Chapter 2
Information Operations and Decisive Action

2-1. Unified land operations applies land power as part of unified action to defeat the threat on land and establish conditions that achieve the joint force commander's end state. Combat power is the primary means by which Army forces apply land power. IO synchronization supports combat power by harnessing the information element to optimize the warfighting functions and leadership. In turn, this optimization enables commanders to seize the initiative through decisive action.

2-2. *Decisive action* is the continuous, simultaneous combination of offensive, defensive, and stability or defense support of civil authorities tasks (ADRP 3-0). IO contributes to decisive action through the continuous and simultaneous combination and synchronization of IRCs in support of offense, defense, and stability tasks. IO itself is not offensive, defensive, or stabilizing, but contributes to all of these simultaneously by weighting its efforts in such a way that it achieves requisite effects in and through the information environment in support of the commander's intent.

2-3. To support decisive action effectively, the commander and staff undertake three enabling activities—analyze and depict the information environment, determine IRCs and IO organizations available, and optimize IRC effects. These activities start with understanding and visualizing the information environment in all its complexity. They progress to determining the array of IRCs and IO organizations available to affect the information environment. They culminate with optimizing IRC effects through effective planning, preparation, execution and assessment (see paragraphs 2-12 to 2-22 for a detailed discussion of these enabling activities).

WEIGHTED EFFORTS

2-4. IO weighted efforts are broad orientations used to focus the integration and synchronization of IRCs to create effects that seize, retain, and exploit the initiative in the information environment. Commanders, supported by their staffs, visualize and describe how IO will support the concept of operations by aligning and balancing the efforts of defend, attack, and stabilize with corresponding decisive action tasks as shown in figure 2-1 on page 2-2.

IO WEIGHTED EFFORT: DEFEND

2-5. When the IO effort necessitates a defend orientation, it seeks to create effects in the information environment that accomplish any one or combination of the following (not all inclusive):

- Physical dimension.
  - Locking or otherwise physically securing documents, equipment and infrastructure that facilitate decision making.
  - Protecting documents, equipment, and structures from destruction or degradation.
  - Protecting key personnel from attack or exploitation.
  - Using obscurants to mask movements.
- Informational dimension.
  - Encrypting communications.
  - Preserving the free-flow of information and access to data and information sources.
  - Employing knowledge management principles.
  - Proactively identifying instances of social engineering or malware and keeping virus and other protections current.
  - Using forensics to determine sources of attack.

- Countering enemy or adversary information efforts.
- Cognitive dimension.
  - Making decentralized decisions.
  - Checking facts and assumptions.
  - Using precedents or best practices.
  - Using red teaming.

