Chapter 4
Planning

4-1. *Planning* is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Planning helps commanders create and communicate a common vision between commanders, their staffs, subordinate commanders, and unified action partners. Planning results in a plan and orders that synchronize the action of forces in time, space, and purpose to achieve objectives and accomplish missions.

4-2. Commanders, supported by their staffs, ensure IO is fully integrated into the plan, starting with Army design methodology (ADM) and progressing through the military decisionmaking process (MDMP). The focal point for IO planning is the IO officer (or designated representative for IO). However, the entire staff contributes to planning products that describe and depict how IO supports the commander's intent and concept of operations. The staff also contributes to IO planning during IO working group meetings to include assessing the effectiveness of IO and refining the plan.

PLANNING OVERVIEW

4-3. Planning activities occupy a continuum ranging from conceptual to detailed. Conceptual planning involves understanding operational environments and problems, determining the operation's end state, and visualizing an operational approach to attain that end state. Detailed planning translates the commander's operational approach into a complete and practical plan. Generally, detailed planning is associated with the science of control including synchronizing forces in time, space, and purpose to accomplish missions.

4-4. ADM helps commanders and staffs with the conceptual aspects of planning. These aspects include understanding, visualizing, and describing operations to include framing the problem and identifying an operational approach to solve the problem. The MDMP helps commanders and staffs translate the commander's vision into an operations plan or operations order that synchronizes the actions of the force in time, space, and purpose to accomplish missions. Both the problem the commander needs to solve and the specific operation to advance towards its solution have significant information-related aspects.

IO AND ARMY DESIGN METHODOLOGY

4-5. ADM is a methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them (ADP 5-0). By first framing an operational environment and associated problems, ADM enables commanders and staffs to think about the situation in depth. From this understanding, commanders and staffs develop a more informed approach to solve or manage identified problems. During operations, ADM supports organizational learning through reframing—a maturing of understanding that leads to a new perspective on problems or their resolution.

4-6. Problems typically facing Army forces and unified action partners, within a given area of operations, are human-centered. Human problems are driven by human decision making, which can be affected directly or indirectly through the use of IRCs, including effects produced by movement and maneuver. Therefore, the most essential part of ADM from an IO perspective is framing the current state of the information environment to determine key decision makers and the ways by which their decision process can be altered. This analysis identifies and creates understanding of decision makers' beliefs, motivations, grievances, biases, and preferred ways of communicating and obtaining information.

4-7. Framing the current state and desired future state of the information environment are key aspects of framing an operational environment and developing an operational approach. The operational approach provides a guide for more detailed IO planning, to include determining the effects necessary to bring about

the desired end state in the information environment and the required combinations of IRCs needed to produce these effects.

4-8. Commanders typically employ a combination of direct and indirect approaches to defeating the enemy. A direct approach attacks the threat's center of gravity or principal strength by applying combat power against it. An indirect approach attacks the enemy's center of gravity by applying combat power against a series of decisive points that iteratively lead to the defeat of the center of gravity while avoiding the enemy's strengths. IO contributes to both approaches, especially when the threat's center of gravity or principal strength is information-related. (See ATP 5-0.1, *Army Design Methodology* for a comprehensive discussion of various techniques used in framing the operational environment, framing the problem, developing an operational approach, and reframing).

IO AND THE MILITARY DECISIONMAKING PROCESS

4-9. Commanders use the MDMP to understand the situation and mission confronting them and make informed decisions resulting in an operations plan or order for execution. (See FM 6-0 for a detailed description of the MDMP.) Their personal interest and involvement is essential to ensuring that IO planning is integrated into MDMP from the beginning and effectively supports mission accomplishment. IO planning is integral to several other processes, to include intelligence preparation of the battlefield (IPB) and targeting. (See ATP 2-01.3 for further information on IPB and Chapter 7 of this manual and ATP 3-60 for further information on targeting.) The G-2 (S-2) and fire support representatives participate in the IO working group and coordinate with the IO officer to integrate IO with their activities and the overall operation. Commanders use their mission statement for the overall operation, the IO mission statement, scheme of IO, IO objectives, and IRC tasks to describe and direct IO, as seen in figure 4-1.

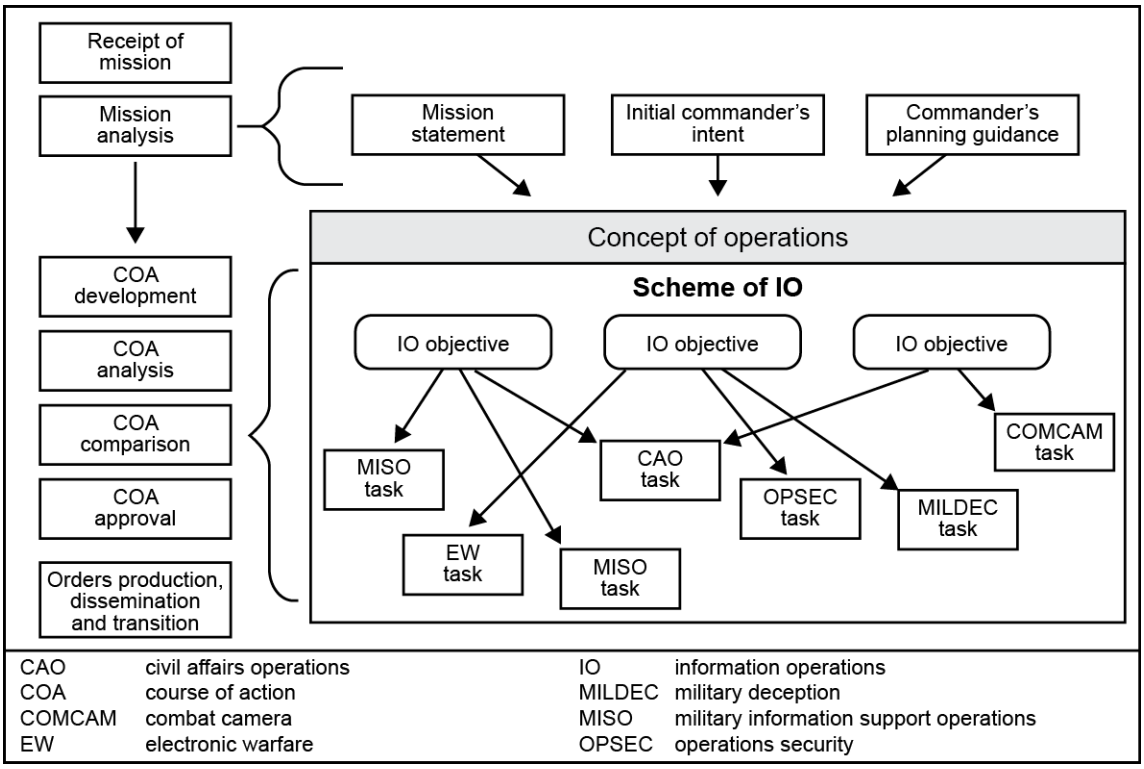

Figure 4-1. Relationship among the scheme of IO, IO objectives, and IRC tasks.

Scheme of IO

4-10. 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 support overall

operations and achieve the mission. Based on the commander's planning guidance, to include IO weighted efforts, the IO officer develops a separate scheme of IO for each course of action (COA) the staff develops. IO schemes of support are written in terms of IO objectives—and their associated weighted efforts—and IRC tasks required to achieve these objectives. For example, the overall scheme may be oriented primarily on defending friendly information but also include attack and stabilize objectives.

IO Objectives

4-11. IO objectives express specific and obtainable outcomes or effects that commanders intend to achieve in and through the information environment. In addition to be being specific, these objectives are measurable, achievable, relevant, and time-bounded (or SMART), which facilitates their attainment and assessment (see chapter 8). IO objectives serve a function similar to that of terrain or force-oriented objectives in maneuver operations. They focus the IO effort on achieving synchronized IRC effects, at the right time and place, to accomplish the unit's mission and support the commanders' intent and concept of the operation.

4-12. Accurate situational understanding is key to establishing IO objectives. Operational- and tactical-level IO objectives must nest with strategic theater objectives. Joint and component staffs develop IO objectives to help integrate and synchronize their campaigns and major operations.

4-13. The IO officer develops objectives as part of developing the scheme of IO during COA development. These objectives help the staff determine tasks to subordinate units during COA development and analysis.

Tasks

4-14. Tasks are developed to support accomplishment of one or more IO objectives. These tasks are developed specifically for a given IRC. In concert with IRC representatives, the IO officer develops tasks during COA development and finalizes them during COA analysis. During COA development and COA analysis, tasks are discussed in general terms but not assigned to a subordinate unit. During orders production, these tasks are assigned to IRC units.

Flexibility and Lead Times

4-15. IO planning requires innovation and flexibility. Some IRCs, such as military information support operations (MISO), operations security (OPSEC), and military deception, require a long lead time for planning and preparation. Synchronizing IRCs into multiple lines of operation or effort requires extensive coordination. Achieving certain IO objectives may require senior-leader review and approval and more up-to-date intelligence. For some IRCs, there is a significant lag between execution and assessment of their effects. Planning requires a concentrated information collection effort during preparation and execution to obtain and analyze information for assessing effectiveness. These factors increase the challenges facing planners and decrease the time available to prepare. Nevertheless, early execution of select tasks can enhance efforts to shape the information environment in the area of operations.

