Joint Publication 3-13.4

Military Deception

14 February 2017

PREFACE

1. Scope

This publication provides joint doctrine to plan, execute, and assess military deception in support of joint operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs), and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces in preparing and executing their plans and orders. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of objectives.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, subordinate unified commands, joint task forces, subordinate components of these commands, the Services, and combat support agencies.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the CJCS, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the US, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

KEVIN D. SCOTT
Vice Admiral, USN
Director, Joint Force Development

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-13.4
DATED 26 JANUARY 2012

- **Consolidated multiple general information paragraphs into an introduction section.**
- **Clarified that military or *other valid decision makers* may be the deception target.**
- **Added a figure outlining a sample information pathway to show how information can move through a conduit to a decision maker.**
- **Added a figure to illustrate various leadership styles planners should consider when evaluating the deliberative process a decision maker or body uses to reach a conclusion.**
- **Added a section to reinforce the linkage between operations security and military deception.**
- **Added a more expansive analysis of prohibited military deception in accordance with DOD Law of War Manual.**
- **Added a section on cyberspace contributions to military deception in the classified appendix.**
- **Expanded the discussion on military deception and irregular warfare in the classified appendix.**
- **Expanded the discussion on violent extremist organization susceptibility to deception operations in the classified appendix.**
- **Expanded the discussion on human intelligence support to operations in the classified appendix.**
- **Modifies, adds, and removes terms and definitions from the DOD Dictionary of Military and Associated Terms.**

Intentionally Blank

TABLE OF CONTENTS

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides a General Overview of Military Deception**
- **Discusses Military Deception and Information Operations**
- **Covers Roles, Coordination, and Considerations for Military Deception**
- **Explains Intelligence Support to Military Deception**
- **Discusses Military Deception Planning**
- **Discusses Execution of Military Operations**
- **Discusses Counterdeception**

General Overview of Military Deception

Introduction

Military deception (MILDEC) is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. When properly integrated with operations security (OPSEC), other information-related capabilities (IRCs), and the visible activities of the joint force and its components, MILDEC can be a decisive tool in altering how the adversary views, analyzes, decides, and acts in response to friendly military operations.

The Functions and Role of Military Deception

MILDEC can mask, protect, reinforce, exaggerate, minimize, distort, or otherwise misrepresent US technical and operational capabilities, intentions, operations, and associated activities. When properly resourced and integrated, MILDEC has the potential to deter or induce actions that are favorable to the joint force and thus increase the success of friendly activity.

Military Deception and Information Quality

Information quality refers to the accuracy, completeness, relevance, and believability of information available for decision making. MILDEC should affect the quality of information available for adversary decisions.

Military Deception Planning Methodology

The following interrogatories describe the **"see, think, do" deception methodology** process:

- See: Does the target see the deceptive event?
- Think: Does the target conclude the observations are valid?
- Do: What action or inaction may the target take or not take as a result of the conclusions based upon those observations?

Tenets of Military Deception

Just as the principles of war provide general guidance for the conduct of military operations, the six tenets of MILDEC provide guidance to plan and execute MILDEC operations. The tenets are focus, objective, centralized planning and control, security, timeliness, and integration.

Military Deception and Information Operations

Military Deception as an Information-Related Capability

While MILDEC uses a broad spectrum of techniques, tactics, and means to portray inaccurate friendly capabilities and intentions, its success is dependent on the application of other IRCs to enable the delivery of deceptive information and to disrupt accurate adversary information collection, content, and flow to decision makers. Successful MILDEC also requires a holistic and seamless integration with OPSEC to conceal or protect vulnerable physical, technical, and administrative indicators of our true capabilities and intent.

Information Operations Planning

The joint force commander's (JFC's) senior MILDEC planner is normally a standing member of the information operations (IO) cell. Within the IO cell, the MILDEC planner provides deception plan information to incorporate and deconflict MILDEC with other IRCs.

Military Deception and Camouflage, Concealment, and Decoys

Camouflage and concealment are OPSEC measures used to protect friendly forces and activities from adversary detection and attribution. Decoys may be used in conjunction with other MILDEC activities to mislead adversary intelligence collection and direct the adversary's attention away from actual forces.

Roles, Coordination, and Considerations for Military Deception

Roles and Responsibilities of Military Deception Planners

JFCs make the decision to use MILDEC after evaluating the analysis and recommendations from the joint planning process (JPP). According to their specific planning responsibilities (tailored to clearances, access levels, and need to know of specific individuals), the **operations directorate of a joint staff (J-3)/plans directorate of a joint staff (J-5)** supervise the incorporation of MILDEC into the IO portion of operations estimates. Based on these estimates, the J-3/J-5 recommend various options for IO (including MILDEC) to the commander. Once the JFC has selected a particular IO course of action (COA) and received approval through the chain of command, the J-3/J-5 supervise the completion of planning for the selected COA. The J-3 normally supervises MILDEC execution. The **command military deception officer (CMDO)** is the primary designated officer with overall oversight and management responsibility for each MILDEC program within the combatant commands (CCMDs), agencies, and Service components which support joint military operations. The **military deception officer (MDO)** works closely with the CMDO to ensure all component MILDEC plans are in accordance with command and Department of Defense guidance and policy. The **MILDEC planner** plans and executes MILDEC plans within their organization.

Coordination Requirements

The Joint Staff J-3 [Operations Directorate] supports the combatant commanders in development, assessment, coordination, and recommendation of MILDEC options. The Joint Staff J-3 ensures CCMD MILDEC requirements do not conflict with MILDEC operations occurring in other areas of responsibility. The JFC-designated IO cell chief is normally the single point of contact to manage and obtain coordination requirements and related points of contact information pertaining to the deception element. However, a JFC may want to appoint a CMDO who would be the single manager for MILDEC.

Intelligence Support to Military Deception

General

Focused intelligence support is essential to the successful planning, execution, and assessment of any MILDEC.

The Deception Intelligence Estimate

The deception intelligence estimate (DIE) is a specialized intelligence product derived from the intelligence directorate of a joint staff's (J-2's) joint intelligence preparation of the operational environment and responses to situation-specific requests for information submitted by MILDEC planners. The DIE is a "living" product. It is refined as additional information and intelligence become available, or as conditions evolve and change within the operational environment.

Conduit Analysis

Conduit analysis is the detailed mapping of individual conduits or information pathways to the potential deception target(s). A simple conduit is one which transmits data to the intended decision maker without the application of an intermediate filter. A complex conduit is one which includes one or more filters that might substantially alter the content, add context to the observable, or alter the timeframe for delivery.

Support to Military Deception Assessment

One way to easily conceptualize measures of performance (MOPs) and measures of effectiveness (MOEs) for MILDEC is to use the "see, think, do" methodology. A MOP is most closely associated with **see**: did we portray the planned indicator, and did the adversary see our execution and transmit the desired message to the deception target creating an observable? MOEs are associated with **think** and do: what perceptions and conclusions did the adversary draw from a particular observable (alone or in the context of other observations), and are those perceptions leading toward the desired action/inaction captured in a deception objective?

Military Deception Planning

Military Deception Planning and Joint Planning Processes

To ensure proper integration with the commander's objectives and desired end state, MILDEC planning is conducted as part of the JPP. Because of its inherent sensitivity, access to MILDEC planning is usually protected. MILDEC planning takes place in an access-

controlled, parallel planning process rather than through open discussion in the joint planning group or the IO working group.

Military Deception Planning Basics

The deception planning cell (DPC) oversees MILDEC planning and execution. The DPC normally consists of the CMDO, any MILDEC planners appointed by the command, and the component MDOs. In most circumstances, the DPC will form a larger deception operations working group to facilitate the planning, coordination, and discrete integration of MILDEC throughout planning, execution, and assessment.

The Military Deception Planning Process

The MILDEC planning process is an iterative process that requires continual reexamination and validation throughout the planning and execution phases. The MILDEC planning process consists of five steps that generally align with similar activities in the JPP. The steps are: deception mission analysis, deception concept development, deception concept approval, deception plan development, and deception plan review and approval.

Execution of Military Operations

Execution of Military Deception Events and Actions

The MILDEC plan is normally executed as a component of the operation plan/operation order. When a CCMD or functionally organized joint task force receives an execute order for a given plan, the associated MILDEC plan may also be activated within the given authorities and approval processes as outlined in Chairman of the Joint Chiefs of Staff Instruction 3211.01, *(U) Joint Policy for Military Deception.*

Deception Execution Coordination

Once a plan is activated, it is critical that constant coordination at the strategic, operational, and tactical levels continues. There is potential for a tactical or operational level deception to have strategic implications. With this in mind, a continual process of coordination, called the deception execution cycle, must take place.

Terminating Military Deception Operations

The termination of a MILDEC is concerned with ending the MILDEC in a way that protects both the short- and long-term interests of the command. When termination is ordered, the selected termination concept becomes the basis for final termination actions. These actions conclude the operation in line with the deception events that have been executed, the assessed state of awareness

of the target, and the commander's specific termination objectives at the time.

Counterdeception

Counterdeception as an Element of Military Deception

Counterdeception is an effort to detect, confirm, and subsequently negate, neutralize, or diminish the effects of, or gain advantage from, a foreign deception operation. Friendly decision makers must be aware of adversary deception activities so they can formulate informed and coordinated responses, but more importantly, so that friendly forces are not placed at an operational disadvantage. Knowledge of an adversary's deception plan enables a commander to take appropriate action against the deception. It also provides an opportunity to gain valuable insight into the means used to portray the deception and analyze adversary deception targets and objectives as an indicator of the broader context in which the adversary views friendly forces and operations.

Detecting Adversary Deception

The intelligence community (IC) has the primary responsibility to identify adversary deception. The first step in identifying adversary deception is to understand the adversary's deception doctrine, techniques, capabilities, and limitations. Knowing how the adversary has used deception in the past is also important. The DPC and the J-2, supported by the broader IC, collaborate to collect and provide this information as part of the DIE.

Confirming Adversary Deception

If intelligence reveals or suggests adversary deception activity, it is the responsibility of the JFC staff to fully analyze the situation and ensure that this intelligence and its potential impact on the friendly operation are presented to the commander. One method is to form a counterdeception working group (CWG) to perform this function. A sample CWG might consist of the CMDO, selected component MDOs, J-2 analysts, IC liaison officers if assigned, red team members, J-3 planners, and any other staff members who could provide expertise on the suspected adversary deception means or methods.

Countering or Exploiting Adversary Deception

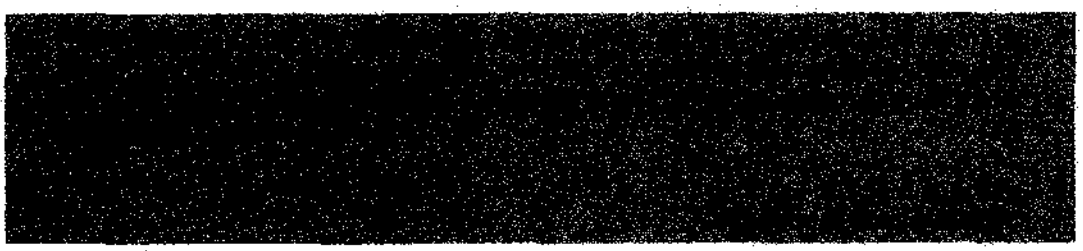
After an adversary's deception operation is confirmed, the CWG has two primary functions. The first is to examine past intelligence collection and analysis to determine the impact the deception may have had on

friendly planning, decision making, or current operational activities. The second function of the CWG is to develop and present proposed counterdeception COAs to the commander.

CONCLUSION

This publication provides joint doctrine to plan, execute, and assess MILDEC in support of joint operations.

CHAPTER I
GENERAL



1. Introduction

a. Military deception (MILDEC) is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. MILDEC is applicable at all levels of warfare, across the range of military operations, and can be conducted during all phases of military operations. When properly integrated with operations security (OPSEC), other information-related capabilities (IRCs), and the visible activities of the joint force and its components, MILDEC can be a decisive tool in altering how the adversary views, analyzes, decides, and acts in response to friendly military operations. This concept is incorporated in the "see, think, do" methodology that guides MILDEC planning, execution, and assessment. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3211.01, *(U) Joint Policy for Military Deception,* provides joint policy guidance for MILDEC. This joint publication (JP) provides authoritative guidance and best practices to conduct MILDEC. For more specific information concerning responsibilities related to MILDEC, and more specific guidance and restrictions relating to MILDEC in support of joint operations, refer to CJCSI 3211.01, *(U) Joint Policy for Military Deception.*

b. Due to the potentially sensitive nature of MILDEC activities and selected means, MILDEC planners should consider appropriate security and classification measures to properly safeguard MILDEC tactics, techniques, and procedures. The MILDEC planning process and its integration into the overall joint force plan will be discussed in more detail in Chapter V, "Military Deception Planning."

2. The Functions and Role of Military Deception

a. MILDEC has been an aspect of warfare since antiquity. It is most closely aligned with the achievement of surprise and the battlefield displacement of critical adversary capabilities away from the friendly point of action. The functions of MILDEC include, but are not limited to,

(1) Causing ambiguity, confusion, or misunderstanding in adversary perceptions of friendly critical information and indicators such as unit identities, locations, movements, dispositions, weaknesses, capabilities, strengths, supply status, and intentions.

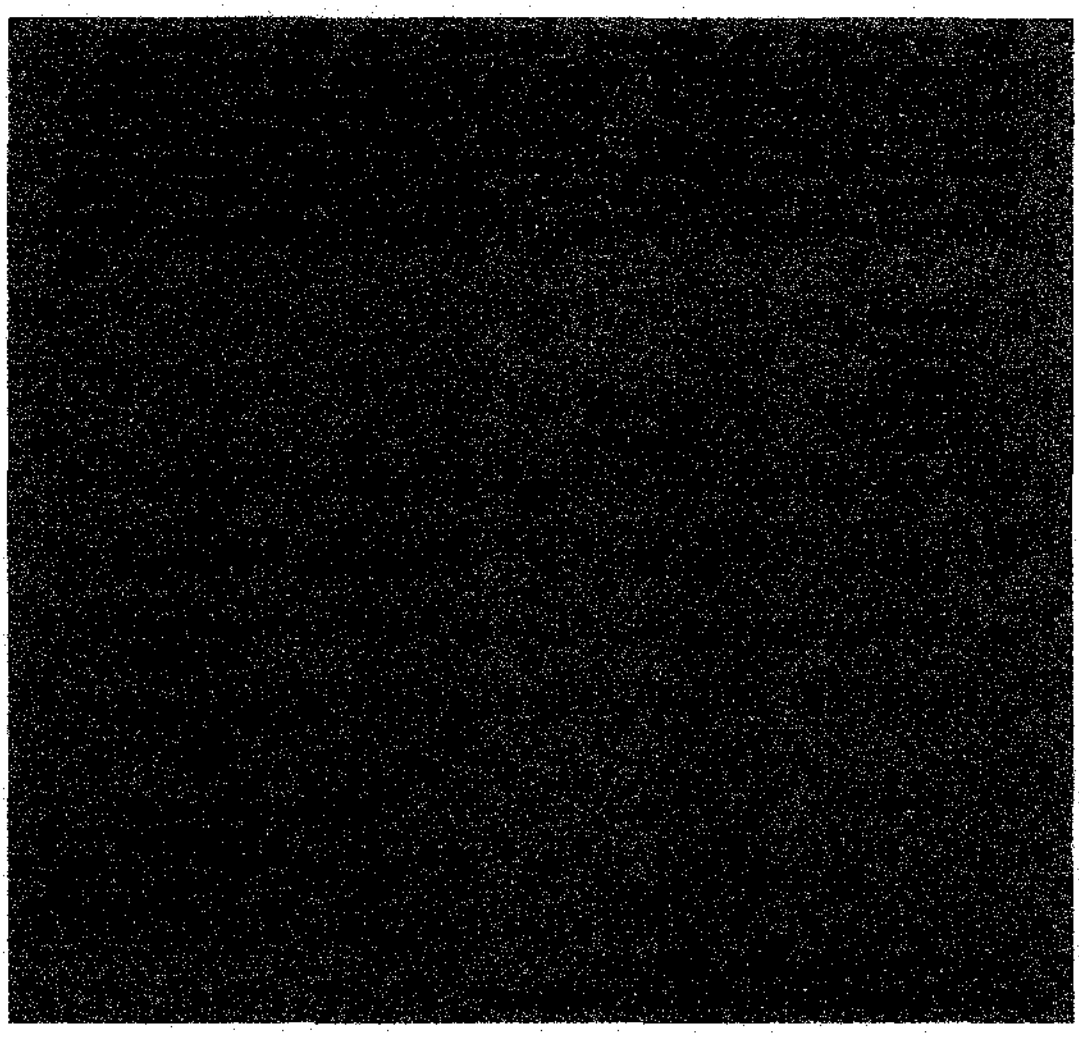
(2) Causing the adversary to misallocate personnel, fiscal, and material resources in ways that are advantageous to the friendly force.

(3) Causing the adversary to reveal strengths, dispositions, and intentions.

(4) Conditioning the adversary to particular patterns of friendly behavior to induce adversary perceptions that can be exploited by the joint force.

(5) Causing the adversary to waste combat power and resources with inappropriate or delayed actions.

b. MILDEC can play a pivotal role in the accomplishment of the commander's objectives and significantly reduce risk. MILDEC can mask, protect, reinforce, exaggerate, minimize, distort, or otherwise misrepresent US technical and operational capabilities, intentions, operations, and associated activities. When properly resourced and integrated, MILDEC has the potential to deter or induce actions that are favorable to



the joint force and thus increase the success of friendly activity. MILDEC can be a critical enabler to achieving operational surprise and maintaining the initiative in offensive operations.

c. MILDEC activities are planned to support objectives detailed in concept plans (CONPLANs), operation plans (OPLANs), and operation orders (OPORDs) associated with approved military operations or activities. There are three categories of MILDEC supporting joint military operations:

(1) **Joint MILDEC.** Joint MILDEC is planned and conducted in a theater of operations to support military campaigns and major operations. Joint MILDEC activities are planned and executed by, and in support of, combatant commanders (CCDRs), joint force commanders (JFCs), and joint task force (JTF) commanders to cause adversaries to take actions or inactions that are favorable to the US commander's objectives. The majority of combatant command (CCMD)-planned and executed MILDEC will be joint MILDEC to create operational-level effects. Joint MILDEC is normally planned prior to, and conducted during, combat operations.

(2) **Tactical Deception (TAC-D).** TAC-D is deception activity planned and executed by, and in support of, tactical-level commanders to cause adversaries to take actions or inactions favorable to the tactical commanders' objectives. TAC-D is conducted to influence military operations in order to gain a tactical advantage over an adversary, mask vulnerabilities in friendly forces, or to enhance the defensive capabilities of friendly forces. TAC-D is unique to the tactical requirements of the local commander and not necessarily linked or subordinate to a greater joint MILDEC plan.

(3) **Deception in Support of Operations Security (DISO).** DISO conveys or denies selected information or signatures to a foreign intelligence entity (FIE) and limits the FIE's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets. DISO differs from joint MILDEC and TAC-D plans in that it only targets FIEs and is not focused on generating a specific adversary action or inaction.

3. Military Deception and Information Quality

a. Information quality refers to the accuracy, completeness, relevance, and believability of information available for decision making. MILDEC should affect the quality of information available for adversary decisions in the following ways:

(1) Deliberately present misleading information and indicators to adversaries to degrade the **accuracy** of adversary information.

(2) Give adversary decision makers a false sense of **completeness** of their understanding about friendly forces or intentions.

(3) Cause the adversary to misjudge the **relevance** of available information and misallocate operational or intelligence resources.

(4) Cause adversaries to **doubt the veracity** of their own intelligence assessments.

b. Care should be taken to protect the quality of information available for friendly decisions and public dissemination by instituting internal processes to identify and isolate information generated as a by-product of any MILDEC activity. This will help prevent the JFC from reaching erroneous conclusions because the staff unknowingly integrated the content or output of the JTF's MILDEC efforts as accurate information. This will also ensure the information made public by the JFC is not part of any MILDEC action that would result in a loss of public trust.

4. Military Deception Planning Methodology

a. As with all joint planning, MILDEC planning is an iterative process that requires continual reexamination of its goals, objectives, targets, stories, and means. Commanders and their staffs must respond to the dynamics of the situation and of their own headquarters.

b. **"See, Think, Do" Deception Methodology.** Successful deception operations are those that do more than make the target **believe** or **think** the deception is true. MILDEC must end in a decision maker's action, or inaction, that supports the JFC's operation. The "see, think, do" methodology is based on historical lessons of successful deceptions, from ancient times to Operation DESERT STORM. The goal of this methodology is to manipulate the cognitive process in the deception target's mind that leads to target decisions that result in adversary actions that are advantageous to the JFC (see Figure I-1). The following interrogatories describe the process:

(1) See: Does the target see the deceptive event?

(2) Think: Does the target conclude the observations are valid?

(3) Do: What action or inaction may the target take or not take as a result of the conclusions based upon those observations?

5. Military Deception Overview

The following sections and paragraphs outline basic terms and concepts necessary for the joint force planner or staff officer to understand the fundamentals of MILDEC. A detailed discussion of their application can be found in Chapter V, "Military Deception Planning."

a. **Deception Goal and Deception Objectives.** The deception goal and associated deception objective(s) are key outputs of MILDEC mission analysis and the foundation for subsequent MILDEC planning. They provide the commander and MILDEC planners with a solid understanding of how the deception supports the overall operation and establishes the conceptual framework for planning and executing MILDEC.

