Chapter 3

Roles, Responsibilities, Relationships, and Organizations

3-1. Every member of a unit—from the commander, to the staff, to the IO officer or representative, to individual Soldiers and Army civilians—contributes to IO. Also essential to mission success are the IRCs supporting the unit's IO efforts, as well as any augmenting IO units. Each has a specific role and important responsibilities to fulfill or undertake, as well as vital relationships to forge and sustain, in order to achieve advantage in and through the information environment.

THE COMMANDER

- 3-2. Commanders, at all levels, are responsible for knowing what threats their units face and how to exploit or defeat them. They are their unit's chief influencers and engage relevant audiences and actors, as necessary, to shape the information environment to their advantage. Commanders rely on their staff and IO officer, in particular, to assist in planning, preparing, executing, and assessing IO. They also personally direct and review analysis of the information environment, issue guidance on the employment and synchronization of IRCs, and direct adjustments based on assessment results.
- 3-3. Cognizant of the pervasive impact of the information environment on operations and the need to affect this environment to their advantage, commanders are mindful of the following:
 - Every operation has, to some degree, an effect on the information environment.
 - IO planning is integral to operations from the start.
 - Effects in and through the information environment, if essential to success, are part of the commander's intent.
 - Combat power cannot be optimized without IO.
 - The warfighting functions (particularly movement and maneuver and fires) produce effects in the information environment, whether intentional or not.
 - IO is essential to operational success at all levels, whether or not the unit has an assigned IO
 officer.
 - All communication can quickly become global and have strategic consequences.
 - IRCs can have lengthy lead times to coordinate and employ, as well as lengthy lag times before
 their effects are realized.
 - The alignment of words, deeds, and images is essential to building trust and confidence with relevant audiences in the area of operations.
 - IO requires prioritized intelligence support.
 - Effects in the information environment are not always caused as expected; assessment is difficult and benefits from commanders' interest, prioritization and support.
 - U.S. IO can be constrained by policy and law, while the threat is often unconstrained in its use of information.

THE STAFF

3-4. Each staff section collaborates routinely, but to varying degrees, with the IO officer to plan, synchronize, support, and assess IO. Representatives from the G-2 (S-2), G-3 (S-3), assistant chief of staff, plans G-5 (S-5), assistant chief of staff, signal G-6 (S-6) and assistant chief of staff, civil affairs operations (G-9/S-9), in particular, serve as core members of the IO working group.

ASSISTANT CHIEF OF STAFF, G-1 (S-1), PERSONNEL

- 3-5. The G-1 (S-1) is the principal staff officer for personnel functions. The G-1 (S-1) processes requirements for individual, team and unit augmentation or attachment. It coordinates reception of these individuals, teams, or units and validates their requirements. It also builds manning documents, as required. Additional IO-related responsibilities include, but are not limited to:
 - Designating a representative to the IO working group.
 - Providing IO-focused instructions in the personnel appendix of the sustainment annex.
 - Reviewing the IO mission and mission, enemy, terrain and weather, troops and support available, time available, and civil considerations from a personnel support perspective.

ASSISTANT CHIEF OF STAFF, G-2 (S-2), INTELLIGENCE

- 3-6. The G-2 (S-2) is the principal staff officer for all matters concerning military intelligence, security operations, and military intelligence training. The G-2 (S-2) produces the intelligence used by the IO officer, element, working group and IRCs. IO-related responsibilities of the G-2 (S-2) include, but are not limited to:
 - Participating as a core member of the IO working group and providing intelligence briefings or updates.
 - Providing IO-focused instructions in the intelligence annex.
 - Including requests for information from the IO officer in intelligence reach.
 - Answering information requirements (IRs) submitted by the IO officer.
 - Coordinating with counterintelligence; law enforcement; and information system developers, providers, administrators, and users to ensure timely sharing of relevant information.
 - Preparing a threat assessment of enemy command and control systems, including:
 - Political, economic, social, and cultural influences.
 - Targets and methods for offensive operations.
 - Enemy decision-making processes.
 - Biographical backgrounds of key threat leaders, decision makers, and communicators, and their advisors. Including motivating factors and leadership styles.
 - A comprehensive comparison of enemy offensive information capabilities against friendly IO vulnerabilities.
 - Collecting data to establish an electronic warfare database and command and control target list.
 - Providing intelligence support to military deception operations; specifically:
 - Helping the G-6 (S-6) plan use of friendly information systems as deception means.
 - Establishing counterintelligence measures to protect the military deception operation from detection.

