Chapter 3
Information-Related Capabilities

DETERMINATION OF ASSETS

3-1. As a part of mission analysis, the IO officer or representative reviews available assets and identifies resource shortfalls. The IO officer inventories available IRCs, IRCs to request from higher headquarters, and IRCs available through unified action partners. The IO running estimate—paragraph 1.b.(4) "Friendly Forces"—or a suitable block in a graphical estimate reflects the results of the inventory (see the FM 6-0 chapter on running estimates).

3-2. Without accurate accounting for what assets—particularly IRCs—are available, the IO officer cannot effectively formulate schemes of IO during COA development. The scheme of IO is a clear, concise statement of where, when, and how the commander intends to employ and synchronize IRCs to create effects in and through the information environment to achieve the mission and support decisive operations. Based on the commander's planning guidance, the IO officer develops a separate scheme of IO for each COA the staff develops. Schemes of IO are written in terms of IO objectives—and their associated weighted efforts (attack, defend, stabilize)—and IRC tasks required to achieve these objectives (see FM 3-13, Chapter 2, for more information on IO weighted efforts). For example, the overall scheme may be weighted heavily on defending friendly information but also include attack and stabilize objectives (see chapter 4 for more information about schemes of IO).

3-3. IRCs exist at all echelons but are more numerous and diverse at higher levels. Table 3-1 on page 3-2 depicts IRCs by echelon (not in any order of priority). This echeloning is not absolute and varies depending on mission and task organization. As discussed beginning in paragraph 3-4, IRCs are broadly categorized as intrinsic or extrinsic. As JP 3-13 and FM 3-13 make clear, any capability that produces an effect in the information environment is considered an IRC. For example, when units employ fires to create an effect in the information environment (to influence or change behavior), it is an IRC in that instance. Examples of other capabilities that create effects in the information environment include, but are not limited to—

- Commander's communication synchronization.
- Foreign disclosure.
- Knowledge management and information management.
- Military intelligence and counterintelligence.
- Military police engagement.
- Physical security.

CATEGORIES OF INFORMATION-RELATED CAPABILITIES

3-4. Two broad categories of IRCs exist: intrinsic and extrinsic. Intrinsic IRCs are those capabilities internal to or embedded in an Army unit. Extrinsic IRCs are those capabilities that exist outside the unit, such as those available at or through higher or other headquarters or that are joint, interagency, non-governmental, or belong to other unified action partners. Table 3-1 arrays intrinsic and extrinsic IRCs by echelon.

INTRINSIC INFORMATION-RELATED CAPABILITIES

3-5. Intrinsic IRCs are inherent in a unit's mission and table of organization or modified table of organization. They are either leader- or staff-led. As an example, presence, profile, and posture (PPP) is inherent in every unit because it relies on effectively combining decision making, available personnel, and systems to project influence. Similarly, Soldier and leader engagement (SLE) is inherent in every unit.

Operations security is a program and a process that protects friendly information and relies on an assigned staff person to plan and execute it. Similarly, military deception is executed through an assigned staff person.

EXTRINSIC INFORMATION-RELATED CAPABILITIES

3-6. Extrinsic IRCs are external capabilities made available through assignment, attachment, or other command or support relationships for specific times or missions (see FM 6-0, Appendix B, for more information on command and support relationships). The operations of these capabilities are planned and coordinated with the unit to which they have a command or support relationship, but executed by the commander or senior representative of that capability. For example, a brigade combat team is typically supported by both a reserve component civil affairs company and a psychological operations (PSYOP) company. These capabilities often have elements or representatives on the supported unit's staff that provide liaison between them. These capabilities also are characterized by their alignment to a force modernization proponent. For example, the John F. Kennedy Special Warfare Center and School is the proponent for both CAO and MISO.

