Chapter 1
Information Operations Terms and Considerations

INFORMATION OPERATIONS TERMINOLOGY

1-1. Understanding information operations (IO) begins with understanding the terminology used to discuss it. *Information operations* 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). An *information-related capability* 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 3-13). Examples of information-related capabilities (IRCs) include military information support operations (MISO), military deception, operations security, public affairs, electronic warfare (EW), civil affairs operations (CAO), and cyberspace operations (see chapter 3 for an expanded discussion of IRCs).

1-2. Army commanders conduct IO to affect the information environment. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). Staffs support commanders by synchronizing the employment of IRCs to gain an advantage over an enemy, an adversary, or a threat in the information environment. This advantage contributes to achieving the commander's intent, executing the concept of operations by countering and ultimately defeating the enemy or adversary's ability to operate in the information environment, and protecting and preserving friendly freedom of action in an operational environment to gain and maintain positions of advantage.

1-3. Information is an element of combat power. Units conduct IO to maximize the impact of the information element on operations. Leaders of IO units consider the following:

- IO focuses on affecting decision making. First it influences, usurps, corrupts, or destroys the enemy or adversary's ability to make timely, accurate, and relevant decisions. Second it protects, preserves, and enhances the leader's ability to make timely, accurate, and relevant decisions.
- Commanders are responsible for the conduct of IO. They are supported by their staffs and, depending on the mission or situation, by all members of the unit.
- IO synchronizes IRCs to create effects in the information environment that, in turn, shape and affect an operational environment.

1-4. The conduct of IO requires commanders, staffs, and particularly the IO officer or designated representative to—

- Analyze, understand, visualize, and describe an operational environment with specialized focus on the information environment, including—
  - The threat's use of the information environment.
  - Relevant stakeholders (those who affect friendly and threat decision making or are affected by it).
- Determine available IRCs and understand what each brings to the fight; request additional capabilities, as required.
- Plan IO as part of the operations process.
- Develop supporting products and input to plans and orders, such as combined information overlays, synchronization matrixes, an IO running estimate, and Appendix 15 (IO) to Annex C (for an example of an IO appendix, see FM 3-13).
- Establish and conduct an IO working group or otherwise coordinate with staffs, IRCs, and unified action partners to create effects in the information environment.

- Synchronize IRCs.
- Coordinate intelligence support to IO.
- Integrate IO into the targeting process.
- Assess IO within the operations assessment process.

These elements are continuous, cyclical, and iterative (see chapters 3 and 4 for additional details).

INFORMATION OPERATIONS CONSIDERATIONS ACROSS ECHELONS

1-5. IO supports operations from company level to Army Service component command (ASCC) level and above; however, the conduct of IO differs at each level. IRCs that an ASCC can employ are more expansive than a battalion can employ. Still, both echelons have the same responsibility to create effects in and through the information environment in their operational areas.

1-6. Factors that differentiate the conduct of IO from the lowest through the highest levels include—

- The supported operations and objectives.
- The size and complexity of the information environment.
- The presence of organic IO expertise.
- Tasks, knowledge, and skillsets required of IO personnel.
- Availability of IRCs.
- Access to staff support forces and reachback.
- Authorities and legal considerations.

SUPPORTED OPERATIONS AND OBJECTIVES

1-7. The type of operation and its objectives that IO supports vary with echelon. An *operation* is a sequence of tactical actions with a common purpose or unifying theme (JP 1) to achieve one or a limited set of objectives whose attainment is necessary to achieve the mission. *Unified land operations* are simultaneous offensive, defensive, and stability or defense support of civil authorities tasks to seize, retain, and exploit the initiative to shape the operational environment, prevent conflict, consolidate gains, and win our Nation's wars as part of unified action (ADRP 3-0). Unified land operations shape the information environment for IO. At higher echelons, the operations occurring are larger, more numerous, and more complex, as is the number of objectives being pursued. Also at higher levels, IO may be a major component of the lines of operation, its own line of effort, and in support of other lines of effort for a given operation.

SIZE AND COMPLEXITY OF THE INFORMATION ENVIRONMENT

1-8. The size and complexity of the information environment varies with echelon. The information environment—comprising individuals, organizations, and systems that collect, process, disseminate, or act on information—has three dimensions: physical, informational, and cognitive. The information environment is global but can be described in the context of regions and operational areas. It is both bound by culture, language, access to technology, and customs and traditions, and unbound in that information can readily flow into and out of a region or operational area into the global environment. The environment of an ASCC is considerably larger and more complex in physical and informational terms than an environment of a battalion. Yet, in terms of the cognitive dimension of this environment, similar challenges—such as how best to influence relevant audiences and to affect enemy or adversary decision making—exist at all echelons.

PRESENCE OF ORGANIC INFORMATION OPERATIONS EXPERTISE

1-9. Echelons vary in how much organic IO expertise they contain. IO officers and elements are currently found at the division level through ASCC. Whether or not an IO officer is assigned to a unit does not eliminate the responsibility of commanders at all levels to conduct IO. Commanders at brigade and below must, therefore, assign IO responsibilities to someone in their unit and ensure this individual receives the requisite training necessary to plan, prepare, execute, and assess IO (see appendix A for information on IO training).

