Chapter 4
Synchronization of Information-Related Capabilities

SYNCHRONIZATION COMPONENTS

4-1. Creating effects in the information environment is not random. Units synchronize and sequence IRCs so that they actively contribute to fulfilling the unit's mission in accordance with the commander's intent and concept of operations. Mission command places responsibility for IRC synchronization on the staff; however, without the commander's direct involvement, stated intent, guidance, concept of operations, and narrative, the staff will fail to achieve desired and required operational outcomes.

COMMANDERS' RESPONSIBILITIES

4-2. Commanders drive the conduct of IO and are their unit's key informers and influencers. Their influence is a function of their position, authority, decisions, personal actions, and the combat power their unit generates. Every action they take, operation they lead, capability they employ, and word or image they convey sends a message. Ultimately, they have the responsibility to align and combine each message into a comprehensive and compelling narrative while ensuring their unit fulfills this narrative. Their narrative explains the *why* of military operations.

Note. Commanders ensure all members of the Army Profession live by, adhere to, and uphold the moral principles of the Army Ethic, starting with themselves. As trusted Army professionals, commanders set the example and demonstrate character, competence, and commitment. They strive to consistently make right decisions and take right actions that are ethical, effective, and efficient. The Army Ethic is essential to the conduct of IO, as it ensures actions, words, and images are aligned and mutually reinforcing, thereby enhancing credibility and trust.

4-3. The *why* of operations comes down to establishing credibility and legitimacy. No matter the unit's mission, credibility and legitimacy are essential to success. Both credibility and legitimacy build on the Army bedrock of trust. Credible units match or align their actions with their messages (words and images). Trusted Army leaders and units fulfill commitments, are consistent in what they do, and ensure follow through. Legitimacy maintains legal and moral authority in the conduct of operations. Legitimacy, which can be a decisive factor in operations, is based on the actual and perceived legality, morality, and rightness of the actions from interested audiences' point of view. These audiences include American national leadership and domestic audiences; foreign governments, leaders, and civilian populations in the operational area; threats and adversaries; and other nations and organizations around the world.

4-4. Commanders (and subordinate leaders) are responsible for driving the conduct of IO through their narrative, stated intent, guidance, concept of operations, and risk assessment to achieve desired and required operational outcomes.

COMMANDER'S NARRATIVE

4-5. Aligned and synchronized actions and messages help create and convey a credible narrative comprising legitimate actions. To build trust, enable unity of effort, and strengthen legitimacy, commanders, leaders, and IO professionals demonstrate their character, competence, and commitment through their decisions and actions.

4-6. A *narrative* is an overarching expression of context and desired results (JDN 2-13). It focuses primarily on shaping perceptions of relevant audiences in the AO. Not only does it provide rationale to audiences

affected by military operations but the narrative serves as a guide to units so that their actions (deeds), words, and images appropriately align. The final result: a unit whose actions support and reinforce the narrative and ensure its consistency, viability, and effectiveness.

4-7. The IO officer plays a significant role in assisting the commander to craft the narrative. As the unit's effects coordinator for IRCs, the IO officer advises the commander on ways IRCs can affect operations and ways operations can affect the information and operational environments. An effective narrative helps shape both environments by creating or facilitating conditions favorable to the commander's intent, especially in bolstering confidence in the U.S.'s or coalition's mission and creating an alternative to the enemy's or adversary's narrative.

4-8. Commanders typically develop formal, explicit narratives at the strategic and possibly operational levels and convey them downward, within which subordinate units nest their messages, actions, and activities. Yet even the lowest-level commanders or leaders consciously envision how their units' actions, words, and images either support or confound the approved narrative. These leaders then tailor and adapt unit actions and messages to their AOs. If necessary, subordinate commanders get clarification from higher headquarters (for more information on narratives, see the list of recommended readings in the references).

COMMANDER'S INTENT

4-9. *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). Mission command requires commanders to convey a clear commander's intent for operations in which multiple operational and mission variables interact with the lethal application of ground combat power. Such dynamic interactions—many of which occur in the information environment—often compel subordinate commanders to make difficult decisions in unforeseen circumstances. Commander's intent is also essential for exercising disciplined initiative, which is particularly critical to executing a range of IO actions and activities. Such actions and activities can include military deception, SLE, and PPP.

COMMANDER'S INITIAL AND SUBSEQUENT GUIDANCE

4-10. Commander's planning guidance conveys the essence of the commander's visualization and may be broad or detailed. It outlines an *operational approach*—a broad description of the mission, operational concepts, tasks, and actions required to accomplish the mission (JP 5-0) and discusses COAs the commander initially favors from those the staff should not consider. It broadly describes when, where, and how the commander intends to employ combat power to accomplish the mission within the higher commander's intent. In terms of IO, if commanders determine that an information-related line of effort is decisive or that attaining an IO objective requires a significant lead time, they will issue relevant instructions as part of their guidance. In this guidance, they may frame their narrative and subordinating themes and messages, request information about the information environment, identify key leaders with whom they must engage, and discuss how IRCs will support COAs.

CONCEPT OF OPERATIONS

4-11. The concept of operations describes how the commander or leader envisions an operation unfolding from its start to its conclusion or end state. It determines how accomplishing each task leads to executing the next. It identifies the best ways to use available terrain (both physical and virtual) and employs unit strengths against enemy weaknesses. As a line of effort that supports the overall operation—as well as specific lines of operation or effort—IO is an essential element of any concept of operations. IO's contribution to the concept of operation is expressed in its scheme of IO (see paragraph 4-34 for more information on scheme of IO).

RISK ASSESSMENT

4-12. Commanders and their staffs, as trusted Army professionals, incorporate ethical risk assessments in their planning and conduct of operations. These assessments seek to—

- Mitigate unnecessary risk to personnel and mission accomplishment, friendly and allied forces, and noncombatants.
- Avoid improper use of resources and assets.
- Avert decisions and actions that may produce short-term tactical benefits to operations but long-term negative strategic consequences.

STAFF RESPONSIBILITIES

4-13. The staff has responsibility for conducting IO through synchronizing IRCs. As the staff lead for IO, the IO officer or designated representative develops a range of products and chairs the IO working group. The IO working group is the primary mechanism for synchronization and produces several outputs that drive the unit's efforts in the information environment. These outputs include the IO running estimate; the logic of the effort, commander's critical information requirements and essential elements of friendly information, IO input to base orders and plans, IO synchronization matrix, battle drills, and other products as needed.