RECEIPT OF MISSION

4-16. Upon receipt of a mission, the commander and staff perform an initial assessment. Based on this assessment, the commander issues initial guidance and the staff prepares and issues a warning order (WARNORD). Between receiving the commander's initial guidance and issuing the WARNORD, the staff performs receipt of mission actions. During receipt of mission, the IO officer—

- Reviews and updates the running estimate.
- Participates in the initial assessment.
- Provides input to the commander's initial guidance.
- Provides input to the warning order.
- Prepares for subsequent planning.

REVIEW AND UPDATE THE RUNNING ESTIMATE

4-17. Running estimates are integral to IO planning. A *running estimate* is the continuous assessment of the current situation, and is used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (ADP 5-0). Running estimates help the IO officer record and track pertinent information about the information environment leading to a basis for recommendations to the commander.

4-18. The IO officer uses the running estimate to assist with completion of each step of the MDMP. An effective running estimate is as comprehensive as possible within the time available but also organized so that the information is easily communicated and processed. Normally, the running estimate provides enough information to draft the applicable IO sections of WARNORDs as required during planning and ultimately to draft applicable IO sections of the operation order (OPORD) or operation plan (OPLAN).

4-19. Variations on the standard, narrative format, such as the example provided in figure 4-2, enable the IO officer to spotlight facts and assumptions, critical planning factors, and available forces. The latter of these requires input from assigned or available IRCs. The graphical format also offers a clear, concise mechanism for the IO officer to articulate recommended high-payoff targets, commander's critical information requirements, and requests for forces. Maintaining both formats simultaneously provides certain benefits: the narrative format enables the IO officer to cut-and-paste sections directly into applicable sections of orders; the graphical format enables the element to brief the commander and staff with a single slide.

4-20. Running estimate development never stops. The IO officer continuously maintains and updates the running estimate as pertinent information is received. While at home station, the IO officer maintains a running estimate on friendly capabilities. If regionally aligned, the unit prepares its estimate based on research and analysis of the information environment within its region and anticipated mission sets.

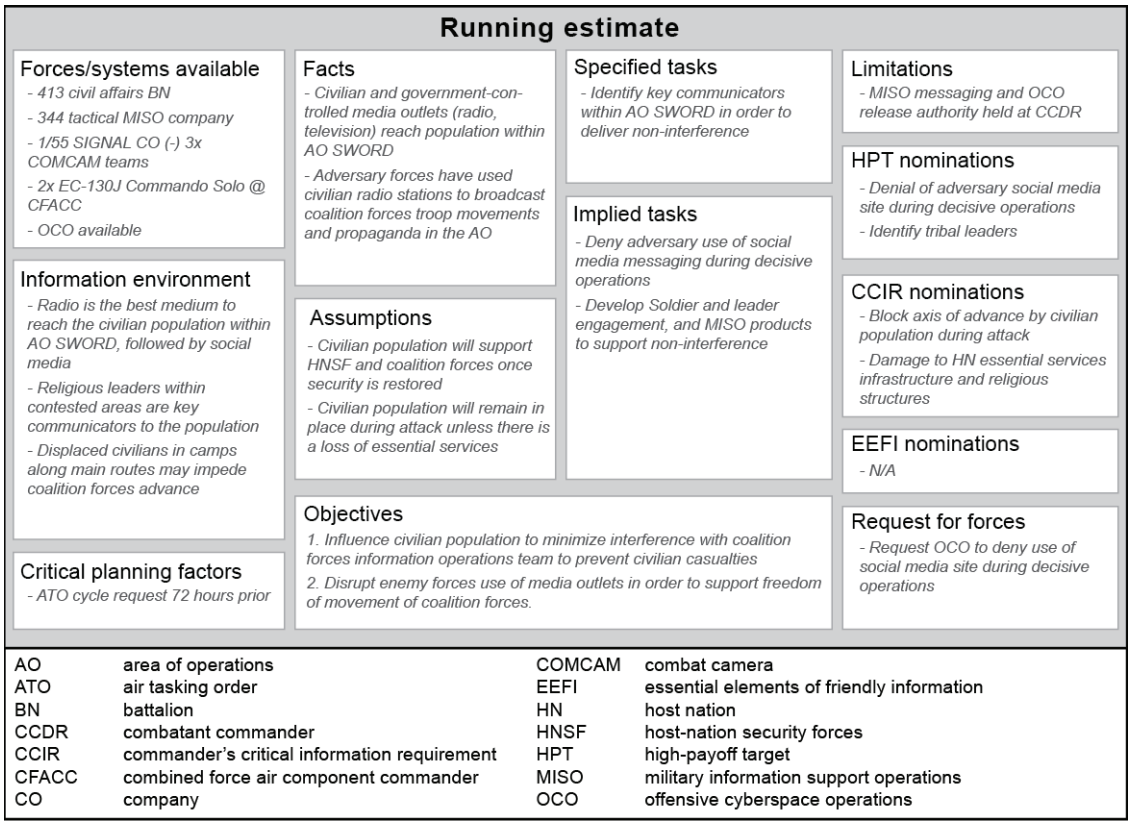

Figure 4-2. Example graphical IO running estimate

PARTICIPATE IN COMMANDER'S INITIAL ASSESSMENT

4-21. Initial assessment primarily focuses on time and resources available to plan, prepare and begin execution of an operation. The IO officer assesses readiness to participate in ADM and MDMP, as well as what external support might be necessary to ensure effective IO planning.

4-22. During the initial assessment, the IO officer establishes a battle rhythm, including locations, times, preparation requirements, and the anticipated schedule. Upon receiving a new mission, the IO officer begins gathering planning tools, including a copy of the higher command OPLAN or OPORD, maps of the area of operations, appropriate references, and the running estimate. During initial assessment, the IO officer also coordinates with organic, assigned, and available IRCs and subordinate units to gauge their planning readiness.

4-23. Initial time allocation is important to IO because some operations and activities require significant time to produce effects or for assessment. The time available may be a limiting factor for some IRCs. The IO officer identifies activities for which this is the case and includes these limitations in estimates and recommendations.

4-24. The commander determines when to execute time-constrained MDMP. Under time-constrained conditions, the IO officer relies on existing tools and products, either his or her own or those of higher headquarters. The lack of time to conduct reconnaissance requires planners to rely more heavily on assumptions and increases the importance of routing combat information and intelligence to the people who need it. A current running estimate is essential to planning in time-constrained conditions.

PROVIDE INPUT TO THE COMMANDER'S INITIAL GUIDANCE

4-25. Commanders include IO-specific guidance in their initial guidance, as required. Examples include authorized movements of IRCs, initiation of information collection necessary to support IO, and delineation of IRs.

PROVIDE INPUT TO THE INITIAL WARNING ORDER

4-26. A WARNORD is issued after the commander and staff have completed their initial assessment and before mission analysis begins. It includes, at a minimum, the type and general location of the operation, initial timeline, and any movements or reconnaissance that need to be initiated. When they receive the initial WARNORD, subordinate units begin parallel planning.

4-27. Parallel planning and collaborative planning are routine MDMP techniques. The time needed to achieve and assess effects in the information environment makes it especially important to successful IO. Effective parallel or collaborative planning requires all echelons to share information fully as soon as it is available. Information sharing includes providing higher headquarters plans, orders, and guidance to subordinate IO officers or representatives.

4-28. Because some IRCs require a long time to plan or must begin execution early in an operation, follow-on WARNORDs may include detailed IO information. Although the MDMP includes three points at which commanders issue WARNORDs, the number of WARNORDs is not fixed. WARNORDs serve a purpose in planning similar to that of a fragmentary order (FRAGORD) during execution. Commanders issue both, as the situation requires. Possible IO officer input to the initial WARNORD includes:

- Tasks to subordinate units and IRCs for early initiation of approved IO actions, particularly for military deception operations and MISO.
- Essential elements of friendly information (EEFIs) to facilitate defend weighted efforts and begin the OPSEC process.
- Known hazards and risk guidance.
- Military deception guidance and priorities.

MISSION ANALYSIS

4-29. Commanders and their staff conduct mission analysis to better understand the situation and problem, and to identify the purpose of the operation. It is the most important step in MDMP and consists of 18 sub-steps, many of which are performed concurrently. (See FM 6-0, Chapter 9) The IO officer ensures each output or product from this step includes relevant factors or tie-ins. The IO officer also participates in other staff processes (such as IPB and targeting) to ensure IO is properly integrated. For the IO officer, mission analysis focuses on developing information and products that will be used during the rest of the operations process.

ANALYZE HIGHER HEADQUARTERS' PLAN OR ORDER

4-30. Mission analysis begins with a thorough examination of the higher headquarters OPLAN/OPORD in terms of the commander's initial guidance. By examining higher echelon plans, commanders and staffs learn how higher headquarters plan to conduct IO and which resources and higher headquarters assets are available. The IO officer researches these plans and orders to understand the—

- Higher commander's intent and concept of operations.
- Higher headquarters area of operations and interest, mission and task constraints, acceptable risk, and available assets.
- Higher headquarters schedule for conducting the operation.
- Missions of adjacent units.

4-31. Planning to conduct IO without considering these factors may result in an uncoordinated operation, which will hamper overall mission effectiveness. A thorough analysis also helps to determine if additional, external IO support is necessary.