Table 3-1. Intrinsic and extrinsic information-related capabilities by echelon

Battalion and Below	*Brigade*	*Echelons Above Brigade*	
PPP	PPP	PPP	Intrinsic
PA	PA	PA	
SLE	SLE	SLE	
OPSEC	OPSEC	OPSEC	
CMO	CMO	CMO	
MILDEC	MILDEC	MILDEC	
PR	PR	PR	
Soldier camera	COMCAM	COMCAM	
Physical security	Physical security	Physical security	
Physical maneuver	Physical maneuver	Physical maneuver	
Destruction & lethal action	Destruction & lethal action	Destruction & lethal action	
MISO	MISO	MISO	Extrinsic
CAO	CAO	CAO	
Police engagement	Police engagement	Police engagement	
	EW	EW	
		CO	
		Space operations	
		IJSTO	
		SAP	

CAO	civil affairs operations	MISO	military information support operations
CMO	civil-military operations	OPSEC	operations security
CO	cyberspace operations	PA	public affairs
COMCAM	combat camera	PPP	presence, profile, and posture
EW	electronic warfare	PR	personnel recovery
IJSTO	integrated joint special technical operations	SAP	special access program
MILDEC	military deception	SLE	Soldier and leader engagement

LISTING OF INFORMATION-RELATED CAPABILITIES

3-7. Paragraphs 3-7 through 3-51 provide overviews of each IRC. They are listed alphabetically, in part to reinforce the idea that they are co-equal in their potential contribution to the scheme of IO. Every IRC has one characteristic in common: a representative of each capability is a member of the IO working group. Some are habitual or core members while others attend on an as-needed basis. In either case, their participation is governed by the mission, current situation, and commander's discretion.

CIVIL AFFAIRS OPERATIONS

3-8. CAO encompass actions planned, executed, and assessed by civil affairs forces. These actions—

- Enhance awareness of and manage the interaction with the civil component of an operational environment.
- Identify and mitigate underlying causes of instability in civil society.
- Involve the application of functional specialty skills normally the responsibility of civil government.

Civil affairs forces engage and influence the civil populace and authorities by planning and conducting CAO. These forces enable civil-military operations, shape the civil environment, and set the conditions for military operations.

3-9. The staff focal point for CAO and civil-military operations is the civil affairs staff officer. This officer is a core member of the unit's IO working group (see FM 3-57 for a detailed discussion of civil affairs).

CIVIL-MILITARY OPERATIONS

3-10. Civil-military operations are activities of a commander performed by designated civil affairs or other military forces that establish, maintain, influence, or exploit relations between military forces, indigenous populations, and institutions. Civil-military operations directly support attaining objectives related to reestablishing or maintaining stability in a region or host nation.

3-11. Civil-military operations (known as CMO) activities establish, maintain, influence, or exploit relations among military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area to achieve U.S. objectives. In civil-military operations, personnel perform functions normally provided by the national, regional, or local government, placing them into direct contact with civilian populations. This level of interaction results in civil-military operations significantly affecting the perceptions of the local populace (see JP 3-57 for more information on civil-military operations).

COMBAT CAMERA

3-12. Combat camera (COMCAM) provides operational imagery; supports combat, information, humanitarian, special force intelligence, engineering, legal, and public affairs requirements; provides imagery that supports strategic, operational, and tactical levels of war; speeds decision making; and facilitates the vertical and horizontal flow of information. Further, COMCAM supports information collection, battle damage assessment, military deception, legal, and historical or archival functions. COMCAM units maintain the capability to acquire, edit, disseminate, archive, manage, and transmit imagery. All COMCAM units are equipped to acquire imagery in darkness and inclement weather.

3-13. Normally, COMCAM augments the IO officer or IO elements. If assigned, the COMCAM officer manages all COMCAM assets by planning, preparing, and executing COMCAM activities; if not assigned, the IO officer provides planning and guidance on COMCAM employment. When COMCAM units are unavailable, particularly at battalion and below levels, units can designate one or more Soldiers to use unit-issued or personal cameras (referred to as Soldier camera); however, the unit must have a procedure in place for the review, clearance, and disposition of any images taken (see ATP 6-02.40).

CYBERSPACE ELECTROMAGNETIC ACTIVITIES

3-14. *Cyberspace electromagnetic activities* is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADRP 3-0). Cyberspace electromagnetic activities (CEMA) is, therefore, not an IRC in and of itself; cyberspace operations and EW operations are IRCs. Through CEMA, the Army plans, integrates, and synchronizes these missions, supports and enables the mission command system, and provides an interrelated capability for information and intelligence operations. CEMA also plays a significant role in attacking enemy or adversary decision making, while protecting friendly forces. The continuous planning, integration, and synchronization of cyberspace operations and EW, enabled by spectrum management operations, can produce singular, reinforcing, and

complementary effects. Cyberspace operations and EW both operate using the electromagnetic spectrum. *Spectrum management operations* is the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations (FM 6-02).