INFORMATION OPERATIONS WORKING GROUP

4-14. The IO working group has a purpose, agenda and proposed timing, inputs and outputs, and structure and participants. Figure 4-1 on page 4-4 illustrates these components. To enhance the IO working group's effectiveness, the IO officer and element (if one exists) consider a number of best practices before, during, and after the meeting. Because it relies on information from the commander's daily update briefing and feeds the targeting process, the IO working group occurs between the two events in the unit's battle rhythm (see FM 3-13 for an extended discussion of the IO working group).

4-15. Before the IO working group convenes, the IO officer prepares and disseminates the agenda. Typically, the agenda is pre-set and the same template used at every meeting. However, effective IO officers send the agenda out as a reminder to participants and to give advance notice of possible changes. Additionally, before the meeting, the IO officer ensures that all inputs are up-to-date and shared, if possible.

4-16. Efficient IO officers start on time, keep the meeting on the agenda and running time (typically an hour or less), employ a designated note taker, and summarize key points and due outs before the meeting adjourns. Most importantly, IO officers tie critical discussions, outcomes, and decisions back to the commander's narrative, intent, concept of operations, and guidance.

4-17. Post meeting, the IO officer disseminates the meeting minutes, follows up on due outs, and updates the commander and other unit leaders on key outcomes and outputs. The IO officer also finalizes target nominations in advance of the next targeting meeting.

INFORMATION OPERATIONS RUNNING ESTIMATE

4-18. A *running estimate* is the continuous assessment of the current situation 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.

4-19. 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 warning orders as required during planning and, ultimately, to draft applicable IO sections of the operation order or operation plan.

Purpose	*Agenda and Proposed Timing*	
Prioritize, request, and synchronize IRCs and IO augmentation to optimize effects in and through the information environment. **Battle rhythm**: Before targeting working group	Part 1: Operations and intelligence update	30 min
	• Intelligence update	5 min
	• Information environment update	3 min
	• Operations update or significant activities	7 min
	• Review plans, future operations, and current operations	5 min
	• Assessment update (information requirements, indicators)	5 min
	• Calendar update, due outs, and responsibilities from previous meeting	5 min
	Part 2: Stabilize efforts, if any Part 3: Defend efforts Part 4: Attack efforts } • Review and update synchronization matrix • Guidance and comments	6 min 12 min 12 min

Inputs and Outputs		*Structure and Participants*
Inputs: • Higher headquarters orders and guidance • Commander's intent, concept of operations, and narrative • IRC status (running estimates) • Intelligence collections assets • CIO and IPB • Media monitoring analysis • Cultural calendar • Engagements schedule • Audience analysis • Scheme of IO and synchronization matrix • Commander's objectives for IO • Measures of effectiveness and performance	**Outputs:** • Updated scheme of IO • Updated IO synchronization matrix • Key leader engagement recommendations • Refined themes and messages • Refined operational products • Target nominations • Updated CIO • Plans and orders update • Information requirements	**Lead:** IO officer or representative [Chair: G-3 (S-3), executive officer, deputy commanding officer, or commander] **Core participants:** MISO, G-2 (S-2), subordinate unit representatives, G-3 (S-3), fires, G-9 (S-9), operations security, public affairs, CEMA (CO and EW) **Other participants (mission and situation dependent):** G-1 (S-1), G-4 (S-4), G-5 (S-5), G-6 (S-6), space operations, MILDEC, combat camera, FAO, FDO, special forces liaison, KM officer, engineer, STO chief, chaplain, staff judge advocate, unified action partner representatives

CEMA	cyberspace electromagnetic activities	IPB	intelligence preparation of the battlefield
CIO	combined information overlay	IRC	information-related capability
CO	cyberspace operations	KM	knowledge management
EW	electronic warfare	MILDEC	military deception
FAO	foreign area officer	min	minute
FDO	foreign disclosure officer	MISO	military information support operations
G-1	assistant chief of staff, personnel	S-1	personnel staff officer
G-2	assistant chief of staff, intelligence	S-2	intelligence staff officer
G-3	assistant chief of staff, operations	S-3	operations staff officer
G-4	assistant chief of staff, logistics	S-4	logistics staff officer
G-5	assistant chief of staff, plans	S-5	plans staff officer
G-6	assistant chief of staff, signal	S-6	signal staff officer
G-9	assistant chief of staff, civil affairs operations	S-9	civil affairs operations staff officer
IO	information operations	STO	special technical operations

Figure 4-1. Components of an information operations working group

4-20. Running estimates enable planning officers to track and record pertinent information and provide recommendations to commanders. A generic written format of a running estimate contains six general considerations: situation, mission, course of action, analysis, comparison, and recommendation (see FM 6-0 for a detailed discussion on running estimates). Figure 4-2 provides an IO-specific version of the generic

written format. Variations on this format, such as the example provided in Figure 4-3 on page 4-6, 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 graphic 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 graphic format enables the IO officer to brief the commander and staff with a single slide.

1. SITUATION AND CONSIDERATIONS.

a. Area of Interest. Identify and describe those factors of the area of interest that affect functional area considerations.

b. Characteristics of the Area of Operations.

(1) Terrain. State how terrain affects a functional area's capabilities.

(2) Weather. State how weather affects a functional area's capabilities.

(3) Enemy Forces. Describe enemy disposition, composition, strength, and systems in a functional area. Describe enemy capabilities and possible courses of action (COAs) and their effects on a functional area.

(4) Friendly Forces. List current functional area resources in terms of equipment, personnel, and systems. Identify additional resources available for the functional area located at higher, adjacent, or other units. List those capabilities from other military and civilian partners that may be available to provide support in the functional area. Compare requirements to current capabilities and suggest solutions for satisfying discrepancies.

(5) Civilian Considerations. Describe civil considerations that may affect the functional area, including possible support needed by civil authorities from the functional area as well as possible interference from civil aspects.

c. Facts/Assumptions. List all facts and assumptions that affect the functional area.