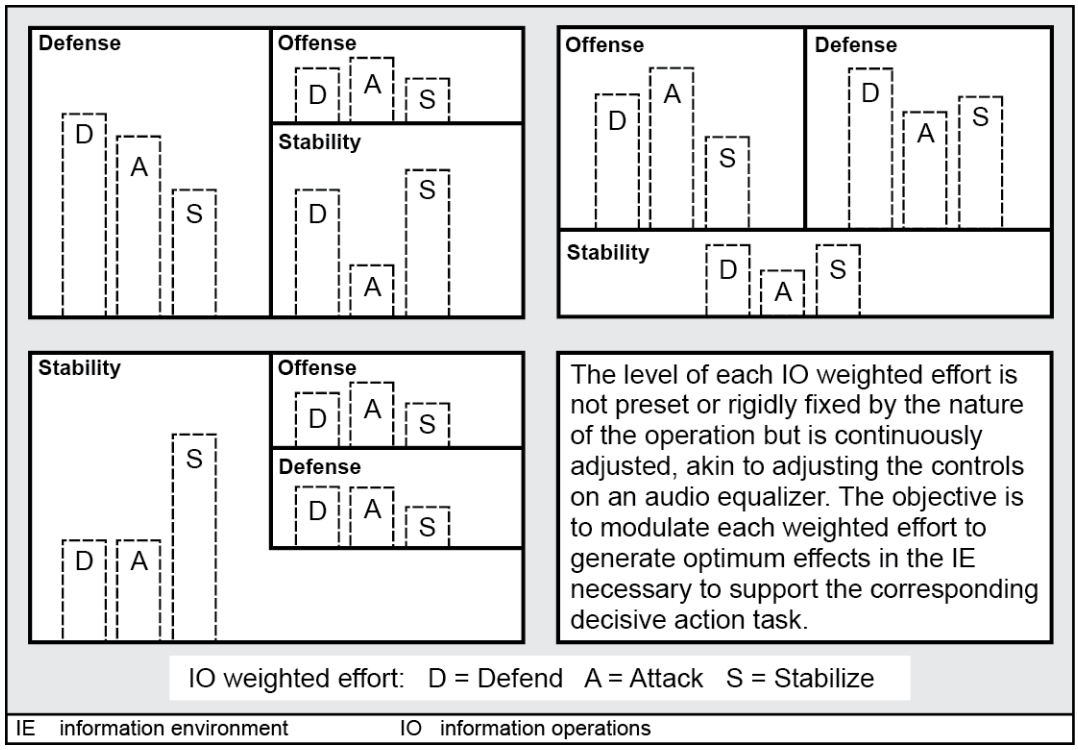

Figure 2-1. IO weighted efforts

2-6. IRCs that are most often synchronized to achieve a defend orientation in the information environment include, but are not limited to:

- Cyberspace operations.
- Electronic warfare.
- Military deception.
- MISO.
- Operations security (OPSEC).
- Physical security.
- Destruction and lethal actions.
- Special technical operations.

IO WEIGHTED EFFORT: ATTACK

2-7. When the IO effort necessitates an attack orientation, it seeks to create effects in the information environment that accomplish any one or combination of the following (not all inclusive):

- Physical dimension.
  - Destroying or degrading threat command and control (C2) systems.
  - Degrading or destroying threat leadership.
  - Destroying or impairing threat networks and critical nodes (human or infrastructure).

- Using feints, ruses, demonstrations, and displays.
- Informational dimension.
  - Jamming communication and signals.
  - Corrupting data and information.
  - Employing denial of service attacks.
  - Intercepting or misdirecting data or content.
  - Manipulating information provided to adversary leaders.
  - Attacking the enemy's or adversary's narrative(s).
  - Using social engineering or spoofing.
- Cognitive dimension.
  - Creating ambiguity or confusion.
  - Causing an incorrect understanding of friendly intent.
  - Creating hesitancy or procrastination.
  - Enabling overconfidence in false signals and signs; under confidence or uncertainty in the true ones.
  - Degrading support for the threat.
  - Degrading legitimacy of threat narrative(s).

2-8. IRCs that are most often synchronized to achieve an attack orientation in the information environment include, but are not limited to:

- Cyberspace operations.
- Electronic warfare.
- Military deception.
- MISO.
- Destruction and lethal actions.
- Special technical operations.
- Space operations.
- Soldier and leader engagement (SLE).

IO WEIGHTED EFFORT: STABILIZE

2-9. When the IO effort necessitates a stabilize orientation, it seeks to create effects in the information environment that accomplish any one or combination of the following (not all inclusive):

- Physical dimension.
  - Meeting with key leaders, decision makers, or people who can influence the behaviors of others.
  - Visibly demonstrating mutual commitment or support.
  - Establishing, supporting and utilizing new infrastructure or media that increases or enhances quantity and quality of communication between U.S.-led forces and relevant audiences.
  - Identifying and cultivating traditional or indigenous communicators.
  - Aligning Soldier and unit actions with their words and images.
- Informational dimension.
  - Employing audience- and culturally-attuned messages.
  - Countering threat or adversary information efforts and narratives through coordinated actions.
  - Aligning images and words with unit and individual Soldier actions.
  - Using messages crafted by native speakers and communicators.
  - Nesting messages with higher headquarters themes and messages and strategic communication guidance.
- Cognitive dimension.
  - Creating support for rule of law, local security forces, and legitimate authority.

- Enhancing understanding of U.S. operations and desired outcomes.
- Changing perceptions, attitudes, and, ultimately, behaviors.

2-10. The IRCs that are most often synchronized to achieve a stabilize orientation in the information environment include, but are not limited to:

- Combat camera.
- MISO.
- Presence, posture and profile.
- Public affairs.
- Civil affairs operations and civil military operations.
- SLE, including police engagement.
- OPSEC.
- Foreign disclosure.

IO and Defense Support of Civil Authorities

2-11. IO does not participate in defense support of civil authorities. However, if requested by civil authorities and approved by the Secretary of Defense, select IRCs may support civil authorities in the conduct of their operations.

