APPENDIX D
INFORMATION OPERATIONS

> *"The side possessing better information and using that information more effectively to gain understanding has a major advantage over its opponent."*
>
> FM 3-0(FM 100-5), *Operations*

While many information operations (IO) will be planned and executed at levels above the brigade, brigades and below will often benefit from the results of properly executed IO, especially during urban operations. IO are primarily shaping operations that create and preserve opportunities for decisive operations. IO are both offensive and defensive. Related activities, such as public affairs and civil-military operations (CMO), support IO. This appendix will define IO, describe the elements of IO, and describe their effects on brigade urban operations.

D-1. DEFINITIONS

These IO terms are defined as follows:

a. **Information Operations.** IO are actions taken to affect the threat's, and influence others', decision-making processes, information, and information systems while protecting one's own information and information systems.

(1) The value of IO is not in their effect on how well an enemy transmits data. Their real value is measured only by their effect on the enemy's ability to execute military actions. Commanders use IO to attack enemy decision making processes, information, and information systems. Effective IO allow commanders to mass effects at decisive points more quickly than the enemy. IO are used to deny, destroy, degrade, disrupt, deceive, exploit, and influence the enemy's ability to exercise C2. To create this effect, friendly forces attempt to influence the enemy's perception of the situation. Similarly, IO and related activities affect the perceptions and attitudes of a host of others in the AO. These include the local population, displaced persons, and civilian leaders. IO are shaping operations that help commanders create favorable conditions for not only decisive operations but also sustaining operations. Commanders use IO and related activities to mitigate the effects of enemy IO, as well as adverse effects stemming from misinformation, rumors, confusion, and apprehension.

(2) Successful IO require a thorough and detailed IPB. IPB includes information about enemy capabilities, decision making style, and information systems. It also considers the effect of the media and the attitudes, culture, economy, demographics, politics, and personalities of people in the AO. Successful IO influences the perceptions, decisions, and will of enemies, adversaries, and others in the AO. Its primary goals are to produce a disparity in enemy commanders' minds between reality and their perception of reality and to disrupt their ability to exercise C2.

b. **Offensive IO.** Offensive IO are the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers or to influence others to achieve or promote specific objectives. The desired effects of offensive IO are to destroy, degrade, disrupt, deny, deceive, exploit, and influence enemy functions. Concurrently, Army forces employ elements of offensive IO to affect the perceptions of adversaries and others within the AO. Using the elements of IO offensively, Army forces can either prevent the enemy from exercising effective C2 or leverage it to their advantage. Ultimately, IO targets are the human leaders and human decision making processes of adversaries, enemies, and others in the AO.

c. **Defensive IO.** Defensive IO are the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Defensive IO protect friendly access to relevant information while denying adversaries and enemies the opportunity to affect friendly information and information systems. Defensive IO limit the vulnerability of C2 systems.

d. **Effects of Offensive and Defensive IO.** Offensive and defensive operations use complementary, reinforcing, and asymmetric effects to attack enemies, influence adversaries and others, and protect friendly forces. On a battlefield where concentrating forces is hazardous, IO can attack enemy C2 systems and undermine enemy capabilities and will to fight. It can reduce friendly vulnerabilities and exploit enemy weaknesses. Where the use of force is restricted or is not a viable option, IO can influence attitudes, reduce commitment to a hostile cause, and convey the willingness to use force without actually employing it. Information used in this manner allows friendly forces to accomplish missions faster, with fewer casualties.

D-2. ELEMENTS OF INFORMATION OPERATIONS

Integrating offensive and defensive IO is essential to success. Many activities or operations comprise IO. Each element may have offensive or defensive applications (Figure D-1).

ELEMENTS OF IO

- Military deception
- Counterdeception
- Operations security
- Physical security
- Electronic warfare
  - *Electronic attack*
  - *Electronic protection*
  - *Electronic warfare support*
- Information assurance
- Physical destruction
- Psychological operations
- Counterpropaganda
- Counterintelligence
- Computer network attack
- Computer network defense

Figure D-1. Elements of information operations.

a. **Military Deception.** Military deception includes measures designed to mislead adversaries and enemies by manipulation, distortion, or falsification. Its aim is to influence the enemy's situational awareness and lead him to act in a manner that favors friendly forces.

b. **Counterdeception.** Counterdeception includes efforts to negate, neutralize, or diminish the effects of, or gain advantage from, a hostile deception operation. Counterdeception supports offensive IO by reducing harmful effects of enemy deception. Defensively, counterdeception can identify enemy attempts to mislead friendly forces.

c. **Operations Security.** Operations security (OPSEC) denies the enemy information critical to the success of friendly military operations. It contributes to the security of Army forces and their ability to surprise enemies and adversaries. OPSEC identifies routine activities that may telegraph friendly intentions, operations, capabilities, or military activities. It acts to suppress, conceal, control, or eliminate these indicators. OPSEC includes countersurveillance, signal security, and information security.

d. **Physical Security.** Physical security prevents unauthorized access to equipment, installations, and documents. It safeguards and protects information and information systems.

e. **Electronic Warfare.** Electronic warfare (EW) is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW can cause an enemy to misinterpret the information received by his electronic systems. EW includes:

(1) ***Electronic Attack.*** Electronic attack involves actions taken to degrade, neutralize, or destroy enemy electronic combat capabilities. Actions may include lethal attack, such as antiradiation missiles and directed energy weapons, and nonlethal electronic attack, such as jamming.