ASSISTANT CHIEF OF STAFF, G-3 (S-3), OPERATIONS

- 3-7. The G-3 (S-3) is the principal staff officer for all matters concerning training and leader development, operations and plans, and force development modernization. IO-related responsibilities include, but are not limited to:
 - Exercising primary responsibility for IO staff functions and overseeing the IO officer, who is part of the movement and maneuver cell.
 - With assistance from the IO officer, integrating IO planning into the military decisionmaking process.
 - Validating or approving, as necessary, IO officer inputs, actions and outputs. Among the inputs
 and outputs, the mission statement, scheme of IO, and IO objectives require G-3 (S-3) review,
 refinement, and emphasis.
 - If additional IRCs or IO units are required, prioritizing and facilitating the augmentation request or request for forces.
 - Tasking units and assets necessary to achieve IO objectives.

- Providing plans and current operations briefings to IO working group meetings.
- Integrating information collection into operations, supported by the G-2 (S-2).
- Ensuring effective coordination and synchronization among the IO officer and IRC staff representatives and other members of the IO working group.

ASSISTANT CHIEF OF STAFF, G-4 (S-4), LOGISTICS

- 3-8. The G-4 (S-4) is the principal staff officer for all matters concerning sustainment operations. IO-related responsibilities of the G-4 (S-4) include, but are not limited to:
 - Ensuring required resources are included on the baseline resources item list and the commander's track item list.
 - Coordinating sustainment per priorities and requirements.
 - Tracking the operational readiness of IO units and equipment.
 - Providing sustainment capability or vulnerability input to the IO estimate and course of action analyses.
 - Advising the deception and IO working groups on how military operations will affect logistics personnel and equipment.
 - Designating a representative to the IO working group.
 - Providing IO-focused instruction in the sustainment annex.

ASSISTANT CHIEF OF STAFF, G-5 (S-5), PLANS

3-9. The G-5 (S-5) is responsible for incorporating future plans into ongoing operations. The IO officer works closely with the G-5 (S-5) to ensure its efforts to affect the information environment support future plans and provide the commander necessary freedom of action to sustain the initiative and achieve decisive results. When required, the G-5 (S-5) and IO officer work closely to plan and implement deception efforts and ensure objectives are incorporated effectively into plans and operations orders.

ASSISTANT CHIEF OF STAFF, G-6 (S-6), SIGNAL

- 3-10. The G-6 (S-6) is the principal staff officer for all matters concerning Department of Defense information network operations (also called DODIN operations), applicable portions of defensive cyberspace operations, network transport, information services, and spectrum management operations within the unit's area of operations. IO-related responsibilities of the G-6 (S-6) include but are not limited to:
 - Coordinating information management with and providing information management data to the G-3 (S-3).
 - Providing a representative to the IO working group.
 - Providing IO-related instructions in relevant annexes and appendices.
 - Directing the actions of subordinate DODIN operations and information management staff elements.
 - Coordinating DODIN operations and information management support of information collection with the G-2 (S-2).
 - Coordinating with the Army Cyber Operations and Integration Center for antivirus software and threat analysis and advisories, after receiving notification of its support from the G-3 (S-3).
 - Coordinating with the regional cyber center for network intrusion devices, information, approved systems, and software, after receiving notification of its support from the G-3 (S-3).

ASSISTANT CHIEF OF STAFF, G-9 (S-9), CIVIL AFFAIRS OPERATIONS

- 3-11. The G-9 (S-9) is the principal staff officer for all matters concerning civil affairs and civil military operations. The G-9 (S-9) evaluates civil considerations within missions and identifies centers of gravity that are civil in nature. IO-related responsibilities of the G-9 (S-9) include, but are not limited to:
 - Providing a G-9 (S-9) representative to the IO working group.
 - Providing IO-focused instructions in the civil affairs operations annex.

- Interfacing with IO officer on the use of civil military operations in support of the scheme of IO.
- Identifying and procuring civilian resources to support the scheme of IO.
- Advising the military deception officer of implications of military deception operations on civil affairs operations.
- Coordinating with the IO and psychological operations officers on trends in public sentiments.
- Coordinating with the IO officer, public affairs officer, and psychological operations officer to ensure messages are not contradictory.