PERFORM INITIAL INTELLIGENCE PREPARATION OF THE BATTLEFIELD

4-32. During mission analysis, the G-2 (S-2) prepares IPB products or updates existing products and the initial IPB is performed upon receipt of the mission. The G-2 (S-2), with assistance and input from other staff elements, uses IPB to define the area of operations/interest, describe its effects, evaluate the threat, and determine threat courses of action. Figure 4-3, on page 4-8, lists possible IO-related factors to consider during each IPB step. During IPB, the IO officer works with the G-2 (S-2) to determine threat capabilities and vulnerabilities in the information environment regarding both the threat and other relevant targets and audiences in the area of operations.

Define the Information Environment

4-33. The information environment has always affected military operations. IO officers, working with the G-2 (S-2), use available intelligence to analyze the information environment and the threat's use of information. This information is submitted to the G-2 (S-2) to answer intelligence gaps that address how information environment factors affect operations. The G-2 (S-2) obtains the information from strategic and national-level databases, country studies, collection assets and, when necessary, other intelligence agencies.

4-34. As part of defining the battlefield environment, the G-2 (S-2) establishes the limits of the area of interest. The area of interest includes areas outside the area of operations that are occupied by threat or other forces/groups that can affect mission accomplishment. This fact is particularly true from an information environment perspective. The ability to obtain and pass information has vastly expanded the capacity of actors to affect areas of operations from anywhere. The IO officer ensures that the G-2 (S-2) considers this factor of the information environment in defining the area of interest for IPB.

4-35. As stated in Chapter 2, one of the enabling activities of IO is analyzing and understanding the information environment in all its complexity. Using the IPB process to accomplish this task, the IO officer develops a series of information overlays, as well as combined information overlays, to depict the information aspects of the operational environment.

4-36. The IO officer provides input to help the G-2 (S-2) develop IPB templates, databases, social network diagrams, and other products that portray information about threats and other key groups or audiences in the

areas of operation and interest. These products contain information about each group's leaders and decision makers. Information relevant to conducting IO includes, but is not limited to:

- Religion, language, culture, and internet activities of key groups and decision makers.
- Agendas of non-governmental organizations.
- Military and civilian communication infrastructures and connectivity.
- Population demographics, linkages, and related information.
- Location and types of radars, jammers, and other non-communication information systems.
- Audio, video, and print media outlets and centers; the populations they serve; and their dissemination characteristics, such as frequency, range, language, etc.
- Command and control or mission command vulnerabilities of friendly, adversary, and other forces or groups.
- Conduit analysis describing how threat decision makers receive information.

4-37. Threat templates portray how adversaries use forces and assets unopposed by friendly forces and capabilities. Threat templates are often developed before deployment. The G-2 (S-2) and IO officer may add factors from the information environment to a maneuver-based threat template, or they may prepare a separate IO threat template. The situation, available information, and type of threat affect the approach taken. IO-related portions of IPB products become part of paragraph 1b of the running estimate.

4-38. The G-2 (S-2) uses IPB to determine possible threat courses of action and arrange them in probable order of adoption. These courses of action, depicted as situation templates, include threat IRCs. A comprehensive IPB addresses threat offensive and defensive capabilities and vulnerabilities, and it is efficacious to friendly mission analysis to develop situation templates depicting how threats and others may employ these capabilities to achieve advantage.

IPB Support of Targeting

4-39. IPB identifies high-value targets (HVTs) and shows where and when they may be anticipated. Some of these HVTs are IO-focused or related, such as a specific population group within an area of operation. The G-2 (S-2) works with the IO officer to develop IO-related HVTs into high-payoff targets (HPTs) for the commander’s approval. The IO officer determines which HPTs are related to one or more objectives and develops tasks to engage those targets during COA development and analysis.

Other IPB Products

4-40. IPB identifies facts and assumptions concerning threats and the operational environment that the IO officer considers during planning. These are incorporated into paragraph 2 of the running estimate. The IO officer submits IRs to update facts and verify assumptions. Working with the G-2 (S-2) and other staff sections, the IO officer ensures IRs are clearly identified and requests for information (RFIs) are submitted to the appropriate agency when necessary. IPB may create priority intelligence requirements (PIRs) pertinent to IO planning. The IO officer may nominate these as commander's critical information requirements (CCIRs) and also identify OPSEC vulnerabilities. The IO officer analyzes these to determine appropriate OPSEC measures.

Define the Operational Environment	Describe the Environmental Effects on Operations	Evaluate the Threat	Determine Threat COAs
Portions or aspects of the information environment that can effect friendly operations. Features/activities that can influence information and threat command and control (C2) or friendly mission command systems. Political and governmental structures and population demographics. Major cultures, languages, religions, and ethnic groups. Civilian communication and power infrastructures (both physical and informational). Non-state actors, non-governmental organizations and significant non-threat groups. Types of and public access to media or press outlets.	IE effects on decisionmakers, C2 or mission command systems, and decision-making processes. How the IE relates to the area of operations. IE effects on friendly, threat, and other operations. Combined effects of friendly, threat, and other information, and C2 or mission command systems on the information environment. Effects of terrain, weather, and other characteristics of the area of operations on friendly and enemy information and C2 or mission command systems. Effect of public media or press on friendly and threat operations.	Adversary and other group C2 systems, including functions, assets, capabilities, and vulnerabilities (both offensive and defensive). Assets and functions (such as decisionmakers, C2 systems, and decision-making processes) that adversaries and others require to operate effectively. Adversary capabilities to attack friendly information systems and defend their own. Models of threat and other group C2 systems. IO or information-related strength, vulnerabilities, and susceptibilities of adversaries and other groups.	How threats and other groups pursue operational or decisive advantage in the IE. How, when, where, and why (to what purpose) threats and other groups will use information-related capabilities to achieve their likely objectives.
C2 command and control	**COA** Course of Action	**IE** Information environment	**IO** Information operations

Figure 4-3. IO-related factors to consider during IPB

DETERMINE SPECIFIED, IMPLIED, AND ESSENTIAL TASKS

4-41. While the staff determines specified, implied, and essential tasks the unit must perform, the IO officer identifies specified IO tasks in the higher headquarters OPLAN or OPORD. The IO officer also develops IO-related implied tasks that support accomplishing identified specified tasks. These identified tasks are the basis of the initial scheme of IO developed during COA development.

IO officers look for specified tasks that may involve IO in the higher headquarters OPLAN or OPORD, paying particular attention to:

- Paragraph 1, Situation.
- Paragraph 2, Mission.
- Paragraph 3, Execution, especially subparagraphs on IO, tasks to subordinate units, and CCIRs.
- Annexes and appendices that address intelligence, operations, fire support, rules of engagement, IO, IRCs, information collection, assessment, and interagency coordination.

4-42. Some IO specified tasks, such as support to the higher headquarters deception plan, become unit objectives. Others, particularly those that address only one IRC, are incorporated under IO objectives as tasks. As the staff identifies specified tasks for the overall operation, the IO officer deduces the steps that are necessary to accomplish these specified tasks. These tasks become IO implied tasks. Once the IO officer identifies specified and implied tasks and understands each task's requirements and purpose, essential tasks are identified. An essential task is a specified or implied task that must be executed to accomplish the mission. If the command must accomplish an IO task to accomplish its mission, that task is an essential task for the command and is included in the recommended mission statement.

REVIEW AVAILABLE ASSETS AND IDENTIFY RESOURCE SHORTFALLS

4-43. During this sub-step, the commander and staff determine if they have the assets required to perform the specified, implied, and essential tasks. The IO officer performs this analysis to determine if the requisite capabilities are on hand or available through coordination with higher echelons to achieve the effects in the information environment necessary to support the mission. At echelons below division, units have few organic IRCs other than movement and maneuver; Soldier and leader engagement; and presence, posture, and profile. If additional IRCs are required, the IO officer works with the operations officer to request these

capabilities and ensure appropriate authorities exist. (See chapter 9 for further discussion of IO at brigade and below).

4-44. The IO officer compares available IRCs with the tasks that need to be accomplished to identify capability shortfalls and additional resources required. The IO officer considers how the following will affect attainment of IO objectives and whether additional capacity is required—

- Changes in task organization.
- Limitations of available units and IRCs.
- Nature of effects that need to be achieved in the information environment and the tasks to accomplish them.
- The need for redundancy or repetition to achieve desired effects.
- The level, quantity, and quality of expertise on hand.

DETERMINE CONSTRAINTS

4-45. A constraint is a restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action of a subordinate commander (FM 6-0). IO constraints include legal, moral, social, operational, and political factors. They also include limitations imposed by various authorities, such as the Secretary of Defense or U.S. ambassador. Constraints may be listed in the following paragraphs, annexes or appendices of the higher OPLAN/OPORD—

- Commander's intent and guidance.
- Tasks to subordinate units.
- Rules of engagement (no strike list, restricted target list)
- Civil affairs operations.
- MISO
- Fire support.

4-46. Constraints establish limits within which the commander can conduct IO. Constraints may also limit the use of military deception and some OPSEC measures. One output of this sub-step is a list of the constraints that the IO officer believes will affect the scheme of IO.

