making it difficult to distinguish threat from non-threat. This fact requires U.S. forces to interact and communicate, in nuanced fashion, with a wide range of audiences and actors in order to separate those willing to support U.S. intentions from those who are not. The ability of the threat to operate among populations and harness commonalities provides the threat yet another asymmetric advantage.

INFORMATION ENVIRONMENT

1-9. The information environment is not separate or distinct from the operational environment but inextricably part of it. In fact, any activity that occurs in the information environment simultaneously occurs in and affects one or more of the operational environment domains.

1-10. The information environment is comprised of three dimensions: physical, informational, and cognitive. Within the physical dimension of the information environment is the connective infrastructure that supports the transmission, reception, and storage of information. Also within this dimension are tangible actions or events that transmit a message in and of themselves, such as patrols, aerial reconnaissance, and civil affairs projects. Within the informational dimension is the content or data itself. The informational dimension refers to content and flow of information, such as text or images, or data that staffs can collect, process, store, disseminate, and display. The informational dimension provides the necessary link between the physical and cognitive dimensions. Within the cognitive dimension are the minds of those who are affected by and act upon information. These minds range from friendly commanders and leaders, to foreign audiences affecting or being affected by operations, to enemy, threat or adversarial decision makers. This dimension focuses on the societal, cultural, religious, and historical contexts that influence the perceptions of those producing the information and of the targets and audiences receiving the information. In this dimension, decision makers and target audiences are most prone to influence and perception management.

1-11. The information environment has increased in complexity. Due to the widespread availability of the Internet, wireless communications and information, the information environment has become an even more important consideration to military planning and operations, because the military increasingly relies on these technologies. Activities occurring in and through the information environment have a consequential effect on the operational environment and can impact military operations and outcomes. Therefore, commanders and their staffs must understand the information environment, in all its complexity, and the potential impacts it will have on current and planned military operations.

SECTION II – INFORMATION OPERATIONS DEFINED AND DESCRIBED

1-12. *Information Operations* (IO) is the integrated employment, during military operations, of information-related capabilities 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 (JP 3-13). This manual uses the term IO comprehensively to capture all activity employed to affect the information environment and contribute to operations in and through the information environment. IO includes:

- Integration and synchronization of information-related capabilities.
- Planning, preparing, execution, and assessment.
- The capability and capacity that ensures the accomplishment of IO, to include the units and personnel responsible for its conduct.

Breaking down the definition into constituent parts helps to understand its meaning and implications for land forces.

Integrated Employment of Information-Related Capabilities (IRCs)

1-13. IO brings together IRCs at a specific time and in a coherent fashion to create effects in and through the information environment that advance the ability to deliver operational advantage to the commander. While IRCs create individual effects, IO stresses aggregate and synchronized effects as essential to achieving operational objectives.

1-14. An *information-related capability* (IRC) is a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions (JP 1-02). The formal definition of IRCs encourages commanders and staffs to employ all available resources when seeking to affect the information environment to operational advantage. For example, if artillery fires are employed to destroy communications infrastructure that enables enemy decision making, then artillery is an IRC in this instance. In daily practice, however, the term IRC tends to refer to those tools, techniques, or activities that are inherently information-based or primarily focused on affecting the information environment. These include—

- Military deception.
- Military information support operations (MISO).
- Soldier and leader engagement (SLE), to include police engagement.
- Civil affairs operations.
- Combat camera.
- Operations security (OPSEC).
- Public affairs.
- Cyberspace electromagnetic activities.
- Electronic warfare.
- Cyberspace operations.
- Space operations.
- Special technical operations.

1-15. All unit operations, activities, and actions affect the information environment. Even if they primarily affect the physical dimension, they nonetheless also affect the informational and cognitive dimensions. For this reason, whether or not they are routinely considered an IRC, a wide variety of unit functions and activities can be adapted for the purposes of conducting information operations or serve as enablers to its planning, execution, and assessment. Some of these include, but are not limited to:

- Commander's communications strategy or communication synchronization.
- Presence, profile, and posture.
- Foreign disclosure.
- Physical security.
- Physical maneuver.
- Special access programs.
- Civil military operations.
- Intelligence.
- Destruction and lethal actions.

