

# Training and Evaluation Outline Report

**Task Number:** 71-9-5630

**Task Title:** Conduct Military Deception in the Joint Operations Area (Division Echelon and Above [Operational])

**Supporting Reference(s):**

Step Number	Reference ID	Reference Name	Required	Primary
	ADP 3-0	Unified Land Operations	Yes	No
	FM 5-0	THE OPERATIONS PROCESS	Yes	No
	FM 6-0	MISSION COMMAND	Yes	No
	JOINT PUB 3-0	Joint Operations	Yes	No
	JOINT PUB 3-13.4	Military Deception	Yes	Yes

**Condition:** The command is conducting or preparing to conduct operations as a joint task force, joint force land component command, Army forces, or Army service component command headquarters. The command's headquarters may or may not have integrated joint staff augmentation, liaisons, unit, and individual attachments. The command has received an operations plan, or warning, operations, or fragmentary order from higher headquarters and is exercising mission command. The commander has issued guidance on conducting military deception in the joint operations area. The command is prepared to interface with joint, interagency, governmental authorities, nongovernmental organizations, and multinational forces. The command has established communications with subordinate and adjacent units, and higher headquarters. The mission command system is operational and processing information in accordance with standard operating procedures. Some iterations of this task should be performed in MOPP.

**Standard:** The staff conducts military deception by planning actions to deliberately mislead threat decision makers as to friendly military capabilities, intentions and operations. The staff executes military deception actions that cause the threat to take specific actions/inactions that contribute to the accomplishment of the friendly mission.

Note: Task steps and performance measures may not apply to every staff, unit or echelon. Prior to evaluation, coordination should be made between evaluator and the evaluated staffs or units' higher headquarters to determine the performance measures that may not be evaluated.

**Special Equipment:** None

**Safety Level:** Low

## Task Statements

**Cue:** None

## DANGER

Leaders have an inherent responsibility to conduct Composite Risk Management to ensure the safety of all Soldiers and promote mission accomplishment.

## WARNING

Composite Risk Management is the Army's primary decision-making process to identify hazards, reduce risk, and prevent both accidental and tactical loss. All soldiers have the responsibility to learn and understand the risks associated with this task.

## CAUTION

Identifying hazards and controlling risks across the full spectrum of Army functions, operations, and activities is the responsibility of all Soldiers.

**Remarks:** While Army doctrine has changed to mission command over command and control (C2 - which is now a component of mission command), and changed from using ISR (Intelligence, Reconnaissance and Surveillance) to information collection (comprised of reconnaissance and surveillance, security operations, and intelligence operations), joint doctrine still retains the primacy of C2 over mission command as well as the use of ISR. Commanders and staffs of Army headquarters serving as a joint task force, joint force land component command, Army forces, or Army service component command headquarters should refer to applicable joint or multinational doctrine for the exercise and use of C2 and ISR.

Note: Task content last updated: 12 March 2012

**Notes:** None

## TASK STEPS

1. The staff, led by the Plans Cell, plans military deception (MILDEC) operations.
  - a. Use the "See, Think, Do" deception planning methodology.
  - b. Plan MILDEC from the top down.
  - c. Coordinate MILDEC plans with senior commanders to ensure unity of effort.
  - d. Execute the six-step MILDEC planning process.
    - (1) Deception mission analysis.
    - (2) Issuance of deception planning guidance.
    - (3) Deception estimate.
    - (4) Commander's deception estimate.
    - (5) Deception plan development, to include feedback channels.
    - (6) Deception plan review and approval.
  - e. Establish a deception planning cell.
    - (1) Interface with unit operations planners to review plans for deception requirements.
    - (2) Respond to higher headquarters' deception taskings.
    - (3) Provide resource requirements to higher headquarters for deception program development and sustainment.
    - (4) Look for opportunities to implement deception in support of military objectives.
  - f. Consider the following during MILDEC planning:
    - (1) MILDEC capabilities available to the unit.
    - (2) Limitations of resources.
    - (3) Risks.
      - (a) Deception failure.
      - (b) Exposure of means of feedback channels.
      - (c) Minimize risk to third parties.
  - g. Verify the plan includes application of the following, in accordance with the commander's guidance:
    - (1) Appropriate functions of MILDEC.