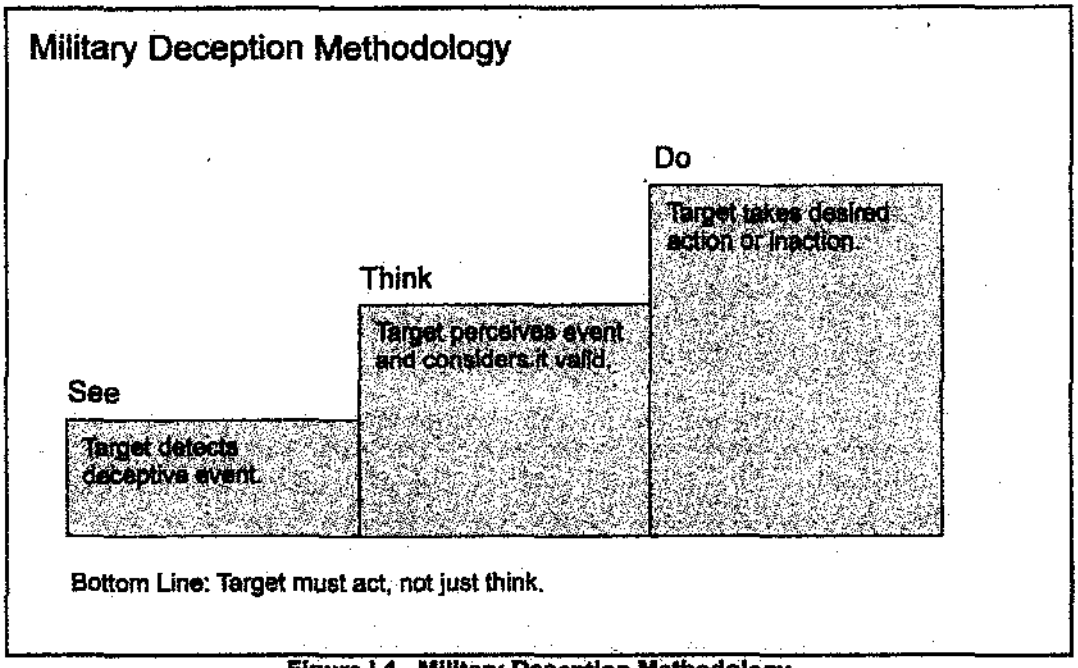


Figure I-1. Military Deception Methodology

(1) The **deception goal** is the commander's statement of the purpose of the MILDEC as it contributes to the successful accomplishment of the assigned mission. The deception goal is usually stated as a positive friendly advantage or condition such as: "Successful MILDEC will create a decisive combat power advantage for the coalition main effort attack along AXIS MONTANA." MILDEC is not an end to itself. Like any other form of military operation, the measure of success for MILDEC is its direct contribution to the accomplishment of the mission. MILDEC often requires substantial investments in effort and resources that would otherwise be applied against the adversary in a more direct fashion. Consequently, it is important for the commander to first envision the deception goal in terms of its specific contribution to accomplishing the designated mission.

(2) The **deception objective** is a concise statement of what MILDEC will cause the adversary to do or not do. It is expressed in terms of adversary action or inaction that directly leads to the advantage or condition stated in the deception goal. For example: "Successful MILDEC will cause the adversary to hold their armored reserve in a position or status unable to impact forces along AXIS MONTANA through D+36 hours." Deception objectives are the desired outcome of the MILDEC operation.

b. **The deception target** is the adversary military or other valid decision maker with the authority and means to make the decision and subsequently direct the action or inaction of the military capability captured in the MILDEC objective. The deception target or targets are the key individuals on whom the entire deception operation will be focused.

c. **Conduits and Filters**

(1) **Deception conduits** are information or intelligence pathways to the deception target. Collectively, they define how the adversary will register or "see" activity in the information environment and how those observations are transmitted, processed, and ultimately delivered to the decision maker. The MILDEC planner chooses and deconflicts access to specific conduits in order to deliver a synchronized portrayal of selected information and indicators. In general terms, an individual conduit consists of a sensor that registers a signature, a transmission means from the sensor to an intermediate node or nodes that might act on the information in a variety of ways, and delivery to the deception target(s).

(2) In general terms, conduits consist of all the systems, organizations, and individuals through which information reaches the target. The selection of appropriate conduits is a critical part of the process of developing a successful MILDEC plan. A **filter** is any node within a conduit that applies aggregation, synthesis, or bias to the observable on its path to the deception target. MILDEC planners must understand the detailed construct, filtering, and estimated function time of each conduit, relationships and redundancy with other conduits, and their comparative value as perceived by the target in order to craft the most effective portrayal of the deception story.

d. **Desired Perceptions and the Deception Story**

(1) **Desired perceptions** are the conclusions, official estimates, and assumptions the MILDEC target must believe in order to make the decision that will achieve the MILDEC objective (think). These adversary perceptions will be formed from both objective (observation and analysis) and subjective (intuition and experience) analysis. They are also heavily impacted by biases, preconceptions, and filters applied in the collection, analysis, delivery, and reception of information.

(2) The **deception story** is a scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. It is a succinct statement or narrative of exactly what the MILDEC planner wants the target to believe to be the true situation, then decide and act on that basis. The deception story should read like the adversary's intelligence estimate about friendly forces' actions and intentions. The deception story identifies those friendly actions, both real and simulated, that, when observed by the deception target, will lead it to develop the desired perception. Deception story development is both an analytic and creative process that involves a variety of information on enemy data acquisition and processing.

e. **Indicators, Observables, and Competing Observables**

(1) An **indicator** is information or a detectable action (specific facts or evidence) that is likely to be interpreted or pieced together by an adversary to form assumptions and assessments about friendly activity, capability, and intent. MILDEC planners work to identify key indicators that align with the friendly activities, capability, and intent portrayed by the deception story. These include visible elements and selected

indicators of the actual JFC's course of action (COA), as well as indicators that must be created using deceptive activities or means to mislead and deceive. It is generally desirable to have a very high ratio of actual (truthful) versus deceptive indicators for a deception and the associated deception story to be believable, verifiable, consistent, and executable.

(2) The key link between selected indicators and the deception story is the tentative identification of one or more adversary conduits that the indicator will be exposed to. The combination of an indicator with an adversary conduit creates an **observable.** Unless exposed to one or more active conduits, an indicator is ineffective in conveying the deception story: the adversary cannot register or respond to what they cannot see.

(3) A **competing observable** is any observable that contradicts the deception story. In order to minimize the impact of competing observables on adversary cognition, they must be mitigated as part of the MILDEC plan. Examples of mitigation for competing observables include protection with OPSEC, including DISO; incorporation into the deception story; neutralization of the adversary conduit to which they are likely to be exposed; or assumption of risk based on detailed analysis of minimal impact to the operation.

6. Tenets of Military Deception

Just as the principles of war provide general guidance for the conduct of military operations, the six tenets of MILDEC (see Figure I-2) provide guidance to plan and execute MILDEC operations.

a. **Focus.** MILDEC should target the adversary decision maker capable of causing the desired action(s). The collection system is normally not the target; rather, it is the primary conduit used in MILDEC to convey selected information to the decision maker.

b. **Objective.** The principal objective of MILDEC operations is to focus actions and resources to cause an adversary to take (or not to take) specific actions, not just to believe certain things.

c. **Centralized Planning and Control.** MILDEC operations should be centrally planned and directed. This approach is required in order to avoid confusion and to ensure the various elements involved in MILDEC portray the same story and are not in conflict with other operational objectives or evolving conditions in the operational environment. Execution of MILDEC may, however, be decentralized as long as all participating organizations adhere to a single plan.

d. **Security.** Successful MILDEC operations require strict security. This begins prior to execution with measures to deny knowledge of the friendly force's intent to deceive. Apply strict need to know criteria to each MILDEC operation and to each aspect of that operation. Employ active OPSEC to deny critical information about both actual operations and MILDEC activities; knowledge of MILDEC plans and orders must be carefully protected. To ensure adequate protection of information, all MILDEC

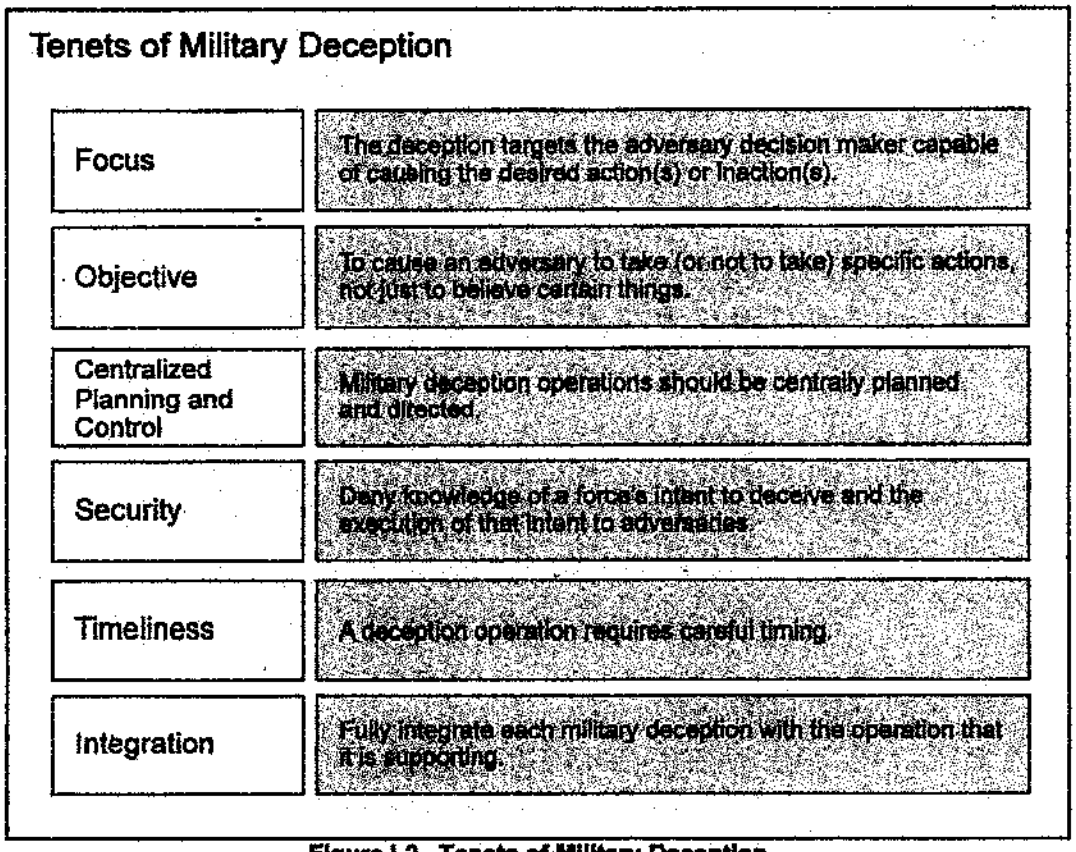


Figure I-2. Tenets of Military Deception

information must be correctly classified and handled in accordance with the *Joint MILDEC Security Classification Guide.*

e. **Timeliness.** A MILDEC operation requires careful timing. Sufficient time must be provided for its portrayal; for the adversary conduits to collect, analyze, and report; for the adversary decision maker to react; and for the friendly intelligence collection system to detect the action resulting from the adversary decision maker's decision. Further detection may lead to a decision point, requiring a friendly commander's decision on how to proceed with an operation.

f. **Integration.** Fully integrate each MILDEC with the operation that it is supporting. The development of the MILDEC concept must occur as part of the development of the commander's concept of operations (CONOPS). MILDEC must be considered early in planning at all levels to ensure subordinate deception plans are integrated within higher-level plans.

7. Military Deception Types, Techniques, Tactics, and Means

a. **Deception Types.** There are two generally recognized types of military deception: ambiguity increasing and ambiguity decreasing. More complex operational

level deceptions might combine both ambiguity increasing and decreasing types of deception. Operation BODYGUARD protected the World War II Allied D-Day landings in Normandy with the threat of parallel invasions through Norway and the Balkans (ambiguity increasing) while simultaneously convincing the Germans that any invasion through France would occur at the Pas-de-Calais (ambiguity decreasing).

(1) **Ambiguity increasing deception** provides the adversary with multiple plausible and equally viable friendly COAs. Ambiguity increasing type deceptions are designed to generate confusion and conflict in the mind of the adversary decision maker. Anticipated effects of an ambiguity increasing type deception can include operational paralysis or the distribution of adversary forces to locations well away from the intended location of the friendly efforts.

(2) **Ambiguity decreasing deceptions** cause the adversary decision maker to be "very certain and very wrong." Anticipated effects of the ambiguity decreasing type of deception normally include the displacement of key adversary resources and increased operational surprise relative to the timing, location, or method of the friendly main effort. Ambiguity decreasing deceptions cause the adversary to be "at the wrong place, at the wrong time, with the wrong stuff."

b. **Deception Techniques.** Deception techniques can be characterized as operational-level constructs that encompass a broad range of deceptive activity and information (including tactics and means) integrated as a component of the overall plan. MILDEC operations apply four basic deception techniques: feints, demonstrations, ruses, and displays.

(1) **Feints.** A feint is an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action.

(2) **Demonstrations.** A demonstration is a show of force where a decision is not sought and no contact with the adversary is intended. A demonstration's intent is to cause the adversary to select a COA favorable to friendly goals.

(3) **Ruses.** A ruse is designed to deceive the adversary to obtain friendly advantage. It is characterized by deliberately exposing false or confusing information for collection and interpretation by the adversary.

(4) **Displays.** Displays are the simulation, disguising, and/or portrayal of friendly objects, units, or capabilities in the projection of the MILDEC story. Such capabilities may not exist, but are made to appear so (simulations) (e.g., show of force).

c. **Deception Tactics.** Deception tactics may be employed in a localized manner or as a component of a larger deception technique. The application of tactics varies with each operation depending on variables such as time, assets, equipment, and objectives, and is assessed for feasibility accordingly. Sample MILDEC tactics include:

(1) Amplifying signatures to make a force appear larger and more capable or simulate the deployment of critical capabilities.

(2) Suppressing signatures to make a force appear smaller and less capable or to conceal the deployment of critical capabilities.

(3) "Dazzling" adversary sensors by overloading them with multiple false indicators and displays to distract or dissipate their collection assets.

(4) "Repackaging" known organizational or capability signatures to generate new or deceptive profiles that increase or decrease the ambiguity of friendly activity or intent.

(5) "Conditioning" to desensitize the adversary to particular patterns of friendly behavior and induce adversary perceptions that are exploitable at the time of friendly choosing.

d. **Deception Means.** Deception means are resources, methods, or techniques used to portray selected information and indicators to the deception target. Deception means are divided into three basic categories: physical, technical, or administrative. An individual deception means may have multiple attributes that allow it to be characterized in more than one category. MILDEC means are normally applied in a complementary manner that misleads multiple types of adversary sensors to increase credibility and the likelihood of creating the desired perception. This grouping of related deception events or executions is referred to as a deception series.

(1) **Physical Means.** Physical means are resources, methods, and techniques used to convey or deny information or signatures normally derivable from direct observation or active sensors by the deception target. Most physical means also have technical signatures visible to sensors using scientifically or electronically enhanced collection. Physical means are normally evaluated by characteristics such as shape, size, function, quantity, movement pattern, location, activity and association with their surroundings. Examples include:

(a) Movement of forces.

(b) Exercises and training activities.

(c) Decoy equipment and devices.

(d) Tactical actions.

(e) Logistics actions, and location of stockpiles and repair facilities.

(f) Visible test and evaluation activities.

(g) Reconnaissance and surveillance activities.

(2) **Technical Means.** Technical means are resources, methods, and techniques used to convey or deny selected information or signatures to or from the deception target by manipulating electromagnetic (EM), acoustic, or other forms of energy or through olfaction. Technical means may be applied in conjunction with corresponding physical means or may be used alone to replicate a physical means absent direct visual observation by the adversary. As with any use of US military material resources, any use of technical means to conduct MILDEC must comply with US and international law. Examples of technical means include:

(a) The establishment of communication networks and interactive transmissions that replicate a specific unit type, size, or activity.

(b) Emission or suppression of chemical or biological odors associated with a specific capability or activity.

(c) Multi-spectral simulators that replicate or mimic the known electronic profile of a specific capability or force.

(d) Selected capabilities that disrupt an adversary sensor or affect data transmission.

(3) **Administrative Means.** Administrative means are resources, methods, and techniques to convey or deny selected written, oral, pictorial, or other documentary information or signatures to or from the deception target. They normally portray information and indicators associated with coordination for ongoing or planned military activity to the deception target. Examples of administrative means normally visible to an adversary at some level include:

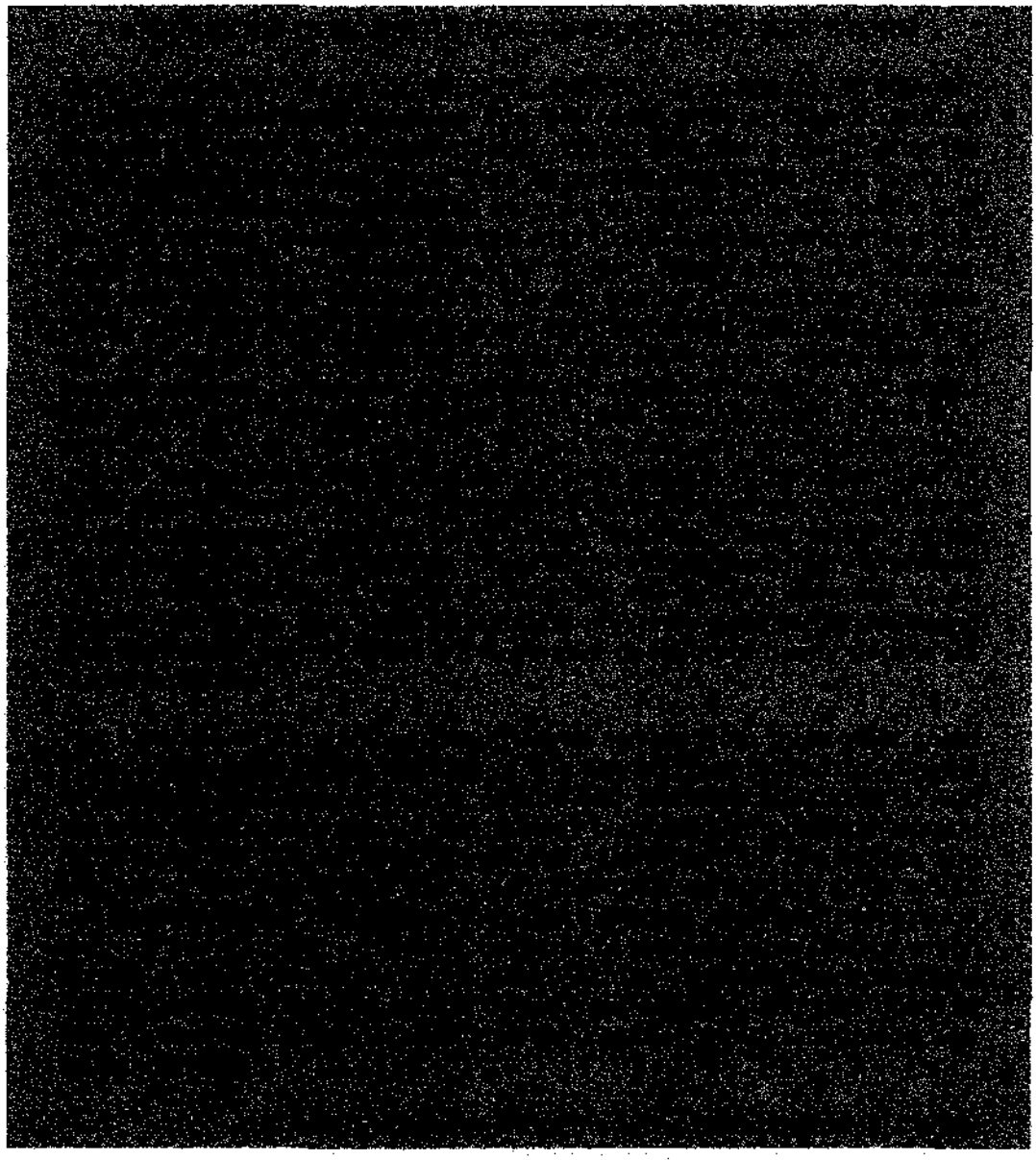
(a) Contracting activity for services or supplies.

(b) Movement, transit, or overflight requests including flight planning, port call, or traffic control coordination.

(c) Basing inquiries; construction requests.

(d) Other preparatory coordination associated with a military operation that is normally done through unclassified channels.

e. **Unlawful Deceptions.** Certain MILDEC activities or techniques are prohibited because they violate the law of war, including killing or wounding the enemy by resort to perfidy. Acts of perfidy are acts that are designed to invite the confidence of an enemy to lead him to believe that he is entitled to, or obliged to accord, protection under the law of war, with intent to betray that confidence. Moreover, the law of war prohibits misusing certain protected signs such as the Red Cross or Red Crescent, fighting in the enemy's uniform, and feigning nonhostile relations in order to seek a military advantage. These actions are prohibited because they undermine the protections afforded by the law of war to civilians, persons who are hors de combat, or other protected classes of persons and



objects; impair nonhostile relations between opposing belligerents; and may damage the basis for the restoration of peace.

For further guidance on unlawful deception, refer to the Department of Defense's Law of War Manual (June 2015), *Sections 5.21 through 5.25.*

8. Assessment

Assessment is an essential and resource-intensive aspect of any successful MILDEC and must be considered from the initiation of planning. Deception objectives that cannot be associated with a progressive and observable adversary response are not preferred for

development into a more detailed deception concept or subsequent execution. MILDEC is assessed in the same manner as other operations: using measures of performance (MOPs) to determine if a MILDEC event was executed according to plan and measures of effectiveness (MOEs) to determine if the event created the desired impact or effect. In MILDEC operations, MOPs involve everything up to and including delivery of the observable (filtered or unfiltered) to the deception target. Accurately assessing MOEs for MILDEC is complicated by the fact that MILDEC planners need to measure desired changes in perception, as well as the action/inaction manifested by their success. Because of this complexity, each planned deception event should be accompanied by a detailed assessment plan that includes MOPs, MOEs, and coordination with the intelligence directorate of a joint staff (J-2) for intelligence collection assets to collect and report indicators in real-time. A more detailed discussion of MILDEC assessment is found in Chapter IV, "Intelligence Support to Military Deception."

Intentionally Blank

CHAPTER II
MILITARY DECEPTION AND INFORMATION OPERATIONS

1. Information Operations

Information operations (IO) are the integrated employment, during military operations, of IRCs in concert with other lines of operation (LOOs) to influence, disrupt, corrupt, or usurp the decision making of adversaries while protecting our own.

For further guidance on IO, refer to JP 3-13, Information Operations.

2. Military Deception as an Information-Related Capability

A properly planned and executed MILDEC is one of the most effective IRCs available to the JFC. It can directly influence, corrupt, disrupt, and usurp the adversary's military decision-making process and the subsequent direction of their forces. MILDEC targets the informational and cognitive processes of the adversary military decision maker by using means and information to lead them to incorrect conclusions about friendly capabilities and intentions. This in turn causes the adversary decision maker to respond to a faulty construct of the operational environment and order the action or inaction of critical capabilities that, when misallocated, generate a planned friendly advantage and substantially reduce risk to the friendly mission and forces. In order to create these effects, MILDEC must be integrated not only with the overall plan, but very closely with other IRCs, in both parallel and mutually supporting activities. While MILDEC uses a broad spectrum of techniques, tactics, and means to portray inaccurate friendly capabilities and intentions, its success is dependent on the application of other IRCs to enable the delivery of deceptive information and to disrupt accurate adversary information collection, content, and flow to decision makers. Successful MILDEC also requires a holistic and seamless integration with OPSEC to conceal or protect vulnerable physical, technical, and administrative indicators of our true capabilities and intent.