3-15. The staff focal point for CEMA at and below the division level is the EW officer, who has additional responsibility as the cyberspace planner. The EW officer serves as the commander's designated staff officer for planning, integrating, synchronizing, and assessing cyberspace operations and EW. This officer is typically a core member of the unit's IO working group (see FM 3-12 for a discussion of CEMA).

Electronic Warfare

3-16. *Electronic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). EW capabilities enable Army forces to create conditions and effects in the electromagnetic spectrum to support the commander's intent and concept of operations. EW includes electronic attack, electronic protection, and electronic warfare support, and includes activities such as electromagnetic jamming, electromagnetic hardening, and signal detection, respectively. EW affects, supports, enables, protects, or collects on capabilities operating within the electromagnetic spectrum, including cyberspace capabilities. With proper integration and deconfliction, EW can create reinforcing and complementary effects by affecting devices that operate in and through wired and wireless networks.

Cyberspace Operations

3-17. *Cyberspace operations* are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). Army cyberspace operations range from defensive to offensive, establish and maintain secure communications, and detect and deter threats in cyberspace to the Department of Defense information network as they support Army and joint forces from strategic to tactical levels.

INTEGRATED JOINT SPECIAL TECHNICAL OPERATIONS AND SPECIAL ACCESS PROGRAMS

3-18. Integrated joint special technical operations (IJSTO) are classified operations that harness specialized technical capabilities to gain a decisive advantage over an enemy or adversary. These technical capabilities can be information-related or, in some way, complement IO efforts. Therefore, IJSTO and IO must be deconflicted and synchronized through close coordination, primarily through the IO working group. According to JP 3-13, detailed information about IJSTO and its contribution to IO can be obtained from IJSTO planners at combatant command or Service component headquarters.

3-19. Special access programs (known as SAPs) are sensitive acquisition, intelligence, or operations and support programs that impose need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information (see DODD 5205.07 for more information on special access programs). As with IJSTO, detailed information related to special access programs can be obtained, when authorized, from the designated representative at combatant command or Service component headquarters.

MILITARY DECEPTION

3-20. Military deception (MILDEC) involves actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers. The intent of MILDEC is to feed information that deliberately misleads the enemy decision makers as to friendly military capabilities, intentions, and operations and lead the enemy to take actions (or inactions) that contribute to accomplishment of the friendly mission. When properly integrated with operations security, other IRCs, and visible activities of the joint force and its components, MILDEC can be a decisive tool in altering how the adversary views, analyzes, decides, and acts in response to friendly military operations.

3-21. MILDEC is both a process and a capability. As a process, MILDEC is a methodical, information-based strategy that systematically, deliberately, and cognitively targets individual decision makers. The objective

is the purposeful manipulation of decision making. As a capability, MILDEC is useful to a commander when integrated early in the planning process as a component of the operation focused on causing an enemy to act or react in a desired manner.

3-22. MILDEC is accomplished various ways. Chief among these ways are tactical deception, counterdeception, and deception to support operations security.

3-23. Tactical deception consists of deception activities planned and conducted to support battles and engagements in real time. Tactical-level commanders plan and execute tactical deception to cause enemy actions favorable to U.S. objectives. These activities aim to gain a tactical advantage over an adversary, to mask vulnerabilities in friendly forces, or to enhance the defensive capabilities of friendly forces.

3-24. Counterdeception contributes to situational understanding by protecting friendly human and automated decision making from adversary deception. Counterdeception strives to make Army commanders aware of adversary deception activities so they can formulate informed and coordinated responses.

3-25. The goal of deception to support operations security is to help protect friendly operations, personnel, programs, equipment, and other assets against foreign intelligence entities, insurgents, and adversarial collection. It creates multiple false indicators to confuse the enemy or adversary. Sometimes they make friendly intentions harder for the enemy or adversary intelligence gathering apparatus to interpret or limit the enemy's ability to collect accurate information on friendly forces.

3-26. The staff focal point for deception is the assigned or designated MILDEC officer, who should be part of the operations staff section in the IO element. The MILDEC officer is a core member of the IO working group (see JP 3-13.4 for a detailed discussion on MILDEC).

MILITARY INFORMATION SUPPORT OPERATIONS

3-27. *Military information support operations* are 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 (JP 3-13.2). PSYOP forces conduct three distinct missions: military information (known as MILINFO), interagency-intergovernmental support (known as IIS), and civil authority information support (known as CAIS). Military information is the only mission relevant to IO planning.