2. MISSION. Show the restated mission resulting from mission analysis.

3. COURSES OF ACTION.

a. List friendly COAs that were war-gamed.

b. List enemy actions or COAs that were templated that impact the functional area.

c. List the evaluation criteria identified during COA analysis. All staffs use the same criteria.

4. ANALYSIS. Analyze each COA using the evaluation criteria from COA analysis. Review enemy actions that impact the functional area as they relate to COAs. Identify issues, risks, and deficiencies these enemy actions may create with respect to the functional area.

5. COMPARISON. Compare COAs. Rank order COAs for each key consideration. Use a decision matrix to aid the comparison process.

6. RECOMMENDATIONS AND CONCLUSIONS.

a. Recommend the most supportable COAs from the perspective of the functional area.

b. Prioritize and list issues, deficiencies, and risks and make recommendations on how to mitigate them.

Figure 4-2. Generic IO running estimate format

4-21. Running estimate development is continuous. The IO officer 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. The unit prepares its running estimate based on researching and analyzing the information environment within its region and anticipated mission sets.

Forces or systems available
- 413 civil affairs BNs
- 344 tactical MISO COs
- 1-55th Signal CO (-) 3x
- 2x EC-130J Commando Solo @ CFACC
- OCO available

Information environment
- Radio is the best medium to reach the civilian population within AO SWORD, followed by social media
- Religious leaders within contested areas are key communicators to the population
- Displaced civilians in camps along main routes may impede coalition forces' advance

Facts
- Civilian and government-controlled media outlets (radio and television) reach population within AO SWORD
- Adversary forces have used civilian radio stations to broadcast coalition forces' troop movements and propaganda in the AO

Assumptions
- Civilian population will support HNSF and coalition forces once security is restored
- Civilian population will remain in place during attack unless there is a loss of essential services

Specified tasks

Identify key communicators within AO SWORD in order to deliver non-interference

Implied tasks
- Deny adversary use of social media messaging during decisive operations
- Develop Soldier and leader engagement, and MISO products to support non-interference

Limitations

MISO messaging and OCO release authority held by CCDR

HPT nominations
- Denial of adversary social media site during decisive operations
- Identify tribal leaders

CCIR nominations
- Block axis of advance by civilian population during attack
- Damage to HN essential services infrastructure and religious structures

EEFI nominations

N/A

Critical planning factors

Air tasking order cycle request 72 hours prior

Objectives

1. Influence civilian population to minimize interference with coalition forces information operations team to prevent civilian casualties

2. Disrupt enemy forces use of media outlets in order to support freedom of movement of coalition forces.

Request for forces

Request OCO to deny use of social media site during decisive operations

AO	area of operations	EEFI	essential element of friendly information
BN	Battalion	HN	host nation
CCDR	combatant commander	HNSF	host-nation security forces
CCIR	commander's critical information requirement	HPT	high-payoff target
CFACC	combined force air component commander	MISO	military information support operations
CO	Company	N/A	not applicable
COMCAM	combat camera	OCO	offensive cyberspace operations

Figure 4-3. Example graphical information operations running estimate

LOGIC OF THE EFFORT

4-22. An essential part of planning and assessing IO is the need to develop an explicit logic of the effort for each objective or effect. The logic of the effort makes explicit how specific efforts lead to attaining objectives. The value of this logic is that its assumptions are made explicit and can become hypotheses that can then be tested and, if necessary, refined. Figure 4-4 provides a simple example of a logic statement and how it evolves when its hypothesis is tested. More complex examples would include additional threat countermeasures that would test each successive hypothesis and refine the IRC mix necessary to create logic that is as foolproof as possible, balanced against risk, available assets, time, and cost.

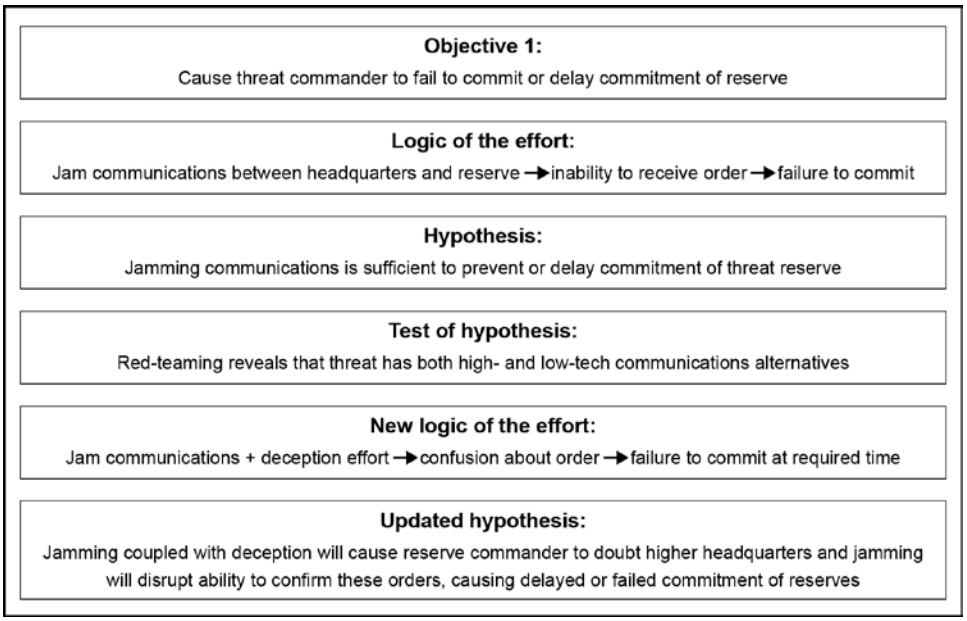

Figure 4-4. Logic of the effort example

COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

4-23. Commander's critical information requirements (CCIRs) identify information needed by the commander to visualize an operational environment and make critical decisions. CCIRs also filter information to the commander by defining what is important to mission accomplishment. If the information operation requires the commander to make a timely tactical decision, then staffs include IO input to the CCIRs, with supporting analysis and input to the decision support template produced during war gaming.

4-24. CCIRs are derived from information requirements, which are maintained and nominated by each staff element to the intelligence or operations staff officer. From the complete array of these requirements, the staff nominates those critical to the commander's decision making to become CCIRs, using the commander's guidance, higher headquarters' CCIRs, the essential-task list, and the IPB (situation template) to narrow and refine the list. Two types of CCIRs exist:

- Priority intelligence requirements.
- Friendly force information requirements.