3. Military Deception's Relationship to Information-Related Capabilities

IRCs play a coordinated and interrelated role in the overall MILDEC effort. In many cases, IRCs provide the specific means for accomplishing a MILDEC task. Just as MILDEC is integrated with the overall plan, it must also be coordinated and deconflicted with IRC plans to eliminate potentially counterproductive activities. This is normally accomplished through the operations directorate of a joint staff (J-3) or other IO planning staff. Not all IRC planners will be fully cognizant of the existence or extent of MILDEC activity; access to the plan remains on a need to know basis.

a. MILDEC and OPSEC

(1) OPSEC is a capability that identifies and controls critical information indicators of friendly force actions attendant to military operations and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. The purpose of OPSEC is to reduce the vulnerability of US and multinational forces from successful adversary exploitation of critical information. Joint forces often display personnel, organizations, assets, and actions to public view and to a variety of adversary intelligence collection activities, including sensors and systems. Joint forces can be under observation at their peacetime bases and locations, in training or exercises, while moving, or when deployed conducting actual operations. In addition, the adversary could compile and correlate enough information to facilitate predicting and countering US operations. The analysis of friendly information and planned activity by trained OPSEC practitioners leads to the understanding of what information or observable activity rises to the level of critical information and indicators. If the adversary is able to collect critical information and indicators, they can potentially derive an accurate operational picture of key friendly aspects such as presence, capability, strength, intent, readiness, location of future operations or activity, timing, and method of operations (the commander's objectives and operational design).

(2) OPSEC planners, in conjunction with the intelligence community (IC) and joint and component planners, apply OPSEC to identify critical information and indicators by phase, type of operation, or mission; determine how the adversary collects (sees) and how they will perceive potentially visible friendly critical information and indicators; weigh the adversary ability to collect, analyze, and respond to the critical information and indicators to a level that generates an unacceptable risk (time and operational ability to respond); and develop and apply OPSEC measures and countermeasures to protect and deny critical information and indicators that would enable the adversary to accurately determine and subsequently interdict planned operations.

(3) The holistic integration of OPSEC and MILDEC into a shaped portrayal of friendly activities and intent is a traditional military art that is sometimes referred to as denial and deception. When properly integrated, OPSEC and MILDEC work together to effectively and collaboratively shape how the adversary observes, analyzes, perceives, predicts, and responds to friendly operations and activities. It is a conscious and continuous effort to analyze and manage our own operational profiles so what is visible to the adversary is no more or less than what we deliberately plan it to be. While OPSEC focuses primarily on identifying and protecting critical information and indicators associated with the planned COA, MILDEC leverages the visible aspects of friendly operations and combines them with deceptive activity to create plausible alternative facts and conditions in the operational environment to which the targeted decision makers feel they must respond. This activity performs the MILDEC functions found in Chapter I, "General," and generates a friendly force advantage at the time and place of our choosing. Figure II-1 illustrates how OPSEC and MILDEC might be viewed in terms of their intent related to the adversary's observe, orient, decide, act (OODA) loop. The intent of OPSEC can be described as "short circuiting" the OODA loop by protecting critical information and indicators to the level that a friendly force, capability, or activity

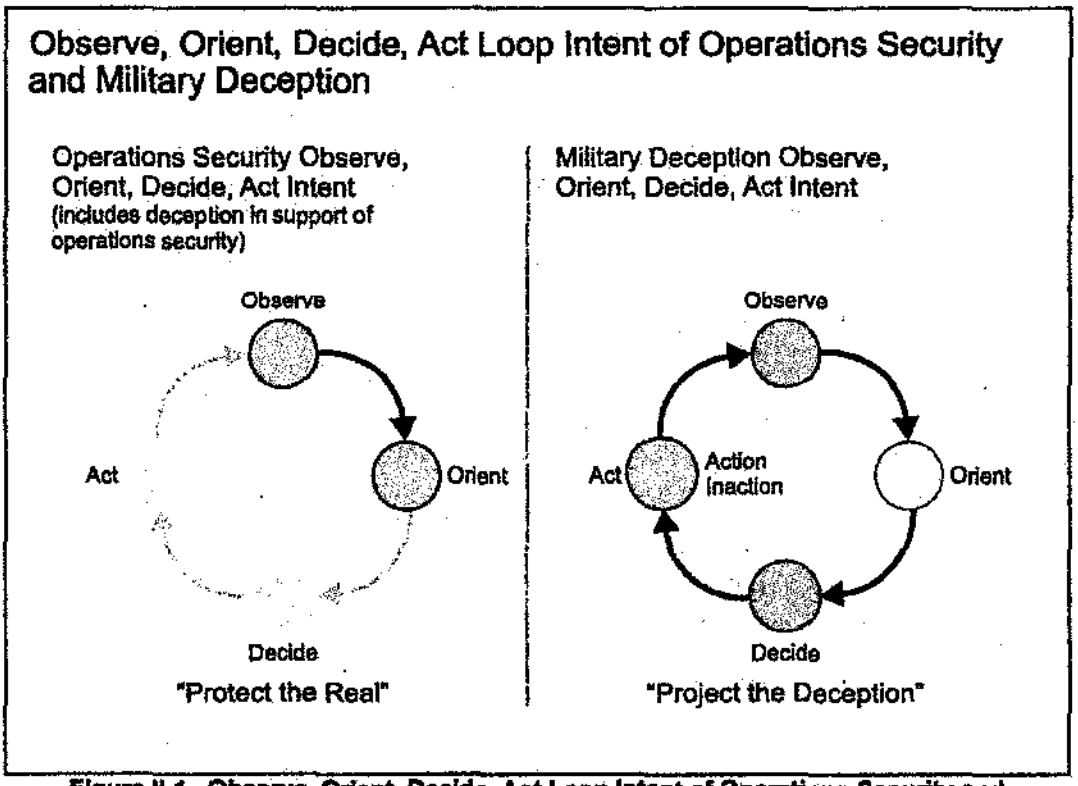


Figure II-1. Observe, Orient, Decide, Act Loop Intent of Operations Security and Military Deception

is either unobserved or lacks the required fidelity for adversary analysts to make accurate assessments or predictions. The intent of a MILDEC execution or event series (multiple executions toward the same objective), by contrast, is to cause the OODA loop to function in its entirety, but with misleading and inaccurate information designed to generate specific adversary decision maker action/inaction favorable to friendly objectives and end states. Of all the IRCs, the interrelationship and synchronization of activities between MILDEC and OPSEC is arguably the most critical.

(4) DISO presents false, confusing, or misleading information and indicators to FIEs as part of a larger OPSEC plan. DISO makes it difficult for FIEs to identify or accurately derive the critical information and indicators protected by OPSEC. DISO will be discussed in greater detail in Chapter V, "Military Deception Planning."

(5) In order to achieve the desired level of control over adversary perceptions, OPSEC and MILDEC planners coordinate their activities across a spectrum of influence that includes truth (factual information and actions visible to all), denial (critical information and indicators protected by OPSEC), misdirection (DISO and other activities designed to confuse adversary analysts and decision makers), and deceit (deceptive activity and information delivered as part of the approved MILDEC plan). While OPSEC identifies and protects critical information and indicators about the actual COA, MILDEC actively generates what appears to be critical information and indicators supporting the

deception story. MILDEC deliberately leads the adversary decision maker to the wrong conclusion, thus usurping their decision making and subsequent action (see Figure II-2).

(6) MILDEC and OPSEC planners can achieve significant savings in time and resources by collaborating during the joint planning process (JPP). Adversary threat assessment in the OPSEC planning process to determine technical aspects of **how** an adversary sees and perceives friendly activity correlates directly with MILDEC planner identification of conduits necessary to deliver deceptive information to military decision makers. Both OPSEC and MILDEC require a detailed knowledge of adversary decision making to project the impact of planned activities. In concept development, the OPSEC planner and MILDEC planner both require detailed knowledge of friendly indicators (signature, association, profile, contrast, and exposure): OPSEC to identify and protect critical information and indicators, MILDEC in order to replicate desired indicators that effectively portray the deception story.

(7) OPSEC also supports MILDEC directly during planning, preparation, and execution. The existence of a MILDEC operation in and of itself is critical information, and indicators require protection. An OPSEC analysis of the planned MILDEC is needed to protect against an inadvertent or unintentional disclosure of MILDEC existence, techniques, or particular means being used. Failure to maintain good OPSEC can lead to identification of the operation as a deception effort with the resulting second- and third-order effects such as the refocusing of adversary intelligence collection and combat power against actual friendly force dispositions and intent.

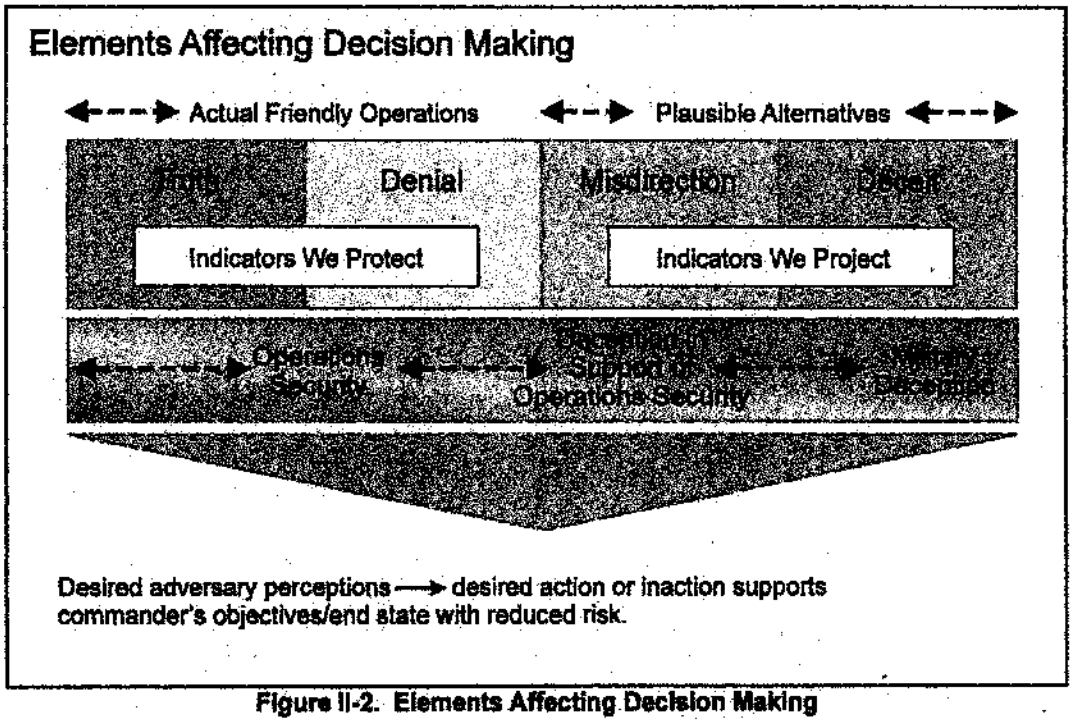
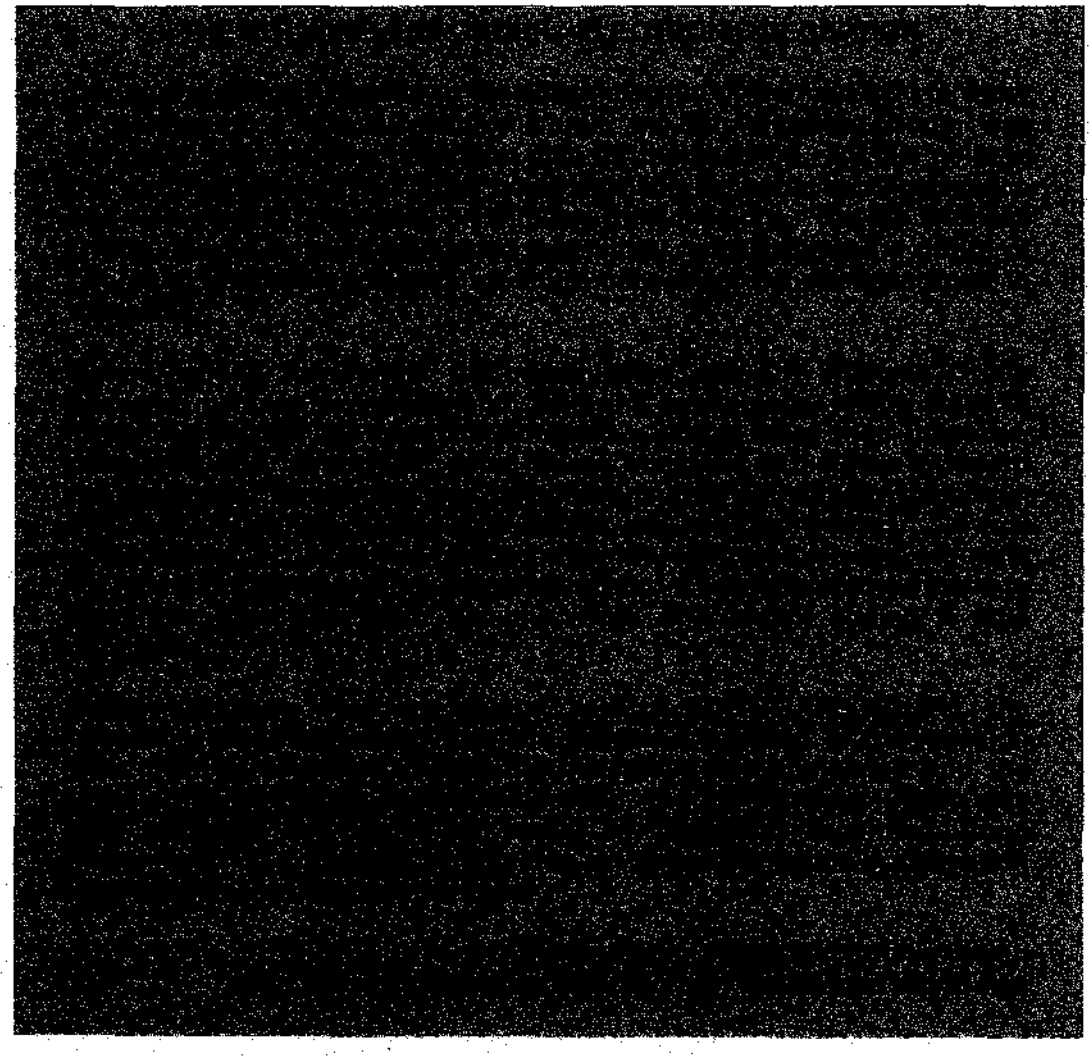


Figure II-2. Elements Affecting Decision Making



For further guidance on OPSEC, refer to JP 3-13.3, Operations Security.

b. MILDEC and Military Information Support Operations (MISO)

(1) MISO are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.

(2) Deception targets may also be MISO target audiences. MILDEC observables used to deceive MILDEC targets should be deconflicted with MISO themes and messages in order to maintain believability and credibility.

(3) MISO products and activities are generally truth based. This practice is not based upon legal or policy restrictions, but is upon a requirement to maintain credibility with target audiences in order to execute future MISO.

(4) MILDEC planners should be aware of MISO themes and messages that the intended MILDEC target may receive. MISO themes and messages contain both objective and subjective truth, and must be generally "verifiable" by the target audience. MILDEC events and deceptive information inserted into adversary conduits contain falsehoods and need only be believable to the target. The two can be mutually beneficial, but they may also run counter to each other; therefore, MISO and MILDEC should be carefully coordinated.

(5) MISO products directed at specific adversary target audiences may be used in conjunction with MILDEC techniques such as feints, demonstrations, ruses, and displays to add credibility to the deception story or event. MISO products warning of impending multinational force arrival, providing surrender instructions, or attacking the morale of adversary military or paramilitary forces are examples of this type of cooperation. However, because of the requirement for MISO to retain credibility with its broader target audiences, any use of MISO in this manner, and proposed themes, must be carefully evaluated for the potential cost/benefit and/or second- and third-order effects of its use.

For further guidance on MISO, refer to JP 3-13.2, Military Information Support Operations.

c. **MILDEC and Electronic Warfare (EW)**

(1) All modern forces depend on the electromagnetic spectrum (EMS). The military requirement for unimpeded access to, and use of, the EMS is the key focus for joint EMS operations, both in support of military operations and as the focus of operations themselves. EW is essential for protecting friendly operations and denying adversary operations within the EMS throughout the operational environment. The term EW refers to military action involving the use of EM energy and directed energy to control the EMS or to attack the enemy.

(2) MILDEC, in conjunction with OPSEC, supports EW operations by protecting the development, acquisition, and deployment of sensitive EW capabilities. MILDEC can also support the employment of EW units and systems.

(3) EW can support feints, ruses, demonstrations, and displays. The positioning of a majority of a command's EW systems in a particular area can create an indicator of the command's intended main effort. The disruption of an adversary's communications and intelligence collection systems and assets can facilitate the insertion of deceptive information. EW employed against intelligence collection assets can shape and control the adversary's ability to obtain information about certain activities. Close coordination is required between friendly EW, MILDEC, communications, cyberspace and space support elements, frequency management, and intelligence planners to ensure EW does not disrupt any adversary communications systems that are used as MILDEC conduits or that are providing intelligence feedback.

(4) EM deception is the deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of EM deception are the following:

(a) **Manipulative.** This involves actions to eliminate revealing, or convey misleading, EM telltale indicators that may be used by hostile forces.

(b) **Simulative.** This involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.

(c) **Imitative.** This involves actions to imitate enemy emissions to mislead hostile forces.

For further guidance on EW, refer to JP 3-13.1, Electronic Warfare.

d. **MILDEC and Cyberspace Operations (CO)**

(1) MILDEC and CO can be mutually supportive in a number of ways. A few examples are noted below:

(a) Because the adversary may also be resident in cyberspace, and leverages the same systems and processes, CO are an effective conduit for the placement or delivery of deceptive material to affect adversary military decision making and subsequent action/inaction.

(b) MILDEC planners can help protect friendly use of information systems (ISs) by applying deceptive activities similar to those used in the physical dimension for maneuver forces. Such an operation may include the construction of false servers, communications nodes, and other hardware associated with a tactical computer network to include the replication of IS traffic and false data storage.

(c) Enemy intelligence and targeting systems, which make a priority of attacking or subverting a friendly IS, can be dissuaded from doing so via a successful MILDEC operation. Enemy collection assets can be redirected toward deceptive events (such as the presentation of a false "weakness" in friendly ISs) and then targeted for destruction or exploitation by friendly forces.

For further guidance on CO, refer to JP 3-12, Cyberspace Operations.

(2) **Planning Considerations for Integrating CO and MILDEC.** Because most physical activities of a JTF and its components are mirrored in cyberspace, the integration of MILDEC and CO planners in all phases of planning and operations is critical.

(a) Any MILDEC plan must consider the abilities and limitations of friendly and adversary CO. Careful and detailed planning is required to ensure MILDEC

executions using CO assets are tracked, recorded, and deconflicted with other nondeceptive CO.

(b) The MILDEC plan should be properly classified and not exposed to unprotected computer networks or sent via unsecured e-mail. Any exposure can lead to plan failure.

(c) Careful consideration must be taken for the application of limited friendly CO assets to MILDEC. Several questions must be answered before CO are used:

1. Can the target see the information? Will presenting a deceptive vulnerability be believable, or will the target discount anything received?

2. What are the CO assets on hand? How much nondeceptive demand is being placed on the limited CO assets?

3. How much time is necessary to set up, monitor, and use CO to support MILDEC?

4. How can MILDEC support CO? Ensure the MILDEC plan supports ongoing CO, as well as the overall OPLAN, and presents an integrated, but false, picture to the target.

4. Military Deception and Physical Attack

a. Physical attack refers to the use of lethal means against designated targets as an element of an integrated IO effort. MILDEC and physical attack interact in a variety of circumstances with examples provided below.

(1) Physical attack can support MILDEC by:

(a) Targeting adversary systems in support of feints, demonstrations, ruses, or displays to create the desired perception that a targeted area is a primary maneuver objective.

(b) Destroying or nullifying selected adversary intelligence collection capabilities or sites that might be in a position to register and report friendly indicators that contradict the deception story.

(2) MILDEC can support physical attack by:

(a) Misleading adversaries or FIEs about key operational aspects such as the presence, capability, strength, intent, readiness, or method of employment for key physical attack capabilities.

(b) Misleading the adversary about the location, timing, and method of planned friendly physical attack/destruction, thus increasing adversary vulnerability.

b. MILDEC planners should be an integral part of developing the joint integrated prioritized target list to ensure gain versus loss assessments are conducted prior to destroying potential MILDEC conduits such as intelligence collection or radar sites.

c. **MILDEC and Cybersecurity.** Cybersecurity is critical to IO because it protects and defends information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of ISs by incorporating protection, detection, and restoration capabilities. With regard to MILDEC, cybersecurity safeguards information and indicators that may reveal (or provide a competing observable to) friendly deception operations. Cybersecurity can also support counterdeception by identifying adversary attempts to insert false or misleading information into friendly systems.

d. **MILDEC and Physical Security.** Physical security consists of all the functional areas that make up those measures necessary to protect and safeguard personnel, facilities, and installations. Security is an integral tenet of MILDEC. Without adequate physical security, a MILDEC plan can be compromised. Commanders should ensure physical security measures are integrated into every phase of the deception planning process.

e. **MILDEC and Public Affairs (PA).** MILDEC activities, including planning efforts, are prohibited from explicitly or implicitly targeting, misleading, or attempting to influence the US Congress, the US public, or the US news media. All MILDEC activities are reviewed to eliminate, minimize, or mitigate the possibility that such influence might occur. US policy prohibits the use of PA to misinform the US public, the US Government, or US and international media about military capabilities and intentions in ways that influence US decision makers and public opinion. Coordinate MILDEC operations that have activities potentially visible to the media or the public with the appropriate PA officers to identify any potential problems. Coordination will reduce the chance that PA officers will inadvertently reveal information that could undermine ongoing or planned MILDEC operations.

For further guidance on PA, refer to JP 3-61, Public Affairs.

f. **MILDEC and Civil-Military Operations (CMO).** CMO are the activities of a commander performed by designated civil affairs or other military forces that establish, maintain, influence, or exploit relationships between military forces and indigenous populations and institutions, by directly supporting the attainment of objectives relating to the reestablishment or maintenance of stability within a region or host nation. CMO are conducted to gain maximum support for US forces from the civilian population. CMO contribute to the success of military operations and project a favorable US image throughout the operational area. Coordinate MILDEC with CMO and with those MISO activities that support CMO to ensure MILDEC operations do not inadvertently undermine the relationships with the civilian population or with host nation military authorities. Failure to consider CMO could result in the compromise of MILDEC plans or other unintended consequences to the overall mission.