During Military Operations

1-16. Army forces, as part of a joint force, conduct operations across the conflict continuum and range of military operations. Whether participating in security cooperation efforts or conducting major combat operations, IO is essential during all phases (0 through V) of a military operation. (See JP 5-0 for a detailed discussion of the joint phasing model).

In Concert with Other Lines of Operation

1-17. Commanders use lines of operations and lines of effort to visualize and describe operations. A *line of operations* is a line that defines the directional orientation of a force in time and space in relation to the enemy and that links the force with its base of operations and objectives (ADRP 3-0). Lines of operations connect a series of decisive points that lead to control of a geographic or force-oriented objective. A *line of effort* is a line that links multiple tasks using the logic of purpose rather than geographical reference to focus efforts toward establishing operational and strategic conditions (ADRP 3-0). Lines of effort are essential to long-term planning when positional references to an enemy or adversary have little relevance. Commanders may describe an operation along lines of operations, lines of effort, or a combination of both. Commanders, supported by their staff, ensure information operations are integrated into the concept of operation to support each line of operation and effort. Based on the situation, commanders may designate IO as a line of effort to synchronize actions and focus the force on creating desired effects in the information environment. Depending on the type of operation or the phase, commanders may designate an IO-focused line of effort as decisive.

TO INFLUENCE, DISRUPT, CORRUPT, OR USURP

1-18. IO seeks to create specific effects at a specific time and place. Predominantly, these effects occur in and through the information environment. Immediate effects (disrupt, corrupt, usurp) are possible in the information environment's physical and informational dimensions through the denial, degradation, or destruction of adversarial or enemy information-related capabilities. However, effects in the cognitive dimension (influence) take longer to manifest. It is these cognitive effects—as witnessed through changed behavior—that matter most to achieving decisive outcomes.

THE DECISION MAKING OF ENEMIES AND ADVERSARIES

1-19. While there are differences among the terms adversaries, threats, and enemies, all three refer to those individuals, organizations, or entities that oppose U.S. efforts. They therefore must be influenced in some fashion to acquiesce or surrender to or otherwise support U.S. national objectives by aligning their actions in concert with commanders' intent. [The joint phrasing "adversaries and potential adversaries" is revised to "enemies and adversaries" to better align with Army terminology.]

1-20. Affecting enemy and adversary decision making necessitates affecting all contributing factors that enable it. These factors include, but are not limited to:

- Command and control systems, as well as other systems that facilitate decision making.
- Communications systems.
- Information content (words, images, symbols).
- Staffs, advisors, counselors, and confidants.
- Human networks and constituencies that influence the decision maker and to whom the decision maker seeks to influence; in other words, all relevant audiences in the areas of operations and interest.

WHILE PROTECTING OUR OWN

1-21. Friendly commanders, like enemy and adversary leaders, depend on an array of systems, capabilities, information, networks, and decision aids to assist in their decision making. Gaining operational advantage in the information environment is equally about exploiting and protecting the systems, information, and people that speed and enhance friendly decision making, as it is about denying the same to the threat.

THE PURPOSE OF INFORMATION OPERATIONS

1-22. The purpose of IO is to create effects in and through the information environment that provide commanders decisive advantage over enemies and adversaries. Commanders achieve this advantage in several ways: preserve and facilitate decision making and the impact of decision making, while influencing, disrupting or degrading enemy or adversary decision making; get required information faster and with greater accuracy and clarity than the enemy or adversary; or influence the attitudes and behaviors of relevant audiences in the area of operations having an impact on operations and decision making.

1-23. To support achievement of these various ways, IO employs and synchronizes IRCs to affect the will, awareness, understanding, and capability of these audiences, while protecting our own. Will, awareness, understanding, and capability all contribute to and sustain decision making and, if compromised, can impair that decision making. In terms of will, awareness, understanding, and capability, advantage is achieved when commanders preserve their will to fight, as well as their situational understanding and their full capacity and ability to prosecute operations. Further, commanders achieve advantage when they preserve their freedom of action in the information environment while degrading enemy or adversary freedom of action.

THREE INTERRELATED EFFORTS

1-24. IO is comprised of three inter-related efforts: a commander-led staff planning and synchronization effort; a preparation and execution effort carried out by IRC units, IO units, or staff entities in concert with the IO working group; and an assessment effort carried out by all involved. These three efforts work in tandem and overlap each other.