Priority Intelligence Requirements

4-25. Priority intelligence requirements (PIRs) are information the commander must know about the threat and other aspects of an operational environment. For IO, PIRs focus on conditions in the information environment and adversary actions that affect the information environment. PIRs that may be required for IO include the following questions:

- Hostile forces using or preparing to use a key media outlet to produce or disseminate hostile propaganda.
- Adversary forces preparing to attack friendly information networks (either human or technological).

Friendly Force Information Requirements

4-26. Friendly force information requirements (known as FFIRs) are items of information the commander must know about the friendly force. For IO, friendly force information requirements provide information on

critical aspects of the command's information system, IRCs, and execution of the information operation. Friendly force information requirements that may be required for IO include the following:

- Death or serious injury of noncombatants by friendly forces.
- Media coverage of alleged friendly force misconduct.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

4-27. Essential elements of friendly information (EEFIs) are critical aspects of a friendly operation that, if known by the adversary, subsequently lead to compromise, failure, or limited success of an operation, and, therefore, must be protected from detection. In other words, EEFI is a list of information that must be protected from the adversary's intelligence system to prevent the adversary from making timely decisions and allowing friendly forces to retain the initiative. Typically, EEFI include the command intentions, subordinate element status, or the location of critical assets (such as command posts and signal nodes). EEFI should be refined throughout the planning process, as some information may not be identified until COA development. Once EEFI are developed, measures (as tasks to subordinate units) are developed to protect the information (OPSEC process). Two examples of EEFI are:

- Friendly forces' time of departure for an operation.
- Tribal leaders assisting friendly forces.

INFORMATION OPERATIONS INPUT TO OPERATION ORDERS AND PLANS

4-28. Operation orders and plans are products or outputs of planning. They provide a directive for future action. Commanders issue plans and orders to subordinates to communicate their understanding of the situation and their visualization of an operation. Plans and orders direct, coordinate, and synchronize subordinate actions and inform those outside the unit how to cooperate and provide support (see FM 6-0 for a detailed discussion of operation orders and operation plans). As with all other functions and capabilities, IO provides input to these plans and orders.

Base Orders and Plans

4-29. While every part of an operation order or plan matters, most personnel read the base order or plan (the initial part of the document before the annexes and appendices) because it contains the most mission-essential information. Usually staff sections or specialists involved with a respective function or capability read only those annexes and appendices. If the base order or plan does not contain that information, it might not get read. Increasingly, some aspect of IO is essential to overall operational success. Sections of the base order or plan in which IO may be found include the following:

- Commander's intent, paragraph 3a.
- Concept of operations, paragraph 3b.
- Scheme of IO, paragraph 3c.*x* (*x* is non-specific; the exact subparagraph will vary by order or plan).
- Tasks to subordinate units, paragraph 3j.
- Coordinating instructions, paragraph 3k.

The information contained in these paragraphs and subparagraphs depends on the mission and results of the operations process (an expanded discussion of IO in the operations process appears in FM 3-13 and FM 6-0).

Appendix 15 (Information Operations) to Annex C (Operations)

4-30. The most detailed discussion of IO support to an operation is found in Appendix 15 to Annex C of the operation order or plan. Appendix 15 typically includes several tabs or exhibits that provide the following products or guidance:

- Combined information overlay.
- Synchronization matrix.
- Instructions for IRCs not covered by other appendices, such as operations security, visual information, and combat camera.

4-31. IO officer crafts an IO mission statement while preparing or updating the running estimate. They later refine the mission statement to complete Appendix 15 (IO), which occurs with receipt of an order and commencement of mission analysis. FM 6-0 provides a template for attachments, such as annexes and appendixes. For the mission paragraph (paragraph 2), it instructs planners to state the mission of the functional area to support the base plan or order. In the case of Appendix 15, the functional area is IO.

4-32. The IO mission statement is a short paragraph or sentence describing what the commander wants IO to accomplish and the purpose for accomplishing it. The IO officer develops the proposed IO mission statement at the end of mission analysis based on the unit's proposed mission statement and IO-related essential tasks. During the mission analysis briefing or shortly thereafter, commanders approve the unit's mission statement and CCIRs. They then develop and issue their commander's intent and planning guidance. The IO officer may refine a final IO mission statement based on relevant input from the commander's intent and planning guidance and get it approved by the operations officer. The final IO mission statement includes IO effects and most significant IO-related target categories identified in the information environment during mission analysis. A sample mission statement follows:

> No later than 130600JAN19, IO supports 1 Stryker Brigade Combat Team's defense of key terrain in AO RAIDER by disrupting Donovian command and control and influencing the population of Erdabil Province to support the Government of Atropia to engage the enemy from a position of advantage.

4-33. The mission statement differs from the scheme of IO in its level of detail. The mission statement describes IO in the aggregate. The scheme of IO addresses how IRCs contribute to the scheme and, as a result, accomplish the mission.

Note. There is legitimate debate about whether more than one mission statement can or should exist for a given operation. Some commanders may direct that all attachments reiterate the restated mission in the base order. Functional mission statements are not intended as replacements for the base order mission but, instead, to support it. They are doctrinally justified per FM 6-0.

Scheme of Information Operations

4-34. The scheme of IO begins with a clear, concise statement of where, when, and how the commander intends to employ synchronized IRCs to create effects in and through the information environment to support the overall operation and accomplish the mission. Based on the commander's planning guidance, the IO officer develops a separate scheme of IO for each COA the staff develops during COA development. IO schemes of support are expressed both narratively and graphically, in terms of IO objectives and IRC tasks required to achieve these objectives. Figure 4-5 on page 4-10 provides a sample scheme of an IO statement. Figure 4-6 on page 4-10 illustrates a supporting sketch with articulated objectives and IRCs.