For further guidance on CMO, refer to JP 3-57, Civil-Military Operations.

5. Information Operations Planning

a. The JFC normally establishes an IO cell. Joint force staffs plan, integrate, and synchronize IO efforts through the IO cell within the overall JPP. At the combatant and subordinate joint force command levels, the IO cell is the focal point for IO coordination and deconfliction of activities and associated operations. All joint force planning activities should include IO cell representation, and the cell is composed of select representatives from each of the staff elements and components responsible for IO activities and other staff representatives as required. The JFC's senior MILDEC planner is normally a standing member of the IO cell. Within the IO cell, the MILDEC planner provides deception plan information to incorporate and deconflict MILDEC with other IRCs. Some MILDEC details may be compartmentalized.

b. The IO cell is also the coordination entity for the MILDEC representative with other US Government departments, agencies, organizations, and partner nations. Military planners interface with the IO cell when developing plans for specific geographic areas. The MILDEC representative also deconflicts the MILDEC plan with the activities of these entities in the operational area. Because the interagency process usually takes significant staffing time, the MILDEC representative ensures this is accounted for in the planning timeline. The same close coordination is necessary between the MILDEC planner and representatives of partner nations, whether represented in the IO cell or not.

For further guidance on IO planning, refer to JP 3-13, Information Operations.

6. Military Deception and Camouflage, Concealment, and Decoys

Camouflage and concealment are OPSEC measures used to protect friendly forces and activities from adversary detection and attribution. Camouflage makes friendly capabilities or activities blend in with the surroundings. Concealment makes friendly capabilities or activities unobservable or unrecognizable to the adversary. Both use physical, technical, and administrative signatures to deceive the adversary and protect the deception story. MILDEC measures use the same signatures for simulating friendly forces and activities. Decoys may be used in conjunction with other MILDEC activities to mislead adversary intelligence collection and direct the adversary's attention away from actual forces.

7. Legal Support to Military Deception

MILDEC and Legal Support. Staff judge advocate (SJA) personnel shall be included in coordination efforts to ensure compliance with applicable US and international law, treaties, and agreements to which the US is a party; presidential and Department of Defense (DOD) policy and regulations; rules of engagement (ROE); and applicable component policy. SJA personnel assist in planning the operation to meet the objective while complying with legal requirements, as well as providing training to deception planning cell (DPC) personnel on law and policy applicable to MILDEC operations.

For further guidance on legal support, refer to JP 1-04, Legal Support to Military Operations.

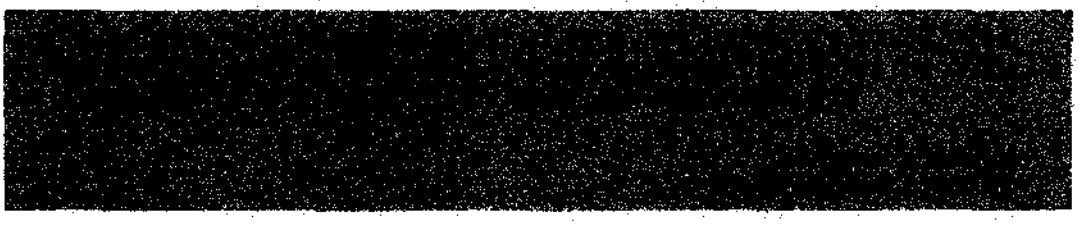
8. Military Deception and Personnel Recovery

MILDEC may be used to deny adversaries knowledge of personnel recovery tasks: report, locate, support, recover, and reintegrate. These efforts focus on deceiving the enemy as to the personally identifiable information, location, status, friendly efforts to recover, and post recovery activities of the isolated person(s).

For further guidance on the personnel recovery system, functions, options, categories, tasks, and methods, refer to JP 3-50, Personnel Recovery.

Intentionally Blank

CHAPTER III
ROLES, COORDINATION, AND CONSIDERATIONS FOR MILITARY DECEPTION



1. Roles and Responsibilities of Military Deception Planners

MILDEC plans and operations require integrated timing and deconfliction in order to increase the probability of meeting the objectives. Therefore, MILDEC planners must understand the roles and responsibilities of everybody involved with MILDEC planning and execution. JFCs should consider the use of any assigned forces and methods subject to the ROE and law of war to accomplish their MILDEC objective.

a. Roles

(1) **Commanders.** While MILDEC may not be appropriate to every joint operation, the JFC determines the utility of MILDEC's contribution to achieving objectives. JFCs make the decision to use MILDEC after evaluating the analysis and recommendations from the JPP. Commanders should guide applicable MILDEC operations while also understanding their potential importance during planning and execution of the MILDEC operation.

(2) **J-3/Plans Directorate of a Joint Staff (J-5).** The division of planning labor between the J-3 and the J-5 is command-specific. The IO cell and the MILDEC element are normally assigned to the J-3 but participate in J-5 planning. According to their specific planning responsibilities (tailored to clearances, access levels, and need to know of specific individuals), the J-3/J-5 supervise the incorporation of MILDEC into the IO portion of operations estimates. Based on these estimates, the J-3/J-5 recommend various options for IO (including MILDEC) to the commander. Once the JFC has selected a particular IO COA and received approval through the chain of command, the J-3/J-5 supervise the completion of planning for the selected COA. The J-3 normally supervises MILDEC execution.

(3) **IO Cell Chief.** The IO cell chief is normally responsible to the J-3 for the development of the IO portion of any planning effort conducted by the staff. These responsibilities include supervision of MILDEC planning and integration into the overall IO plan. The IO cell chief monitors the implementation and execution of the MILDEC portion of IO. For DISO, the IO chief will ensure OPSEC planners and MILDEC planners work together for an integrated, effective OPSEC execution.

(4) **Command Military Deception Officer (CMDO).** The CMDO is the primary designated officer with overall oversight and management responsibility for each MILDEC program within the CCMDs, agencies, and Service components which support joint military operations. The CMDO establishes (through the CCDR) the review and approval processes for joint MILDEC, DISO, and TAC-D, which fall under the authority of the CCMD. The CMDO also provides support to the approved MILDEC plans and operations of other CCMDs as required. Duties and responsibilities of the CMDO are specified in CJCSI 3211.01, *(U) Joint Policy for Military Deception.*

(5) **Military Deception Officer (MDO).** Personnel at subordinate components, appointed by their component command leadership, are responsible for planning and execution of MILDEC. The MDO works closely with the CMDO to ensure all component MILDEC plans are in accordance with command and DOD guidance and policy.

(6) **MILDEC Planner.** The MILDEC planner plans and executes MILDEC plans within their organization. These planners report to the CMDO or MDO of their organizations. MILDEC planners work with other planners (internal and external to the IO cell) as necessary to integrate detailed plans and coordinate execution.

(7) **Other Planners.** All joint staff planners should consider using MILDEC when developing COAs. Other planners may not be aware of the potential contribution of MILDEC to their planning area. It is incumbent upon the senior MILDEC planner to evaluate the mission and contact planners outside the IO cell who may benefit from the addition of MILDEC actions to their part of the plan.

b. **Responsibilities**

(1) **Commander.** The JFC has explicit and inherent responsibilities for the deception effort. The commander should:

(a) Assess the mission order for stated and implied deception tasks.

(b) Consider the use of deception in every operation.

(c) Task the staff to evaluate the utility of deception.

(d) If deception appears feasible (it may be infeasible due to lack of time or resources), state the tentative deception objective with the JFC's initial planning guidance.

(e) Approve the deception objective, story, and plan and allocate resources to ensure successful execution.

(f) When required, seek appropriate approval for employment of certain deception means.

(g) Determine when to exploit deception and/or counterdeception.

(2) **J-2.** The process of identifying MILDEC objectives to complement operational objectives is an iterative process, with the commander in a central role orchestrating the efforts of the operations, intelligence, and counterintelligence (CI) resources. The J-2 is a primary participant in this process. The J-2:

(a) Assists the commander and staff in gaining insight into the adversary and the adversary's capability to process, filter, and evaluate intelligence on the friendly situation.

(b) Provides assessments on the adversary's vulnerabilities to MILDEC.

(c) Provides assessments on adversary targets, sensors, most dangerous and most likely COAs, acceptance of the deception story, and MOEs.

(d) Provides comprehensive assessments and continual feedback to the deception element in support of MILDEC planning, execution, and termination.

(e) Supports counterdeception operations to protect friendly deception operations and to expose adversary deception attempts.

(f) Responds to MILDEC planners' request for information (RFI) inputs that solicit behavioral influences analysis/human factors analysis data on adversary military, paramilitary, or violent extremist organizations.

(g) Produces the deception intelligence estimate (DIE) in collaboration with the MILDEC planner.

(3) **J-3.** The J-3 normally establishes a staff deception element to manage MILDEC operations as part of the IO cell. The J-3:

(a) Recommends to the JFC the deception objective, story, and plan.

(b) Plans the deception effort.

(c) Ensures the deception effort is coordinated through the IO cell with all other aspects of the plan integrated through the joint targeting process.

(d) Ensures, in coordination with the SJA, that the deception effort is planned and conducted in accordance with the US law, ROE, and the law of war.

(e) Supervises execution of the deception plan.

(f) Develops MOEs to assess the deception operation in conjunction with the MILDEC planner.

(g) Controls termination of the deception plan.

(h) Submits detailed and clear RFI to J-2 for intelligence information key to deception planning, execution, and assessment.

(i) Collaborates with J-2 to produce the DIE.

(j) Provides feedback to J-2 on intelligence products to include clarification or additional RFI if needed.

(4) **Logistics Directorate of a Joint Staff (J-4).** The J-4 provides the logistic support and guidance needed to conduct MILDEC operations in coordination with MILDEC planners. The J-4:

(a) Assesses logistic requirements needed to conduct the MILDEC operation.

(b) Determines logistic capabilities to support the deception operation.

(c) Provides input to and assessment of the deception plan to ensure logistics feasibility.

(d) Assesses the ability of logistic assets to support the deception plan without hindering the support necessary for execution of the overall operation.

(e) Develops logistic plans that support the MILDEC operation.

(5) **J-5.** The J-5 normally maintains contingency plans and initiates crisis action planning efforts.

(a) Coordinates with the CMDO to ensure deception planning is included in OPLANs, CONPLANs, and campaign plans.

(b) Includes deception elements in operations planning teams to ensure MILDEC operations are considered from the inception of planning.

(6) **Communications System Directorate of a Joint Staff (J-6).** The J-6 ensures communications system support and related communications system support activities necessary to support MILDEC. The J-6:

(a) Provides planning guidance on communications system support to MILDEC planners.

(b) Assesses supporting communications system network capabilities and interoperability required to support MILDEC operations.

(c) Reviews MILDEC plans and coordinates communications system support requirements.

(d) Develops and implements technical solutions to reduce the possibility of deception compromise and high-risk information vulnerability.

(e) Develops communications system support plans to support the MILDEC operation.

(7) **Others.** Other staff members ensure compliance and deconfliction of the planning with respect to their functional areas. They also provide expertise in the planning activities to support MILDEC.

2. Coordination Requirements

a. Coordination and deconfliction of MILDEC plans between CCDRs' areas of responsibility is essential for the success of a MILDEC operation. The Joint Staff has the authority and responsibility to plan, coordinate, and integrate DOD IO capabilities that cross areas of responsibility or that directly support national objectives. For those MILDEC plans, the Joint Staff J-3 [Operations Directorate] serves as the coordinating authority for the planning of MILDEC and the integration of joint MILDEC with other IRCs. The Joint Staff J-3 supports the CCDRs in development, assessment, coordination, and recommendation of MILDEC options. The Joint Staff J-3 ensures CCMD MILDEC requirements do not conflict with MILDEC operations occurring in other areas of responsibility.

b. MILDEC and its supporting actions should be coordinated with higher, adjacent, subordinate, and supporting staffs.

c. Within a joint staff, coordination is required between deception planners and other planners and analysts on the staff.

d. Coordination with CMO, PA, SJA, and other US Government department and agency personnel is imperative to avoid destabilizing military-civilian relationships and to prevent the unintentional compromise of MILDEC operations. This coordination is of increasing importance in situations where MILDEC operations are viewed by the media and/or the general public.

e. The JFC-designated IO cell chief is normally the single point of contact to manage and obtain coordination requirements and related points of contact information pertaining to the deception element. However, a JFC may want to appoint a CMDO who would be the single manager for MILDEC. Despite coordination requirements, it is important to restrict knowledge of information relating to planned and ongoing MILDEC operations to only those personnel who need to know.

(1) The JFC provides guidance concerning the dissemination of deception-related information. During multinational operations, the JFC should be aware of information requirements and concerns of the non-US partners.

(2) During planning, MILDEC planners develop need to know criteria that permit necessary coordination while limiting the number of individuals with knowledge of the deception. Only a few individuals require access to the entire deception plan. Others require only knowledge of limited portions of the plan. The need to know criteria should address these different levels of required access.

f. When MILDEC operations incorporate or involve multinational partners, the command's foreign disclosure officer should be utilized to help determine appropriate access to MILDEC information and operations.

For further information on multinational personnel access to MILDEC plans, refer to CJCSI 3211.01, (U) Joint Policy for Military Deception.

g. MILDEC operations can benefit from normally occurring activity provided the activity fits the deception story. Conversely, actual operations have the potential to create OPSEC indicators that pose a threat to the effectiveness of MILDEC operations. These real indicators may conflict with the deception story. MILDEC and OPSEC planners will have to coordinate with organizations that create these indicators to limit potential adverse effects or to maximize their deception potential.

h. Assign liaison officers (LNOs) from the appropriate intelligence staffs and organizations to support MILDEC planning. LNOs provide all-source estimates upon which to base plans and real-time all-source feedback about the effectiveness of deception actions. Assign LNOs from MILDEC supporting organizations to provide expertise on unit indicators and to facilitate parallel planning.

CHAPTER IV
INTELLIGENCE SUPPORT TO MILITARY DECEPTION

[redacted]

1. General

Focused intelligence support is essential to the successful planning, execution, and assessment of any MILDEC. The requirement is substantive to the point that "support friendly deception efforts" and "counter adversary deception and surprise" are listed as two of the five roles and responsibilities of joint intelligence in JP 2-0, *Joint Intelligence*. There are five principal ways in which intelligence supports the execution of effective MILDEC.

a. Assist in the completion of the DIE. Begun during mission analysis, the DIE is the foundation for effective MILDEC planning, as well as subsequent execution and assessment.

b. Answer RFIs submitted during the planning and execution phases.

c. Support the conduit analysis step of the MILDEC planning process.

d. Support the development, collection, and analysis of planned MILDEC MOPs, MOEs, and indicators to facilitate assessment of the MILDEC plan and the current application of the commander's means and resources

e. Identify and confirm instances of adversary deception and supporting counterdeception exploitation. (See Chapter VII, "Counterdeception.")

2. The Deception Intelligence Estimate

a. The DIE is a specialized intelligence product derived from the J-2's joint intelligence preparation of the operational environment (JIPOE) and responses to situation-specific RFIs submitted by MILDEC planners. While a high percentage of information in the DIE can be derived from JIPOE, much of the detail required is unique to MILDEC. MILDEC-trained intelligence analysts collaborate with selected members of the DPC and deception operations working group (DOWG) to build the DIE.

b. The DIE is a "living" product. It is refined as additional information and intelligence become available, or as conditions evolve and change within the operational environment. During the initial planning stages, MILDEC planners and intelligence analysts will likely be required to make assumptions requiring later validation to continue with planning. These assumptions must be tracked, aligned with an open RFI, and considered during risk analysis. Step four of the JPP (COA analysis and wargaming) will help refine the DIE and may add support to key planning assumptions about probable

adversary responses to planned friendly activity. The greater the number of assumptions underpinning a MILDEC plan, the higher the risk that one or more assumptions will prove false and threaten the success of the plan.

c. The following topics are examples of essential information required to complete a functional DIE that supports effective MILDEC planning: understanding adversary goals and operational objectives, characterization of adversary decision making, identification of key military decision makers and development of individual or group profiles, understanding the adversary's intelligence and CI organization and capabilities (to include external intelligence sources), analyzing the adversary's potential vulnerability to MILDEC, understanding adversary deception and counterdeception doctrine and resources, and identification of the most probable and most dangerous adversary COAs.

(1) Understanding adversary goals and objectives. These provide the "why" behind adversary decision making and subsequent actions or inaction. It is the first step in understanding and predicting adversary behavior. Effective MILDEC supporting other joint force activity could potentially cause an adversary to reevaluate the viability or risk associated with a given COA.

(2) Characterization of adversary decision making. In order to affect adversary decision making, we must first understand and characterize its functional components. A sample method of structuring this process for joint MILDEC application is to analyze and describe the adversary's decision-making **structure,** decision-making **style,** and cognitive biases and preconceptions that will likely affect or skew decision-making outcomes. JP 3-25, *Countering Threat Networks,* provides comprehensive techniques and analytical framework discussion for understanding this critical aspect of the information environment.

(a) Decision-making **structure** refers to how the adversary is organized to collect, transmit, analyze, and deliver relevant information to support military decision making, their formal or informal organization for decision making, and the transmission and implementation of its outcomes to the action element or capability we are seeking to affect. This product is an expanded link node analysis and sometimes referred to as an information pathways diagram (see Figure IV-1). Characterizing the adversary's military decision-making structure is primarily an objective process. It combines a hierarchical analysis and representation of the military, paramilitary, or violent extremist organization with an analysis of communication linkages and the collection capabilities and analytical functionality of its formal and informal intelligence and CI support apparatus. External governing bodies, such as a military council within the adversary's political branch or its equivalent and foreign (external) intelligence support, should also be included in the characterization of the military decision-making structure. Analysts must identify additional sources of information feeding political-military oversight, as well as open-source information. While the example appears in traditional line and block form, it is built on a functional design that reflects a notional military decision-making structure and includes only those elements relevant to that process. Information pathways will frequently include key civilian influencers that serve, formally or informally, as a component of military decision making. Their ultimate eligibility as a MILDEC target

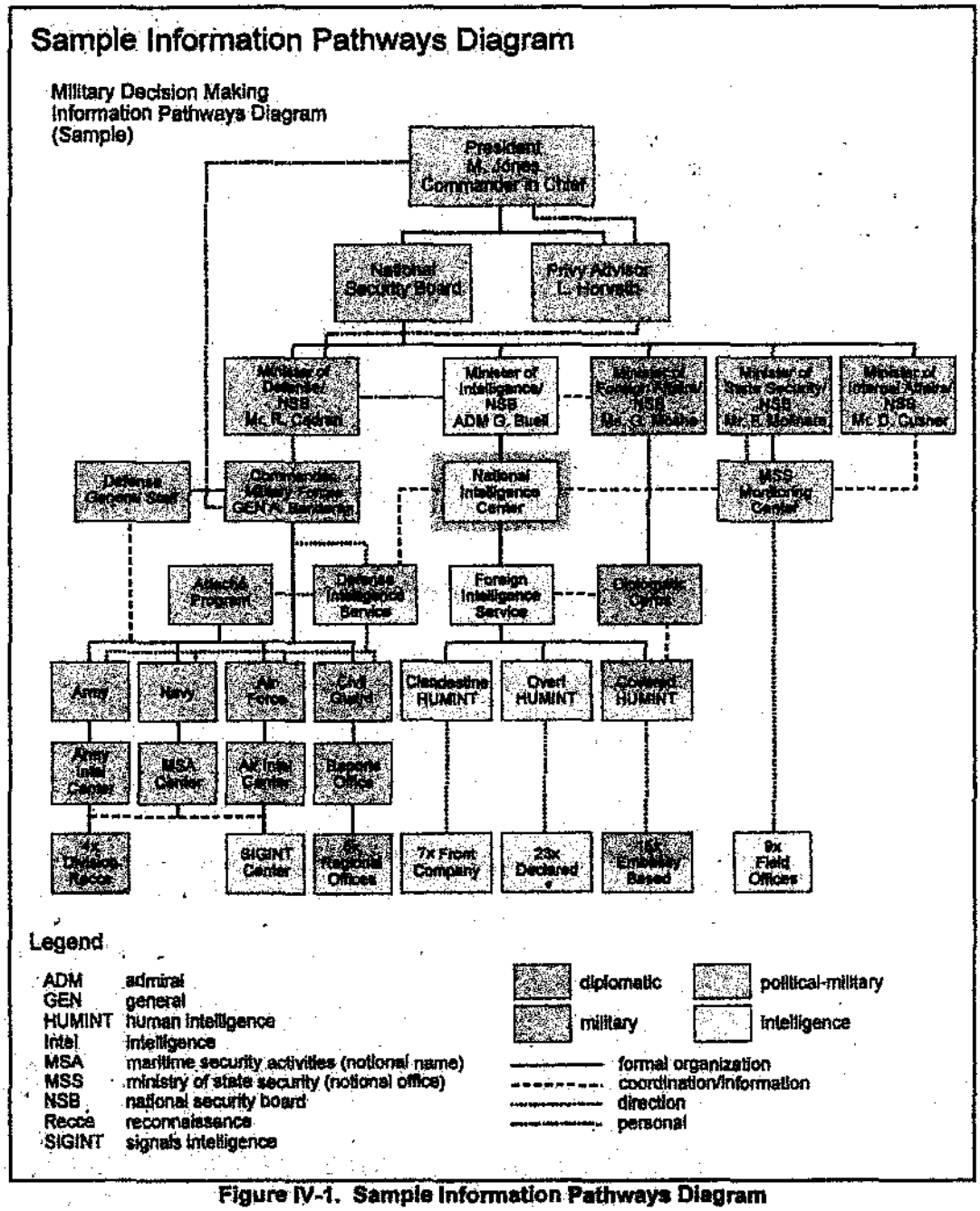


Figure IV-1. Sample Information Pathways Diagram

would require legal analysis as part of the subsequent joint MILDEC plan review and approval process. A military decision-making information pathways diagram for a decentralized, trans-regional violent extremist organization might take a decidedly different graphic form to facilitate common understanding. Later in the planning process, when planners have identified the tentative deception target that controls the action or inaction of a desired military capability, the specific information pathways that feed and

potentially influence a given deception target's decision making will be characterized in much greater detail through the conduit analysis process.

(b) The analysis of adversary military decision-making **structure** includes identifying key decision makers at the strategic or operational level who exercise some level of direct control over the adversary capabilities we are seeking to affect. These individuals or groups are potential deception targets. As such, the J-2 should be tasked with collecting all available information relating to such things as their backgrounds, psychological profile, personal relationships and key influencers, known biases, predispositions or vulnerabilities, current perceptions, and previous behavior in similar circumstances. As a reminder, MILDEC is prohibited by policy from deliberately targeting anyone outside the adversary military decision-making process without further legal review.