IDENTIFY CRITICAL FACTS AND DEVELOP ASSUMPTIONS

4-47. Sources of facts and assumptions include existing plans, initial guidance, observations, and reports. Some facts concerning friendly forces are determined during the review of the available assets. During IPB, the G-2 (S-2), with assistance from the IO officer and other staff elements, develops facts and assumptions about threats and others, the area of operations, and the information environment. The following categories of information are important to the IO officer—

- Intelligence on threat commanders and other key leaders.
- Threat morale.
- Media and/or press coverage of threat and other relevant audiences in the area of operations.
- The weather.
- Dispositions of adversary, friendly, and other key groups.
- Available troops, unit strengths, and materiel readiness.
- Friendly force IO vulnerabilities.
- Threat and other key group IO vulnerabilities.

4-48. The primary output of this sub-step is a list of facts and assumptions that concern IO. These are placed in paragraph 1c of the running estimate. The IO officer prepares and submits to appropriate agencies IO IRs for information that would confirm or disprove facts and assumptions. The IO officer reviews facts and assumptions as information is received and revises facts or converts assumptions into facts.

BEGIN RISK MANAGEMENT

4-49. Commanders and staffs assess risk when they identify hazards, regardless of type. The IO officer assesses IO-associated risk throughout the operations process. The G-3 (S-3) incorporates the IO risk assessment into the command's overall risk assessment.

4-50. IO-related hazards fall into three categories:

- OPSEC vulnerabilities, including hazards associated with compromise of essential elements of friendly information.
- Mission command vulnerabilities, including those associated with the loss of critical assets or identified during the vulnerability assessment.
- Hazards associated with executing IO tasks.

4-51. During mission analysis, the IO officer assesses primarily OPSEC- and mission command-related hazards, as well as hazards associated with IO-related specified and implied tasks identified up to this point in mission analysis. The list of task-associated hazards is refined during COA development, after articulating IRC tasks that support IO objectives. The IO element uses experience in previous operations as a means of identifying known or expected hazards, and IRC representatives often best articulate hazards associated with their tasks.

4-52. As with all operations, IO entails risk. Resource constraints, combined with threat reactions and initiatives, reduce the degree and scope of advantage possible in the information environment. Risk assessment is one means commanders use to allocate resources. Staffs identify which hazards pose the greatest threat to mission accomplishment. They then determine the resources required to control them and estimate the benefits gained. This estimate of residual risk gives commanders a tool to help decide how to allocate resources and where to accept risk. (For detailed information on the integration of the risk management process, see ATP 5-19).

DEVELOP COMMANDER'S CRITICAL INFORMATION REQUIREMENTS AND ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

4-53. A *commander's critical information requirement* (CCIR) is an information requirement identified by the commander as being critical to facilitating timely decision making (JP 3-0). CCIRs include priority intelligence requirements (PIRs) and friendly forces information requirements (FFIRs). Staff sections, including the IO officer, recommend CCIRs to the G-3 (S-3). In a time-constrained environment, the staff may collectively compile this information. The G-3 (S-3) presents a consolidated list of CCIRs to the commander for approval. The commander determines the final CCIRs.

4-54. Establishing CCIRs is one means commanders use to focus assessment efforts. CCIRs change throughout the operations process because the information that affects decision making changes as an operation progresses.

4-55. During planning, staff sections establish IRs to obtain the information they need to develop the plan. Commanders produce CCIRs to support decisions they must make regarding the form the plan takes.

4-56. During preparation, the focus of IRs and CCIRs shifts to decisions required to refine the plan. During execution, commanders establish CCIRs that identify the information they need to make execution and adjustment decisions.

4-57. During mission analysis, the IO officer derives the information needed by the commander to determine how to employ IO during the upcoming operation. The IO officer recommends the IO IRs to be included in the CCIRs. This sub-step produces no IO-specific product unless the IO officer recommends one or more IO IRs as CCIRs. However, at this point, the IO officer should have assembled a list of IO IRs and submitted friendly-force-related IRs to the G-3 (S-3) and threat-related IRs to the G-2 (S-2).

4-58. The following is an example of CCIRs for a stability operation in which an information operation is the decisive operation:

- Who are the municipality's key players in ethnic violence?
- What are the interests of the political parties?

- Who are the formal and informal leaders within the political parties?
- How can friendly forces exploit political party interests to garner support?
- Which party represents the majority of the people, but also actively support progress within the municipality?
- What is the status of IRCs within the area of operations?

4-59. In addition to nominating CCIRs to the commander, the staff also identifies and nominates essential elements of friendly information, or EEFIs. EEFIs are elements of information to protect rather than to collect, and identify those elements of friendly force information that, if compromised, would jeopardize mission success. Although EEFIs are not CCIRs, they have the same priority as CCIRs and require approval by the commander. Like CCIRs, EEFIs change as an operation progresses (FM 6-0).

4-60. Submission of IO-focused requirements for potential inclusion as CCIRs, along with other CCIRs, enable the staff to develop the initial information collection plan. Approval of EEFIs enable the staff to plan and implement friendly force information protection measures, such as provided by military deception and OPSEC.

DEVELOP THE INITIAL INFORMATION COLLECTION PLAN

4-61. The staff identifies information gaps, especially those needed to answer IRs. The IO officer identifies gaps in information needed to support IO planning, execution and assessment. These are submitted to the G-2 (S-2) as IO IRs. The initial information collection plan sets the priorities for information collection in order to answer CCIRs. The G-3 (S-3) issues the information collection plan as part of a WARNORD, a FRAGORD or an OPORD. Within these orders, the information collection plan is found in Annex L.

UPDATE PLAN FOR THE USE OF AVAILABLE TIME

4-62. At this point, the G-3 (S-3) refines the initial time plan developed during receipt of mission. The IO officer provides input specifying the long lead-time items associated with certain IRC tasks (such as military deception and MISO). Upon receiving the revised timeline, the IO officer compares the time available to accomplish IRC tasks with the command's and threat's time lines, and revises the IO time allocation plan accordingly. The IO product for this sub-step is a revised time plan.

DEVELOP INITIAL THEMES AND MESSAGES

4-63. Gaining and maintaining the trust of relevant audiences and actors is an important aspect of operations. Faced with a diverse array of individuals, organizations, and publics who affect or are affected by their unit's operations, commanders identify and engage entities vital to operational success. The behaviors of these entities can aid or complicate the friendly forces' challenges as commanders strive to accomplish missions.

4-64. The IO officer does not develop themes and messages. This is done by the public affairs officer and MISO element. The public affairs officer adjusts and refines themes and messages received from higher headquarters for use by the command. These themes and messages are designed to inform specific domestic and foreign audiences about current or planned military operations. The Office of the Secretary of Defense, Department of State, or geographic combatant commander (depending on the operation) provides applicable themes to MISO forces, which then develop actions and messages. The highest level MISO element in theater adjusts or refines the themes depending on the situation. It employs themes and messages as part of planned activities designed to influence specific foreign targets and audiences for various purposes that support current or planned operations.

4-65. The commander and the chief of staff approve all themes and messages used to support operations in their area of responsibility. Although the IO officer does not develop themes and messages, they do assist the G-3 (S-3) and the commander to de-conflict and synchronize IRCs used specifically to execute actions for psychological effect and deliver messages during operations.

DEVELOP A PROPOSED PROBLEM STATEMENT

4-66. Problem statements are typically developed during design. If this did not occur prior to mission analysis, it is accomplished during this step of the MDMP. If done during design, the commander and staff revise the problem statement based on their enhanced understanding of the situation. The key is identifying the right problem to solve, because it leads to the formulation of specific solution-sets. In identifying the problem, the commander and staff compare the current situation to the desired end state and list issues that impede the unit from achieving this end state.

4-67. Given the increasing impact of the information environment, the prevailing problem or impeding issues are likely to be information-related. Also, information-related problems can be more complex and multi-dimensional than geographical or technological problems or impediments. Therefore, it is essential to spend the time necessary to articulate the problem and impediments as carefully and clearly as possible.

DEVELOP A PROPOSED MISSION STATEMENT

4-68. The G-3 (S-3) or executive officer develops the proposed restated mission based on the force's essential tasks, which the commander approves or modifies. The IO officer provides input based on the current IO running estimate. The mission statement includes any identified IO essential tasks.

4-69. Mission statements should use tactical mission tasks, which are specific activities performed by units while executing a form of tactical operation or form of maneuver (See ATP 3-90.1). IO tasks do not always neatly fit into this framework, as they are rarely terrain- or combined arms-based. However, if they are framed in terms of friendly force actions (for example, influence the population in a certain area) or effects on threat forces (deceive the threat's reserve forces commander), and if they support the commander's intent and planning guidance, then they can be integrated effectively into the restated mission.

4-70. The IO officer also develops an IO mission statement that guides IO execution and ensures IO objectives are accomplished. The IO mission statement is explicitly stated in Appendix 15 (Information Operations) to Annex C (Operations) of the base order. (See FM 6-0, Appendix C, for additional details on functional area mission statements.)

PRESENT THE MISSION ANALYSIS BRIEFING

4-71. The staff briefs the commander on the results of its mission analysis. The mission analysis briefing is an essential means for the commander, staff, subordinates and other partners to develop a shared understanding of the upcoming operation and the interrelationships among the mission variables and elements of combat power. IO input is based on its running estimate, analysis in the foregoing steps, and how IO impacts or is impacted by other areas and functions. Time permitting, the staff employs the outline provided in figure 4-4.

