

Definition

Military deception operations are actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are as follows (JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*):

- *Strategic military deception.* Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations.
- *Operational military deception.* Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations.
- *Tactical military deception.* Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.
- *Service military deception.* Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.
- *Military deception in support of operations security.* Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities,

capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities.

Types of Deception Operations

A deception operation may contain one or more of the following: a feint, demonstration, ruse or display.

- A *feint* is a limited objective attack that involves contact with the enemy. A feint is conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. Feints may: (1) vary in size from a raid to a supporting attack, (2) occur before, during, or after the main attack, and (3) may be independent of the main effort. Feints may be employed to cause the enemy to react in one of three predictable ways: employ his reserves improperly, shift his supporting fires, and reveal his defensive fires.
- A *demonstration* is an attack or show of force on a front where a decision is not sought, made with the aim of deceiving the enemy. A demonstration differs from a feint in that no contact with the enemy is intended.
- A *ruse* is a trick of war to place false information in the enemy's hand. Ruses are generally single, deliberate actions. It may be necessary to group several ruses together to ensure credibility of a deception story. Ruses are extremely susceptible to detection because of inconsistency and may present the enemy with a windfall of information that he is inclined to reject.
- A *display* is a static portrayal of an activity force or equipment intended to deceive the enemy's visual observation. Displays are simulations, disguises or portrayals that project to the enemy the appearance of objects that do not exist or appear to be something else. Displays include simulations, disguises, decoys, and

dummies. They may include the use of heat, smoke, electronic emissions, false tracks, and fake command posts.

Deception in Support of the Offense

The adversary commander is the target for military deception in support of the offense. Goals may include the following:

- Achieve surprise.
- Preserve friendly forces, equipment, and installations from destruction.
- Minimize a physical advantage the enemy may have.
- Gain time.
- Cause the adversary to employ forces, including intelligence, in ways that are advantageous to the MAGTF.
- Cause the adversary to reveal strengths, dispositions, and future intentions.
- Influence the adversary's intelligence collection and analytical capability.
- Condition the adversary to particular patterns of friendly behavior that can be exploited at a time chosen by the MAGTF.
- Cause the adversary to waste combat power with inappropriate or delayed actions.

Deception in Support of the Defense

Military deception can help protect the MAGTF from adversary offensive IO efforts. Deception that misleads an adversary about friendly C2 capabilities or limitations contributes to friendly protection. An adversary commander who is deceived about friendly C2 capabilities and limitations may be more likely to misallocate resources in his effort to attack or exploit friendly C2 systems.

Operations Security and Deception

OPSEC and deception have much in common. Both require the management of indicators. OPSEC is used to deny information. OPSEC seeks to limit an adversary's ability to detect or derive useful information from his observations of friendly activities. Deception is used to feed information. Deception seeks to create or increase to the likely detection of, certain indicators that the enemy can observe and that will cause an adversary to derive an incorrect conclusion. In short, OPSEC is used to hide the real and deception is used to show the fake.

The Deception Planning Process

See also JP 3-58, *Joint Doctrine for Military Deception*.

Step 1. Deception Mission Analysis

Deception mission analysis is conducted as part of overall mission analysis that is performed by the MAGTF following receipt of a new mission.

Step 2. Deception Planning Guidance

After mission analysis, the commander issues planning guidance to the staff. In addition to other planning guidance, the commander states the deception objective for the operations.

Step 3. Staff Deception Estimate

- The deception estimate is conducted as part of the operations estimate.
- Deception COAs are developed that restate the deception objective, identify the deception target and desired perception, and outline a deception story with potential deception means.
- COA strengths and weaknesses are analyzed.

Step 4. Commander's Deception Estimate

The MAGTF commander selects an operational deception COA for OPLAN development and issues any additional guidance.

Step 5. Deception Plan Development

Developing the complete deception plan is the most time-consuming part of the deception planning process. The five major actions in this step are as follows:

- Complete the deception story.
- Identify the deception means.
- Develop the event schedule.
- Identify feedback channels.
- Develop the termination concept.

Step 6. Deception Plan Review and Approval

The MAGTF commander reviews and approves the completed deception plan as part of the normal OPLAN review and approval process. Need-to-know criteria remain in effect and only a limited number of personnel will participate in this step.

Special Considerations for Deception Planning

Classification

Due to the sensitive nature of deception operations, deception planning is restricted to those personnel who have a strict need-to-know. Deception operations depend on the knowledge and utilization of enemy intelligence collection systems to deliver a deception story to an adversary. Compromise of friendly knowledge of enemy intelligence systems would be harmful and could have far-reaching strategic and operational effects.

Unintended Effects

Third parties, e.g., neutral or friendly forces not aware of the deception, may receive and act upon deception information that is intended for the

enemy. Deception planners should minimize the risk to other parties.

Responsibilities

The G-3/S-3 has primary responsibility for deception. Normally, a deception officer is appointed and is responsible to the G-3/S-3 for deception planning and oversight.

Deception and the Operation Order

Tab A to Appendix 3 (IO) of Annex C (Operations) of the OPOD is the deception tab. This tab implements the recommended COA for deception. It details the specific deception tasks to be performed and specifies coordinating instructions for the control and management of deception missions.

Electronic Warfare

Definitions

Electronic Warfare

Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or the attack the enemy. The three major subdivisions within EW are: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). (JP 1-02)

Electronic Attack

Electronic attack is that division of EW involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: (1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and