(c) Decision-making **style** refers to the deliberative process that a selected military decision maker or body uses to reach a conclusion. The selection and use of a common framework allows intelligence analysts and planners to better focus their analysis and discussions to best support achievement of objectives. There are a variety of formal and informal decision-making styles, and once a framework is selected, it is important to identify what conditions such as compressed time, degradation of systems from combat operations (i.e., communication disruption, destruction of key nodes), probable delegation of certain operational decisions, or other changes in the operational environment might cause adjustments to the base style. Decision-making style is itself the topic of a vast amount of academic and commercial variety and continuing interest. Figure IV-2 is a sample of decision-making styles, and while simple, it provides a basis for analysis, shared comprehension, and context.

(d) The selected model should be conducive to rapid understanding so that it can be quickly used by intelligence analysts and MILDEC planners to better understand overall adversary decision making and subsequently convey the associated rationale for a certain operational approach or series of MILDEC executions to the JFC.

(e) Understanding the adversary's cognitive biases and preconceptions that might subjectively influence adversary decision making is important to any attempt to predict future behaviors. The study of psychology and decision making recognizes numerous potential types of bias. For the purposes of illustration, a commonly recognized summary of bias types includes cultural, organizational, and personal biases.

1. Cultural biases are caused by the interpretation of information through one's own cultural knowledge, beliefs, morals, customs, habits, and cognitive styles acquired as a member of a specific social environment or group.

2. Organizational biases are a potential outcome of the goals, mores, policies, and traditions that characterize the specific organizations in which individuals affiliate.

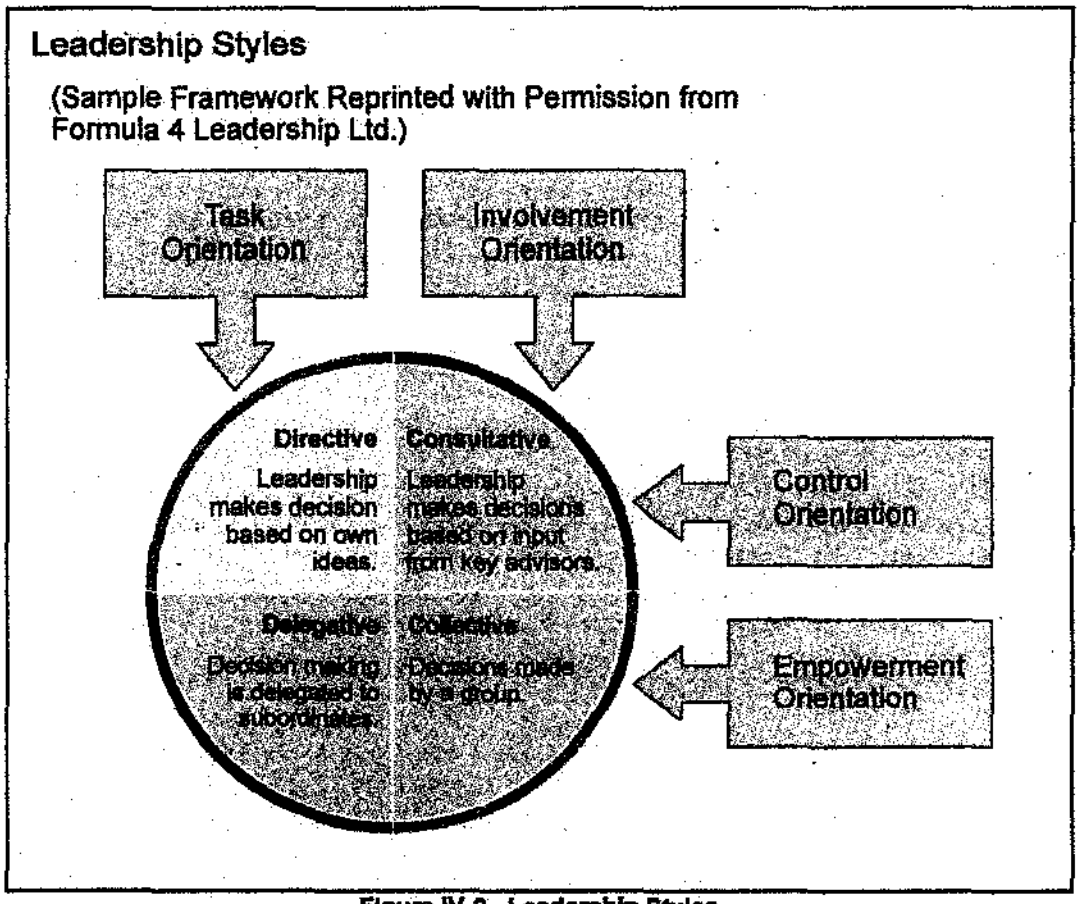


Figure IV-2. Leadership Styles

3. Personal biases come from personality traits, education, and firsthand experiences that affect a person's world view over the course of their lifetime.

4. Preconceptions are conceptions or assumptions formed beforehand. In addition to being highly influenced by bias, preconceptions can also be formed by sustained observation and perceived recognition of patterns. This is particularly relevant to MILDEC planning because known biases and preconceptions can be exploited. "Magruder's principle," found in Appendix A, "Military Deception Maxims," states "it is generally easier to induce a deception target to maintain a preexisting belief than to deceive the deception target for the purpose of changing that belief."

(f) Adversary decision making is informed by the intelligence and CI organizations and capabilities that support it. In order to manipulate or augment the information available to a deception target, the MILDEC planner must have a detailed knowledge of the adversary's ability to "see" and interpret all relevant friendly activities and indicators. Analysis of adversary intelligence and CI capabilities, organization, and function is a traditional J-2 task. By leveraging the full scope of IC resources, the J-2 should be able to provide:

1. The current "red view of blue." This includes adversary perspective analysis of our probable goals and objectives, our most probable and dangerous COAs, a blue center of gravity analysis, and any other fundamental assumptions or perceptions they have developed about friendly activities, capabilities, or intent.

2. Detailed technical estimates of the adversary's collection capabilities. The capabilities of FIEs that share intelligence with the adversary should also be included in this analysis. One method of capturing this information within the DIE is to organize adversary capabilities under the intelligence disciplines familiar to most joint planners from our own doctrine as outlined in JP 2-0, *Joint Intelligence*. They are geospatial intelligence, human intelligence, signals intelligence, measurement and signature intelligence, open-source intelligence, technical intelligence, and CI. For MILDEC planning, it is important that the scope of this analysis identifies a particular adversary's collection capabilities anywhere that they provide potential knowledge of the JFCs plan. This span includes all activities from the employment of national strategic resources and global strike capabilities through force generation to theater employment and sustainment. This range will likely include not only the operational area as a whole, but also multiple locations in the US and any other location which supports the JFCs planned operations to include collection against multinational partners. This same information is required by joint OPSEC program managers and planners, and may already exist in a partially completed form.

3. Knowledge of the adversary's intelligence process represented in our own joint intelligence doctrine as planning and direction, collection, processing and exploitation, analysis and production, and dissemination and integration. To inject deceptive information into the adversary's intelligence system as a MILDEC execution, track its delivery to the decision maker, and evaluate whether the execution produced the desired perception or effect, the MILDEC planner needs to understand every sensor, link, node, and potential filter in the conduit through which that event's execution was transmitted. This requires sufficient fidelity of intelligence in the DIE to conduct a reasonably accurate adversary conduit analysis with minimal assumptions later in the planning process.

4. Identify the adversary's vulnerability to MILDEC, as well as conditions that might favor the adversary in protecting against MILDEC. One method of analysis in achieving this planning requirement is to use the framework of physical, informational, and cognitive dimensions of the information environment found in JP 3-13, *Information Operations*. Cognitive vulnerabilities to MILDEC can include such things as predisposition or bias, an overly burdensome decision process model, poor decision quality (group think, single point of failure, or lack of subordinate autonomy), or poor decision timeliness (a leader who cannot come to a decision quickly). Examples of vulnerabilities in the informational dimension might include such things as poor information management or data processing capability and overdependence on vulnerable or non-redundant communications networks. Sample vulnerabilities in the physical dimension include shortfalls in collection or processing capability and vulnerabilities in force structure or capability. Adversary strengths in the areas mentioned above are normally inverse statements to examples provided.

(g) Analyzing an adversary's deception and counterdeception doctrine and capability is critical to MILDEC planning. Knowing an adversary's deception doctrine and capability may provide J-2 analysts and MILDEC planners with an understanding of the emphasis the adversary places on deception and thus their vigilance in its detection. It also provides the necessary awareness to help friendly forces identify when the adversary might be using deception to influence our own decision making; see Chapter VII, "Counterdeception." Understanding adversary counterdeception doctrine and capability enables the J-2 and MILDEC planners to better evaluate the adversary's potential recognition and response to our MILDEC plan and more accurately identify when it may be compromised. The J-2 will normally consult the broader resources of the national IC in the performance of this task.

(h) Identifying the adversary's current, most likely, and most dangerous COAs is a normal J-2 function supporting the JPP. Understanding this information enables the MILDEC planner to more accurately plan against "anticipated" adversary actions, as well as evaluate the impact of friendly operations in achieving the commander's approved deception objectives.

3. Military Deception Requests for Information

As a result of the MILDEC focus on the cognitive dimension, MILDEC planners are frequently required to make informed assumptions on a variety of topics to continue planning. In addition to RFIs associated with the completion of the DIE, MILDEC planners, at times, require a level of detail and predictive analysis not generally supported within an operational-level JIPOE. Information on potential MILDEC conduits such as air defense radar, maritime visual observation, ground reconnaissance, or CCMD-focused espionage comes from a variety of sources and must be collected and available if a MILDEC plan is to be executed with any level of confidence. This becomes particularly challenging once combat operations have begun and adversary pre-conflict military decision-making structure and flow, access to sensors, and decision-making support networks are disrupted or neutralized. The rapid adversary adaptation to new conditions in the operational environment will require equally agile intelligence support to facilitate the continued flow and delivery of indicators comprising the deception story narrative to the MILDEC target. Unless MILDEC RFIs are aligned with the JFC's priority intelligence requirements (PIRs), the MILDEC plan is at risk of becoming desynchronized or ineffective.

4. Conduit Analysis

a. **Conduit analysis** is the detailed mapping of individual conduits or information pathways to the potential deception target(s). Conduit analysis should begin with the initiation of planning and continue to be refined through the COA development, COA selection, and finalization of the MILDEC plan. The identification of potential conduits is normally done using one of two methods: working outward from the deception target and their "inner circle" of information sources or working inward by visualizing the presentation of a potential indicator to known adversary collection capabilities up through the process flow to the MILDEC target. Whatever method (or combination of methods)

is used, the more conduits that the planner and supporting J-2 analysts can identify and map, the greater the chance that friendly deception operations can be synchronized to feed multiple conduits simultaneously, thus increasing the potential success of the deception. However, the more conduits the adversary can access, the greater chance that the deception might be discovered (see paragraph 4, "Jones' Dilemma," in Appendix A, "Military Deception Maxims").

b. One method of characterizing conduits for better shared context within the planning team is by classification as a simple or complex conduit. A simple conduit is one which transmits data to the intended decision maker without the application of an intermediate filter. A complex conduit is one which includes one or more filters that might substantially alter the content, add context to the observable, or alter the timeframe for delivery. Ideally, the MILDEC planner selects multiple conduits to deliver information to the deception target and sequences the delivery in a manner that builds and confirms the deception story over time. This can cause information about the same observable to be delivered at multiple differing times and sources which can reinforce the desired ambiguity increasing or ambiguity decreasing effect.

c. To enhance the believability of the deception story, the MILDEC planner works with OPSEC, other IRCs, and the joint force components to manage competing observables (any indicator that might contradict the deception story) and limit the function of conduits that are likely to register and report them.

d. While the initial discussion of a given conduit might address the relevant information flow in simple terms, the conduit cannot actually be fully exploited until it is analyzed in detail. Intelligence analysts and MILDEC planners must understand and subsequently collaborate to diagram the key elements and complete a worksheet or other planning template that corresponds to each conduit for use in future planning. Key elements of information include:

(1) A graphic depiction of the conduit.

(2) A description of the sensor, including sensor locations, cueing and function, times of expected availability, technical performance parameters, exploitable vulnerabilities, and reliability.

(3) A description of the transmission means from sensor to deception target including the location and function of any intermediate nodes and/or filters (not all nodes are filters, but all filters are nodes). When filters are present, describe the type of filtering (aggregation of reports, synthesis of data, attribution of organizational or personal bias, etc.) and its probable impact on the observable.

(4) The average transmission time of an observable from sensor to deception target. Normally this is expressed in hours and will include two numbers: a transmission time for "routine" observables presented in the context of summarized reports and an expedited transmission time for observables that rise to the level of probable adversary

PIR. Understanding conduit function time is critical to synchronization of MILDEC execution.

(5) A description of the points in the conduit at which friendly intelligence collection can be utilized to monitor the transmission of data, and to what level of fidelity, to track its delivery to the deception target (MOP). Describe any potential locations where MOEs such as lateral transmission, increased activity or readiness in tactical forces, or actual content monitoring might take place.

(6) Information on any risks incurred by using this conduit. Risks might include exposure of friendly means, forces, or sensitive capabilities, as well as potential awareness by the adversary that a selected means might be part of a friendly deception, causing the conduit to lose credibility. Figure IV-3 shows notional conduit analysis. A simple review of the complex conduit illustrated provides a snapshot of the intelligence fidelity required to support MILDEC planning.

5. Support to Military Deception Assessment

The development of MILDEC MOPs and MOEs differs slightly from similar processes for other capabilities. One way to easily conceptualize MOPs and MOEs for MILDEC is to use the "see, think, do" methodology outlined in Chapter I, "General." A MOP is most closely associated with **see:** did we portray the planned indicator, and did the adversary see our execution and transmit the desired message to the deception target creating an observable? MOEs are associated with **think** and **do:** what perceptions and conclusions did the adversary draw from a particular observable (alone or in the context of other observations), and are those perceptions leading toward the desired action/inaction captured in a deception objective? For a more detailed understanding of operational assessment as a whole, including organization, framework, and process, see JP 5-0, *Joint Planning*.

a. MOP collection for MILDEC involves two conceptual steps: determining that the tasked friendly unit or capability employed the desired means to create an indicator at the appropriate time and location and verifying that the intended adversary conduit(s) cued on the friendly signature(s), transmitted the collected data, and delivered the information to the deception target in a discernable context. This is the defining difference of a MILDEC MOP versus a traditional MOP ("did friendly forces perform the directed action") in that part of every successful MILDEC execution involves action by the adversary. The conduit that the deception seeks to exploit must function. This has significant implications for friendly targeting that will be discussed in Chapter V, "Military Deception Planning."

(1) Determination that a scheduled MILDEC execution took place occurs through J-3 operations reporting channels during the execution of the plan. This reporting by the element controlling a particular execution is to be coordinated by the DOWG through the J-3 ahead of time. It is done as a part of the finalization of the plan within the appropriate access and security controls.

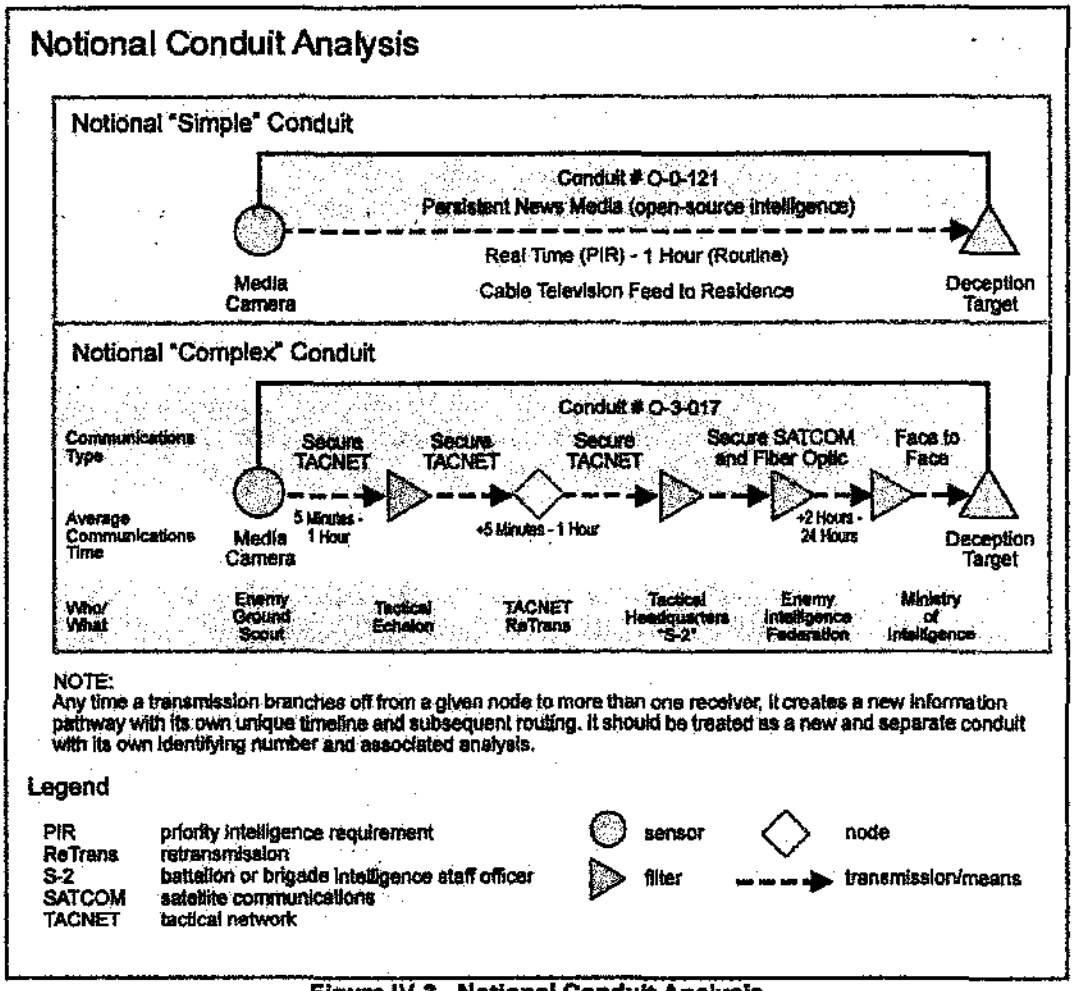


Figure IV-3. Notional Conduit Analysis

(2) Verifying the adversary conduit functioned as diagrammed and the desired information reached the deception target is a more complex activity requiring focused and coordinated intelligence, surveillance, and reconnaissance support. Using their previous conduit analysis work, MILDEC planners, supporting intelligence analysts, and the J-2 collection manager collaborate to identify points at which the information transmission might be susceptible to friendly monitoring and analysis. The presence of filters in the conduit pathway makes this process even more difficult because predicting the level of data aggregation or synthesis with other friendly observables is subjective at best. In some cases, the appearance of an anticipated MOE might be the only validation that a persuasive observable was accurately received and perceived.

b. MOE development and collection for MILDEC focuses on the current cognitive state of the deception target. The adversary's cognitive state can be measured in one of two ways. The first is through the evaluation of known comments or public statements by the decision maker. The second is by identifying and monitoring a related flow of

adversary activity that would indicate the deception target was effectively moved toward the desired perception and subsequent action/inaction. The baseline MOE is whether the adversary capability to be affected is employed in the manner that met our desired effect. However, the knowledge of this activity occurring or not occurring may not be available until the moment our effect is required.

c. To provide the commander with the necessary space to adjust plans as needed based on timely MOEs, the J-2 and DOWG coordinate to develop them. For example, if one of our deception objectives is for the adversary to hold the armored reserve away from the decisive point of ground action, the JFC would develop MOEs related to the accomplishment of that objective. MOE examples related to the action or inaction of the reserve might include such things as an increase or decrease in preparation of defensive positions (implying a period of static activity), increase or decrease in adversary intelligence collection in the vicinity of our main axis of advance at the expense of other sectors (is the adversary "telegraphing" an interest?), an increase or decrease in route reconnaissance toward the friendly sector by armored reserve units or leadership (is this pending or an active branch plan?), or an increase or decrease in battle drill or movement rehearsal by the adversary reserve.

d. Without the close support of the J-2 and a deliberate focus on the development of viable MOPs and MOEs as part of the deception plan, the success or failure of the MILDEC might not be known until the moment that a planned adversary action or inaction is turned against us. This could result in a loss of initiative or increased friendly loss of life.

Intentionally Blank

CHAPTER V
MILITARY DECEPTION PLANNING

[redacted]

1. Military Deception Planning and Joint Planning Processes

To ensure proper integration with the commander's objectives and desired end state, MILDEC planning is conducted as part of the JPP. The early integration of MILDEC in the planning cycle ensures optimum application of resources and maximizes the potential for overall success. Because of its inherent sensitivity, access to MILDEC planning is usually protected. As a result, MILDEC planning takes place in an access-controlled, parallel planning process rather than through open discussion in the joint planning group (JPG) or the IO working group. Key staff members and leadership accessed to the MILDEC plan discretely integrate and deconflict MILDEC planning outputs into the overall planning effort. The need to conduct adequate coordination during MILDEC planning should be balanced against the need to maintain the secrecy required for effective MILDEC operations. Establish and use strict need to know criteria to determine which individuals are allowed to participate in MILDEC planning. The criteria may specify separate levels of access to facilitate coordination, thus allowing more individuals access to the less sensitive aspects of the deception plan. CMDOs can provide further guidance on the classification, handling, review, and approval process for MILDEC.

a. Since MILDEC is considered an IRC, MILDEC planners are routinely organized under the JFC's IO staff proponent or its equivalent within the J-3. MILDEC planners participate in both deliberate planning (used normally during peacetime to develop OPLANs and CONPLANs), and crisis action planning (during time-sensitive situations to rapidly develop campaign plans and orders). See JP 5-0, *Joint Planning;* Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122 Series, *Joint Operation Planning and Execution System (JOPES);* and CJCSM 3130 Series, for discussion on deliberate planning and crisis action planning.

b. MILDEC should be planned and executed as part of the overall CONOPS from its inception. MILDEC is not applicable to every situation, but commanders and planners should consider it with the same emphasis given to other capabilities and assets, particularly at the operational level. Successful military planners rely on deception to mask the real objectives of military operations. MILDEC remains a critical contributor to enabling surprise and economy of force, mass, and security. Capabilities in MILDEC operations vary with the mission type, adversary, location, assets available, and even the political climate. There is a growing availability of MILDEC capabilities. Technological advances now enable joint forces to employ a larger range of deception techniques.

c. Even under conditions where joint MILDEC or TAC-D is inappropriate, there may be a viable role for DISO in protecting the commander's warfighting profiles or obfuscating critical information and indicators, causing FIEs to misdirect their analysis of friendly operations or subsequent application of intelligence resources. In support of an OPSEC plan, DISO may enhance the collective efforts to convey or deny selected information or signatures to a FIE and limit the FIE's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets. The intent of DISO is to use deceptive observables, activities, or measures to support OPSEC that is focused on FIEs, and not to generate a targeted decision maker's action or inaction.

d. The scope of the MILDEC operation is limited by the amount of time and resources available for its planning and execution, the adversary's susceptibility to MILDEC, and the joint force's ability to assess the MILDEC. Progression of adversary activity may lead to the deception plan being overcome by events. Additionally, the lack of accurate intelligence and cultural awareness can hinder MILDEC operations. Proper planning with regard to time, resources, accurate intelligence, cultural awareness, and other factors is essential to a successful MILDEC operation. See Chapter I, "General," for a review of terms and concepts outlined in the planning process.

e. The final output of MILDEC planning is usually captured in accordance with CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance*, as the OPLAN's tab B (Military Deception) to appendix 3 (Information Operations) to annex C (Operations).