1 SBCT coordinates, deconflicts, and synchronizes IRCs in support of Phase III (Defense) in AO RAIDER. CO collects against Donovian frequencies and communications east of PL MAINE. EW conducts jamming of Donovian armor mission command systems in EAs THOMPSON, UZI, and RUGER. CMOC informs IDPs of collection instructions and safe rally points. MISO influences IDPs to not interfere with military movements and counters Donovian propaganda. The goal of all IRCs is to elicit the surrender or desertion of enemy forces, reduce CIVCAS, and prevent massing of enemy armor and indirect fires. PA controls release of operational information in order to bolster OPSEC and facilitates media engagement strategy to highlight operational successes. Maneuver, CAO, and MISO will conduct SLEs to enable 1 SBCT elements freedom of maneuver throughout AO RAIDER. Finally, 1 SBCT will capture operational successes through COMCAM and other visual information capabilities while OPSEC will protect EEFIs.

AO	area of operations	IDP	internally displaced person
CAO	civil affairs operations	IRC	information-related capability
CIVCAS	civilian casualty	MISO	military information support operations
CMOC	civil-military operations center	OPSEC	operations security
CO	cyberspace operations	PA	public affairs
COMCAM	combat camera	PL	phase line
EA	engagement area	SBCT	Stryker brigade combat team
EEFI	essential elements of friendly information	SLE	Soldier and leader engagement
EW	electronic warfare		

Figure 4-5. Sample scheme of information operations statement

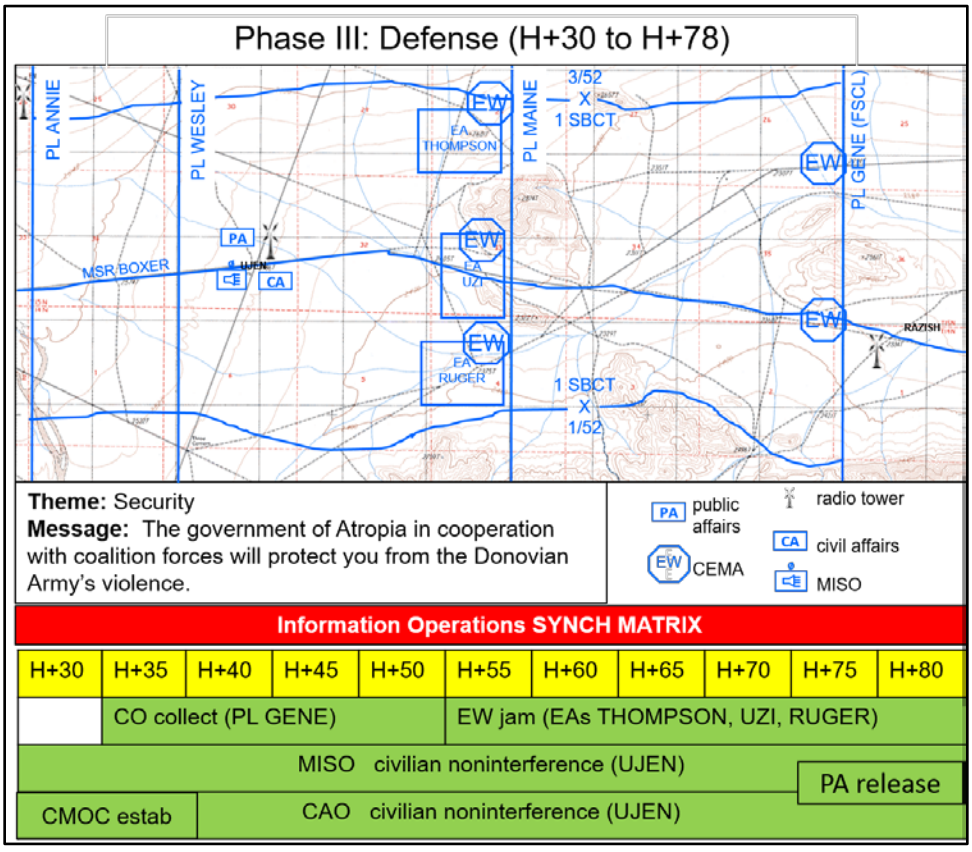

Figure 4-6. Example scheme of information operations sketch

IO Mission Statement: NLT 130600JAN19, IO supports 1 SBCT's defense of key terrain in AO RAIDER by disrupting Donovian C2 and influencing the population of Erdabil Province to support the government of Atropia IOT engage the enemy from a position of advantage.

IO OBJ 1: Influence populace in UJEN to not interfere with 1 SBCT combat operations IOT limit CIVCASs.

IO OBJ 2: Disrupt enemy communications in EAs THOMPSON, RUGER, and UZI to degrade C2 IOT prevent massing of combat power.

Key Tasks

CO/EW

T: Jam Donovian armor mission command systems in EAs THOMPSON, UZI, and RUGER.

P: Degrade C2 capability IOT prevent massing of combat power.

M/MOP: Three precision jamming delivered by tech ops to Donovian C2 systems in EAs THOMPSON, UZI, and RUGER.

MISO

T: Persuade populace in UJEN to not interfere with 1 SBCT movements.

P: Counter Donovian propaganda that misdirects Atropians IOT prevent CIVCASs.

M/MOP: Eight broadcasts by loudspeaker to local nationals vic UJEN.

CAO

T: Inform IDPs of safe rally points.

P: Prevent CIVCASs IOT allow 1 SBCT freedom of movement.

M/MOP: One CMOC established to communicate civil control information with local nationals vic UJEN NLT H+35.

PA

T: Publicize Donovian battle losses to key audiences.

P: Facilitate media engagement strategy IOT highlight operational successes.

M/MOP: Three releases accessible via public sites to key audiences.

MOE 1: Decrease in daily observed number of civilian vehicles or foot traffic on MSR BOXER by 25% from baseline at H+6.

MOE 2: Increase in numbers of tips providing enemy locations and activity by 50% compared to those received at H+6.