1-25. The planning and synchronization effort includes planning and synchronizing IRC employment to create effects in and through the information environment that result in advantage over the threat. Preparation and execution involves positioning and employing IRC assets in accordance with the IO working group synchronization plan to create desired effects at the right place and time. Assessment involves determining whether planned effects were achieved and recommending adjustments, as necessary.

1-26. The IO officer, IO working group, and the assistant chief of staff, intelligence (G-2/S-2), especially, contribute to the assessment. The IO officer prepares the IO portion of the assessment plan. The IO working group monitors execution of the assessment plan and compares desired results with actual results. The G-2 (S-2), in coordination with the assistant chief of staff, operations (G-3/S-3), contributes by ensuring collection assets are available and tasked to gather information needed to validate measure of effectiveness.

ARMY-JOINT RELATIONSHIPS

1-27. IO, by its nature, is joint. Based on the theater campaign plan, each service component contributes to an integrated whole synchronized by the joint force headquarters. Army IO supports joint force missions two ways. The first is when Army or land component command IRCs are specifically tasked to support a joint force mission. The second is when the Army or land component command, in its support of the joint force, develops its own IO plan, specific to its mission and area of operations. In both instances, IRCs are synchronized across the joint force to create desired effects in and through the information environment, as well as prevent the diminishment or negation of one IRC's effects by another. In multinational operations, the U.S. joint force commander is responsible for coordinating the integration of U.S. IO with multinational information activities.

1-28. The IO officer at joint force headquarters (J-39) synchronizes joint IO efforts. All component commands participate in a synchronization process to maximize effects in the information environment. The process is informed by an IO working group, cell, or virtual center that delivers its recommendations to various decision-making boards. Examples include the Joint Targeting Coordination Board and Joint Intelligence Collection Board. The J-39 provides a staff capability that synchronizes all service-specific IRCs to achieve unity of effort in support of the joint force. Army forces submit requests for IRC or IO unit support and deconfliction measures through multiple channels to higher echelons. For example, requests may go through the J-6 for spectrum management, through liaison at the Air Operations Center for electronic warfare support, through a supporting cyberspace operations center for an effects request, or through the targeting cell for targeting vetting and validation. The J-39 and joint IO cell are kept informed in order to publish plans and orders depicting, maximizing, and assessing mutual support mechanisms for the joint force commander.

INFORMATION OPERATIONS ACROSS THE RANGE OF MILITARY OPERATIONS

1-29. Army forces conduct IO within joint force parameters. From peace to war, and across the range of military operations, commanders integrate and synchronize IO to focus combat power and gain advantage in the information environment. In all situations, Army forces do not act in isolation. Army forces conduct operations in support of a larger joint or multinational plan. Figure 1-1, on page 1-6, depicts the three main categories of military operations within the range of military operations construct:

- Military engagement, security cooperation, and deterrence.
- Crisis response and limited contingency operations.
- Major operations and campaigns.

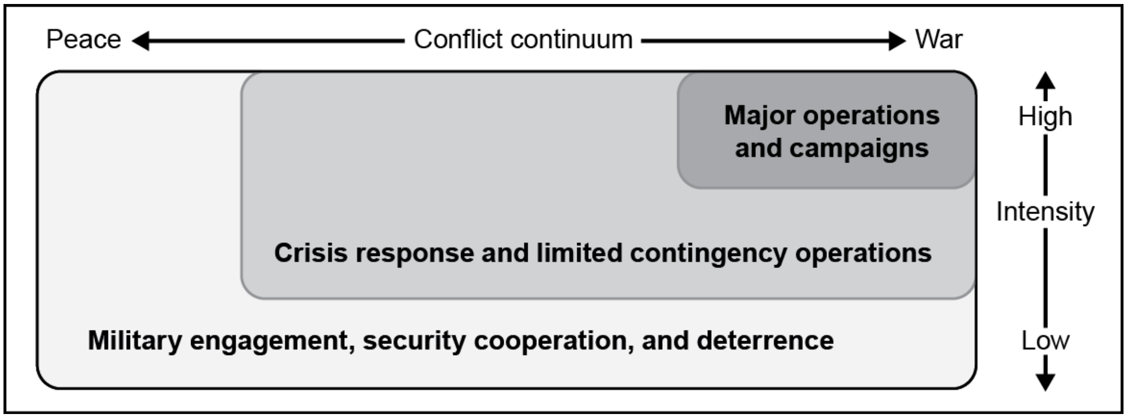
Peace
Conflict continuum
War
Major operations and campaigns
Crisis response and limited contingency operations
Military engagement, security cooperation, and deterrence
High
Intensity
Low