2. Military Deception Planning Basics

a. **Reexamine Planning Criteria.** As with all joint planning, MILDEC planning is an iterative process that requires continual reexamination of its goals, objectives, targets, stories, and means. Commanders and staffs must respond to the dynamics of the situation and of their own headquarters.

b. **Organize for MILDEC Planning Success.** The DPC oversees MILDEC planning and execution. The DPC normally consists of the CMDO, any MILDEC planners appointed by the command, and the component MDOs. In most circumstances, the DPC will form a larger DOWG to facilitate the planning, coordination, and discrete integration of MILDEC throughout planning, execution, and assessment. The DOWG may be formed using existing members of the JPG, IO cell, primary deception capability and means providers, and other key planners the commander or the DPC chief determine. At a minimum, the DOWG should include the core DPC members and representatives from J-2, J-3, J-4, J-5, J-6, and the command OPSEC planner. In accordance with the JFC's guidance and under the authority of the J-3, the DPC (supported by the broader DOWG) plans, directs, monitors, and assesses MILDEC operations. With the JFC's approval, the DPC may also provide planning, execution, and termination support for MILDEC operations undertaken by higher command echelons in their operational area. If established, the DPC is usually tasked with writing tab B (Military Deception) to

appendix 3 (Information Operations) to annex C (Operations) for the OPORD. Other responsibilities of the DPC are to:

(1) Direct and coordinate deception planning activities.

(2) Interface and work closely with unit operations planners to review and analyze deception plan requirements.

(3) Respond to higher headquarters' deception tasking.

(4) Coordinate with higher headquarters on proposed deception efforts to resolve potential conflicts.

(5) Provide resource requirements to higher headquarters for deception program development and sustainment.

(6) Look for opportunities to implement deception in support of military objectives.

c. **Plan MILDEC Operations from the Top Down.** Subordinate deception plans must support higher-level plans. Commanders at all levels can plan MILDEC operations but must coordinate plans with their senior commander to ensure overall unity of effort. OPSEC may dictate that only a select group of senior commanders and staff officers know which actions are purely deceptive in nature. This situation can cause confusion within the force and requires close monitoring by JFCs and their staffs.

d. **Coordinate MILDEC and OPSEC Planning Efforts.** As previously discussed in Chapter II, "Military Deception and Information Operations," MILDEC and OPSEC are complementary IRCs. In addition to the primary planning goal of unifying what is visible to adversary military decision makers into a holistic and managed denial and deception effort, MILDEC and OPSEC planning intercept at multiple points in the JPP. In execution, MILDEC activities themselves frequently require OPSEC measures and countermeasures to protect sensitive means and resources, and ultimately enhance their believability to the adversary.

3. The Military Deception Planning Process

The MILDEC planning process is an iterative process that requires continual reexamination and validation throughout the planning and execution phases. The MILDEC planning process consists of five steps that generally align with similar activities in the JPP as identified in Figure V-1.

a. **Step 1: Deception Mission Analysis.** The primary inputs and outputs for this planning step are outlined in Figure V-2. Deception mission analysis begins following plan initiation as outlined in JP 5-0, *Joint Planning*. Since MILDEC is a protected effort, the commander's initial MILDEC guidance will often come in a separate written or verbal deception planning directive.

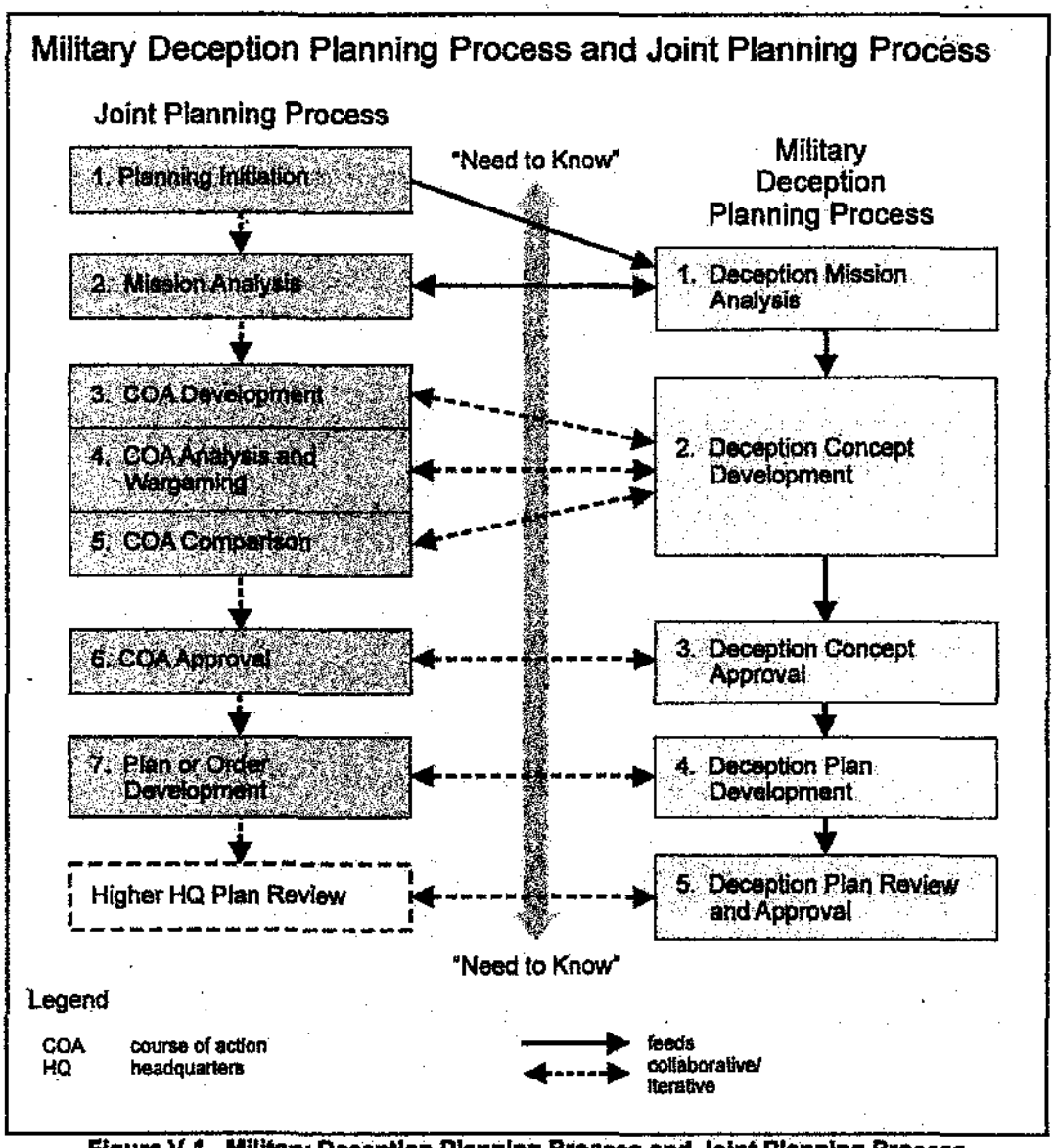


Figure V-1. Military Deception Planning Process and Joint Planning Process

(1) In the absence of specific guidance for inclusion of deception in the commander's initial operational approach, the DPC uses mission analysis to evaluate all appropriate planning references and guidance to determine if MILDEC can or should play a role in the overall campaign. That role, when identified, is stated in the form of proposed deception goal(s) and associated deception objectives. There may be multiple deception goals based on such considerations as operational phasing, duration, or complexity. Figure V-3 provides examples of the format and relationship between MILDEC goals and objectives.

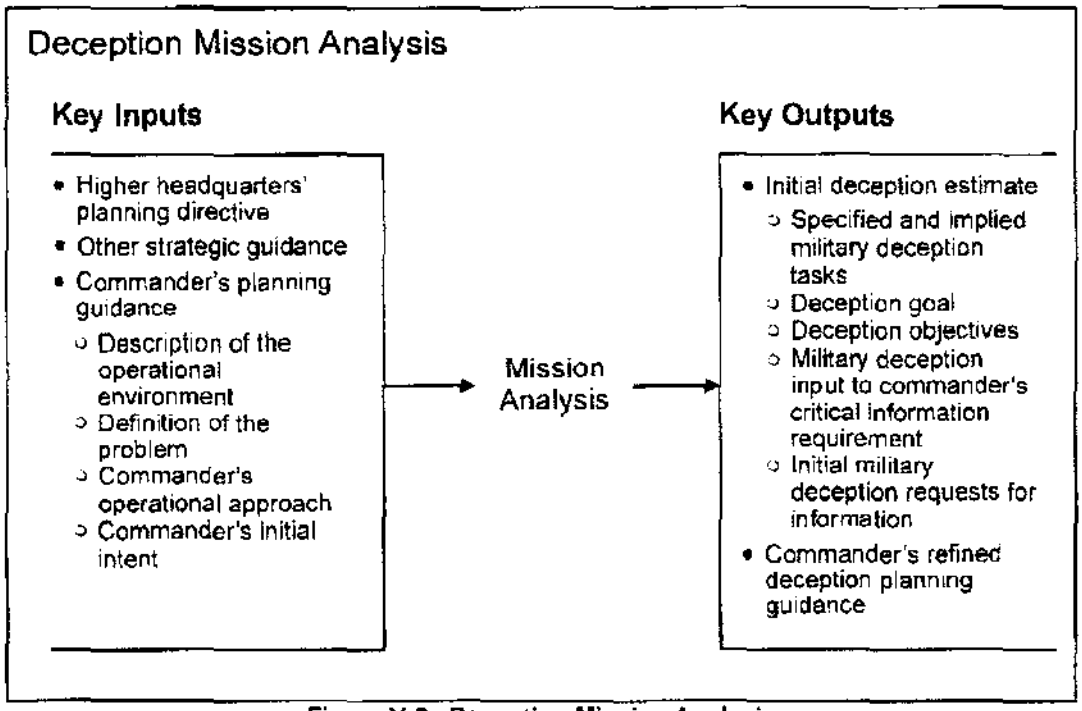


Figure V-2. Deception Mission Analysis

(2) Deception planners participate in the JPG and IO working group mission analysis process under the JPP. MILDEC planners integrate, refine, and contribute to the outputs from other staff sections such as planning facts and assumptions, operational limitations, initial risk determination, and development of overall success criteria as necessary and appropriate within need to know and access caveats.

(3) During the mission analysis step, MILDEC planners work carefully with the J-2 through the RFI process to obtain analysis of the adversary critical to effective deception planning. This information will form the basis of the DIE that feeds the development of a viable deception concept in the next planning step.

(4) The deception mission analysis step ends with the initial staff estimate briefing to the commander, approval of the deception goal(s) and objectives, and the issuance of refined commander's planning guidance for MILDEC. The commander may provide additional guidance concerning specific deception COAs the staff should address when preparing estimates. Once approved, the deception goal(s) and objectives become the focus for all subsequent MILDEC planning.

b. **Step 2: Deception Concept Development**

(1) During this step, MILDEC planners combine operational art with the MILDEC planning process to develop a viable concept of how MILDEC can achieve the commander's approved MILDEC goals and objectives. This may involve the development of one or more distinct operational approaches based on the complexity and

Sample Military Deception Goals and Objectives

Deception Goal: "This military deception will"	Deception Objective: "The adversary (will/will not)"
Enhance deterrent force posture along Yellowland border to provide increased time for force deployment and diplomatic negotiation (Phase I: Deter).	Will not initiate offensive operations across the Yellowland border. Will assume a defensive posture along border positions. Will seek continuing negotiation in lieu of sustained military confrontation.
Provide the joint force land component commander with an overwhelming force ratio along axis red for the attack on Green City (Phase III: Dominate).	Will hold his armored reserves east of the Green River until friendly forces reach phaseline XXXX (course of action dependent). Will split his defense forces along the southern and western approaches to Green City. Will divert paramilitary militia forces toward internal population control.

Figure V-3. Sample Military Deception Goals and Objectives

variety of COAs developed by the JPG. The primary planning inputs and outputs for deception concept development are shown in Figure V-4.

(2) Using their initial staff estimate, any revised commander's planning guidance, and a detailed knowledge of the adversary contained in the DIE, MILDEC planners in the DOWG develop one or more deception concepts or COAs. The actual number will be determined by considerations such as the number of JPG COAs, the suitability of each to some form of deception, or time and personnel available for MILDEC planning.

(3) For ease of understanding by the commander and selected staff, the DOWG normally develops MILDEC COAs using the same baseline operational sequencing and phasing as the JPG. Depending on the scope and complexity of the planned operation, MILDEC plans can range from fairly simple and short in duration to extremely complex, spreading over multiple phases and JFC operating locations. Based on the approved MILDEC goals and objectives, the MILDEC COA might include multiple LOOs. For example, MILDEC activities to mislead the adversary's conventional force commanders, causing them to waste combat power in phase III (Dominate), might begin in phase I (Deter) and be conceptually distinct from proposed MILDEC activity in phase IV (Stabilize) designed to deceive violent extremist organizations about potential vulnerabilities in security infrastructure during transition from major combat operations. As with the Operation BODYGUARD plan, each distinct LOO at the operational level might, as the plan develops, be assigned a different codename with its own access and control measures nested under the overarching plan. MILDEC planners might also be

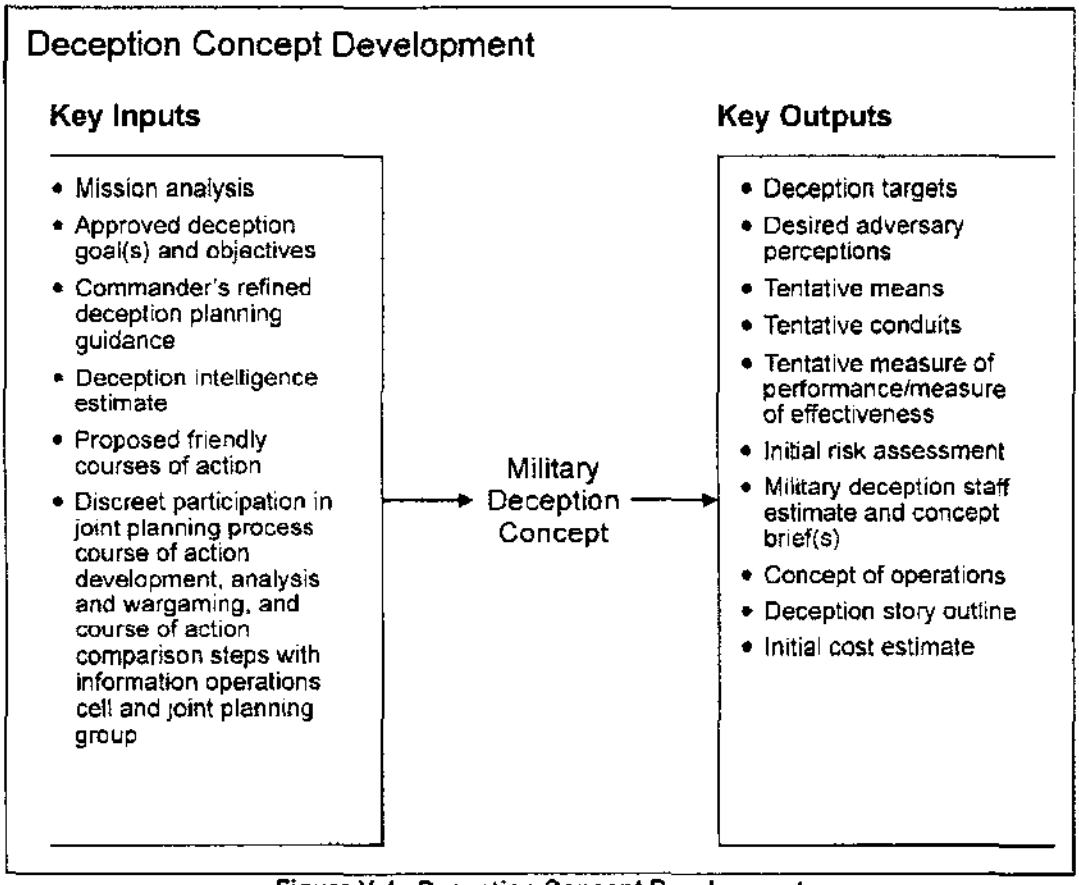


Figure V-4. Deception Concept Development

asked to support branch and sequel planning once a JPG COA is selected and finalized. For a deeper understanding of operational design, see JP 5-0, *Joint Planning*.

(4) Each proposed deception concept or COA must be capable of accomplishing the commander's deception goal(s) and meet the doctrinal requirements for COA sufficiency: adequate, feasible, acceptable, distinguishable, and complete. In some cases, actual COAs developed by the operational planners can provide the basis for MILDEC COAs, for example, portraying the operational indicators associated with COA "A" in support of COA "B" or vice versa. Using alternative COAs developed by operational planners helps to ensure the deception COAs are feasible and practical military options. Additionally, the proposed deception COAs should seek to promote actions the adversary is already conducting or considering.

(5) Each MILDEC COA developed in parallel with the JPP will contain, as a minimum, the deception target(s); desired perceptions arranged in a preliminary deception story; proposed deception types, techniques, or tactics; tentative conduits; draft MOPs and MOEs; preliminary sequencing, concept sketches, and accompanying narrative for presentation in the COA selection brief; and an initial assessment of risk. Additionally, MILDEC planners will observe the JPG wargaming process for each COA

in order to incorporate the "action, probable reaction, counteraction, assets, and time used" understanding in refining their associated MILDEC COA.

(6) The first step in creating the desired action or inaction as defined in the deception objective is the identification of the deception target that has the authority to make that action or inaction. Key considerations in the appropriate selection of the deception target include understanding the target's relationship to the MILDEC objective's action or inaction; their position relative to adversary goals, aims, and strategy; current perceptions; decision-making process; key advisors; and primary means of collecting information. As planning progresses, intelligence analysts supporting MILDEC planning are frequently asked to develop individual target folders on specific deception targets to aid in later completion of the plan.

(7) The operational design reflected in the development of the deception goals and associated objectives, and their alignment with potential LOOs, will determine the number of MILDEC targets across phased operations. For example, approved MILDEC activity prior to the initiation of major combat operations in phase II (Seize the Initiative) might target a national-level military council that is exercising tight control over escalatory confrontations. Later on in phase III (Dominate), when adversary command and control communication systems have been substantially disrupted or destroyed, and operational decisions are likely delegated based on "red lines," the MILDEC target might be a corps-level commander that controls the operational reserve or another capability that we are seeking to affect.

(8) In some cases, MILDEC planners and supporting intelligence analysts may identify key individuals who, by virtue of their position or personal relationships with a decision maker, affect or influence the MILDEC target's decision making without actually participating in it formally or directly. For clarity of discussion, these persons are stakeholders and can either be conduits or filters depending on how they are utilized within the MILDEC plan. For example, stakeholders may affect the MILDEC's target's decision through the addition of aggregation, synthesis, or bias to an observable on the way to the deception target, and/or influence the deception target without actually participating in the formal decision process generating the action or inaction. Because of their proximity to planned MILDEC activities (closer in the conduit/information pathway flow than the deception target), stakeholders within the operational-level construct may also simultaneously be the deception target of a subordinate component's TAC-D.

(9) After selection of the deception target(s), the MILDEC planner establishes the desired perceptions that will focus later MILDEC events. **Desired perceptions** are the conclusions, official estimates, and assumptions the MILDEC target uses in their assessment and decision-making process. These adversary perceptions will be formed from both objective (observation and analysis) and subjective (intuition and experience) thought processes. They are also heavily impacted by biases, preconceptions, and filters applied in the collection, analysis, delivery, and reception of information. To properly construct a logical flow blending truthful and deceptive information and indicators (observable conditions) later in the plan, MILDEC planners should determine the target's current perceptions and assess the level of change (or reinforcement) to create the desired

perception. Desired perceptions should also exploit known adversary vulnerabilities in the physical, informational, and cognitive dimensions of the information environment.

(10) Planners arrange desired perceptions into the preliminary deception story. The **deception story** is a narrative statement, written from the perspective of the deception target or key intelligence analysts, which summarizes the deception portrayal. It is stated as a series of logical adversary conclusions about our capability, activity, and intent derived from all available observables. Deception stories are usually arranged in chronological sequence to facilitate planning and synchronization of events across phases and/or LOOs. The deception story is the operational-level "think" in the "see, think, do" methodology.

(11) Time is a key element to consider in developing the deception story. MILDEC planners must determine how much time is available to present the deception story and estimate how much time is required for the deception target to make a decision and direct the desired action. The available time may determine the scope and depth of the story. Analyze the following time-related issues during the development of the deception story:

(a) **Time of Maximum Disadvantage.** When does the adversary's action (or inaction) best suit the JFC objectives?

