Chapter 6
Execution

6-1. Execution of IO includes IRCs executing the synchronization plan and the commander and staff monitoring and assessing their activities relative to the plan and adjusting these efforts, as necessary. The primary mechanism for monitoring and assessing IRC activities is the IO working group. There are two variations of the IO working group. The first monitors and assesses ongoing planned operations and convenes on a routine, recurring basis. The second monitors and assesses unplanned or crisis situations and convenes on an as-needed basis.

INFORMATION OPERATIONS WORKING GROUP

6-2. The IO working group is the primary means by which the commander, staff and other relevant participants ensure the execution of IO. The IO working group is a collaborative staff meeting led by the IO officer, and periodically chaired by the G-3 (S-3), executive officer, chief of staff or the commander. It is a critical planning event integrated into the unit's battle rhythm. Figure 6-1 on page 6-2 provides a possible template for the conduct of the IO working group that can be applied at the tactical through strategic levels. Core and other participants are not static; they will fluctuate by level and by mission/situation.

PURPOSE

6-3. The IO working group is the primary mechanism for ensuring effects in and through the information environment are planned and synchronized to support the commander's intent and concept of operations. This means that the staff must assess the current status of operations relative to the end state and determine where efforts are working well and where they are not. More specifically, they must ensure targets are identified and nominated at the right place and time to achieve decisive results. The IO working group occurs regularly in the unit's battle rhythm and always before the next targeting working group. The only exception is a crisis IO working group (also referred to as consequence management or crisis action working group), which occurs as soon as feasible before or after an event or incident that will significantly alter the information environment and give the threat operational advantage unless handled quickly and adeptly.

INPUTS/OUTPUTS

6-4. The example in figure 6-1 is not exhaustive. In terms of inputs, it identifies those documents, products, and tools that historically and practically have provided the IO working group the information necessary to achieve consensus and make informed recommendations to the G-3 (S-3) and commander. The outputs listed are those considered essential to ensuring the staff can effectively conduct IO.

6-5. One tool that the IO working group uses to affirm and adjust the synchronized employment of IRCs is the IO synchronization matrix. An updated synchronization matrix is the working group's key output and essential input to the next targeting meeting.

AGENDA

6-6. Like other aspects of the IO working group, the proposed agenda is flexible to the needs of the commander and the staff/participants. Figure 6-1 breaks the meeting down by weighted effort, recognizing that some members of the working group may not need to participate in all parts and that classification levels may adjust depending on the capabilities or assets under consideration and discussion. For example, the public affairs officer/representative will likely be present for Parts 1, 2 and possibly 3, but not for Part 4. Another possible agenda format is by time horizon and yet another by phase of the operation.

<table>
<tr><th colspan="2">Purpose</th><th colspan="2">Agenda</th></tr>
<tr><td colspan="2">Prioritize, request, and synchronize information-related capabilities and IO augmentation to optimize effects in and through the IE.

Battle Rhythm:
• Before targeting work group</td><td colspan="2">Part 1: Operations and Intelligence Update
• Intelligence update
• Information environment update
• Operations update or significant activities
• Review plans, future operations, and current operations
• Assessment update (information requirements, indicators)
• Calendar update, due outs, and responsibilities from previous meeting

Part 2: Stabilize
Part 3: Protect and defend
Part 4: Attack
• Review and update synch matrix
• Guidance and comments</td></tr>
<tr><th colspan="2">Inputs/Outputs</th><th colspan="2">Structure/Participants</th></tr>
<tr><td>Inputs:
• Higher headquarters orders and guidance
• Commander's intent, concept of operations and narrative
• Information-related capabilities status (running estimates)
• Intelligence collection assets
• Combined information overlays, intelligence preparation of the battlefield
• Media monitoring analysis
• Cultural calendar
• Engagements schedule
• Audience analysis
• Scheme of IO and synchronization matrix
• Commander's objectives for IO
• Success criteria: measures of effectiveness and performance</td><td>Outputs:
• Updated scheme of IO
• Updated IO synchronization matrix
• Key leader engagement recommendations
• Refined themes and messages
• Refined operational products
• Target nominations
• Updated combined information overlay
• Plans and orders update
• Information requirements</td><td colspan="2">Lead: IO Officer
(chair: G-3 (S-3), XO, DCO, or CDR)