DEVELOP AND ISSUE INITIAL COMMANDER'S INTENT

4-72. The *commander's intent* is a clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned (JP 3-0). The IO officer develops recommended input to the commander's intent and submits it to the G-3 (S-3) for the commander's consideration. When developing recommended input to the commander's intent, the IO officer assists the commander in visualizing and understanding the information environment, ways it will affect operations, and ways that IO can affect the information environment to the commander's advantage.

DEVELOP AND ISSUE INITIAL PLANNING GUIDANCE

4-73. After approving the restated mission and issuing the intent, commanders provide additional guidance to focus staff planning activities. As appropriate, the commander includes their visualization of IO in this guidance. Commanders consider the following when developing their IO planning guidance:

- Aspects of higher headquarters IO policies or guidance that the commander wants to emphasize.

- Aspects of the mission for which IO is most likely to increase the chance of success or which may be IO-dominant.
- Risks they are willing to take with respect to IO.
- IO decisions for which they want to retain or delegate authority.

Outline	Information Operations Input
Mission and commander's intent of headquarters two echelons up.	IO specified and implied tasks
Mission commander's intent, concept of operations of headquarters one echelon up.	IO specified and implied tasks
Proposed problem statement	Information-related problems within the IE.
Proposed mission statement	IO essential tasks
Review of commander's initial guidance	• Guidance concerning IO • EEFI and CCIR • Essential narrative elements
Initial IPB products	Information overlays
Specified, implied, and essential tasks	Specified, implied, and essential tasks for IO
Constraints	Any constraints placed on the command affecting IO
Initial risk assessment	• Recommended OPSEC planning guidance • Recommended controls to protect information-related vulnerabilities and critical assets. • Recommended controls for risk associated with IO tasks
Proposed themes and messages	Possible overlaps or conflicts among IRCs used to disseminate approved themes and messages.
Proposed timeline	• Time required to accomplish IO • Analysis of time needed versus time available

CCIR	EEFI	IO	IPB
Commander's Critical Information Requirements	Essential element of friendly information	Information Operations	Intelligence preparation of the battlefield

Figure 4-4. Information operations input to mission analysis briefing

4-74. Planning guidance focuses on the command's essential tasks. Commanders may give guidance for IO separately or as part of their overall guidance. This guidance includes any identified or contemplated IO objectives, stated in finite and measurable terms. It may also include OPSEC planning guidance, military deception guidance, and targeting guidance.

4-75. Factors that the IO officer considers when recommending input to initial planning guidance include:

- The extent that the command is vulnerable to hostile information-based warfare.
- Specific IO actions required for the operation.
- The command's capability to execute specific actions or weighted efforts.
- Additional information needed to conduct IO.

DEVELOP COURSE OF ACTION EVALUATION CRITERIA

4-76. Course of action (COA) evaluation criteria are used during course of action analysis and comparison to measure the relative effectiveness and efficiency of COAs to another. They are developed during this sub-step to enhance objectivity and lessen the chances of bias. Typically, the chief of staff will develop the criterion and associated weight. The IO officer will propose possible refinement to ensure consideration of IO factors affecting success or failure and then employ approved criteria to score each COA.

ISSUE WARNING ORDER

4-77. As the mission and operation dictate, the WARNORD will include essential IO tasks within the mission statement. It will note changes to task organization involving IRC or IO units and address IO factors in other relevant paragraphs, sections, or annexes, as appropriate.

4-78. Table 4-1 provides a summary of the inputs, actions and outputs required of the IO officer. Only those sub-steps within mission analysis with significant IO activity are listed.

Table 4-1. Mission Analysis

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Conduct IPB	• Higher HQ IPB • Higher HQ running estimates • Higher HQ OPLAN or OPORD • Higher HQ combined information overlay	• Develop IPB products • Analyze and describe the information environment in the unit's area of operations and its effect on friendly, neutral, adversary, and enemy information efforts • Identify threat information capabilities and vulnerabilities • Identify gaps in current intelligence on threat information efforts • Identify IO-related high-value targets • Determine probable threat information-related COAs • Assess the potential effects of IO on friendly, neutral, adversary, and enemy operations • Determine threat's ability to collect on friendly critical information • Determine additional EEFIs (OPSEC)	• Input to IPB products • IRs to G-2 (S-2), as well as the foreign disclosure officer • Refined EEFIs (OPSEC)

Table 4.1. Mission Analysis (continued)

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Determine Specified, Implied, and Essential Tasks	• Specified tasks from higher HQ OPLAN or OPORD • IPB and combined information overlay products	• Identify specified tasks in the higher HQ OPLAN or OPORD • Develop implied tasks • Determine if there are any essential tasks • Develop input to the command targeting guidance • Assemble critical and defended asset lists, especially low density delivery systems • Determine additional EEFIs (OPSEC)	• Specified, implied and essential tasks • List of IRCs to G-3 (S-3) • Input to command targeting guidance • Refined EEFIs (OPSEC)
Review Available Assets	• Current task organization for information related capabilities • Higher HQ task organization for information related capabilities • Status reports • Unit standard operating procedure	• Identify friendly IRCs (include capabilities that are joint, interorganizational, and multinational) • Analyze IRC command and support relationships • Determine if available IRCs can perform tasks necessary to support lines of operation or effort • Identify additional resources (such as air assets) needed to execute or support IO	• List of available IRCs [IO running estimate paragraph 1b(4)] • Request for additional IRCs, if required
Determine Constraints	• Commander's initial guidance • Higher HQ OPLAN or OPORD	• Identify IO-related constraints	• List of constraints (IO appendix to Annex C; scheme of IO or coordinating instructions)
Identify Critical Facts and Develop Assumptions	• Higher HQ OPLAN or OPORD • Commander's initial guidance • Observations and reports	• Identify facts and assumptions affecting IRCs • Submit IRs that will confirm or disprove assumptions • Identify facts and assumptions regarding OPSEC indicators that identify vulnerabilities	• List of facts and assumptions (IO running estimate paragraph 1c.) • IRs that will confirm or disprove facts and assumptions

Table 4.1. Mission Analysis (continued)

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Begin Risk Management	• Higher HQ OPLAN or OPORD • IPB • Commander's initial guidance	• Identify and assess hazards associated with IO • Propose controls • Identify OPSEC indicators • Assess risk associated with OPSEC indicators to determine vulnerabilities • Establish OPSEC measures	• List of assessed hazards • Input to risk assessment • Develop risk briefing matrix • List of provisional OPSEC measures
Develop Initial CCIRs and EEFIs	• IO IRs	• Determine information the commander needs in order to make critical decisions concerning IO efforts • Identify IRs to recommend as commander's critical information requirements	• Submit IRs
Determine Initial Information Collection Plan	• Initial IPB • PIRs or IO IRs	• Identify gaps in information needed to support planning, execution, and assessment of early initiation actions • Confirm that the initial information collection plan includes IRs concerning enemy capability to collect EEFIs	
Update Plan for the Use of Available Time	• Revised G-5 (S-5)/G-3 (S-3) plans timeline	• Determine time to accomplish IO planning requirements • Assess viability of planning timeline vis-à-vis higher HQ timeline and threat timeline as determined during IPB • Refine initial time allocation plan	• Timeline (provided to G-5 (S-5), with emphasis on the effect(s) of long-lead time events
Develop Initial Themes and Messages	• Public affairs themes and messages adjusted and refined from higher HQ • MISO actions and messages adjusted and refined from higher HQ	• Assess impact of initial themes and messages on the information environment • Assess whether planned IO effects will reinforce themes and messages • Contribute to development of talking points aimed at influencing perceptions and behaviors	• PA themes/ messages and MISO actions/ messages de-conflicted • Initial list of talking points • IRC actions to disseminate approved messages/ talking points

Table 4.1. Mission Analysis (continued)

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Develop Proposed Problem Statement and Mission Statement	• Initial IO mission • Initial IO objectives • Approved themes and messages	• List issues and determine primary obstacles that impede achieving the desired end state in the information environment • Recommend possible initial objectives for inclusion in the restated mission	• Input to proposed problem statement • Essential tasks • Restated mission • Revised or additional initial objectives recommended for inclusion in the restated mission • Updated synchronization of themes and messages with actions
Present Mission Analysis Briefing	• IO running estimate. • Unit standard operating procedure	• Prepare to brief IO portion of mission analysis	• IO portion of mission analysis briefing
Develop and Issue Initial Commander's Intent	• Higher HQ commander's intent • Results of mission analysis • IO running estimate	• Develop recommended input to the commander's intent and narrative	• Recommend input to the commander's intent and narrative
Develop and Issue Initial Planning Guidance	• Higher HQ OPLAN or OPORD • Results of mission analysis • IO running estimate	• Develop recommended input to the commander's guidance • Combine the refined EEFIs with the provisional OPSEC measures to produce the planning guidance	• Recommended input to the commander's guidance • Recommended OPSEC planning guidance • Recommended military deception guidance, to include guidance on using deception in support of OPSEC, if appropriate • Recommended IO targeting guidance

Table 4.1. Mission Analysis (continued)

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Issue a Warning Order	• Commander's intent and guidance • Approved restated mission and initial objectives • Mission analysis products	• Prepare input to the warning order. Input may include — – Early tasking to subordinate units – Initial mission statement – OPSEC planning guidance – Reconnaissance and surveillance tasking • Military deception guidance	• Input to mission, commander's intent, commander's critical information requirements, and concept of the operations

COA course of action
EEFI essential element of friendly information
G-2 assistant chief of staff, intelligence
G-3 assistant chief of staff, operations
G-5 assistant chief of staff, plans
HQ headquarters
IO information operations
IPB intelligence preparation of the battlefield
IR information requirements
IRC information related capability
MISO military information support operations
OPLAN operations plan
OPORD operations order
OPSEC operations security
PA public affairs
PIR priority intelligence requirement
S-2 battalion or brigade intelligence officer
S-3 battalion or brigade operations staff officer
S-5 battalion or brigade plans staff officer

COURSE OF ACTION DEVELOPMENT

4-79. After the mission analysis briefing, the staff begins developing COAs for analysis and comparison based on the restated mission, commander's intent, and planning guidance. During COA development, the staff prepares feasible COAs that integrate the effects of all combat power elements to accomplish the mission. Based on the unit's approved mission statement, the IO officer develops a distinct scheme of IO, IO objectives, and IRC tasks for each COA.