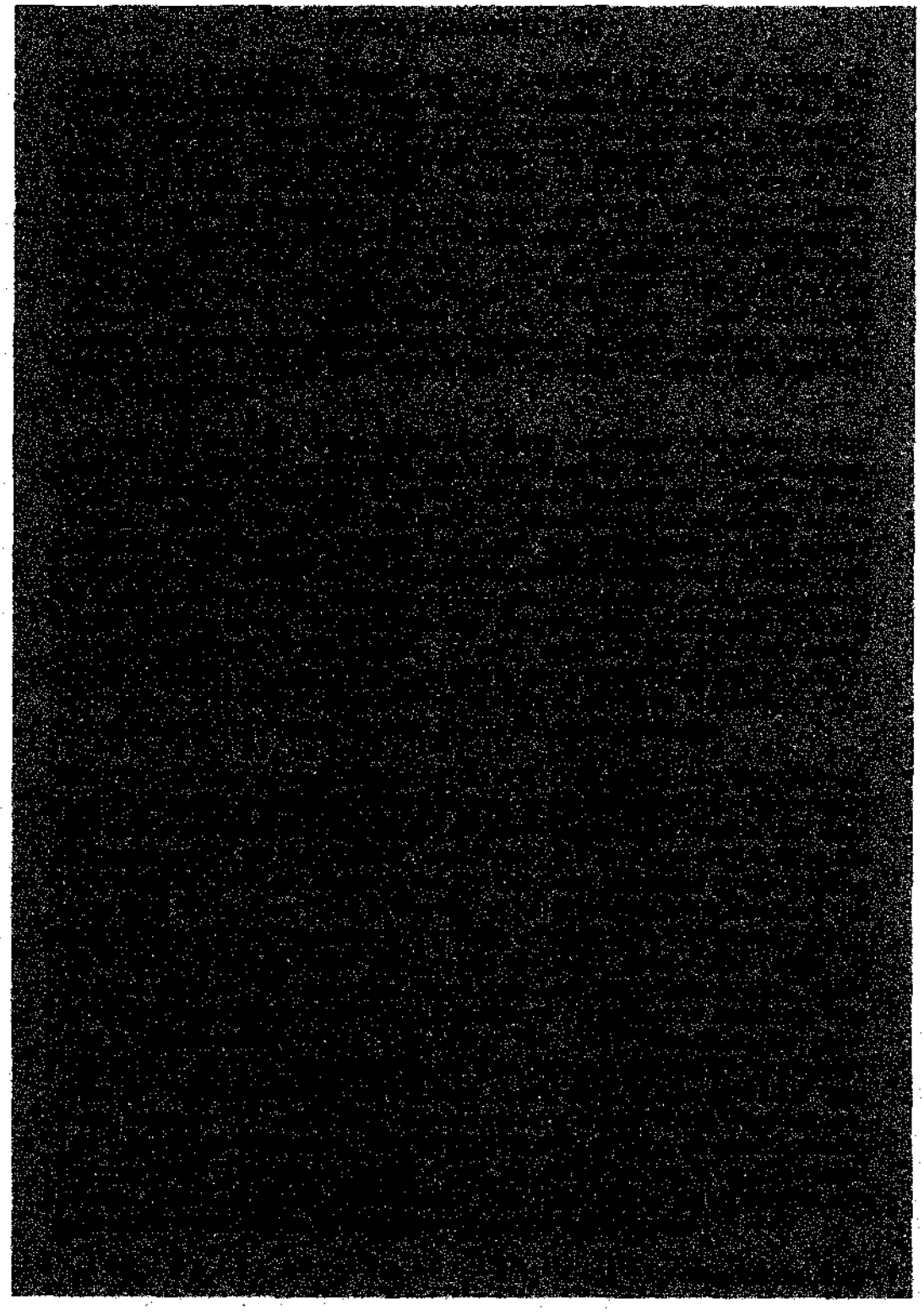
(b) **The Deception Target.** Is the target cautious or bold? Will the target react to initial indicators, or will the target require a series of events before reaching a decision? How long does it normally take the target to make a decision?

(c) **Adversary Response Time.** Once the decision is made, how long will the target need to formulate and issue an order? For example, if the deception objective is the movement of an adversary mobile reserve to some distant point, allow time for the deception target to issue the movement order and for the unit to receive and execute the order.

(d) **Intelligence Processing.** How much time is needed for the adversary's detection and collection systems to collect, analyze, and provide false intelligence created by the deception to the deception target? This will vary depending on the target's level of command.

(e) **Execution of the Deception Tasks.** When must displays, demonstrations, feints, and other actions be detected or recognized by the adversary's intelligence collection methods and systems? How long should each last?

(12) At this time in concept development, the MILDEC planner normally begins to refine their operational design construct by selecting appropriate MILDEC types (ambiguity increasing or ambiguity decreasing), MILDEC techniques (feints, demonstrations, ruses, or decoys), and applicable MILDEC tactics to help structure the development of key MILDEC events that will constitute the detail required to determine COA viability and desirability. See Chapter I, "General," for a description of these terms.



(13) Using the preliminary deception story and operational design considerations, the DOWG identifies indicators that most effectively portray the deception story, mentally aligns those indicators with one or more adversary conduits to create an observable, and begins the selection of MILDEC means to activate those conduits to create the "see" in the "see, think, do" deception methodology. By analyzing which indicators most effectively portray the friendly activities and profiles that convey the deception story, the MILDEC planner is able to better focus his selected techniques and apply limited or costly means in a more effective manner. Contrast and anticipated exposure must also be factored into the deceptive portrayal.

(a) Indicators are the "puzzle pieces" the MILDEC planner creates for the adversary to most effectively and efficiently lead them to a desired perception and subsequent conclusion. This activity directly complements the denial and deception construct outlined in Figure II-2, where OPSEC is focused on concealing critical information and indicators that constitute the commander's essential secrets related to the JPG's actual COA while the MILDEC plan provides plausible alternatives that require an adversary response. JP 3-13.3, *Operations Security*, identifies five characteristics of an indicator that provide important understanding to the MILDEC planner in the selection of indicators to portray the deception story. See Figure V-5 for their meaning.

(b) Identification of the most appropriate indicators to portray the deception story requires detailed knowledge of friendly operational profiles, as well as reliable, current intelligence on "how" the adversary sees the operational environment. An operational profile is everything that a friendly force does to prepare for, conduct, and sustain operations. The creation of observables in this step aligns key indicators with adversary collection conduits and processes identified in the DIE (see Chapter IV, "Intelligence Support to Military Deception"). If, for example, the plan calls for creating indicators supporting the perception that there is an additional carrier task force available to the JFC outside the observation range of adversary visual sensors, MILDEC planners will work through the DOWG with the maritime component and OPSEC planners to determine what emitters are normally associated with that element and how they are normally employed to include the location and signatures of supporting surface ships and assigned aircraft flight and communication patterns. If the deception plan calls for creating the perception that an additional Army brigade combat team (BCT) is positioned on an alternate axis of advance observable by adversary signals intelligence and human intelligence, the MILDEC planner will need to know not only what communications systems are found in the dispersed units and how they normally operate, but also how many vehicles and of what types, where and in what pattern they are normally deployed, and the supporting logistical infrastructure and footprint. While it is not the JTF-level MILDEC planner's job to plan the details of each execution to be performed by the tasked component in the examples above, the joint MILDEC planner does need the level of detail outlined to assess concept feasibility during COA development.

(c) Indicator and profile information is available through each of the components. To facilitate more efficient planning, joint deception planners, working with component MILDEC and OPSEC planners, can develop friendly component profile databases prior to the initiation of planning. This is particularly helpful when planning is

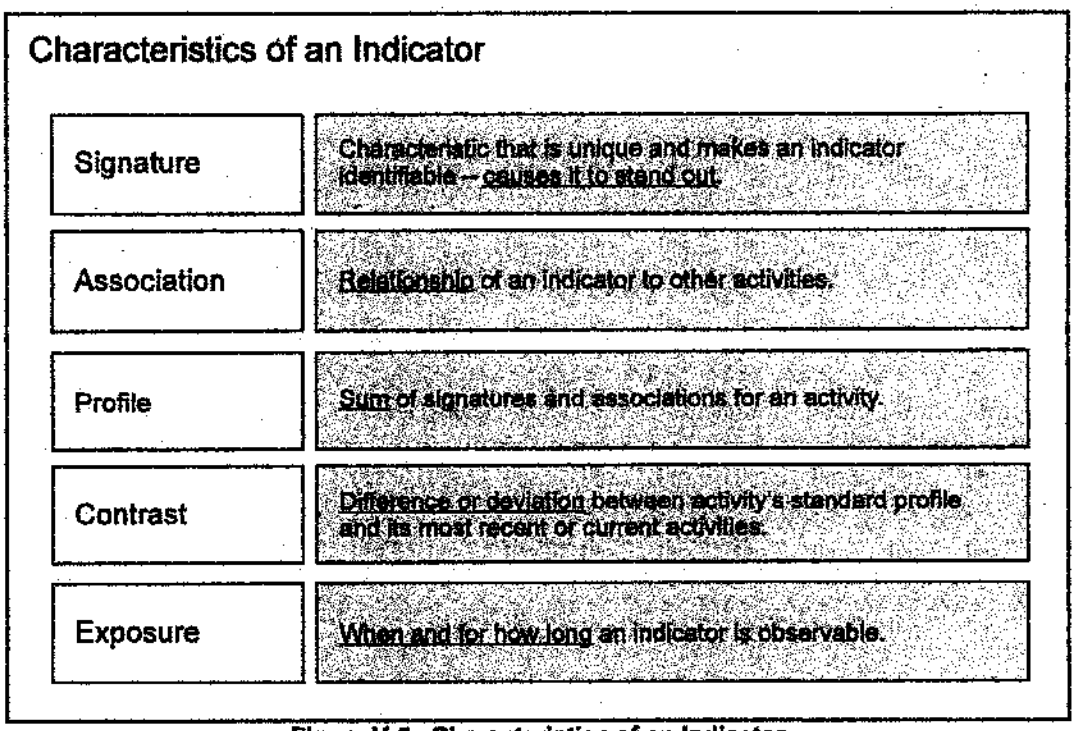


Figure V-5. Characteristics of an Indicator

time constrained. Such a database might contain profile data (all physical, technical, and administrative signatures and normal associations) for each service, capability, or function (e.g., IRCs, logistics, intelligence collection) by mission-essential task, by OPLAN activity, or any other logical conceptual boundary that facilitates analysis and subsequent ease of reference.

(d) Contrast and anticipated exposure must also be factored into the deceptive portrayal. While an unintended contrast can draw adversary attention to something friendly forces were attempting to conceal, planned contrasts can be used to draw adversary attention in unproductive directions. Exposure, the frequency and duration that an indicator is visible, can be used by the adversary to confirm or deny analysis, and must be factored in the development of the overall deception progression. By determining which indicators most effectively portray the friendly activities and profiles that convey the deception story, the MILDEC planner is able to better focus his selected techniques and apply limited or costly means in a more effective manner.

(e) Once the MILDEC planner understands the indicators and available adversary conduits that will be used to create the observables required for each perception in the deception story, the planners can begin to determine which are already visible to the adversary as part of the planned JPG COA and identify observables that must be altered or created as part of the deception plan. An example of this blending would be the actual mobilization and deployment of multiple mechanized Army BCTs from the US to theater versus using deceptive means to portray the operational

positioning and readiness of those same BCTs aligned with the deception story following their arrival. As with other steps in MILDEC planning, this requires a detailed and current understanding of the actual plan as formulated by the JTF JPG, as well as the activities of the IRCs coordinated by the J-3.

(f) Another key aspect of this process step is the identification and mitigation of competing observables. Use OPSEC measures to hide competing observables. If the observation of the competing observable cannot be mitigated, use other deceptive means to create plausible explanation for the existence of those observables.

(g) Once the DOWG identifies which observables best convey the deception story, the process of aligning specific means to create them begins. MILDEC means are the resources, methods, or techniques used to portray observables to the adversary deception target. A detailed discussion of MILDEC techniques, tactics, and means is found in Chapter I, "General." There are several factors to consider in developing and planning MILDEC events. The DOWG develops a sufficient number of tentative events for each proposed COA to facilitate the COA analysis and wargaming, comparison, and COA approval (selection) steps of the JPP.

(h) One of the first considerations in potential means selection is sensor-conduit linkage. What adversary sensors are in a position to observe the selected indicator in the location and timeframe it would logically occur? Ideally, we want to employ complementary physical, technical, and administrative means that activate a variety of sensor types that process information through both simple and complex conduits to the deception target. Considerations include such things as how will we know the sensor is active and transmitting information through the conduit? What is the anticipated reaction of adversary forces when the means are employed? What risks are associated with means employment (in terms of risk to force or risk to mission)?

(i) Selecting tentative deception means employment also has substantial implications for friendly forces and operations. The DOWG coordinates with other planning groups to address such considerations as who will control the means employment and what are the preparatory steps and associated timeline. What is the breadth of need to know for the unit conducting the deceptive activity? How long or frequently will this indicator need to appear (exposure) to make sure it was seen? What is the concept for means employment and what are the operational conditions and criteria that need to be established to optimize their effectiveness in portraying the desired indicator? How will the means employment be terminated and under what conditions? What is the estimated cost (in dollars, other resources, and operational efficiency) associated with this event?

(j) When developing tentative deception events, the MILDEC planner must also consider MOPs and MOEs (see Chapter IV, "Intelligence Support to Military Deception"). Proposed events that cannot be aligned with viable assessment criteria are not suitable for further development. MILDEC planners should be able to identify at least one solid MOP and MOE for each proposed event or event series.

(14) As the MILDEC planner begins aligning MILDEC means with selected indicators to generate observables, there needs to be a logical sequencing of events that supports completing and briefing the concept or COA. Planners can sequence and align tentative events by a variety of typographies to include LOO, desired perception, phase, component, geography, time, or any combination of the above. The DOWG will use this initial sequencing and alignment to build a more detailed product called the deception event schedule (DES) in MILDEC planning process step 4 (Deception Plan Development).

(15) Once the DOWG has completed the steps above, they prepare sketches and an associated narrative that capture the salient elements of the concept. Sketches should graphically represent such information as the timing, relationship, and control of key proposed events or groups of related events called deception series, the conduits that will be utilized to transmit the planned observables to the adversary decision maker, the location and function of key filters, the time for processing of the observable and any subsequent decision or order by the deception target, and any competing observables, along with their proposed mitigation plan. The narrative ties together all of the illustrative COA sketches and provides any additional detail necessary to facilitate understanding. A sample sketch, one of several that might be part of a final COA briefing, is shown in Figure V-6.

(16) The final component that must be addressed as a basic part of MILDEC concept or COA development is risk. Each deception event, series, LOO, and the deception concept as a whole require the application of risk analysis to inform the commander's evaluation and subsequent approval. Risk management begins in the planning process and continues through preparation, execution, and assessment. There are four general categories of risk associated with MILDEC. They are deception failure, exposure of means or feedback channels (compromise), risk to third parties, and risks associated with success.

(a) **Deception Failure.** MILDECs may fail for many reasons. It is possible the target will not receive the story, not believe the story, be unable to act, be indecisive even if the story is believed, act in unforeseen ways, or discover the deception. The failure or exposure of the deception can significantly affect friendly operations by reducing or eliminating the operational advantage the deception was to provide. For this reason, a commander must understand the risks associated with basing the success of any operation on the assumed success of a deception. There are generally two broad categories of MILDEC failures. Deception planners either fail to plan or implement the MILDEC operation carefully enough, or the intended target detects the deception.

(b) **Exposure of Means or Feedback Channels (Compromise).** Even if a MILDEC is successful, it is possible for the adversary to compromise the deception means or feedback channels. The risk of compromise of sensitive means and feedback channels must be carefully weighed against the perceived benefits of a MILDEC operation.

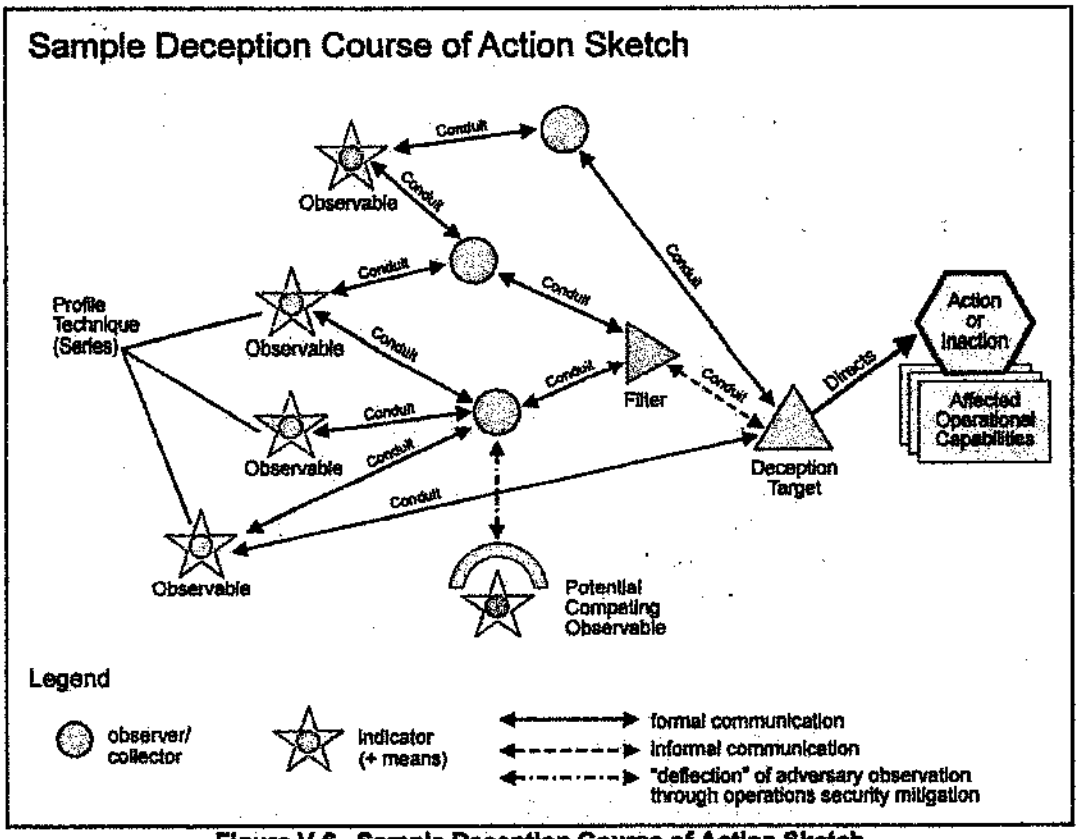


Figure V-6. Sample Deception Course of Action Sketch

(c) **Risk to Third Parties.** Third parties (e.g., neutral or friendly forces not aware of the deception) may receive and act on deception information intended for the deception target. MILDEC planners must ensure they are knowledgeable about friendly operation planning at the joint and multinational force level and at the component level in order to minimize the risk to third parties.

(d) **Risk Associated with MILDEC Success.** MILDEC can have unintended consequences if it is "too" successful or convincing. This is sometimes referred to as "catastrophic success." For example, a MILDEC LOO that portrays a larger force along a supporting attack axis to dissipate adversary defensive preparations might provoke an unintended adversary spoiling attack if it is perceived as an operational-level threat. If the deception means for this sample series of events is a small element using primarily decoys and technical means, the adversary response could cause significant friendly loss of life, control of terrain, or even threaten the progression of the larger plan. For this reason, deception plans and execution must be continuously monitored to help ensure the desired perceptions and effects remain aligned.

c. **Step 3: Deception Concept Approval**

(1) MILDEC concepts or COAs are normally presented in an access-controlled briefing attended by a subset of the staff, the command group, and other personnel with a demonstrated need to know requirement. Prior to the briefing, the DOWG analyzes the strengths and weaknesses of each of the proposed MILDEC COAs using the same or similar criteria as developed by the J-5 for primary COA comparison in the JPG. Some of the major considerations are feasibility, impact on actual operations, and security. How the deception COAs support the overall IO CONOPS is also considered. Planners preparing logistics, personnel, and intelligence estimates must also determine if the concepts they are examining can support the proposed deception COAs and determine the potential impact of the deceptions on their ability to support the operational mission. Normally, the CMDO will identify which MILDEC concept or COA will best achieve the commander's objectives while still aligning with the JPG recommended COA.

(2) The MILDEC concepts and proposed COAs are normally briefed prior to the JPGs briefing that facilitates JPP step 6 (COA Approval). When the commander finalizes JPG COA selection, the DPC will be informed which deception concept or COA is to be developed into a completed plan and provided with any additional commander's guidance or changes to previous guidance necessary to align the MILDEC effort with the approved JPG COA.

d. **Step 4: Deception Plan Development.** This step in the MILDEC planning process is performed in parallel with JPP step 7 (Plan or Order Development). Following COA selection, the entire JFC staff will apply their previous work and any revised commander's guidance issued in the COA selection step to refine and complete their portion of the plan. The J-2 continues to develop intelligence based on the flow of RFIs, while the JPG refines the operational approach. JPG and component planners complete their appropriate written plans to a level of detail resulting in tasks to components captured in the OPLAN, and in tools and formats that support future execution such as the commonly used synchronization matrix. This results in a series of nested joint and functional component plans and orders. MILDEC planners perform these same tasks relative to development and finalization of the MILDEC plan. Figure V-7 illustrates the primary inputs and outputs of this step.

(1) Using the approved MILDEC COA or concept as a base, the MILDEC planner integrates revised commander's guidance, updated intelligence analysis, and revisions to the primary COA to refine and complete the MILDEC plan. The initial step in this process is to review all previous planning products and adjust them as required. Are the MILDEC goals and objectives still appropriate to the commander's objectives and end states? Are the phasing, LOOs, selected deception targets, deception story, and key indicators still valid and complete? Are the selected deception means still appropriate to the conduits identified? Have any previous planning assumptions been invalidated?