AO	area of operations	MISO	military information support operations
C2	command and control	MOE	measure of effectiveness
CAO	civil affairs operations	M/MOP	method/measure of performance
CEMA	cyberspace electromagnetic activities	MSR	main supply route
CIVCAS	civilian casualty	NLT	no later than
CMOC	civil-military operations center	OBJ	objective
CO	cyberspace operations	P	purpose
EA	engagement area	PA	public affairs
estab	establishment	PL	phase line
EW	electronic warfare	SBCT	Stryker brigade combat team
H	hour	synch	synchronization
IDP	internally displaced person	T	task
IO	information operations	tech ops	technical operations
IOT	in order to	vic	vicinity

Figure 4-6. Example scheme of information operations sketch *(continued)*

Information Operations Objectives

4-35. IO objectives express specific and obtainable outcomes or effects that commanders intend to achieve in and through the information environment. In addition to being specific, these objectives enable measurable, achievable, realistic, and time-bounded (known as SMART) measures of effectiveness and performance, which facilitate attaining and assessing established objectives (see Chapter 6 for more details on measures of effectiveness and performance). IO objectives do not stand alone but support the commander's operational intent. Based on the definition of IO, objectives are framed to accomplish the following:

- Attack enemy or adversary decision making and the capabilities or conditions that facilitate that decision making.
- Preserve friendly decision making and the capabilities or conditions that facilitate it.
- Otherwise shape the information environment to provide operational advantage to friendly forces, including freedom of maneuver in this environment.

4-36. For example, if an operational objective is to prevent an enemy force or weapon system from moving from Objective Black before attack, then possible associated IO objectives could be to—

- Disrupt adversary communications within AO Blue to prevent early warning.
- Deceive adversary decision makers on Objective Black to prevent relocation of command and control.
- Influence local populace in Operational Area Blue to support friendly force operations and prevent populace reporting on friendly force activities.

4-37. For each mission or COA considered, IO planners develop IO objectives based on the tasks for IO identified during mission analysis. Depending upon the complexity or duration of the mission (for example, a tactical direct-action mission versus a long-term foreign internal defense mission), there may be only one or numerous IO objectives developed for each phase of the overall operation. Generally, regardless of the mission, no more than five objectives are planned for execution at any one time in the operation.

4-38. Accurate situational understanding is key to establishing IO objectives. Operational- and tactical-level IO objectives must nest with strategic theater objectives. IO objectives further help the staff determine tasks to subordinate units during COA development and analysis.

4-39. No prescriptive format exists for an IO objective. One possible format uses effect, target or target audience, action, and purpose (known as ETAP):

- **E**ffect describes the outcome (for example, influence, destroy, degrade, disrupt, or deceive).
- **T**arget or target audience describes the object of the desired effect.
- **A**ction describes the behavior expected of the recipient.
- **P**urpose describes what will be accomplished for the friendly force.

Chapter 6 provides additional guidance on formulating an IO objective.

Note. Around 2010, the definition of "target" was revised to specify that a target is an entity or object *that performs a function for the adversary*. However, the definition of "target audience" was not similarly adjusted. Per the *DoD Dictionary of Military and Associated Terms*, a target audience is an individual or group selected for influence.

4-40. IO objectives are written in terms of effects, because the desired effect focuses the activities (tasks) of IRCs. For IO, a proper effect falls into one of three categories:

- *Effects against the enemy or an adversary*. IO effects against the enemy or an adversary focus on the threat's ability to collect, protect, and project information. For example, an IO objective might disrupt (effect) an enemy formation's (target) ability to conduct command and control (action) to surprise adversary forces in and around Objective X (purpose).
- *Effects to defend friendly forces*. IO effects regarding friendly forces seek to prevent enemy or adversary interference with friendly abilities to collect, protect, and project information. For example, an IO objective might deny (effect) enemy IRCs (target) the ability to exploit negative effects of friendly force operations (action) to prevent attrition of local populace support away from coalition forces to the enemy (purpose).
- *Effects to shape the information environment*. IO effects shape information content and flow in the operational area's information environment. For example, an IO objective might influence (effect) local populace (target audience) perception of the enemy (action) to increase reporting of enemy activity and locations to coalition forces (purpose).

4-41. Because it is impossible to anticipate all possible effects, terms other than those presented in this publication may be used to describe the desired effects for IO. Effects terms should describe a condition—

not a task. Definitions for the same effect may vary based on the physical, informational, and cognitive nature of the effect and the target of the effect.

4-42. As IO officers develop IO objectives, they establish the criteria—measures of effectiveness (MOEs)—and methods to collect the indicators. If planners cannot identify adequate indications and collection means, then they may need to refine the objective to produce measurable and detectable results. If an objective's MOE is focused on behavior or beliefs, planners must consider physical actions that result from the desired behavior or belief as an indicator.

Information-Related Capability Tasks

4-43. Once IO officers write IO objectives, they develop tasks to subordinate units and staff elements that possess the IRCs needed to accomplish these objectives. These tasks are conveyed through the various types of orders dictated by the MDMP. IRC tasks to subordinate units translate the broad concepts of the objectives into discreet actions. Tasks are often written as—

- **Task**. The task is the action to be performed and the location of the task (for example, prevent local populace interference in Village X).
- **Purpose**. The purpose is the reason why the task is assigned (for example, prevent civilian casualties).
- **Method**. The method describes what unit or capability will conduct the task (for example, MISO Team C121).

4-44. Units take care to ensure that developed tasks do not cause IRCs to violate relevant authorities. For example, MISO tasks are tied directly to Office of the Secretary of Defense-approved MISO objectives (joint) or psychological objectives (Army), which are provided in a MISO program or applicable order. Through direct coordination or the IO working group, IO officers synchronize MISO objectives with IO objectives and align tasks so they support MISO, psychological, and IO objectives simultaneously. Alternatively, if an IO objective requires a MISO task not currently approved, then the IO working group seeks approval through MISO channels, reinforcing the need to plan selected IO objectives well in advance.

4-45. Similar to effects, tasks can be organized into three categories:

- *Tasks against the adversary*. These tasks target threat capabilities and vulnerabilities to collect, protect, and project information (as identified during the COG analysis). An example task might counter enemy propaganda to maintain populace support for capture or kill missions.
- *Tasks to protect friendly forces*. These tasks seek to protect friendly force vulnerabilities in the information environment from threat capabilities to collect and project information. An example task might detect intrusions into friendly force information systems to prevent enemy or adversary collection of critical information.
- *Tasks to shape the information environment*. These tasks shape information content and movement by impacting the key nodes in each subinformation environment to influence local populace perceptions and behavior. An example task might engage religious leaders to bolster friendly credibility and legitimacy.

4-46. Figure 4-7 on page 4-14 depicts how the scheme of IO, IO objectives, and IRC tasks inter-relate to support the MDMP. The relationship among these three is particularly important to the assessment process described in greater detail in Chapter 6.