- (2) Employment of MILDEC means.
  - (3) Appropriate MILDEC tactics.
  - (4) Deception techniques.
  - (5) MILDEC procedures.
- h. Clearly state the goal and objective of the MILDEC operation.
  - i. Fully integrate MILDEC planning with joint planning processes.
  - j. Determine criteria for termination of MILDEC operations.
  - k. Develop measures of effectiveness to assess the deception operation.
2. The staff, led by the Mission Command Cell, integrates MILDEC with information operations (IO).
- a. Verify mutual support between MILDEC and military information support operations (MISO) efforts.
  - b. Identify operations security indicators during actual operations that may pose a threat to the effectiveness of MILDEC operations.
  - c. Use MILDEC to support employment of electronic warfare capabilities.
  - d. Replicate information systems to deceive possible intruders and support protection of computer network operations (CNO).
  - e. Use MILDEC to mislead the threat as to the true capabilities and purposes of weapons systems used in the physical attack/destruction activities of the integrated IO effort.
  - f. Verify information assurance policies safeguard information and indicators that may reveal friendly deception operations.
  - g. Verify physical security measures support MILDEC plan to prevent compromise.
  - h. Integrate MILDEC with intelligence activities to:
    - (1) Identify threat decision makers and their deception vulnerabilities.
    - (2) Estimate threat actions under differing scenarios and assess possible outcomes.
    - (3) Generate feedback regarding threat responses to deception operations.
  - i. Integrate MILDEC with counterintelligence (CI) activities to:
    - (1) Analyze threat intelligence systems to determine the best deception conduits.
    - (2) Control deception conduits within the threat's intelligence system (offensive CI operations).
    - (3) Participate in counterdeception operations.

(4) Analyze the threat's intelligence system to determine susceptibility to deception and surprise.

3. The staff, led by the Mission Command Cell, coordinates MILDEC operations.

a. Verify constant coordination between strategic, operational, and tactical levels since the potential for tactical or operational level deception to have strategic effects is high.

b. Coordinate with higher headquarters on deception execution timing to ensure synchronous and supporting relationships exist.

c. Coordinate both vertically and horizontally with commanders and staffs to ensure up-to-date integration between real-world operations and deception operations.

d. Coordinate with civil-military operations and public affairs organizations, the staff judge advocate, and other government agencies to avoid destabilizing military-civilian relationships, prevent the unintentional compromise of MILDEC activities, and ensure compliance with legal requirements.

e. Coordinate with MISO organizations for additional deception information conveyance capabilities.

4. The staff, led by the Current Operations Cell, executes MILDEC operations.

a. Keep the commander constantly informed of MILDEC successes, failures, or the need to modify the plan.

b. Verify methods in use to communicate the deception story are still appropriate and effective for the target audience.

c. Verify MILDEC activities are synchronized with the commander's overall operational concept.

d. Coordinate constantly with the intelligence staff to compare feedback of MILDEC operations to current rules of engagement and protection warfighting function issues.

e. Compare termination criteria to current intelligence to see if MILDEC operations require termination.

f. Develop security measures to protect MILDEC and the operations that are supporting or being supported.

g. Assign liaison officers from intelligence and CI organizations to support MILDEC operations where needed.

(Asterisks indicates a leader performance step.)