4-80. The IO officer is involved early in COA development. The focus is on determining how to achieve decisive advantage in and through the information environment at the critical times and places of each COA. Depending on the time available, planning products may be written or verbal.

ASSESS RELATIVE COMBAT POWER

4-81. IO synchronization of IRCs enhances the combat power, constructive and destructive, of friendly forces in numerous ways. Some examples include:

- Military deception influences application (or misapplication) of threat forces and capabilities at places and times that favor friendly operations.
- Countering the effects of propaganda degrades threat propaganda efforts by exposing lies and providing accurate information.
- MISO and civil military operations favorably influence foreign audiences by emphasizing the positive actions of U.S. forces.
- Movement and maneuver destroys or disrupts threat communicators, controls territory through which information flows, and influences affected populations.
- Electronic warfare jams threat communications and command and control signals.
- Fires destroys threat communication infrastructure.

4-82. The IO officer ensures that the staff considers IO when analyzing relative combat power. IO can be especially valuable in reducing resource expenditures by other combat power elements. For example, commanders can use electronic warfare to jam a communications node instead of using fires to destroy it.

4-83. IO contributions are often difficult to factor into numerical force ratios. With IO officer support, staff planners consider the effects of IO on the intangible factors of military operations as they assess relative combat power. Intangible factors include such things as the uncertainty of war and the will of friendly forces and the threat. Varied approaches and methods may be used to achieve IO effects. One method is to increase the relative combat power assigned to forces who effectively employ organic IRCs. For example, strict OPSEC discipline by friendly forces increases the difficulty the threat has in collecting information. Units with a Theater IO Group OPSEC support detachment may further increase their relative combat power as a result of this augmentation.

GENERATE OPTIONS

4-84. Options are expressed as COAs. Given the increasing impact of the information environment on operations and the threat's use of information-focused warfare to gain advantage, staffs recognize that, in certain COAs, IO may be the main effort.

4-85. The IO officer assists the staff in considering the ways that IO can support each COA. This requires the IO officer to determine which IRCs to employ and the trade-offs associated with each. In brainstorming options, the IO officer thinks first in an unconstrained manner, then refines available options based on the running estimate and knowledge of available assets and those that are anticipated. During this sub-step, the IO officer also develops input to military deception COAs, if applicable. The main output of this effort is an initial scheme of IO by phase for each COA.

ARRAY FORCES

4-86. The staff arrays forces to determine the forces necessary to accomplish the mission and to develop a knowledge base for making decisions concerning concepts of operations. The IO officer ensures planners consider the impact of available IRCs on force ratios as they determine the initial placements. IRCs may reduce the number of maneuver forces required or may increase the COA options available. Planners consider the deception story during this step because aspects of it may affect unit positioning.

4-87. Although the staff considered IRC availability when developing COAs, this step allows them to further validate if the required capabilities are present and, if not, determine if they can be obtained and positioned in time to achieve required effects. It also enables the IO officer to determine if available IRCs are properly positioned and task-organized.

DEVELOP A BROAD CONCEPT

4-88. The broad concept concisely expresses the “how” of the commander's visualization and will eventually provide the framework for the concept of operations and summarizes the contributions of all warfighting functions (FM 6-0). The IO officer develops schemes of IO and IO objectives for each COA that nest with the broad concept. With input from IRC representatives, the IO officer considers how IRCs can achieve the IO objectives.

4-89. IO schemes of support are further expressed in terms of the weighted efforts required to support the overall concept of operations. Depending on proportion of offense, defense, and stability tasks, the IO officer determines the best mix of attack, defend, and stability IO efforts needed to ensure achievement of objectives. The IO officer then determines which IRCs to allocate to each effort and possible tasking conflicts.

4-90. During this sub-step, the IO officer develops control measures, critical and defended asset lists, and additional EEFIs for each COA, as well as determines OPSEC vulnerabilities and measures. Most importantly, the IO officer produces five essential, often time-intensive, outputs. These are—

- COA worksheets.
- Synchronization matrix.
- Target nominations.

- Risk assessment.
- Measures of performance and effectiveness.

COA Worksheets

4-91. The IO officer employs COA worksheets to prepare for COA analysis and focus IRC efforts. These worksheets can be narrative or graphical or a combination of both. The IO officer prepares one worksheet for each IO objective in each scheme of IO. IO worksheets include the following information, as a minimum:

- A description of the COA.
- The scheme of IO in statement form.
- The IO objective in statement form.
- Information concerning IRC tasks that support the objective, listed by IRC.
- Anticipated adversary counteractions for each IRC task.
- Measures of performance and effectiveness for each IRC task.
- Information required to assess each IRC task.

4-92. The COA worksheet needs to show how each IRC contributes to the IO objective and the scheme of IO for that COA. When completed, the work sheets help the IO officer tie together the staff products developed to support each COA. IO planners also use the worksheets to focus task development for all IRCs. They retain completed work sheets for use during subsequent steps of the MDMP.

Synchronization Matrix

4-93. The IO officer develops an IO synchronization matrix for each COA to determine when to execute IRC tasks. IO synchronization matrices show estimates of the time it takes for friendly forces to execute an IRC task; the adversary to observe, process and analyze the effect(s) of the executed task; and the adversary to act on those effect(s). The IO officer synchronizes IRC tasks with other combined arms tasks. The G-2 (S-2) and G-3 (S-3) time lines are used to reverse-plan and determine when to initiate IRC tasks. Due to the lead time required, some IRC tasks must be executed early in an operation. Regardless of when the IRC tasks start, they are still synchronized with other combined arms tasks. Many IRC tasks are executed throughout an operation; some are both first to begin and last to end. IO synchronization matrices vary in format, depending on commander preference and unit standard operating procedures. At a minimum, the synchronization matrix should include—

- IO objectives.
- IRC tasks.
- The operational timeline to execute the IRC tasks.
- The depiction of how IRC synchronization integrates with lines of operations or lines of effort.

Target Nominations

4-94. The IO officer uses information derived during mission analysis, IPB products, and the high-value target list to nominate high-pay-off targets (HPTs) for each friendly COA. HPTs are selected to be added to the high-payoff target list. HPTs are developed in conjunction with the IRC tasks employed to affect them. Targets attacked by nonlethal means, such as jamming or MISO broadcasts, may require assessment by means other than those normally used in battle damage assessment. The IO officer submits IRs for this information to the G-2 (S-2) when nominating them. If these targets are approved, the IRs needed to assess the effects on them become PIRs that the G-2 (S-2) adds to the information collection plan. If the command does not have the assets or resources to answer the IO IRs, the target is not engaged unless the attack guidance specifies otherwise or the commander so directs. The targeting team performs this synchronization.

Risk Assessment

4-95. The assessment of IO-associated risk during COA development and COA analysis focuses primarily on hazards related to executing the scheme of IO and its associated IRC tasks. However, the IO officer assesses all hazards as they emerge. The IO officer also monitors identified hazards and evaluates the effectiveness of controls established to counter them.

4-96. The IO officer examines each COA and its scheme of IO to determine if they contain hazards not identified during mission analysis. The IO officer then develops controls to manage these hazards, determines residual risk, and prepares to test the controls during COA analysis. The IO officer coordinates controls with other staff sections as necessary. Controls that require IRC tasks to implement are added to the IO COA worksheet for the COA.

4-97. The IO officer considers two types of hazards associated with the scheme of IO: those associated with the scheme of IO itself and its supporting IRC tasks; and those from other aspects of the concept of operations that may affect execution of IO. The IO officer identifies as many of these hazards as possible so the commander can consider them in decisions.

4-98. Some hazards result from the need to focus IO efforts. These hazards require commanders to take prudent risks. Some examples include:

- As part of a military deception operation, the commander limits camouflage, concealment, and deception measures applied to elements they want the adversary to detect. The commander accepts the risk of the threat targeting these elements.
- The commander concentrates cybersecurity efforts on a few critical mission command nodes, accepting the risk that other nodes may be degraded.
- The commander elects to destroy an adversary communications node that is also a valuable intelligence source. The commander accepts the risk of operating without that intelligence.