3-28. Military information consists of psychological actions and persuasive messages executed during military operations to influence selected individuals and groups in ways that support U.S. national objectives. At the tactical level, PSYOP forces execute actions (or coordinate their execution) and deliver audio, visual, and audio-visual messages that encourage enemy forces to defect, desert, flee, surrender, or take any other action beneficial to friendly forces.

3-29. At brigade and above, the focal point is the staff PSYOP officer or noncommissioned officer, in close coordination with the IO officer or representative. Additionally, the commander or officer-in-charge of an attached PSYOP unit may also contribute to synchronizing IRC. Both individuals are core members of the unit's IO working group.

OPERATIONS SECURITY

3-30. *Operations security* is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities (JP 3-13.3). The operations security (OPSEC) process meets operational needs by mitigating risks associated with vulnerabilities to deny the threat critical information and observable indicators. A successfully executed OPSEC program enables operations by preventing misinformation, disinformation, and information fratricide.

3-31. OPSEC aims to enhance the probability of mission success by preserving the advantages of essential secrecy and surprise. Commanders use OPSEC measures to deny the threat knowledge of friendly operations, requiring the threat to expend more resources to obtain critical information needed to make decisions. OPSEC is a force multiplier. It includes—

- Reducing predictability.
- Eliminating indicators of operations.
- Disrupting the adversary's information gathering.
- Preventing the adversary's recognition of indicators by using diversions, camouflage, jamming, and deterrence.
- Preventing counteranalysis, which seeks to prevent accurate interpretations of indicators during adversary analysis of collected material.

Once staffs identify vulnerabilities, they can use other IRCs such as MILDEC to satisfy OPSEC requirements. OPSEC practices must balance the responsibility to account to the American public with the need to protect critical information. OPSEC should not be used as an excuse to deny noncritical information to the public.

3-32. The focal point for OPSEC is the designated OPSEC planner. This individual is typically co-located with the IO officer or representative as part of the IO element (see JP 3-13.3 and AR 530-1 for details on OPSEC).

PERSONNEL RECOVERY

3-33. The core principle of Army personnel recovery (PR) is to recover isolated personnel before detention or capture through a systems-based approach that features proactive, integrated, rehearsed, and resourced measures and capabilities. To fulfill this principle, the Army has an obligation to train, equip, and protect its personnel (Soldier, DA Civilian, and contractor), prevent their capture and exploitation by adversaries, and reduce the potential for using isolated personnel as leverage against U.S. security objectives and national interests. The IO officer works with the personnel recovery officer to—

- Reduce interference between U.S. and coalition PR operations.
- Decrease the effectiveness of hostile propaganda and misinformation because of captured or detained personnel
- Increase support and cooperation from unified action partners for PR operations.
- Integrate PR considerations into MISO, deception, and public affairs plans.
- Synchronize and coordinate IO in the overall operation to mislead the enemy about recovery operations and assets.

Note. PR did not appear in FM 3-13, 1 Dec 2017, but is added here, reinforcing the fact that any capability can serve as an IRC if it is affected by or affects the information environment.

PHYSICAL ATTACK

3-34. When synchronized as a part of information operations, physical attack—which includes physical maneuver, destruction, and lethal action—is the application of combat power to create desired effects in the information environment. Carefully applied force can play a major role in intimidation and deterrence and in obstructing a threat's ability to exercise command and control. It may include direct and indirect fires from ground, sea, and air platforms and direct actions by special operations forces. IO applications of physical attack to consider include—

- Preventing or degrading adversary reconnaissance and surveillance.
- Conducting physical attacks as deception events.
- Degrading the enemy's ability to process information.
- Degrading the enemy's ability to jam communications.
- Destroying command and control and communications systems.
- Reducing the enemy's ability to penetrate mission command systems.

As the list reveals, physical attack typically supports or complements other capabilities such as military deception, electronic warfare, or cyberspace operations.

3-35. When applying physical attack as a component of IO, consideration of second- and third-order effects, as well as consequence management, is a must. Total, or even partial, destruction of threat systems or

capabilities or of indigenous capabilities co-opted by an enemy or adversary, may not be attainable or even desirable. For example, friendly forces may need to use threat command and control systems during the postconflict phase of military operations. Additionally, destructing indigenous capabilities may create animosity among the local populace, the effects of which are greater than any advantage gained over the threat.