TASKS, KNOWLEDGE, AND SKILLSETS REQUIRED OF INFORMATION OPERATIONS PERSONNEL

1-10. The tasks, knowledge, and skillsets required of IO personnel vary by echelon. IO is challenging at all levels; however, the knowledge and skillsets necessary to conduct IO at brigade and below differs from the knowledge and skillsets necessary to conduct IO at echelons above brigade. At brigade and below, IO personnel are responsible for synchronizing a smaller, less technical array of IRCs than are IO officers at division and above. IO personnel at division and above also prepare to operate in a more complex information environment and against advanced threat information systems. Some IO personnel at division and above work as part of a joint force and alongside unified action partners with whom they must achieve common objectives in the information environment.

AVAILABILITY OF INFORMATION-RELATED CAPABILITIES

1-11. The availability of IRCs in IO varies depending on the echelon supported. All units can conduct activities or employ capabilities that—

- Support the commander's task to inform and influence audiences inside and outside an organization.
- Affect enemy or adversary decision making, such as military deception.

Units at all echelons support the commander's task by maintaining a presence, profile, and posture; ensuring operations security; and conducting Soldier and leader engagement. However, the availability of IRCs—in the form of specific expertise, units, operations, and activities—is more limited at brigade and below. For example, space and cyberspace operations capabilities are not readily available to battalions unless requested well in advance and approved by higher headquarters.

ACCESS TO STAFF SUPPORT FORCES AND REACHBACK

1-12. Access to staff support forces and reachback required from IO personnel vary by echelon. When an IO staff lacks the required personnel, knowledge, or skillsets to conduct the tasks assigned to it, the command requests support. This support can come from individual augmentation to fill an approved manning document, by attaching small elements to the IO staff, or by designating a supporting unit that provides a needed capability through reachback. When filling individual augmentation billets or attaching elements to the staff, the command fills from its higher headquarters before requesting support from external units. For example, a corps or division staff that is not deployed may fill out a brigade or battalion staff that is deployed. When external support is necessary, the following units typically provide it:

- 1st Information Operations Command (Land), Active U.S. Army.
- 56th Theater Information Operations Group (TIOG), Washington State Army National Guard.
- 71st TIOG, Texas Army National Guard.
- 151st TIOG, United States Army Reserve.

1st Information Operations Command (Land)

1-13. The 1st IO Command, a major subordinate command of the U.S. Army Intelligence and Security Command, is a brigade-sized, multicomponent unit. Under the operational control and tasking authority of the U.S. Army Cyber Command, it provides distinctly tailored IO and cyberspace operations planning, synchronization, assessment, and reachback support to the Army and other military forces. Consisting of a headquarters and headquarters detachment and two battalions, it augments military forces with tailored IO and cyberspace operations support provided through deployable teams, cyber-opposing forces support, reachback planning and analysis, Army mission readiness exercises, and specialized training to assist units in garrison, during exercises, and during contingency operations.

1-14. The 1st IO Command also supports the Army by working to optimize IO interoperability with joint forces, other military forces, various agencies, and allies. It provides expeditionary cyberspace operations support to help units identify network vulnerabilities and enable IO.

Theater Information Operations Groups

1-15. The Army relies upon TIOGs to provide enhanced IO planning, synchronization, and assessment support to Army echelons from theater and ASCC to brigade levels. Three TIOGs exist:

- The 56th TIOG, U.S. Army National Guard, Fort Lewis, Washington.
- The 71st TIOG, U.S. Army National Guard, Camp Mabry, Texas.
- The 151st TIOG, U.S. Army Reserve, Fort Totten, New York.

Each TIOG consists of a group headquarters, a headquarters and headquarters company, and two IO battalions that have the capability to provide IO field support teams or general field support teams.

1-16. The TIOGs and their battalion elements do not deploy as commands but instead form and deploy purpose-built IO field support teams designed to provide the necessary IO support required by the requesting command. To enhance the capabilities of the field support teams and reduce preparation time, the TIOGs maintain regional focuses. These focuses help provide the supported command with additional regional expertise and capabilities to plan, synchronize, and assess IRCs when conducting IO in the area of operations. Having a regional focus, however, does not preclude a TIOG from deploying IO teams and providing IO support to organizations and commands outside of its regional focus area (see FM 3-13 for more detail on these organizations).

AUTHORITIES AND LEGAL AND ETHICAL CONSIDERATIONS

1-17. Some capabilities integrated and synchronized by the IO officer or designated representative—such as MISO, cyberspace electromagnetic activities, and integrated joint special technical operations (known as IJSTO)—are governed by authorities that dictate parameters or constraints on their employment. While these IRCs tend to reside at higher levels, brigades and below may be impacted by their respective constraints, particularly when these capabilities are augmenting or supporting their operations. Commanders—with advice from IO officers, public affairs officers, IRC representatives, and judge advocate general (known as JAG) officers—make themselves aware of these limitations that affect lead times and dictate how effects will be achieved. When such capabilities are authorized, the best way to understand the parameters or constraints under which units must operate is to request a capabilities briefing from the IRC unit commander or senior representative (see DODD 3600.01 as a starting point for these considerations).

1-18. As trusted Army professionals and stewards of the Army Profession, all commanders, staffs, and IO professionals strive to make right decisions and take actions that enable them to conduct IO ethically, effectively, and efficiently.