4-99. Hazards also result from unintended actions by the threat and other forces/groups in response to friendly IO. In addition, unintended consequences of other tactical activities can affect IO. Examples include:

- An electronic attack may disrupt friendly as well as threat communications.
- In a stability operation, efforts to influence a mayor to support U.S. forces instead of simply not opposing them may boost the popularity of an anti-U.S. rival, risking loss of long-term local political support.

4-100. Thorough planning can reduce, but will never eliminate, unintended consequences. The IO officer identifies possible unintended consequences that cause effects within the information environment and focuses on those most likely to affect mission accomplishment.

4-101. The IO officer considers the effects of IO-related hazards on the local populace and infrastructure as well as on friendly forces. The IO officer assesses these hazards, develops controls, determines residual risks, and advises the commander on risk mitigation measures. These unintended consequences could be caused by an IRC or by other activity that causes effects in the IE.

4-102. The commander alone accepts or rejects risk. The IO officer advises the commander concerning risk associated with IO-related hazards and recommends controls to mitigate this risk. The commander decides what risk to accept. An example of using IO for accident risk mitigation is the synchronized use of civil military operations and MISO, in coordination with public affairs, to warn the local populace of the accident hazards associated with military operations. When risks are attributable to IRC tasks, the IO officer assigns risk mitigation measures to the responsible unit and places them in the IO appendix's coordinating instructions.

4-103. The IO officer produces a list of IO-related hazards and assessments of the associated risks. This list becomes the IO input to the G-3 (S-3) risk assessment matrix. (For detailed information on assessing risk levels, see ATP 5-19.)

Measures of Performance and Effectiveness

4-104. Measures of performance and measures of effectiveness drive information requirements necessary to measure the degree to which operations accomplish the unit's mission. As COA development continues, the IO officer considers how to assess IO effectiveness, by determining:

- IRC tasks that require assessment.
- Measures of performance for IRC tasks and measures of effectiveness for IO objectives, as well as baselines to measure the degree of change, and associated IO-related targets.
- The information needed to make the assessment.

- How to collect the information.
- Who or what will collect the information.
- How the commander will use the information to support decisions.

4-105. The responses to these considerations are recorded on the IO COA worksheets and added to the IO portion of the operations assessment plan. Information required to assess IO effects becomes IRs. The IO officer submits IRs for the COA that the commander approves to the G-2 (S-2). The IO officer establishes measures of performance and effectiveness based on how IRC tasks contribute to achieving one or more IO objectives. If a task's results are not measurable, the IO officer eliminates the task.

ASSIGN HEADQUARTERS

4-106. Headquarters are typically assigned based on their ability to integrate the warfighting functions. Their capacity to plan, prepare, execute, and assess IO varies, depending on such variables as organic capabilities, mission essential tasks, and training. When commanders determines that the decisive operation or a shaping operation is IO-dominant, they turn to the IO officer to assess potential mission command vulnerabilities and ways to mitigate them. Higher headquarters, in particular, conduct this assessment for subordinate headquarters being assigned IO-dominant missions and provides additional assets, as required.

DEVELOP COURSE OF ACTION STATEMENTS AND SKETCHES

4-107. The G-3 (S-3) prepares a COA statement and supporting sketch for each COA for the overall operation. Together, the statement and sketch cover who, what, when, where, how, and why for each subordinate unit. They also state any significant risks for the force as a whole. The IO officer provides IO input to each COA statement and sketch. At a minimum, each COA statement and sketch should include its associated scheme of IO. COA statements may also identify select IO objectives and IRC tasks when they address specific commander concerns or priorities.

CONDUCT COURSE OF ACTION BRIEFING

4-108. Given the increasing impact of the information environment on operations, commanders benefit from ensuring the IO officer is present during all MDMP briefings. For this specific briefing, the IO officer is able to provide essential rationale for the scheme of IO and respond to IO-related questions from the commander or G-3 (S-3).

SELECT OR MODIFY COURSE OF ACTION FOR CONTINUED ANALYSIS

4-109. Whether the commander selects a given COA or COAs, modifies COAs, or creates a new COA altogether, the IO officer prepares for COA analysis and war-gaming. If the commander rejects all COAs, the IO officer develops new schemes of support, mindful of the commander's revised planning guidance.

4-110. Table 4-2 provides a summary of the inputs, actions and outputs required of the IO officer/element. Only those sub-steps within COA development with significant IO activity are listed.

Table 4-2. Course of action development

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Assess Relative Combat Power	• IPB or combined information overlay • Task organization • IO running estimate • Vulnerability assessment	**For each COA —** • Analyze IRC effects on friendly and threat capabilities, vulnerabilities, and combat power	**For each COA —** • Description of the potential effects of relative combat power stated by IRC

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Generate Options	• Commander's intent and guidance • IPB or combined information overlay • Friendly, neutral, and enemy information related capabilities, resources, and vulnerabilities	• Determine different ways for IO to support each COA • Determine IRCs to employ. • Determine how to focus IRCs on the overall objective • Determine IO's role in the decisive and shaping operations for each COA • Determine possible tradeoffs among IRCs • Develop input to military deception COAs (deception stories)	• Scheme of IO for each COA • Input to military deception COAs
Array Forces	• Restated mission • Commander's intent and guidance • IPB or combined information overlay • Input to military deception plan or concept	• Allocate IRCs for each scheme • Identify requirements for additional IRCs • Examine effect of possible military deception COAs on force positioning • Identify military deception means	• Initial IRC location and task organization • Additional IRC requirements

Table 4-2. Course of action development (continued)

MDMP Sub-Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Develop a Broad Concept	• COAs • IPB or combined information overlay • High value target list • IO mission statement • Initial scheme of IO for each COA	**For each COA —** • Develop scheme of IO • Develop objectives • Develop control measures • Identify and prioritize IRC tasks • Nominate selected HPTs • Determine initial IO task execution timeline • Refine input to risk assessment • Develop IO portion of assessment plan • Identify additional EEFIs • Identify and assess OPSEC indicators to determine vulnerabilities • Develop OPSEC measures to shield vulnerabilities • Determine residual risk associated with each vulnerability after OPSEC measures are applied • Determine feedback required for assessment of military deception COAs	**For each COA —** • Refined scheme, objectives, and control measures; IRC tasks; and tasks to subordinate units • IO COA worksheets • Synchronization matrices • Execution time line • IO-related high-payoff target nominations • Critical and defended asset lists • Input to risk management plan, including residual risk associated with each OPSEC vulnerability • Success criteria to support assessment • Additional EEFIs • OPSEC vulnerabilities • OPSEC measures to shield vulnerabilities
Assign Headquarters	• IPB/combined information overlay • IO running estimate • IO vulnerability assessment • IO tasks by IRC and subordinate unit	**For each COA —** • Assess mission command strengths and weaknesses to determine vulnerabilities of specific headquarters regarding ability to execute IO • Assess mission command strengths and weaknesses to determine vulnerabilities of subordinate commands • Reevaluate critical and defended asset lists	**For each COA —** • Recommendations for allocation of G-3 (S-3) IO personnel to headquarters in light of mission command vulnerability assessment • Recommendations of grouping of IRCs to subordinate commands in light of mission command vulnerability assessment • Updated critical and defended asset lists • Initial list of IRCs to tasks assigned

Table 4-2. Course of action development (continued)

MDMP Sub-Step	Inputs	IO Officer Actions	IO Officer Outputs
Develop COA Statements and Sketches	• COA statement • A scheme of IO and objectives for each COA	• Submit input for each COA statement and sketch to G-3 (S-3) • Prepare scheme statement and sketch for each COA	• Input for each COA statement and sketch • Scheme of IO and sketches for each COA, stating the most important objectives

COA course of action
EEFI essential element of friendly information
HPT high-payoff target
IO information operations
IPB intelligence preparation of the battlefield
IRC information-related capability
IPB intelligence preparation of the battlefield
OPSEC operations security

COURSE OF ACTION ANALYSIS AND WAR-GAMING

4-111. COA analysis (war-gaming) enables commanders and staffs to identify difficulties or coordination problems as well as probable consequences of planned actions for each COA being considered. It helps them think through the tentative plan. War-gaming is a disciplined process that staffs use to envision the flow of battle. Its purpose is to stimulate ideas and provide insights that might not otherwise be discovered. Effective war-gaming allows the staff to test each COA, identify its strengths and weaknesses, and alter it if necessary. During war-gaming, new hazards may be identified, the risk associated with them assessed, and controls established. OPSEC measures and other risk control measures are also evaluated.

4-112. War-gaming helps the IO officer synchronize IRC operations and helps the staff integrate IO into the overall operation. During the war game, the IO officer addresses how each IRC contributes to the scheme of IO for that COA and its associated time lines, critical events, and decision points. The IO officer revises the schemes of IO as needed during war-gaming.

4-113. The IO officer uses the synchronization matrices and worksheets for each COA as scripts for the war game. The IRCs are synchronized with each other and with the concepts of operations for the different COAs. To the extent possible, the IO officer also includes planned counter-actions to anticipated threat reactions.

4-114. During preparation for war-gaming, the IO officer gives the G-2 (S-2) likely threat information-related actions and reactions to friendly IO, to include possible threat responses in the information environment to friendly operations. The IO officer also continues to provide input to the G-2 (S-2) for HPT development and selection.