Core participants: Military information support operations, G-2 (S-2), subordinate unit representatives, G-3 (S-3), fires, G-9 (S-9), operations security, public affairs

Other participants: G-6 (S-6), cyber electromagnetic activities, space operations, military deception planner, combat camera, foreign area officer or cultural advisor, special forces liaison, knowledge management officer, G-4 (S-4), engineer, chaplain, staff judge advocate, chaplain and unified action partners (mission and situation dependent)</td></tr>
<tr><td>CCIR commander's critical information requirements
CDR commander
DCO defense coordinating officer
EEFI essential elements of friendly information
G-2 assistant chief of staff, intelligence
G-3 assistant chief of staff, operations</td><td>G-4 assistant chief of staff, logistics
G-6 assistant chief of staff, signal
G-9 assistant chief of staff, civil affairs operations
IE information environment
IO information operations</td><td>IPB intelligence preparation of the battlefield
IRCs information-related capabilities
OPSEC operations security
S-2 battalion or brigade intelligence staff officer
S-3 battalion or brigade operations staff officer</td><td>S-4 battalion or brigade logistics staff officer
S-6 battalion or brigade signal staff officer
S-9 battalion or brigade civil affairs operations staff officer</td></tr>
</table>

Figure 6-1: Example template for an IO working group

6-7. Consistent across all agenda formats are the operational and intelligence updates. These updates are designed to ground participants in the current situation and threat, examine how well operations are meeting the concept of operations and determine whether results are advancing the unit toward the desired end state.

STRUCTURE/PARTICIPANTS

6-8. The IO officer leads and routinely chairs the IO working group. Staff members typically participating in the working group include personnel from the warfighting functional cells (as appropriate to the mission), the coordinating cells, the special staff, IRC managers (organic and augmenting), subordinate unit IO officers, and augmenting IO units or teams. Table 6-1 on page 6-4 provides an example listing of the participants as well as sample responsibilities.

IO WORKING GROUP IN ANTICIPATION OF/RESPONSE TO CRISIS OR SIGNIFICANT INCIDENT

6-9. The IO working group convenes as soon as feasible before or after an event. Anyone can request the convening of the IO working group to deal with crisis or incident through the IO officer who, in consultation with the G-3 (S-3) and commander, determines the merits of the request and those personnel who should comprise the working group's initial membership. The working group's purpose is to determine the additional measures, activities, and effects that must be undertaken or generated in order to sustain operational advantage in the information environment. The group also seeks to mitigate possible negative consequences

resulting from crisis events or incidents, particularly those that would adversely affect U.S. and coalition credibility. Its membership is more ad-hoc than the routine IO working group but also situation dependent.

IO RESPONSIBILITIES WITHIN THE VARIOUS COMMAND POSTS

6-10. IO execution involves monitoring and assessing IO as the operation unfolds and requires coordination among the tactical command post (CP) and main CP, which can be challenging. Each monitors different parts of the operation and not all have an assigned functional area 30 or IO officer. Continuous exchange of information among those assigned responsibility for IO at these CPs is essential to ensuring the effective execution of IO.

6-11. The tactical CP directs IO execution and adjusts missions as required. The IO representative or responsible agent—

- Maintains the IO portion of the common operational picture to support current operations.
- Maintains information requirement status.
- Coordinates preparation and execution of IO with maneuver and fires.
- Recommends adjustments to current IO.
- Tracks IRCs and recommends repositioning, as required.
- Tracks applicable targets in conjunction with the G-2 (S-2).
- Nominates targets for attack.
- Provides initial assessment of effectiveness.

6-12. The main CP plans, coordinates, and integrates IO. It—

- Creates and maintains IO aspects of the common operational picture.
- Maintains the IO estimate.
- Incorporates answers to IRs and requests for information into the IO estimate.
- Maintains a current IO order of battle.
- Deconflicts IO internally and externally.
- Requests/coordinates IO support with other warfighting function representatives, outside agencies, higher headquarters, and augmenting forces.
- Identifies future objectives based on successes or failures of current operations.