THE IO OFFICER

3-12. The IO officer (who heads the IO element at division and higher) or representative (at brigade and below) is the staff focal point for IO. The IO officer is responsible for the following specific tasks, among others:

- Analyzing the information environment to discern impacts it will have on unit operations and to exploit opportunities to gain an advantage over threat forces.
- Identifying the most effective IRCs to achieve objectives.
- Synchronizing IRCs to achieve objectives in the information environment.
- Assessing the risk, typically described as risk to mission and risk to force, associated with the employment of any capability, product, program or message.
- Providing input to the synchronization matrix for the use of available IRCs in support of unit operations.
- Identifying IRC gaps not resolvable at the unit level.
- Coordinating with other Army, Service, or joint forces to use IRCs to augment existing unit capability shortfalls.
- Providing information as required in support of operations security (OPSEC) at the unit level.
- Providing information as required in support of military deception at the unit level.
- Leading the IO working group.
- Assessing the effectiveness of employed IRCs.

3-13. The IO officer contributes to the overall intelligence preparation of the battlefield (IPB) by assisting the G-2 (S-2) in identifying and evaluating threat information capabilities, as well as the means to influence the population. Additionally, the IO officer submits to the G-2 (S-2) any IRs regarding intelligence shortfalls about the information environment and coordinates with the G-2 (S-2) in developing templates, databases, and other relevant products, including but not limited to:

- Religion, language, and culture of key groups and decision makers.
- Agendas of nongovernmental organizations.
- Size and location of threat IO or information warfare forces and assets.
- Military and civilian communication infrastructures and connectivity.
- Population demographics, linkages, and related information.
- Audio, video, and print media outlets and centers and the populations they service.
- Location and types of electromagnetic systems and emitters.
- Network vulnerabilities of friendly, neutral, and threat forces.
- 3-14. Additional tasks for which the IO officer is responsible include, but are not limited to:
 - Participating in the military decisionmaking process.
 - Developing IRs.
 - Producing information and combined information overlays.
 - Developing the scheme of IO.
 - Through commander's communication synchronization, contribute to development of the commander's narrative.
 - Integrating IO into the unit's targeting process.
 - Deconflicting the employment of IRCs.

- Ensuring IO-related information is updated in the common operational picture.
- Integrating external augmentation.
- 3-15. Not all units are authorized an IO officer or element. Commanders may, therefore, adapt their staff structure to ensure IO objectives and IRC tasks are accomplished and appoint an officer or non-commissioned officer to perform the duties of the IO officer, outlined in this manual. Task organizing for IO is situation, mission- and commander-dependent.
- 3-16. A key responsibility of the IO officer is to understand the command relationship with IRC units and build rapport accordingly. Building rapport typically begins with a visit to the IRC site location, an orientation on the IRC's potential contributions and limitations, and a collaborative determination of ways to optimize the IRC's effects with other IRCs through synchronization. This rapport-building is ongoing and primarily channeled through the IO working group, although one-on-one conversations will also occur.
- 3-17. When necessary, the IO officer must be ready to lead the planning and employment of select IRCs not clearly managed by a capability owner or proponent. Examples include, but are not limited to: military deception; OPSEC; and Presence, Posture, and Profile. The IO officer is also ready to coordinate for and integrate IRCs that are only found at higher echelons, such as cyberspace operations.

INFORMATION-RELATED CAPABILITIES

- 3-18. IO seeks to optimize the combined effects of selected IRCs through effective planning, synchronization, and assessment. While a single IRC can affect the information environment to friendly advantage, synchronized IRC activities and operations can amplify and unify each other's effects and produce more efficacious and durable results. For example, variation and repetition of actions and messages tends to increase their overall effect, if not their acceptance. Using different IRCs, in combination, to execute actions and deliver messages, provides this requisite variation.
- 3-19. IRCs are diverse. In some cases, they are part of the force structure, such as military information support operations (MISO) units, civil affairs units, or combat camera units. Coordination of these IRCs will be with the IRC unit commander, G-3 (S-3), or designed representative. In other cases, IRCs are tasks or activities managed by a staff section, such as military deception, OPSEC, or special technical operations. Coordination of these IRCs will occur with the staff element's director or a specified action officer.
- 3-20. All IRCs units work collaboratively with the IO officer, as well as with other IRCs, to facilitate their synchronization into the IO portion of the concept of operations, also called the scheme of IO. They do this primarily through the IO working group but utilize any venue or engagement to advance their capability's contribution to the total effort. Most importantly, they articulate their capability's strengths, limitations, and risks to the commander and staff to facilitate decision making about their employment and synchronization.