PHYSICAL SECURITY

3-36. *Physical security* is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 3-0). Physical security contributes directly to IO and each of its weighted efforts, most especially efforts to defend personnel, information, and systems that contribute to friendly decision making. Information, information-based processes, and information systems—such as mission command systems, weapon systems, and information infrastructures—are protected relative to the value of the information they contain and the risks associated with the compromise or loss of information.

3-37. Physical security is a unit program directed by the commander and overseen by the operations staff officer (see AR 190-13 and AR 190-16 for details on physical security).

PRESENCE, PROFILE, AND POSTURE

3-38. The mere presence of a force can significantly affect all audiences in the AO. Deploying, moving, or assigning forces to the right place at the right time can add substantial credibility to messages being delivered through other channels and provide a major contribution to deterrence. Whenever Soldiers or forces leave base or cross the line of departure, they do two things: collect information and send a message. If either collection or PPP are not a deliberate, coordinated effort, both the information coming back and the message sent appear haphazard and inconsistent. PPP is always in play, and the IO officer should always provide PPP guidance on behalf of the commander.

3-39. Presence is the act of being physically present, although technology is increasingly enabling virtual presence. Presence can be menacing or reassuring, depending on the situation. Absence, or the lack of presence, can create perceptions that work for or against the unit's aims. Being very conscious and deliberate about being present or absent can be a powerful form of influence and should not be left to chance. Once units determine presence is required, or no choice exists but to be present, how they convey that presence is important. Both profile and posture address the way units, patrols, and Soldiers are present.

3-40. Profile is about the degree of presence, both in terms of quantity and quality. Quantity is reflected in how much a unit is present, as in its footprint or task organization. Quality speaks to the nature of that presence, as in its current capability, as well as its reputation.

3-41. The posture of a unit is an expression of its attitude. Whether active or passive, threatening or non-threatening, defensive or welcoming, posture dictates how units or Soldiers appear to others and how Soldiers act towards others. For example, the decision to wear soft caps instead of Kevlar helmets and body armor can considerably affect the perceptions and actions of adversaries and the local populace.

3-42. The operations officer and IO officer or representative are the focal points for PPP. All leaders and Soldiers contribute to it.

PUBLIC AFFAIRS

3-43. Army *public affairs* is communication activities with external and internal audiences (JP 3-61). Public affairs operations help to establish conditions that lead to confidence in the Army and its readiness to conduct unified land operations. It supports the commander's responsibility to keep the American people and the Army informed.

3-44. Public affairs personnel direct their efforts using public information, command information, and community engagement. Public information focuses on informing external audiences. It primarily engages the media and key audiences to convey Army and command themes and messages to American and global

audiences. Command information focuses on internal audiences—Soldiers, DA Civilians, and Family members. Commanders recognize that an informed force is a more ready, reliable, and resilient force. Community engagement focuses on working collaboratively with, and through, groups of people affiliated by a geographic proximity or special interest to enhance the understanding and support for the Army, Soldiers, operations, and activities. It recognizes that a positive rapport between the Army and its host communities is mutually beneficial, supporting the Army as an institution as well as its individual Soldiers.

3-45. The public affairs officer or designated representative is the commander's personal advisor on public affairs matters. The public affairs officer or representative is the focal point for public affairs integration into the operations process and determines the appropriate public affairs posture for a given operation. Close coordination with the IO officer or representative is essential to ensure effects of an IRC are optimized and deconflicted with public affairs and the public affairs posture is supported during SLEs or other engagements; as such, the public affairs officer is a core member of the IO working group (see FM 3-61).

SOLDIER AND LEADER ENGAGEMENT

3-46. *Soldier and leader engagement* is defined as interpersonal Service-member interactions with audiences in an area of operations (FM 3-13). These interactions can be dynamic, such as an impromptu meeting on the street or deliberate, such as a scheduled meeting. SLE can be in-person and face-to-face or conducted at a distance, facilitated by technology.

3-47. A primary purpose of SLE is to convey approved, pre-developed messages (to support approved public affairs or MISO themes) to enhance the credibility of unit personnel and legitimacy of unit operations. Key leader engagement is a subset of SLE.