IO ENABLING ACTIVITIES

2-12. To support decisive action, as well as accomplish IO's purpose, commanders, staffs, and in particular, the IO officer or representative, undertake and accomplish three enabling activities:

- Analyze and depict the information environment in all its complexity.
- Determine the array of IRCs and IO organizations (such as Theater IO Groups) available to affect the information environment and the advantages each offers.
- Optimize the effects of IRCs through effective planning, preparation, execution, and assessment.

Analyze and Depict the Information Environment

2-13. To achieve advantage in the information environment, commanders, with specialized advice and support from the IO officer, ensure that IO planning is fully integrated into the operations process. This begins with analysis to understand, visualize, and describe the information environment.

2-14. A significant part of what makes the operational environment complex is the information environment because it includes such components as cyberspace, the electromagnetic spectrum, data flow, encryption and decryption, the media, biases, perceptions, decisions, key leaders and decision makers, among many others. What occurs in the physical dimension of the information environment and, more broadly, the operational environment, always has second- and third-order effects in the informational and cognitive dimensions of the information environment. Thus, there must be holistic and nuanced understanding of how these various components and dimensions interrelate and the whole operates.

2-15. This understanding is depicted through a series of information overlays and comprehensive combined information overlays, which vary depending on commanders' priorities, the nature of the operation, and the type of analysis being conducted. Modeling or mapping social or human networks also enhances this understanding. While complex, the information environment still needs to be captured in a way that the commander can visualize and understand it, draw necessary insights and conclusions, and make informed decisions. The IO officer should not be locked into any specific method for analyzing and depicting the information environment but develop a process and overlays that best serve the commander and, as appropriate, follow unit standard operating procedures. As new technologies and interactive capabilities emerge, they should be incorporated as tools to facilitate the visualization and understanding processes.

DETERMINE IRCS AND IO ORGANIZATIONS AVAILABLE

2-16. The IO officer is the staff focal point for information environment analysis and expertise, as well as IRC synchronization. The two are inextricably linked: effective IRC synchronization can only occur when the information environment is understood fully. Additionally, effective IRC synchronization can also only occur when a single entity can look across all IRCs and articulate their contribution to the fight and how they can mutually support each other. The IO officer, located in the assistant chief of staff, operations (G-3/S-3) staff section, in concert with the IO working group, is this synchronization entity. Three key responsibilities of the IO officer, therefore, are to build rapport with IRC units, determine ways to optimize each IRC's contribution through synchronization, and facilitate IRC operations and activities by coordinating support for them, while minimizing impediments.

2-17. In addition to building rapport with IRC units, the IO officer must build similar rapport with and knowledge of IO organizations available and the ways they augment and enhance the function's effectiveness. These units include the 1st IO Command (Land) and the reserve component regionally-aligned Theater IO Groups.

2-18. The IO officer also continually assesses whether the necessary assets and capabilities are available to achieve the commander's intent and concept of operations. If it is determined that augmentation—by specific IRCs or by IO units—is necessary, the IO officer or appropriate IRC representative requests augmentation or determines alternative courses of action to fulfill its scheme of IO and meet mission objectives.

2-19. Information-related organizations and entities also exist within the interagency and among Unified Action partners. IO officers not only must know these organizations and entities, they must invite their participation whenever feasible, particularly through their ad hoc or habitual membership in the IO working group, which coordinates, synchronizes, and deconflicts the information-related efforts of these partner organizations with its own efforts.

OPTIMIZE IRC EFFECTS

2-20. Optimizing IRC effects begins in earnest with receipt of mission and continues throughout the operations process. With information environment analysis and understanding already accounted for, other IO officer tasks necessary to ensure effective IRC synchronization and the optimization of their effects are:

- Participate in the military decisionmaking process (MDMP) and develop the scheme of IO.
- Convene and chair the IO working group.
- Work closely with IRC units and IO units to ensure capabilities are positioned, employed, and supported to fulfill the synchronization plan.
- Integrate targets within the information environment into the targeting process and develop, maintain and update IRC synchronization matrix.
- Coordinate and deconflict IRC synchronization with public affairs efforts to ensure unity of effort and compliance with legal and policy limitations and exclusions.
- Assess IO and IRC effectiveness in achieving planned effects and adjust as necessary.

This page intentionally left blank.