Table 6-1. Roles and responsibilities of IO working group representatives

Representative	*Responsibility*
Information Operations	• Distribute read-ahead packets • Lead working group • Establish and enforce agenda • Lead information environment update • Recommend commander's critical information requirements • Keep records, track tasks, and disseminate meeting notes
Cyber Electromagnetic Activities	• Provide cyber electromagnetic activities-related information and capabilities to support information operations analysis and objectives • Coordinate, synchronize and deconflict information operations efforts with cyberspace electromagnetic activities efforts or cyberspace electromagnetic activities efforts with information operations efforts

Table 6.1. Roles and responsibilities of IO working group representatives (continued)

Representative	*Responsibility*
Military Information Support Operations	• Advise on both psychological effects (planned) and psychological impacts (unplanned) • Advise on use of lethal and nonlethal means to influence selected audiences to accomplish objectives • Develop key leader engagement plans • Monitor and coordinate assigned, attached, or supporting military information support unit actions • Identify status of influence efforts in the unit, laterally, and at higher and lower echelons • Provide target audience analysis
G-2 (S-2)	• Provide an intelligence update • Brief information requirements and priority information requirements • Develop the initial information collection plan • Provide foreign disclosure-related guidance and updates
G-3 (S-3)	• Provide operations update and significant activity update • Task units or sections based on due outs • Update fragmentary orders • Maintain a task tracker
Subordinate unit information operations	• Identify opportunities for information operations support to lines of effort • Provide input to assessments • Provide input to information environment update
Public Affairs	• Develop media analysis products • Develop media engagement plan • Provide higher headquarters strategic communication plan • Provide changes to themes and messages from higher headquarters • Develop command information plan
G-9 (S-9)	• Provides specific country information • Ensures the timely update of the civil component of the common operational picture through the civil information management process • Advise on civil considerations within the operational environment • Identify concerns of population groups within the projected joint operational area/area of operations and potential flash points that can result in civil instability • Provide cultural awareness briefings • Advise on displaced civilians movement routes, critical infrastructure, and significant social, religious, and cultural shrines, monuments, and facilities • Advise on information impacts on the civil component • Identify key civilian nodes
Information-related capabilities representatives	• Serve as subject-matter expert for their staff function or capability • Identify opportunities for information-related capability support to lines of effort or operations

G-2 assistant chief of staff, intelligence	**G-9** assistant chief of staff, civil affairs operations	**S-3** battalion or brigade operations staff officer
G-3 assistant chief of staff, operations	**S-2** battalion or brigade intelligence staff officer	**S-9** battalion or brigade civil affairs operations staff officer

6-13. The IO officer monitors IRCs and keeps the G-3 (S-3) informed on overall IO status. The IO officer also recommends to the G-3 (S-3) changes to IRC taskings for inclusion in fragmentary orders, as warranted.

ASSESSING DURING EXECUTION

6-14. Assessment precedes and guides the other activities of the operations process. It involves continuous monitoring of the current situation and evaluation of the current situation against the desired end state to determine progress and make decisions and adjustments.

6-15. The IO officer compiles information from all CPs, the G-2 (S-2), and higher headquarters to maintain a continuous IO assessment in the IO estimate. The primary objective of assessment is to determine whether IO is achieving planned effects. As the situation changes, the IO officer and G-3 (S-3) make sure IO remains fully synchronized with the overall operation.

6-16. Assessment is continuous; it precedes and guides every operations process activity and concludes each operation or phase of an operation. During planning, the commander and staff determine those IO objectives to be assessed, measures of performance and effectiveness, and the means of obtaining the information necessary to determine effectiveness. During orders production, the IO officer uses this information to prepare the IO portion of the overall assessment plan. During execution, the IO officer uses established measures of performance and effectiveness, as well as baselines and indicators, to assess IO objectives.