3-48. The commander is the unit's chief engager and designates a staff focal point for planning, synchronizing, and assessing SLE, whether conducted by unit personnel or other IRCs, such as civil affairs, engineering, or military police forces; chaplains or religious affairs personnel; or medical personnel.

3-49. Chaplains and religious affairs personnel conduct SLEs at the commander's direction as the commander's principle advisor on religion, ethics, morals, and morale while maintaining their noncombatant status (see ATP 1-05.03 for details on religious support). By virtue of their roles as religious leaders, chaplains' very presence in an operational area opens avenues of approach for partnership.

POLICE ENGAGEMENT

3-50. Police engagement occurs in all operational environments in which military police interact with elements external to their own organization. Police engagement is an IRC that occurs among police personnel, organizations, and populations for the purpose of maintaining social order. Military police and U.S. Army Criminal Investigative Command personnel engage local, host-nation, and coalition police partners; police agencies; civil leaders; and local populations for critical police information that can influence military operations or destabilize an AO. Ultimately police engagement aims to develop a routine and reliable interpersonal network through which police information can flow to military police. Based on the tactical situation, police engagement can be formal or informal. Police engagement may be a proactive activity as part of deliberate information gathering, targeting, or collection, or it can be conducted as a reactive response to an episodic event (see FM 3-39 for military police operations).

SPACE OPERATIONS

3-51. Space operations are operations that occur in the space domain and seek to gain superiority over enemies and adversaries in the space domain and its corresponding environment. Army space operations include all aspects of employing specialized Army space forces as well as activities associated with the planning, preparation, integration, and execution required to ensure synchronized and effective space-based capabilities from all sources. Space-based capabilities increasingly facilitate the flow of information and decision making. Space control, one mission area of space operations, can be used to deny communications and propaganda tools, such as satellite television and satellite radio, to enemy leadership. Space surveillance systems monitor the status of enemy and commercial satellite operations to determine potential threats to friendly forces (see FM 3-14 for details on space operations).

SOCIAL MEDIA

3-52. The information environment spotlights the growing impact of social media (see also paragraph 2-14). Although not listed in Table 3-1 because it is still an emergent IRC, social media has the potential to become a powerful capability for IO. Some possible applications include—

- Social media as a media channel, such as radio, newspapers, and television.
- Social media as an interactive medium for exerting influence.
- Social media as a means to communicate with an established network or networks.
- Social media as a near real-time sensor-to-sensor network.

3-53. Social media is rapidly expanding beyond the realm of public affairs, IO, or intelligence functions and becoming an integral component of operations, particularly those occurring in and through the information environment. Even as the institutional Army explores force modernization aspects of social media—such as doctrine, organizations, personnel, and training— commanders and staffs need to understand social media's impact and incorporate this understanding into planning and operations (see *Social Media-The Vital Ground: Can We Hold It?* for a broader discussion of social media).

REQUESTING CAPABILITIES NOT ON HAND

3-54. Effective IO officers or representatives complete prior planning to ensure that required nonorganic capabilities are available to units at the right time and place to support IO effects-generation. The lead time necessary to submit requests varies by echelon and the location of the capability being requested.

3-55. For training support, requests for reserve forces often require six months or more advance notice and must be requested through Army and joint training information management systems. The Army Training Information Management System is the system used by U.S. Army Forces Command and the U.S. Army Civil Affairs and Psychological Operations Command to validate requests and plan support. Required support from nonorganic capabilities, such as field support teams from the 1st IO Command (Land) and TIOGs, should be identified at receipt of mission and invited to all planning conferences through formal means.

3-56. For operational support at lower levels, units submit requests for capabilities or requests for forces. Staffs complete a request for capabilities when units can use the capability remotely while completing a request for forces when units need assets to move into theater. For nontheater assets, the request for forces process is the chief means to request necessary augmentation. The IO officer, working with the operations staff officer, articulates and justifies the need and then submits the request through channels for validation and sourcing, typically through a sourcing conference or other mechanism. Once the requests for capabilities or requests for forces are generated by the combatant commander, the next step is the review and approval process. Once the mission is approved through the review and approval process, the Secretary of Defense directs the Joint Staff to issue an execute order (known as EXORD) directing the provider to use its capability in support.

3-57. IO staffs integrate IRCs used to create effects against an enemy or adversary through targeting. Requesting assets through the joint targeting cycle requires target development and joint certification (for more information on target development and targeting tasks, see ATP 3-60).

This page intentionally left blank.