4-115. Before beginning the war game, staff planners develop criteria to evaluate the effectiveness and efficiency of each COA during COA comparison. These criteria are listed in paragraph 3c of the IO running estimate and become the outline for the COA analysis in paragraph 4. The IO officer develops the criteria for evaluating the schemes of IO. Using IO-specific criteria allows the IO officer to explain the advantages and disadvantages of each COA. Evaluation criteria that may help discriminate among various COAs could include:

- Lead time required for implementation.
- The number of decision points that require support.
- The cost of achieving an IO objective versus the expected benefits.
- The risk to friendly assets posed by threat information activities.

4-116. During war-gaming the IO officer participates in the action-reaction-counteraction process. For example, the action may be patrols designed to enforce curfew; the threat reaction is messaging accusing U.S. forces of causing damage and casualties; the counteraction is assigning combat camera to document U.S. force patrols and interactions with the indigenous population and incorporating the documentation with another IRC in order to provide appropriate content to the target audience. The IO officer uses the

synchronization matrices and COA worksheets to insert IRC tasks into the war game at the time planned. A complete COA worksheet allows the IO officer to state the organization performing the task and its location. The IO officer remains flexible throughout the process and is prepared to modify input to the war game as it develops. The IO officer is also prepared to modify the scheme of IO, IO objectives, and IRC tasks to mitigate possible threat actions discovered during the war game. The IO officer notes any branches and sequels identified during the war game. Concepts of support for these branches or sequels are developed as time permits.

4-117. The results of COA analysis are a refined scheme of IO and associated products for each COA. During war-gaming, the IO officer refines IRs, EEFIs, and HPTs for each COA, synchronizing them with that COA's concept of operations. Staff planners normally record war-gaming results, including IRC effects, on the G-3 (S-3) synchronization matrix. The IO officer may also record the results on the COA worksheets. These help the IO officer subsequently synchronize IRCs. The worksheets and synchronization matrices provide the basis for IO input to paragraph 3 of the OPLAN/OPORD, paragraph 3 of the IO and IRC appendices.

4-118. Table 4-3 on page 4-27 provides a summary of the inputs, actions and outputs required of the IO officer during course of action analysis.

COURSE OF ACTION COMPARISON

4-119. During COA comparison, the staff compares feasible COAs to identify the one with the highest probability of success against the most likely adversary COA and the most dangerous adversary COA. Each staff section evaluates the advantages and disadvantages of each COA from the staff section's perspective, and presents its findings to the staff. The staff outlines each COA in terms of the evaluation criteria established before the war game and identifies the advantages and disadvantages of each with respect to the others. The IO officer records this analysis in paragraph 4 of the IO estimate.

4-120. The IO officer determines the COA that IO can best support based on the evaluation criteria established during war-game preparation. The results of this comparison become paragraph 5 of the IO estimate.

4-121. Table 4-4 on page 4-28 provides a summary of the inputs, actions and outputs required of the IO officer during course of action comparison. Table 4-3. Course of action analysis (war game)

Table 4-3. Course of action analysis (war game)

MDMP Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Course of Action Analysis	• Updated running estimate. • IPB/combined information overlay • Updated assumptions **For each COA —** • Scheme of IO and objectives for each COA sketch • Execution timeline	• Develop evaluation criteria for each COA • Gather the tools • List all friendly IRCs • List assumptions • Synchronize tasks performed by different IRCs and subordinate commands • Coordinate IO with cyber electromagnetic activities • Integrate scheme of IO into the concept of operations for each COA • Synchronize scheme of IO with higher and adjacent headquarters • Identify enemy information warfare capabilities and likely actions and reactions • War game friendly IRCs against enemy vulnerabilities and display the results • War game friendly IRC impacts on various audiences and populations and display the results • War game enemy information warfare capabilities against friendly vulnerabilities and display the results • Synchronize and de-conflict targets • Determine whether modifications to the COA result in additional EEFIs or OPSEC vulnerabilities; if so recommend OPSEC measures to shield them • Assign attack measures to HPTs. • Test OPSEC measures • Determine decision points for executing tasks • War game each military deception COA • Identify each military deception COA's potential branches; assess risk to the COA • List the most dangerous or beneficial branch on the decision support template or synchronization matrix • Participate in the war game briefing (optional)	• Potential decision points • Initial assessment measures • Updated assumptions • An evaluation of each military deception COA in terms of criteria established before the war game **For each COA —** • An evaluation in terms of criteria established before the war game • Recorded input to war game results • Refined scheme of IO • Refined tasks • Refined input to attack guidance matrix and target support matrix • IRs and requests for information identified during war game • Refined EEFIs and OPSEC vulnerabilities and OPSEC measures • Paragraph 4 of the running estimate • Input to the G-3 (S-3) synchronization matrix • Input to the HPTL

COA course of action
EEFIs essential elements of friendly information
HPT high-payoff target
HPTL high-payoff target list
IO information operations
IPB intelligence preparation of the battlefield
IR information requirement
IRC information-related capability
OPSEC operations security
MDMP military decisionmaking process

Table 4-4. COA comparison

MDMP Task	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Course of Action Comparison	• Updated IO running estimate • Refined COAs • COA evaluation criteria • COA evaluations from COA analysis • Updated assumptions	• Compare the COAs with each other to determine the advantages and disadvantages of each • Determine which COA is most supportable from an IO perspective • Determine if any OPSEC measures require the commander's approval	• Advantages and disadvantages for each COA • Most supportable COA from an IO perspective • Input to COA decision matrix • Updated assumptions • Paragraph 4, IO running estimate

COA course of action **IO** information operations **MDMP** military decisionmaking process **OPSEC** operations security

COURSE OF ACTION APPROVAL

4-122. After completing the COA comparison, the staff identifies its preferred COA and recommends it to the commander in a COA decision briefing, if time permits. The concept of operations for the approved COA becomes the concept of operations for the operation itself. The scheme of IO for the approved COA becomes the scheme of IO for the operation. Once a COA is approved, the commander refines the commander's intent and issues additional planning guidance. The G-3 (S-3) then issues a WARNORD and begins orders production.

4-123. The WARNORD issued after COA approval contains information that executing units require to complete planning and preparation. Possible IO input to this WARNORD includes:

- Contributions to the commander's intent/concept of operations.
- Changes to the CCIRs.
- Additional or modified risk guidance.
- Time-sensitive reconnaissance tasks.
- IRC tasks requiring early initiation.
- A summary of the scheme of IO and IO objectives.

4-124. During the COA decision briefing, the IO officer is prepared to present the associated scheme of IO for each COA and comment on the COA from an IO perspective. If the IO officer perceives the need for additions or changes to the commander's intent or guidance with respect to IO, they ask for it.

4-125. Table 4-5 on page 4-29 provides a summary of the inputs, actions and outputs required of the IO officer during course of action approval.

ORDERS PRODUCTION, DISSEMINATION, AND TRANSITION

4-126. Based on the commander's decision and final guidance, the staff refines the approved COA and completes and issues the OPLAN/OPORD. Time permitting, the staff begins planning branches and sequels. The IO officer ensures input is placed in the appropriate paragraphs of the base order and its annexes, especially the IO appendix to the operations annex. When necessary, the IO officer or appropriate special staff officers prepare appendixes for one or more IRCs [(See Appendix A for an annotated format of appendix 15 (Information Operations) to Annex C (Operations)].

4-127. Table 4-6 provides a summary of the inputs, actions and outputs required of the IO officer during course of action approval.

Table 4-5. Course of action approval

MDMP Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Course of Action Approval	• Updated IO running estimate • Evaluated COAs • Recommended COAs • Updated assumptions	• Provide input to COA recommendation • Re-evaluate input to the commander's intent and guidance • Refine scheme of IO, objectives, and tasks for approved COA and update synchronization matrix • Prepare input to the WARNORD • Participate in the COA decision briefing • Recommend the COA that IO can best support • Request decision on executing any OPSEC measures that entail significant resource expenditure or high risk	• Finalized scheme of IO for approved COA • Finalized tasks based on approved COA • Input to WARNORD • Updated synchronization matrix

COA course of action **IO** information operations **MDMP** military decisionmaking process **WARNORD** warning order

Table 4-6. Orders production, dissemination and transition

MDMP Task	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Orders Production, Dissemination and Transition	• Approved COA • Refined commander's guidance • Refined commander's intent • IO running estimate • Execution matrix • Finalized mission statement, scheme of IO, objectives, and tasks	• Ensure input is placed in tasks to subordinate units and coordinating instructions • Produce Appendix 14 (MILDEC) to Annex C (Operations) • Produce Appendix 15 (IO) to Annex C (Operations) • Produce Appendix 3 (OPSEC) to Annex E (Protection) • Coordinate tasks with IRC staff officers • Conduct other staff coordination. • Refine execution matrix • Transition from planning to operations	• Synchronization matrix • Approved Paragraph 3.k. (10) • Approved Appendix 14 to Annex C • Approved Appendix 15 to Annex C • Approved Appendix 3 to Annex E • IO input to AGM and TSM • Subordinates understand the IO portion of the plan or order

AGM attack guidance matrix **COA** course of action **IO** information operations **IRC** information-related capability **MDMP** military decisionmaking process **MILDEC** military deception **OPSEC** operations security **TSM** trunk signaling mission

This page intentionally left blank.