INFORMATION OPERATIONS SUPPORT UNITS

3-21. The G-3 (S-3), with the assistance of the IO officer, and in concert with organic IRCs, serves as the entry point for external IRCs (excluding public affairs) and IO support units, assets and resources and ensures their integration into overall planning, preparation, execution, and assessment. Among the support organizations that the IO officer helps the G-3 (S-3) to integrate are the 1st Information Operations Command (Land) (1st IO Command) and the reserve component theater information operations groups, which provide a range of IO subject-matter expertise, skills augmentation, and reachback.

1ST INFORMATION OPERATIONS COMMAND (LAND)

3-22. The 1st IO Command, a major subordinate command of the U.S. Army Intelligence and Security Command, is a brigade-sized, multi-compo unit. Under the operational control and tasking authority of the U.S. Army Cyber Command, it provides uniquely tailored IO and cyberspace operations (CO) 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, opposing forces support, reachback

planning and analysis, and specialized training to assist units in garrison, during exercises, and during contingency operations.

3-23. 1st IO Command also supports the Army by working to optimize IO interoperability with joint forces, other military forces, inter-agencies, and allies. It provides expeditionary cyberspace operations support to help units identify network vulnerabilities and enable IO.

Deployable Modular IO Teams

3-24. Deploys a variety of mission-tailored IO and cyberspace operations teams. The configuration of each deploying team varies to meet operational requirements.

Field Support Team

3-25. Provides IO subject-matter expertise to supported commands to assist with the planning, execution and assessment of IO during crisis, contingency, and exercise operations. Field support team members are trained in the operational integration of military deception, electronic warfare, MISO, OPSEC, cyberspace operations, and other activities impacting the information environment.

Vulnerability Assessment Team

3-26. Assists supported commands in identifying and resolving IO and cyberspace vulnerabilities in order to improve the command's defensive posture. The vulnerability assessment teams deploy to provide either: Train and Assist (Blue Team) or Emulation of an Adversarial Attack (Red Team) support. Both are capable of assessing the supported command's OPSEC, physical security, and electronic security training and policies to identify vulnerabilities. Both vulnerability assessment teams also assist the supported command in identifying IO and cyberspace vulnerabilities tied to issues associated with unit procedures, equipment, and other resources, and in finding means to resolve or mitigate identified issues. In addition, the vulnerability assessment teams augment the U.S. Army Forces Command mission command assessment teams in conducting pre-deployment home station cybersecurity training, as well as execute the Command Cyber Readiness Inspections for Army Cyber Command in coordination with the Defense Information Systems Agency.

OPSEC Support Team

3-27. The OPSEC support team is part of the 1st IO Command organizational structure, and augments vulnerability assessment teams and executes independent OPSEC support team missions. OPSEC support teams provide supported commands with OPSEC training, assist with developing OPSEC programs, and assess unit OPSEC programs.

World Class Cyber Opposing Force

3-28. Provides cyber and information warfare opposing force support to designated commands during operational training events, such as major exercises and combat training center rotations. This force serves as a non-cooperative, multiple tier (criminal, hybrid, nation state) cyberspace threat opponent that challenges, trains, and develops leaders to successfully operate within a hostile information environment. The World Class Cyber Opposing Force executes its opposing force mission as the exercise dictates, and will operate either as an independent force or as a member of a larger opposing force.

Reachback and Training Support

- 3-29. Provides IO planning support, intelligence analysis, and technical assistance to deployed 1st IO Command support teams, and to other commands requesting reachback support. Reachback tailors its analytical and intelligence efforts and products to support the current and future operations of the supported commands. Lastly, the reachback provides technical support for the execution of vulnerability assessments and World Class Cyber Opposing Force missions.
- 3-30. The 1st IO Command conducts training instruction throughout the year on the planning, integration and execution of IRCs in both a resident (at Fort Belvoir) and mobile training team format. The 1st IO

Command deploys mobile training teams to requesting commands and installations to provide IO and cyberspace training. Deployed mobile training teams have the ability to tailor instruction to meet the specific requirements of the requesting command. A list of the 1st IO Command training courses can be found in the Army Training Requirements and Resources System.