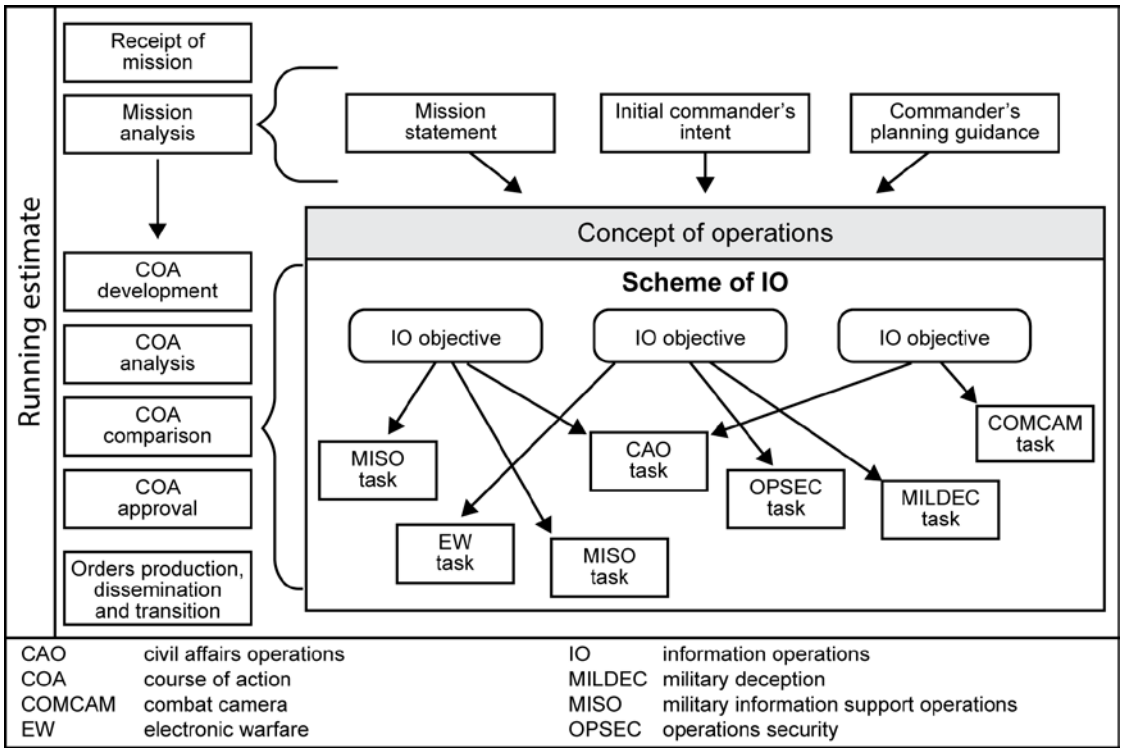

Figure 4-7. Relationship of scheme of IO, IO objectives, and IRC tasks

Information Operations Synchronization Matrix

4-47. The synchronization matrix is used to monitor progress and results of IO objectives and IRC tasks as well as to keep IO execution focused on contributing to the overall operation. It is one of the IO working group's primary tools for monitoring and evaluating progress and assessing whether planned effects have been achieved.

4-48. No specific format exists for a synchronization matrix. The format will be determined by commander's preferences, unit standard operating procedures, mission and situation, and time available. Table 4-1 provides an example matrix that arrays IRC activities by phase. Table 4-2 on page 4-16 provides an alternative example that arrays IRC activities by unit and task.

Table 4-1. Example 1 – Information operations synchronization matrix

IRC	*Phase I*	*Phase II*	*Phase III*	*Phase IV*
EW	Monitor signals of interest. Electronic protection for personnel and equipment.	Electronic attack to disrupt enemy communications. Electronic protection for personnel and equipment.	N/A	N/A
MISO	Broadcast harassment messages against enemy. Broadcast noninterference messages for local populace.	N/A	Broadcast via mobile radio to keep population informed on mission.	Broadcast on mission success. Coordinate with COMCAM for post-mission messaging and countering the effect of adversary information activities.
OPSEC	Determine essential elements of friendly information for mission.	Implement measures to protect essential elements of friendly information to protect movement routes, mission command, and objective.	N/A	N/A
MILDEC	N/A	N/A	N/A	N/A
CAO	Prepare Commander's Emergency Response Program paperwork for funds disbursement. Coordinate with Provincial reconstruction team.	N/A	N/A	Assist personnel returning to villages. Assess small-scale immediate projects.
PA	Prepare press releases. Embed media.	N/A	N/A	Distribute press releases. Conduct press conference and set up interviews with subject matter experts.
COMCAM	Document operation.	Document operation.	Document operation.	Document operation.

CAO	civil affairs operations	MISO	military information support operations
COMCAM	combat camera	N/A	not applicable
EW	electronic warfare	OPSEC	operations security
IRC	information-related capability	PA	public affairs
MILDEC	military deception		

Table 4-2. Example 2 – Information operations synchronization matrix

Tasked unit or system	*IO task*	*Time on target or time of effect*	*Location*	*Remarks*
EA-6B	EW-01	H-1 through H-hour	TAI 002 and 003	Successful if enemy is unable to send early warning
Tactical PSYOP team	MISO-01	H-24 and continue	Objective SPRUCE	Successful if no civilian interference
Civil affairs team	CAO-01	H-24 through H-hour	Objective PINE	N/A
Special Instructions: None				

CAO	civil affairs operations	N/A	not applicable
EA-6B	electronic warfare aircraft (Prowler)	PSYOP	psychological operations
IO	information operations	TAI	target area of interest
MISO	military information support operations		

BATTLE DRILLS

4-49. Battle drills are planning aids designed to speed response to crisis situations occurring during the conduct of a mission. For IO, quick responses to enemy or adversary activities, actions, and events in the operational area are necessary to prevent the enemy or adversary from gaining advantage in the information environment or, conversely, to sustain friendly advantage.

4-50. Staffs develop battle drills during the planning process; however, drills are not complete and final COAs. Rather, battle drills are predeveloped concepts that anticipate crises. Once a crisis occurs, units can adjust the battle drill quickly to address the realities of the situation at hand.