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. The staff, led by the Plans Cell, planned military deception (MILDEC) operations.			
a. Used the "See, Think, Do" deception planning methodology.			
b. Planned MILDEC from the top down.			
c. Coordinated MILDEC plans with senior commanders to ensure unity of effort.			
d. Executed the six-step MILDEC planning process.			
(1) Deception mission analysis.			
(2) Issuance of deception planning guidance.			
(3) Deception estimate.			
(4) Commander's deception estimate.			
(5) Deception plan development, to include feedback channels.			
(6) Deception plan review and approval.			
e. Established a deception planning cell.			
(1) Interfaced with unit operations planners to review plans for deception requirements.			
(2) Responded to higher headquarters' deception taskings.			
(3) Provided resource requirements to higher headquarters for deception program development and sustainment.			
(4) Looked for opportunities to implement deception in support of military objectives.			
f. Considered the following during MILDEC planning:			
(1) MILDEC capabilities available to the unit.			
(2) Limitations of resources.			
(3) Risks.			
(a) Deception failure.			
(b) Exposure of means of feedback channels.			
(c) Minimized risk to third parties.			
g. Verified the plan included application of the following, in accordance with the commander's guidance:			
(1) Appropriate functions of MILDEC.			
(2) Employment of MILDEC means.			
(3) Appropriate MILDEC tactics.			
(4) Deception techniques.			
(5) MILDEC procedures.			
h. Clearly stated the goal and objective of the MILDEC operation.			
i. Fully integrated MILDEC planning with joint planning processes.			
j. Determined criteria for termination of MILDEC operations.			
k. Developed measures of effectiveness to assess the deception operation.			
2. The staff, led by the Mission Command Cell, integrated MILDEC with information operations (IO).			
a. Verified mutual support between MILDEC and military information support operations (MISO) efforts.			
b. Identified operations security indicators during actual operations that would pose a threat to the effectiveness of MILDEC operations.			
c. Used MILDEC to support employment of electronic warfare capabilities.			
d. Replicated information systems to deceive possible intruders and support protection of computer network operations.			
e. Used MILDEC to mislead the threat as to the true capabilities and purposes of weapons systems used in the physical attack/destruction activities of the integrated IO effort.			
f. Verified information assurance policies safeguarded information and indicators that would reveal friendly deception operations.			
g. Verified physical security measures supported MILDEC plan to prevent compromise.			



**MOPP:** Sometimes

**MOPP Statement:** None

**NVG:** Never

**NVG Statement:** None

**Prerequisite Collective Task(s):** None

**Supporting Collective Task(s):**

Step Number	Task Number	Title	Proponent	Status
	71-9-3220	Conduct Attack on Operational Targets Using Nonlethal Means (Division Echelon and Above [Operational])	71 - Combined Arms (Collective)	Approved
	71-9-5600	Coordinate Operational Information Operations (Division Echelon and Above [Operational])	71 - Combined Arms (Collective)	Approved
	71-9-5610	Integrate Information Operations (Division Echelon and Above [Operational])	71 - Combined Arms (Collective)	Approved

**Supporting Individual Task(s):**

Step Number	Task Number	Title	Proponent	Status
	150-718-5111	Participate in the Military Decision Making Process	150 - Combined Arms (Individual)	Approved
	701-COM-1000	Identify Joint Force Structures, Capabilities, and Operations	701 - Command and General Staff (Individual)	Approved

**Supporting Drill Task(s):** None

---

**TADSS**

Step ID	TADSS ID	Title	Product Type	Quantity
No TADSS specified				

**Equipment (LIN)**

Step ID	LIN	Nomenclature	Qty
No equipment specified			

**Material Items (NSN)**

Step ID	NSN	LIN	Title	Qty
No equipment specified				

**Environment:** Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to FM 3-34.5 Environmental Considerations and GTA 05-08-002 ENVIRONMENTAL-RELATED RISK ASSESSMENT.

**Safety:** In a training environment, leaders must perform a risk assessment in accordance with FM 5-19, Composite Risk Management. Leaders will complete a DA Form 7566 COMPOSITE RISK MANAGEMENT WORKSHEET during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW FM 3-11.4, NBC Protection, FM 3-11.5, CBRN Decontamination. .