MONITORING IO

6-17. The IO officer monitors IRCs to determine progress towards achieving the IO objectives. Once execution begins, the IO officer monitors the threat and friendly situations to track IRC task accomplishment, determine the effects of IO during each phase of the operation, and detect and track any unintended consequences.

6-18. Monitoring the execution of defend-weighted tasks is done at the main CP because it is the focal point for intelligence analysis and production, and because the headquarters mission command nodes are monitored there. The IO officer works closely with the intelligence cell, G-2 (S-2), and IO working group representatives to provide a running assessment of the effectiveness of threat information efforts and keeps the G-3 (S-3) and various integrating cells informed.

6-19. With G-2 (S-2), G-3 (S-3), and fire support representatives, the IO officer monitors attack-weighted IO execution in the tactical CP and the main CP. For example, during combined arms maneuver, the IO officer is concerned with attacking threat command and control nodes with airborne and ground-based jammers, fire support, attack helicopters, and tactical air. After preplanned IO-related HPTs have been struck, the strike's effectiveness is assessed. Effective IO support of current operations depends on how rapidly the tactical CP can perform the targeting cycle to strike targets of opportunity. The G-3 (S-3) representative in the tactical CP keeps the main CP informed of current operations, including IO.

6-20. To organize and portray IO execution, the IO officer and working group use several tools, to include:

- IO synchronization matrix.
- Decision support template.
- High-payoff target list.
- Critical asset list and defended asset list.

6-21. IO officer and working group use either the synchronization matrix from the IO appendix or an extract containing current and near-term IO objectives and IRC tasks, depending on the complexity of the operation. The synchronization matrix is used to monitor progress and results of IO objectives and IRC tasks and keep IO execution focused on contributing to the overall operation. The decision support template produced by the G-3 (S-3) is used by the IO officer to monitor progress of IO in relation to decision points and any branches or sequels. The IO officer maintains a list or graphic (for example, a link and node diagram) that tracks the status of IO-related HPTs identified during planning. The IO officer uses the critical asset list and defended asset list to monitor the status of critical friendly information nodes and the status of critical systems supporting IO, for example: electronic warfare systems, military information support operations (MISO) assets, and deep attack assets.

EVALUATING IO

6-22. During execution, the IO officer works with the intelligence cell and integrating cells to obtain the information needed to determine individual and collective IO effects. Evaluation not only estimates the effectiveness of task execution, but also evaluates the effect of the entire IO effort on the threat, other relevant audiences in the area of operations, and friendly operations. Task execution is evaluated using measures of performance. Task effectiveness is evaluated using measures of effectiveness, which compare achieved results against a baseline. Additional information on assessment and the unique considerations involved in assessing IO are found in chapter 8.

6-23. Based on the IO effects evaluation, the IO officer adjusts IO to further exploit enemy vulnerabilities, redirects actions yielding insufficient effects, or terminates actions after they have achieved the desired result. The IO officer keeps the G-3 (S-3) and commander informed of IO effects and how these impact friendly and adversary operations. Some of the possible changes to IO include:

- Strike a target or continue to protect a critical asset to ensure the desired effect.
- Execute a branch or sequel.

DECISION MAKING DURING EXECUTION

6-24. Decision making during execution includes:

- Executing IO as planned.
- Adjusting IO to a changing friendly situation.
- Adjusting IO to an unexpected enemy reaction.

EXECUTING IO AS PLANNED

6-25. Essential to execution is a continuous information flow among the various functional and integrating cells. The IO officer tracks execution with intelligence and current operations cells, as well as with the targeting staff. The IO officer, in concert with the IO working group, maintains a synchronization matrix. This matrix is periodically updated and provided to the headquarters' functional and integrating cells. Using the matrix, the IO officer and working group keep record of completed IRC tasks. As tasks are completed, the IO officer passes the information to the intelligence cell. The IO officer and working group use this information to keep IO synchronized with the overall operation.

6-26. The IO officer determines whether the threat commander and other identified leaders are reacting to IO as anticipated during course of action analysis. The IO officer, in concert with the IO working group, looks for new threat vulnerabilities and for new IO-related targets. The IO officer proposes changes to the operation order (OPORD) to deal with variances throughout execution. The G-3 (S-3) issues FRAGORDs pertaining to IO, as requested by the IO officer. These FRAGORDs may implement changes to the scheme of IO, IO objectives, and IRC tasks. The IO officer updates the IO synchronization matrix and IO assessment plan to reflect these changes.