4-51. A military operation can be thought of as a series of events, planned and unplanned, that force both friendly and enemy forces to react to a changing situation. Some of these events, referred to as critical events, directly link to or precipitate mission success of friendly or enemy forces. Critical events—

- Can create both intended and unintended effects and may be brought on by friendly, adversary, or third-party actions.
- Can be either negative or positive. The staff can develop drills that react to either type:
  - For negative critical events, a battle drill should mitigate the impact of the event on the populace and friendly forces.
  - For positive critical events, a battle drill should exploit the event to maximize the impact on the populace and adversary forces.
- Can be triggers or cues for the staff to initiate a battle drill.

4-52. An IO battle drill is a generic scheme of IO that addresses a friendly force IO response to a critical event that may occur during execution of the operation. While no doctrinally established format exists for a battle drill, its format should mirror existing products or follow unit standard operating procedure. Battle drills are developed to suit specific missions and potential branches and sequels of missions. Each battle drill should—

- Identify critical events.
- Define the desired information end state.
- Develop the scheme of IO.

The information contained in a battle drill is not a final and complete plan but rather a concept that must be refined to the realities of the situation at hand.

Identify Critical Events

4-53. Planners determine what critical events may result from friendly, enemy, adversary, or third-party action. Planners focus on events that will either occur in or affect the information environment and are

significant enough to affect the command's mission. The following list provides some examples of critical events:

- Civilian collateral damage.
- Civilian casualties.
- Fratricide incidents.
- Populace interference with friendly force operations (for example, civil demonstrations).
- Quick reaction force deployment.
- Adversary or friendly forces violation of law of land warfare (for example, atrocities against civilians, mass-grave discovery).
- Environmental incident (for example, hazardous material spill).
- Propaganda directed against friendly forces.
- EEFI or any other sensitive or classified information disclosure.

Define Information End State

4-54. Battle drills are designed to respond to specific situations. These situations must be sufficiently defined so planners can adjust the battle drill's concept to compensate for the differences between the planned and actual situations. For IO, this means defining the information end state for each battle drill. Examples of information end states for mitigation and exploitation battle drills are as follows:

- A mitigation battle drill:
  - *Event*. Disclosure of EEFI or classified information.
  - *Target*. Adversary.
  - *Information end state*. Adversary decision makers cannot take advantage of sensitive information about the friendly force.
- An exploitation battle drill:
  - *Event*. Destruction of key infrastructure by enemy forces.
  - *Audience or recipient*. Populace.
  - *Information end state*. Populace is mobilized to support friendly forces against the enemy to prevent future attacks.

Develop Battle Drill Scheme of Information Operations

4-55. The scheme of IO is a concise and easily understandable word picture describing how IRCs may be employed and what staff coordination must be conducted to employ these capabilities. The scheme must be integrated with the overall operation. How much information is known when the battle drill is created determines its level of detail.

4-56. As part of the scheme of IO, leaders develop tasks, purposes, methods, and means, and, if appropriate, targets for each participating IRC. A purpose for each task is included to explain each IRC's part in the operation. If appropriate, general target sets are identified for each tasked IRC. All IO-relevant capabilities—maneuver units and those staff entities that may have important roles in responding to the battle drill event—are considered. A purpose for each task is included to maximize IRC initiative. IRCs develop measures of performance (MOPs) for their assigned tasks.

4-57. Figure 4-8 on page 4-18 provides a sample format for a battle drill. Leaders modify the format as needed to fit the situation, mission, and commander's preference. Figure 4-9 on page 4-19 illustrates an abbreviated staff battle drill.

SITUATION: Insurgent forces attack friendly forces, a friendly third-party organization, or an opposing faction (for example, a bombing, shooting, or mortar attack).

ASSUMPTIONS: The insurgent attack does not cause significant friendly causalities.

LIKELY FRIENDLY ACTION: A response force is deployed to secure the site and find and destroy the insurgent force. Security operations are conducted in and around the area of attack. If necessary, force protection measures are increased.

SCHEME OF IO: Gain populace support for counterinsurgency activities and identify hidden insurgent cells for targeting. IRCs provide direct support to the response force. MISO teams disseminate print products to the populace near the attack site. Unit leaders, MISO teams, and CAO teams engage local leaders to gain support for friendly operations. PA issues a press release to explain the command's position and counter misinformation concerning the situation.

Restrictions: MISO products must conform to and support approved programs.

Measure of Effectiveness: Increase reporting by populace of insurgent activity by 15% compared to the level of reporting before attack.

Capability	Key Tasks	Purpose	Method	Target or TA
MISO	Disseminate print products and radio broadcasts to the populace of villages in and around the attack site.	Identify hidden insurgent cells. Reduce populace support for insurgent forces and activities.	Handbills and posters. Contract radio.	Local populace. Insurgent fence sitters.
SLE	Engage local leaders.	Gain support for counterinsurgency activities.	Face-to-face.	Civil leaders.
PPP or CMO	Response force decreases threatening signatures or activities without compromising force protection.	Build rapport and gain support for counterinsurgency activities.	Soccer matches.	Local populace

CAO	civil affairs operations	PA	public affairs
CMO	civil-military operations	PPP	presence, profile, and posture
IO	information operations	SLE	Soldier and leader engagement
IRC	information-related capability	TA	target audience
MISO	military information support operations		

Figure 4-8. Sample battle drill format for insurgent-related violence

1. **Situation**: React to collateral damage resulting from coalition-force action.

2. **Information end state**: Preempt adversary propaganda and negative media reporting.

3. **Immediate** (onsite):
- Notify commander.
- Document the scene (for example, COMCAM photos).
- Conduct on-site key-leader engagement to determine facts and conduct initial mitigation.

4. **Within 2 hours**:
- Notify operational area owner.
- Notify local-government officials.
- Public affairs makes a public statement of the facts for broadcast by local print, radio, and TV media.

5. **Within 24 hours**:
- Conduct key-leader engagements with local elders using HN partner-unit commanders, coalition commanders, and local-government officials.
- Assess damage for possible CAO projects.

6. **After 24 hours**:
- Coordinate for follow-up media coverage and key-leader engagement by operational-area owner.
- Compensate families (if appropriate) and conduct CMO or CAO activities.

CAO	civil affairs operations	HN	host nation
CMO	civil-military operations	TV	television
COMCAM	combat camera		

Figure 4-9. Sample abbreviated battle drill format

This page intentionally left blank.