Figure 1-1. The range of military operations across the conflict continuum

MILITARY ENGAGEMENT, SECURITY COOPERATION, AND DETERRENCE

1-30. Military engagement, security cooperation, and deterrence operations are ongoing and recurring military activities that establish, shape, maintain, and refine relations with other nations and domestic civil authorities. The general objective is to protect U.S. interests at home and abroad. IO contributes significantly to military engagement, security cooperation, and deterrence. Military engagement and security cooperation depend heavily on influencing partners and potential partners to align with U.S. interests and, thereby, prevent threats from achieving objectives in or through these same partners and the countries and regions they inhabit. Military engagement and security cooperation are themselves forms of deterrence, but other forms are possible. Deterrence is not only the actual capacity to harm another state or non-state entity who fails to comply with or accommodate U.S. demands, but also the perception of that entity that the U.S. has the ability to do harm, if provoked. IO provides essential support to the shaping and maintaining of this perception through, among other things, the protection of friendly information (OPSEC).

1-31. Complementing IO support to military engagement, security cooperation, and deterrence, as well as crisis response, contingency operations and major operations and campaigns is the Attack the Network framework. This framework consists of activities that employ lethal and nonlethal means to support friendly networks, influence neutral networks, and neutralize threat networks. Since the aim of this framework and the purpose of IO are highly similar, commanders ensure their close coordination. (See ATP 3-90.37 for more information).

CRISIS AND LIMITED CONTINGENCY OPERATIONS

1-32. Contingencies and crisis response operations may be single small-scale, limited-duration operations or a significant part of a major operation of extended duration involving combat. General objectives are to protect U.S. interests and prevent surprise attack or further conflict. These operations typically occur during periods of slightly increased U.S. military readiness, and the use or threat of force may be more probable. Many of these operations involve a combination of military forces in close cooperation with other organizations. Examples include counter-terrorism operations; counter-proliferation; sanctions enforcement; noncombatant evacuation operations; peacekeeping and peace enforcement operations; show of force; strikes and raids; and support to counterinsurgency.

1-33. Army forces conduct IO in accordance with existing contingency or crisis action plans (see JP 5-0). A potential or actual contingency requires commanders at all echelons to gather additional information and refine their contingency plans based on a specific area of operations or target set. Geographic combatant commanders may use the relationships and conditions in the information environment created during peace to influence threat decision makers to act in ways that will resolve the crisis peacefully. Other IO efforts may attempt to influence actors within a target group's political, economic, military, and social structures. Operational and tactical commanders prepare for IO as part of their deployment preparations. They coordinate preparations with the joint force commander to ensure unity of effort and prevent ***information fratricide*****, which is defined as adverse effects on the information environment resulting from a failure to effectively synchronize the employment of multiple information-related capabilities which may impede the conduct of friendly operations or adversely affect friendly forces**.

1-34. The objectives during crisis are to halt escalation and move the level of conflict back towards peace. Therefore, commanders conduct IO to develop the situation and refine their situational understanding. Through the deliberate selection and effective synchronization of IRCs, commanders increase the potential that adversaries or other relevant decision makers will choose alternatives other than conflict or war.

MAJOR OPERATIONS AND CAMPAIGNS

1-35. Major operations and campaigns are large-scale, sustained combat operations to achieve national objectives and protect national interests. Such operations may place the United States in a wartime state and are normally conducted against a capable enemy with the will to employ that capability in opposition to or in a manner threatening national security. Major operations may be part of a joint campaign comprised of multiple phases. The goal is to achieve national objectives and conclude hostilities with conditions favorable to the United States and its multinational partners, generally as quickly, with as few casualties as possible, and in a manner that conveys continuing strategic advantage for the United States and its partners.

1-36. During major operations and campaigns, commanders conduct IO to achieve decisive effects in and through the information environment against enemy forces. Well-synchronized IO planning and operational integration supports offense, defense, and stability tasks by weighting IO efforts appropriate to each task. For example, during offense, units conduct IO attack, defend, and stabilize actions, in appropriate combination, to help defeat and destroy enemy forces and capabilities, especially those that are information-related. Units also conduct IO to deny aspects of the information environment (physical, informational, and cognitive) that facilitate threat decision making, while preserving critical information infrastructure, content, and networks essential to friendly decision making.