6-27. Given the flexibility of advanced information systems, the time available to exploit new threat command and control vulnerabilities may be limited and requires an immediate response from designated IRCs. Actions to defeat threat information efforts need to be undertaken before exploitation advantage disappears. The G-3 (S-3) may issue a verbal FRAGORD when immediate action is required.

ADJUSTING IO TO A CHANGING FRIENDLY SITUATION

6-28. As IO is executed, it often varies from the plan. Possible reasons for a variance include:

- An IO task is aborted or assets redirected.
- An IO-related target did not respond as anticipated.
- The threat effectively countered an IO attack.
- The threat successfully disrupted friendly mission command.
- The initial plan did not identify an emergent IO-related target or target of opportunity.

6-29. The IO officer's challenge is to rapidly assess how changes in IO execution affect the overall operation and to determine necessary follow-on actions. Based on the commander's input, the IO officer, in coordination with the rest of the headquarters' functional and integrating cells, considers COAs, conducts a quick COA analysis, and determines the most feasible COA.

6-30. If the selected COA falls within the decision-making authority of the G-3 (S-3), IO execution can be adjusted without notifying the commander. When changes exceed previously designated limits, the IO officer obtains approval from the commander. At this point, a more formal decision-making process may be required before issuing a FRAGORD, especially if a major adjustment to the operation order (OPORD) is needed. In such a case, the IO officer, working with the G-3 (S-3), participates in a time-constrained military decisionmaking process (MDMP) to develop a new COA.

ADJUSTING IO TO AN UNEXPECTED THREAT REACTION

6-31. The threat may react in an unexpected manner to IO or to the overall operation. If threat actions diverge significantly from those anticipated when the OPORD was written, the commander and staff look first at branch and sequel plans. If branch or sequel plans fail to adequately address the new situation, a new planning effort may be required.

6-32. The IO officer prepares branches that modify defend weighted efforts when threat actions cause new friendly vulnerabilities, or when friendly attack or stabilize efforts prove ineffective. The intelligence and current operations integration cells work with the IO officer to maintain a running assessment of threat capability to disrupt friendly mission command, and look for ways to lessen friendly vulnerabilities. Concurrently, they look for opportunities to reestablish IO effectiveness. Under these conditions, the IO officer determines the adequacy of existing branches and sequels. If none fit the situation, they create a new branch or sequel and disseminate it by FRAGORD.

6-33. If a new plan is needed, time available dictates the length of the decision-making process and the amount of detail contained in an order. The IO officer may only be able to recommend the use of IRCs that can immediately affect the overall operation: for example, electronic warfare, and MISO. Other IRCs proceed as originally planned and are adjusted later, unless they conflict with the new plan.

OTHER EXECUTION CONSIDERATIONS

6-34. Other considerations include, but are not limited to—

- IO execution begins early.
- IO execution requires flexibility.

IO EXECUTION BEGINS EARLY

6-35. Potential adversary and enemy commanders begin forming perceptions of a situation well before they encounter friendly forces. Recognizing this fact, commanders establish a baseline of IO that is practiced routinely in garrison and training. Selected IRCs (for example, MISO, OPSEC, combat camera, and military deception) begin contributing to an IO objective well before a deployment occurs. To support early execution of the overall operation, IO planning, preparation, and execution frequently begin well before the staff formally starts planning for an operation.

IO EXECUTION REQUIRES FLEXIBILITY

6-36. Actions by threat decision makers sometimes take surprising turns, uncovering unanticipated weaknesses or strengths. Similarly, friendly commanders may react unexpectedly in response to threat activities. Flexibility is key to success in IO execution. Effective commanders and well-trained staffs are flexible enough to expect the unexpected and exploit threat vulnerabilities/friendly strengths and protect against threat strengths/friendly vulnerabilities.

This page intentionally left blank.