THEATER INFORMATION OPERATIONS GROUPS

- 3-31. The Army relies upon Theater Information Operations Groups to provide enhanced information operations planning, synchronization, and assessment support to Army echelons at theater and army service component command down to brigade level. There are two Theater IO Groups, the 56th and 71st Theater IO Groups, in the U.S. Army National Guard and two Theater IO Groups in the U.S. Army Reserve, the 151st and 152nd Theater IO Groups. Each Theater IO Group consists of a group headquarters, a headquarters and headquarters company, and two IO battalions which mirror each other in their capabilities.
- 3-32. The mission of the Theater IO Groups is to provide IO subject-matter expertise to a supported command in the form of deployable modular IO teams and a reach back, as well as home station support capability. The Theater IO Groups and its battalion elements do not usually deploy as commands but instead form and deploy purpose-built IO teams designed to provide the necessary IO support required by the requesting command. To enhance the capabilities of the IO teams and reduce preparation time, the Theater IO Groups maintain regional focuses. This focus helps provide the supported command additional regional expertise and capability to plan, synchronize, and assess IRC activities in the conduct of IO within the area of operations. Having a regional focus, however, does not preclude a Theater IO Groups from deploying IO teams and providing IO support to organizations and commands outside of its regional focus area.

Deployable Modular IO Teams

3-33. The Theater IO Groups task organize and deploy mission-focused, modular IO teams created from the various capabilities resident within the Theater IO Groups. In the field, the modular IO teams provide the supported command with IO planning, synchronization, assessment, and analysis of the information environment. These teams have the capability to plan, synchronize, and assess OPSEC and military deception in the supported command. When dictated by mission requirements, the Theater IO Groups S-2 can attach intelligence specialists to a deployed modular IO team. If a modular IO team is not required, Theater IO Groups can deploy individual elements to meet requested mission support focused on planning, synchronization, and assessment of IRCs. In the creation of the modular IO teams, the Theater IO Groups draw upon the expertise resident in the following Theater IO Groups elements.

Army Service Component Command Support Detachment

3-34. Provides the regionally-aligned Army Service Component Command with a culturally-aware, regionally-focused IO planning, synchronization, and assessment capability that can synchronize and assess IO. This detachment provides the supported Army Service Component Command with the expertise to integrate IRCs in concert with other activities into theater security cooperation plans, war plans, and contingency planning. The detachment augments the supported unit's organic IO element or acts as the supported command's IO element. It also serves as the base Theater IO Group element for task organization with other Theater IO Groups capabilities to create a theater, Army Service Component Command-level modular team.

Field Support Detachment

3-35. Provides a culturally-aware, regionally-focused IO planning, synchronization, and assessment capability that can synchronize and assess IO. This detachment provides the supported command with the expertise to integrate IRCs in concert with other activities into operations plans, operations orders, and contingency planning. It can either augment the supported command's G-3 (S-3) IO element or serve as that element. It also serves as the base Theater IO Group element for task organization with other Theater IO Groups capabilities to create a Corps and below modular IO team.

Military Deception Support Detachment

3-36. Equips the supported command with a regionally-aligned military deception-focused planning, coordination, implementation, and assessment capability. Military deception support detachments are trained to identify deception opportunities, deception conduits and means, and develop plans focused on exploiting those opportunities and means. As part of its support functions, the military deception support detachment develops and maintains social-cultural threat databases to include methods and means of communication (conduits) for input to the targeting process. It can either augment or act as the supported command's deception cell.

Assessment Detachments

3-37. Provide multi-disciplined IO effects assessments. They assess the information environment and integrate IO-related collection and assessment into initial planning. They develop criteria in the form of measures of effectiveness and measures of performance and establish indicators for evaluation. Each indicator represents an IR that should identify a set of sources and staff members who collect the information in the assessment plan. Measures of performance and effectiveness are simply criteria—they require relevant information in the form of indicators for evaluation.