SECTION III – INFORMATION OPERATIONS AND COMBAT POWER

1-37. The information element of combat power is integral to optimizing combat power, particularly given the increasing relevance of operations in and through the information environment to achieve decisive outcomes. IO and the information element of combat power are related but not the same.

1-38. Information is a resource. As a resource, it must be obtained, developed, refined, distributed, and protected. IO, along with knowledge management and information management, are the ways that units harness this resource and ensure its availability, as well as operationalize and optimize it.

1-39. IO, a component of the mission command warfighting function, supports all other warfighting functions and makes each one more potent. The effects that IO achieves in the information environment amplify the effects of movement and maneuver, intelligence, fires, sustainment and protection, both constructive and destructive.

MISSION COMMAND

1-40. The mission command warfighting function enables commanders to balance the art of command and the science of control in order to integrate the other warfighting functions. It also enables a shared understanding of an operational environment and the commander's intent. IO's focus on protecting information, information systems, and decision making, enhances commanders' ability to integrate the other warfighting functions and create necessary shared understanding. At the same time, it seeks to degrade the enemy's decision-making ability.

1-41. IO supports the accomplishment of several mission command warfighting tasks, including inform and influence audiences inside and outside an organization, conduct knowledge management and information management, synchronize IRCs, and conduct cyberspace electromagnetic activities. Informing and influencing are effects that occur in the cognitive dimension of the information environment. By effectively synchronizing IRCs and, when appropriate, conducting cyberspace electromagnetic activities, commanders tailor their influence and manner of informing to the situation and audience at hand. Information and knowledge management support the commander and staff's ability to access information quickly and completely, as well as segment and protect information, thereby enhancing their decision making and gaining advantage over adversaries and enemies.

MOVEMENT AND MANEUVER

1-42. The movement and maneuver warfighting function moves and employs forces to achieve a position of relative advantage over the enemy through direct fire and close combat. IO seeks to influence or affect enemy decision making so that relative advantage is achieved even before close combat becomes necessary or diminishes the potency of threat actions so that they ultimately fail. Movement and maneuver, along with fires, always produce effects in the information environment, whether intentional or not, and these effects must be considered when planning operations (not just IO). At the same time, movement and maneuver can itself serve as an IRC when its chief objective is to send a message and influence behavior, such as when it is tied to a deception effort.

INTELLIGENCE

1-43. Intelligence facilitates understanding the threat, terrain, and civil considerations. IO enhances and sharpens focus on the aspects of the information environment that influence or are influenced by the threat, such as the threat's IRCs. IO also enhances understanding of the ways that messages are received, transmitted and processed by relevant audiences in the area of operations. In turn, intelligence supports IO by collecting information essential to defining the information environment, understanding the threat's information capabilities, and assessing and adjusting information-related effects.

FIRES

1-44. Fires provides collective and coordinated use of Army indirect fires, air and missile defense, and joint fires through the targeting process. IO effects are typically indirect rather than direct and like indirect fire, greatly benefit from deliberate selection, development and delivery. This fact is why IO targets, like offensive cyberspace operations and space targets, are a part of the targeting process and get nominated to the targeting board for approval.

SUSTAINMENT

1-45. Sustainment provides support and services to ensure freedom of action, extend operational reach, and prolong endurance. IO, through the synchronization of IRCs, seeks to ensure freedom of action in the information environment which, in turn, contributes to enhanced mental and emotional endurance, not just of U.S. forces and their partners, but also of the indigenous populations affected by operations. While morale is a leadership function, it is facilitated through the preservation and sustainment of information, information systems, content, and flow and the ability of leaders to create shared understanding and purpose. Sustainment support and services, such as air dropping supplies to displaced persons or providing health service support, often contribute to effects in the information environment, making coordination between the IO officer and the assistant chief of staff, logistics or G-4 (S-4) essential.

PROTECTION

1-46. The protection warfighting function preserves the force so that commanders can apply maximum combat power to accomplish the mission. IO is focused on the preservation of decision making and ensuring decision-oriented information is available at the right time and place. This means more than simply blunting or preventing the effectiveness of the threat's access to information; it means securing and defending our own.