(2) ***Electronic Protection.*** Electronic protection involves actions taken to protect friendly use of the electronic spectrum by minimizing the effects of friendly or enemy EW. Actions may include radio silence and antijamming measures.

(3) ***Electronic Warfare Support.*** Electronic warfare support involves detecting, identifying, locating, and exploiting enemy signal emitters. It contributes to achieving situational awareness, target development and acquisition, damage assessment, and force protection.

f. **Information Assurance.** Information assurance protects and defends information systems. Threats to information systems include physical destruction, denial of service, capture, environmental damage, and malfunctions. Information assurance provides an enhanced degree of confidence that information and information systems possess the following characteristics: availability, integrity, authentication, confidentiality, and nonrepudiation. Computer network defense is part of this element.

g. **Physical Destruction.** Physical destruction applies combat power against IO-related targets. Targets include information systems, EW systems, and command posts. Physical destruction that supports IO is synchronized with other aspects of the operation. For example, when deciding whether to destroy an enemy command post, the friendly commander weighs the advantages gained from disrupting enemy C2 against those gained from collecting information from the command post's radio traffic.

h. **Psychological Operations.** Psychological operations (PSYOP) are planned operations that influence the behavior and actions of foreign audiences by conveying selected information and indicators to them (FM-05.30[FM 33-1]). The aim of PSYOP is to create behaviors that support US national interests and the mission of the force. PSYOP are closely integrated with OPSEC, military deception, physical destruction, and EW to create a perception of reality that supports friendly objectives.

i. **Counterpropaganda.** Counterpropaganda includes activities directed at an enemy or adversary conducting PSYOP against friendly forces. Counterpropaganda can contribute to situational awareness and expose enemy attempts to influence friendly populations and military forces. Preventive actions include propaganda awareness programs that inform US and friendly forces and friendly populations about hostile propaganda.

j. **Counterintelligence.** Counterintelligence consists of activities that identify and counteract threats to security posed by espionage, subversion, or terrorism. It detects, neutralizes, or prevents espionage or other intelligence activities. Counterintelligence supports the commander’s requirements to preserve essential security and protect the force.

k. **Computer Network Attack.** Computer network attack consists of operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks. It may also target computers and networks themselves. Although theater or national elements normally conduct computer network attack, the effects may be evident at corps and below.

D-3. RELATED ACTIVITIES

Public affairs and civil-military operations (CMO) are activities related to IO. Both communicate information to critical audiences to influence their understanding and perception of military operations. Related activities are distinct from IO because they do not manipulate or distort information; their effectiveness stems from their credibility with the local populace and news media. Public affairs and CMO—prime sources of information—link the force, the local populace, and the news media. They also provide assessments of the impact of military operations on civilians, neutrals, and others within the battlespace.

a. **Public Affairs.** Public affairs operations influence populations by transmitting information through the news media. They fulfill the Army’s obligation to keep the American people and the Army informed. Public affairs help to establish conditions that lead to confidence in the Army and its readiness to conduct operations in peace, conflict, and war. Disseminating this information is desirable and consistent with security. Information disseminated through public affairs counters the effects of propaganda and misinformation.

b. **Civil-Military Operations**. CMO applies civil affairs to military operations. It encompasses activities that commanders take to establish, maintain, influence, or exploit relations between military forces and civil authorities—both governmental and nongovernmental—and the civilian populace. Commanders direct these activities in friendly, neutral, or hostile AOs to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur before, during, or after other military actions. They may also occur as stand-alone operations. CMO is the decisive and timely application of planned activities that enhance the relationship between military forces and civilian authorities and population. They promote the development of favorable emotions, attitudes, or behavior in neutral, friendly, or hostile groups. CMO range from support to combat operations to assisting countries in establishing political, economic, and social stability.

D-4. INFORMATION OPERATIONS AND THEIR EFFECTS ON BRIGADE URBAN OPERATIONS

The IO, at brigade level, is planned and executed as a coordinated effort between the S2 and S3, and, when assigned, the S5. The IO affects all four elements of urban operations—assess, shape, dominate, and transition.

a. **Assess.** The brigade staff assesses the results of IO conducted by the division or JTF. For example, the results of military deception, PSYOP, electronic attack, counterpropaganda, and computer network attack conducted by higher headquarters may force the threat to act in a manner that facilitates brigade offensive operations and minimizes the need for close combat. During defensive operations, IO may force the threat to deploy into engagement areas that will facilitate the synchronization of fires and nonlethal capabilities.

b. **Shape.** Brigades can use IO to shape the urban battlespace. For example, continuous OPSEC and physical security can deny the threat valuable information concerning friendly forces. Likewise, brigades can use PSYOP teams, if available, to help shape desired threat behaviors prior to the execution of UO.

c. **Dominate.** Brigades may be given missions from higher headquarters to physically destroy or control IO related targets such as command posts or media centers. Moreover, the effects of IO during assessing and shaping may permit brigades to dominate without having to employ fires and close combat or by minimizing their use.

d. **Transition.** Brigades may use the results of IO to facilitate the transition to stability and support operations. For example, a civil-military operations center (CMOC) may be established within a brigade AO in order to permit restoration of utilities such as electricity, water, and sewage.