OPSEC Support Detachments

3-38. OPSEC support detachments provide planning, synchronization, implementation, and assessment of OPSEC programs to identify friendly critical capabilities, critical vulnerabilities, and critical information in military plans, operations, and supporting activities and prevent exposure to enemy intelligence systems. They determine and advise supported commanders on indicators that threat intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to enemies. In concert with other IRCs, they nominate and employ OPSEC measures that eliminate or reduce to an acceptable level, the vulnerabilities of friendly actions to enemy exploitation.

Web OPSEC Support Detachment

3-39. Administers planning, synchronization, implementation and assessment of web-based OPSEC programs to identify friendly critical capabilities, critical vulnerabilities and critical information in military plans, operations, and supporting activities and prevent exposure to enemy intelligence systems. Recommends and advises on OPSEC implications to cyberspace operations.

Reachback and Home Station Support

3-40. The Theater IO Groups maintain an intelligence support capability designed to produce detailed IO-centric analysis of the operational environment and potential threats (infrastructure; key leaders; information systems; IRCs; composition; vulnerabilities; and friendly, neutral, and threat indigenous networks and their relation to each other) in support of deployed teams. The Theater IO Groups also maintain a habitual relationship with intelligence organizations to provide IO-centric support and products. Deployed teams coordinate with the Theater IO Group's S-2 and Intelligence Integration Element for information which is used in the development of courses of action, target analysis, and creation of a combined information overlay.

The Intelligence Integration Element and Other Support

- 3-41. Contains intelligence specialists who provide multidiscipline intelligence analysis in support of individual Theater IO Groups elements and deployable modular IO teams. Trained on IO in order to provide tailored intelligence support, these specialists can support from home station, deploy to augment command's resident IO element, or as members of an IO team. When deployed, these specialists can serve as the focal point for coordination with other intelligence elements.
- 3-42. In addition to intelligence reachback support, the Theater IO Groups can also provide technical support from home station through the Army Service Component Command support detachments and the web OPSEC support detachment. The Army Service Component Command support detachments are capable of providing theater support planning from either home station or on site at the supported theater Army Service Component Command headquarters. The web OPSEC support detachment is capable of deploying as part of

a modular IO team but more often it provides support from home station where it has assured access to the internet and web based mission command systems.

Note: Commanders can request Theater IO Group's IO team augmentation, reach back support, and home station support by submitting a Request for Forces through their chain of command to their respective Army Service Component Command, where the request for forces will be forwarded to U.S. Army Forces Command for approval. After approval by Forces Command, the request for forces is passed to the National Guard Bureau or the United States Army Reserve for servicing. The employment will consist of mission-tailored and scaled IO teams provided, as needed, to either a single or multiple commands and echelons, or the dedication of the entire IO group to support an Army Service Component Command. In the latter case, the IO group will provide IO support to the Army Service Component Command and its subordinate command structures down to brigade.

56th Theater IO Group: Assigned to the Washington Army National Guard with one battalion located in the Maryland Army National Guard. Regional focus areas are U.S. Pacific Command, U.S. Central Command, and U.S. Northern Command.

71st Theater IO Group: Assigned to the Texas Army National Guard. Regional focus areas are U.S. Southern Command, U.S. Northern Command and U.S. Africa Command.

151st Theater IO Group: Assigned to the U.S. Army Reserve. Regional focus areas are U.S. Africa Command, U.S. European Command, and U.S. Central Command.

152nd Theater IO Group: Assigned to the U.S. Army Reserve. Regional focus areas are U.S. Central Command, U.S. Pacific Command, and U.S. European Command. (To be inactivated FY 2017)

INDIVIDUAL SOLDIERS AND ARMY CIVILIANS

3-43. IO seeks to influence adversaries or enemies, as well as foreign audiences to acquiesce to or support our demands or align their actions in concert with the friendly commander's intent and objectives. One of the most potent and readily-available IRCs to influence these audiences is Soldier and leader engagement. Soldier and leader engagements are interpersonal Service-member interactions with audiences in an area of operations. When Soldiers and leaders, inclusive of Army civilians and contractors, align their words, images, and actions in support of the commander's communications strategy, they contribute to mission accomplishment in a forceful and enduring way. Additional actions necessary to conduct Soldier and leader engagements include, but are not limited to:

- Knowing and understanding the commander's intent.
- Studying local culture, habits, and ways of communicating.
- Memorizing approved talking points.
- Being alert to non-verbal cues or signals on both sides of any conversation or engagement.
- Following through on commitments.