(2) Following adjustment of the original concept, the DOWG finalizes the deception story to guide completion of the MILDEC plan. Using the same flow of

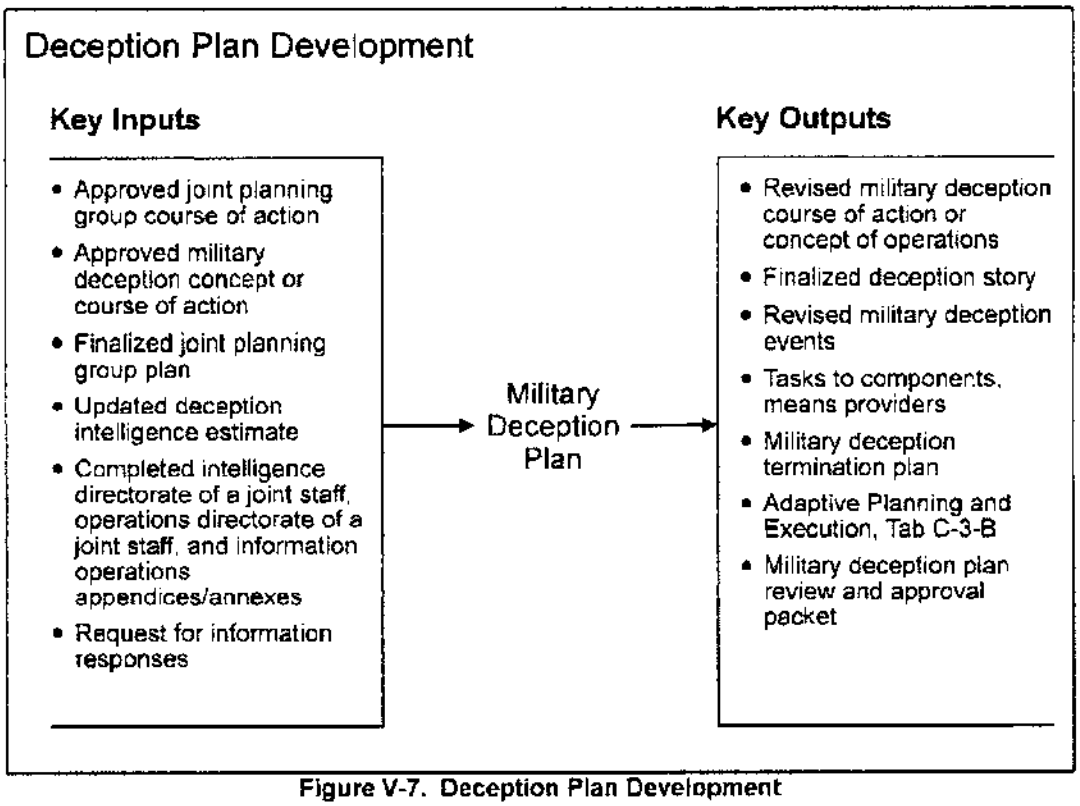


Figure V-7. Deception Plan Development

activity used to build the MILDEC COA, the DOWG refines and increases the level of detail to what would actually be required to fully execute the plan. This involves significant coordination with component and MILDEC means providers to build out planned deception events and series. Planners must also continue coordination with the J-2 to identify remaining intelligence gaps and plan the appropriate intelligence collection assets to support MOP and MOE collection necessary to assess and adjust the MILDEC plan (see Chapter IV, "Intelligence Support to Military Deception").

(3) One of the most tangible outputs of this step is the DES. The DES is the tool used to sequence MILDEC events for logical progression of the deception story and to synchronize the MILDEC with the broader plan. This requires identifying when specific means are employed. The objective is to ensure the deception target's perceptions are influenced in time to complete the desired action (the deception objective) at the most operationally advantageous time. The DES captures **what** will occur, **when** it will take place, **where** it will occur, and **who** will control the execution.

(4) Consider the following factors during scheduling:

(a) The timing of actual friendly activities.

(b) The time required for friendly forces to conduct the deception activity.

(c) Where a particular activity fits in the normal sequence of events for the type of operation being portrayed.

(d) The time required for the adversary intelligence collection assets to collect, analyze, and report on the activity.

(e) The time required for the deception target to make the desired decision and order the desired action.

(f) The time required to execute the desired action/inaction.

(5) Each planned deception event will be given a unique number to facilitate coordination and execution tracking.

(6) The DES is published as an exhibit to tab B (Military Deception) to appendix 3 (Information Operations) to annex C (Operations) of the OPLAN or OPORD. Figure V-8 provides an example of a simple DES.

(7) The completed DES forms the basis for the tasking and integration of JFC components and MILDEC means providers in the completed order.

(8) There are a variety of circumstances that might create a requirement to terminate the MILDEC in whole or in part. Developing contingencies for this eventuality is referred to as termination planning.

(a) Termination planning ensures the controlled, orderly cessation of planned MILDEC events, protects means and resources, and sets the parameters for any release of information relating to the deception. Planning the termination of a deception operation requires the same care and attention to detail that went into planning the deception's execution. Termination planning should include contingencies for unforeseen events such as the deception's premature compromise. In the event of compromise, termination planning for MILDEC should include a notification to rapidly inform those who may be affected.

(b) Controlling the exposure of the existence of a MILDEC operation or of elements of a MILDEC may be difficult because of the nature of the operation. The deception target may know that it was fooled. Most of the time, it is better not to reveal a MILDEC—either to the adversary or to friendly forces—to avoid deception exposure. In some cases, however, it is useful to announce the contribution of MILDEC to operational successes, if a MISO goal is to degrade the effectiveness of the deception target or to degrade the adversary leadership.

(c) There are numerous potential termination scenarios. These scenarios are similar in concept to those used to identify risk in the previous step. Termination scenarios include:

Sample Deception Event Schedule

Identification Number	Objective	Deception Target	Date/ Time to Initiate	Action	Means	Unit	Date/ Time to Terminate	Remarks
29	Simulate preparation for movement south.	Enemy 8th Corps Commander	131500	1. Establish traffic control points. 2. Install radio nets. 3. Pass scripted messages traffic per scenario.	Friendly force movement and organic systems	Headquarters 2nd Division	131800	Initiate counter surveillance measures to prevent adversary visual proof reconnaissance of notional route.

Figure V-8. Sample Deception Event Schedule

1. The **successful MILDEC operation scenario,** in which the deception has run its natural course, achieved its objectives, and termination will not expose or affect the deception.

2. The **change of mission scenario,** in which the overall operational situation changes and the circumstances that prompted the MILDEC no longer pertain.

3. The **recalculated risks and/or probability of success scenario,** in which some elements of the MILDEC estimate have changed in a way that increases the risk and costs to the friendly forces and the commander elects to end the MILDEC component of the COA.

4. The **poor timing scenario,** in which the MILDEC is proceeding and may succeed, but it is not along a time line that is synchronous with other IRCs or other aspects of the operation or campaign. Or it becomes evident that the window of opportunity for exploiting certain conduits or the target itself has closed. In this case, the MILDEC ceases to be relevant to the overall operation.

5. The **new opportunity scenario,** in which at some point in the execution of the MILDEC it becomes apparent that if some elements of the MILDEC (e.g., choice of conduits, objectives, targets) are modified, the probability of success will increase, risks will be reduced, or the impact of the deception will be greater. In this case, the commander may want to terminate some MILDEC events and activities, while reorienting other elements of the MILDEC.

6. The **MILDEC compromise scenario,** in which the commander has cause to believe that all or some elements of the MILDEC have become known to the adversary.

(d) The termination concept provides the initial planning considerations to implement and should include the following:

1. A brief description of each termination scenario circumstance included in the plan.

2. Initial steps for initiating termination operations in each scenario circumstance included in the plan.

3. Identification of the commander who has termination authority.

(e) The DPC should anticipate that, as the plan proceeds in execution, the circumstances of termination will probably change. A termination concept that may be entirely suited to the initial set of conditions may be far different from what is required as the MILDEC matures.

(f) The termination concept should identify if and when information about the MILDEC is released. It may provide a cover story should questions arise about the role of MILDEC in a particular operation. The termination concept should also include classification and dissemination instructions for deception-related information.

(9) Following completion of the DES and the termination plan, the MILDEC planner has everything required to complete tab B (Military Deception) to appendix 3 (Information Operations) to annex C (Operations) of the OPLAN or OPORD. The use of exhibits, worksheets, and templates used in the development of the MILDEC plan can add clarity and detail to an "on the shelf" plan so personnel who were not part of the original planning process can rapidly grasp its contents (for review or contingency activation). Tab B (Military Deception) to appendix 3 (Information Operations) to annex C (Operations) and selected exhibits also form the basis of the deception plan review and approval package.

e. **Step 5: Deception Plan Review and Approval.** Review and approval requirements and processes are stipulated in CJCSI 3211.01, *(U) Joint Policy for Military Deception*. The need to know criteria remain in effect, however, and only a limited number of personnel participate in the deception plan review and approval process.

CHAPTER VI
EXECUTION OF MILITARY DECEPTION OPERATIONS

[redacted]

1. Execution of Military Deception Events and Actions

The MILDEC plan is normally executed as a component of the OPLAN/OPORD. When a CCMD or functionally organized JTF receives an execute order for a given plan, the associated MILDEC plan may also be activated within the given authorities and approval processes as outlined in CJCSI 3211.01, *(U) Joint Policy for Military Deception*. As with the MILDEC planning process, the transition from MILDEC plan to MILDEC execution is handled by the DPC, assisted by a functionally organized DOWG. JP 3-33, *Joint Task Force Headquarters,* illustrates the process for transition of a plan from future plans or future operations to current operations. This same process is applied to transition the MILDEC plan, although it is normally carried through execution by the same core deception team rather than transferred to other personnel.

2. Deception Execution Coordination

Once a plan is activated, it is critical that constant coordination at the strategic, operational, and tactical levels continues. There is potential for a tactical- or operational-level deception to have strategic implications. With this in mind, a continual process of coordination, called the deception execution cycle, must take place. Figure VI-1 represents the primary activities within the deception execution cycle.

a. **Adjust the MILDEC Plan as Necessary for Changed Conditions.** The cycle begins with a review of the plan by the DPC/DOWG. In this step, the DPC/DOWG analyzes the current situation and compares it with the operational environment, anticipated conditions and planning assumptions against which the plan was developed. Existing RFIs are reemphasized, and new RFIs are developed to address shortfalls in necessary intelligence. Sample DPC/DOWG activities in this step are:

(1) Review and identify any changes to the adversary situation, such as adjustment to the adversary decision-making process or key military decision makers; changes in adversary force structure, disposition, and intelligence collection (conduits or information pathways) to best facilitate the effective delivery of the deception story; changes in third-party intelligence support; or potential new sources of open-source intelligence based in rapidly evolving social media or other networks.

(2) Identify and review changes to the friendly plan, such as revised strategic or commander's guidance; changes to allocated forces or their flow into theater; addition, subtraction, or changed relationships with multinational partners; changes to basing or

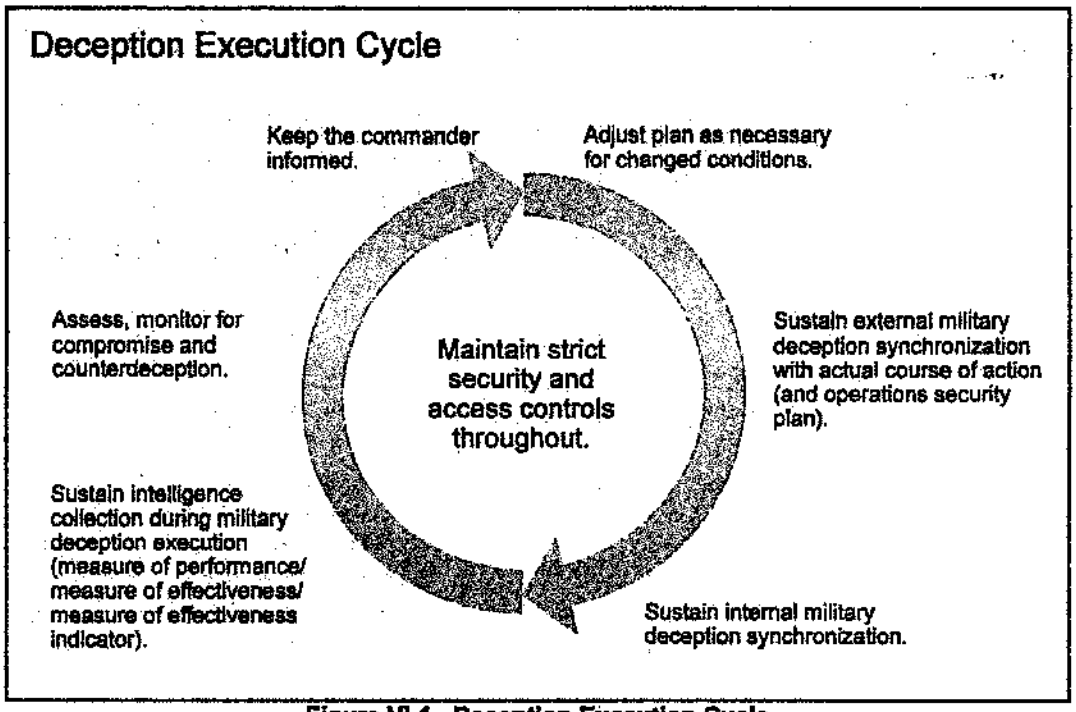


Figure VI-1. Deception Execution Cycle

overflight permissions; changes to available MILDEC authorities, resources, or tools; or adjustments to operational phasing or timing. The DPC coordinates with the J-3 on initial deception and operations execution timing to ensure a synchronous, supporting relationship exists that will aid the MILDEC, the operation, or both.

(3) Once the DPC/DOWG has updated their knowledge of the enemy and friendly situations, all key elements of the plan, from the deception goal and objectives through the final DES, are validated or adjusted as required.

(4) While this is the first step in the deception execution cycle, it is also a **continuous process of analysis and adjustment** as conditions evolve and change over the course of mission execution. The traditional maxim that "no plan survives initial contact" is particularly true when applied to the complex and response-focused application of MILDEC.

b. **Sustain External MILDEC Synchronization with the Actual COA and OPSEC Plan.** Among the MILDEC planner's most critical execution tasks is ensuring the MILDEC is proceeding in synchronization with the commander's overall operational concept and is in line with the command's employment of IRCs.

(1) The DPC/DOWG must conduct coordination both vertically and horizontally with commanders and staffs to ensure up-to-date integration between real-world operations and deception operations. This helps with synchronization of the deception story and helps to ensure the portrayal is credible, believable, and realistic.

Changes to any operational aspect, such as presence, capability, strength, intent, readiness, future location, timing, or method of planned friendly operations, must be accounted for in the scheduled execution of MILDEC activities. This requires discrete MILDEC participation in the JFC's organizational elements that conduct such functions as situational awareness, targeting, assessment, and providing routine updates and operational analysis to the commander.

(2) Since MILDEC and OPSEC work closely together in the holistic portrayal of friendly activities, and MILDEC activities are often supported by focused OPSEC measures and countermeasures to protect their existence, special care is needed in keeping MILDEC and OPSEC closely synchronized. This includes close cooperation in the targeting or exploitation of adversary conduits so they are either neutralized or available as required to create the desired OPSEC and MILDEC effects.

c. **Sustain Internal MILDEC Synchronization.** MILDEC executions, while planned in detail, do not remain static activities on an access-controlled DES or operational-level synchronization matrix. The DPC/DOWG maintains constant communication with components, capability owners, and other resource providers tasked to execute or support each event so the portrayal of the deception story proceeds as planned. This includes operational-level tasks, such as synchronizing different MILDEC LOOs, and balancing or shifting lines of effort as appropriate, to sustain the desired story progression. Based on feedback, some planned executions or event series might need to be adjusted, repeated, postponed, or cancelled as appropriate.

d. **Sustain Intelligence Collection during MILDEC Execution (MOPs, MOEs).** Working with the J-2 collection manager to help ensure intelligence collection assets are in position to collect MOPs, the monitoring of MOEs and indicators by the DPC/DOWG, as outlined in the plan, is essential to the internal synchronization of the MILDEC plan, as well as informing the commander on its status and current levels of success and/or revised risk. During combat operations in particular, the DPC/DOWG will have to actively compete for limited intelligence collection resources with much larger components and capabilities more familiar to the staff as a whole.

e. **Assess and Monitor for Compromise and Counterdeception.** Using the analytical feedback provided by MOEs collection, in conjunction with the assessment process, the DPC/DOWG determines the current progression and success of the MILDEC plan. Specially trained intelligence analysts, supported by MILDEC planners, must remain alert for indicators that one or more components of a deception story may have been compromised. This includes the identification of any possible adversary counterdeception efforts. MILDEC compromise, when detected, may lead to one or more termination or exploitation scenarios as discussed in Chapter IV, "Intelligence Support to Military Deception," and Chapter VII, "Counterdeception."

f. **Keep the Commander Informed.** The status of the MILDEC operation should be part of the commander's routine battlefield update and assessment processes. As the principal authority for the execution of the plan, the commander is responsible for any decision to alter or terminate the deception or, conversely, order a change to either the

MILDEC plan or the primary COA to exploit changing conditions. MILDEC also factors largely in the overall computation of operational risk. Increased risk might generate a requirement for adjustment to the plan in other areas.

g. **Maintain Strict Security and Access Controls Throughout.** It is imperative that tight security is practiced throughout the deception execution cycle to protect the MILDEC plan and its execution. While many decisions on need to know access will be made in the planning process, situations will arise that require legal and policy interpretation in addition to the best judgment of the CMDO and commander, as informed by the complex balance of mission with risk. In the intense and fluid activity of managing complex military operations, it becomes even more critical for all involved personnel to apply appropriate classification, handling, and access controls on a daily basis. Any OPSEC or other security violations of the MILDEC plan at any level (strategic, operational, or tactical) should immediately be reported and evaluated for their potential impact. Frequently, the command CI staff will be assigned responsibility to monitor for foreign intelligence detection, reflections, or responses to the MILDEC plan.

3. Terminating Military Deception Operations

a. As discussed in Chapter V, "Military Deception Planning," the termination of a MILDEC is concerned with ending the MILDEC in a way that protects both the short- and long-term interests of the command.

b. When termination is ordered, the selected termination concept becomes the basis for final termination actions. These actions conclude the operation in line with the deception events that have been executed, the assessed state of awareness of the target, and the commander's specific termination objectives at the time.

c. Termination of a MILDEC also encompasses evaluation and reporting. After action assessment should be conducted by the DPC/DOWG. This provides the commander an objective basis for determining the degree of mission success and for improving future MILDEC operations. Because important information on various elements of the MILDEC may continue to become available over a long period of time, a series of interim after action reports may be required before a final assessment can be made. The after action report provides a comprehensive overview of the deception as it was planned to work and how it actually proceeded in execution.

CHAPTER VII
COUNTERDECEPTION

1. Counterdeception as an Element of Military Deception

a. In today's increasingly complex operational environment, adversaries will more than likely use some form of deception to mislead friendly analysts and decision makers about their activities, capabilities, or intent in order to offset a friendly superiority or gain some other form of operational advantage. Counterdeception is an effort to detect, confirm, and subsequently negate, neutralize, or diminish the effects of, or gain advantage from, a foreign deception operation. Friendly decision makers must be aware of adversary deception activities so they can formulate informed and coordinated responses, but more importantly, so that friendly forces are not placed at an operational disadvantage. Counterdeception contributes to situational awareness and IO by protecting friendly command and control systems and decision makers from responding to deceptive manipulation or faulty analysis of the operational environment. Counterdeception is applicable across the range of military operations where adversaries might use deception in an attempt to alter our military engagement and security cooperation activities or even achieve operational surprise in the initiation of hostilities.

b. Knowledge of an adversary's deception plan enables a commander to take appropriate action against the deception. It also provides an opportunity to gain valuable insight into the means used to portray the deception and analyze adversary deception targets and objectives as an indicator of the broader context in which the adversary views friendly forces and operations. Counterdeception becomes a tool for influencing those perceptions and could subsequently be turned effectively against the adversary.

2. Detecting Adversary Deception

a. The IC has the primary responsibility to identify adversary deception. MILDEC planners can assist in this effort. Trained MILDEC personnel should be postured and have access to intelligence data, information, and products during the deployment and execution of friendly operations.

b. The first step in identifying adversary deception is to understand the adversary's deception doctrine, techniques, capabilities, and limitations. Knowing how the adversary has used deception in the past is also important. The DPC and the J-2, supported by the broader IC, collaborate to collect and provide this information as part of the DIE. Understanding the adversary's operational objectives; normal operational profiles; posture; tactics, techniques, and procedures; and intent are also crucial to identifying tactical or operational indicators of possible deception. Our own OPSEC doctrinal construct of signature, association, profile, contrast, and exposure can be used to assess adversary activity for its congruency with known patterns or expectations based on the evolving operational situation. Indicators of potential deception can range from an intuitive sense that "something is amiss" in the eyes of a dedicated analyst, to the outright compromise of deceptive means, methods, or activity by friendly intelligence collection assets. Properly balancing tactical and operational indicators with strategic assumptions is also important. The likelihood of surprise might be reduced if estimates weigh tactical indicators more heavily than strategic assumptions in some phases of the operation. Dismissing tactical indicators or other minor contrasts because they conflict with our own biases and preconceptions may allow a hostile deception to succeed.

3. Confirming Adversary Deception

If intelligence reveals or suggests adversary deception activity, it is the responsibility of the JFC staff to fully analyze the situation and ensure that this intelligence and its potential impact on the friendly operation are presented to the commander. One method is to form a counterdeception working group (CWG) to perform this function. A sample CWG might consist of the CMDO, selected component MDOs, J-2 analysts, IC LNOs if assigned, red team members, J-3 planners, and any other staff members who could provide expertise on the suspected adversary deception means or methods. If it has not already been done, the CWG should analyze JFC vulnerability to adversary deception using the physical, informational, and cognitive dimensions. They could then review available intelligence products to determine what the adversary deception plan might be. Using our own doctrinal methodology of "see, think, do," the CWG might use an abbreviated wargaming process to construct adversary deception goals and objectives, targets, desired perceptions and deception story narrative, probable events and means, conduits, and anticipated MOEs. The outputs of this technique could then be used to focus friendly intelligence collection assets that confirm or deny the existence and scope of an actual adversary deception plan and related executions.

4. Countering or Exploiting Adversary Deception

After an adversary's deception operation is confirmed, the CWG has two primary functions. The first is to examine past intelligence collection and analysis to determine the impact the deception may have had on friendly planning, decision making, or current operational activities. The outcome of this analysis may span the gamut from simple adjustment of planning assumptions to a fundamental change in the operational approach. The second function of the CWG is to develop and present proposed counterdeception COAs to the commander. For example, commanders can ignore, expose, exploit, or defeat adversary deception efforts. Each COA involves a different level of risk or opportunity that must be weighed in the overall context of the operation and commander's desired end state.

a. Ignoring the deception might be the best option if acknowledging the deception compromises friendly deception identification capabilities. Such a compromise of friendly capabilities might lead to future improvements in adversary deception capabilities. This scenario requires the CWG to continue to identify deceptive indicators and base the friendly force operational decision making and subsequent activity on actual adversary capability, activity, or intent.

b. Commanders might choose to publicly expose the deception to cause embarrassment or to increase risk within an adversary's operational cost/benefit analysis. Through exposure, the adversary might be persuaded that their deception operations are futile, too costly, or too risky to continue or that the discovery of their deception has left a primary LOO uncovered and vulnerable. Exposure of a deception prior to combat operations might also serve to weaken the adversary's political or military position with allies or domestic audiences.

c. Exploitation of adversary deception focuses on forcing an adversary to expend resources and continue deception operations that have been detected by reinforcing the perception that friendly forces are unaware of the deception. In this scenario, friendly forces provide positive MOE that the deception is having the desired effect until the culminating point of the adversary's deception (their desired "do or not do" for one of our operational capabilities) and then reacting in an unexpected manner that turns the adversary's anticipated advantage against himself.

d. Defeating the adversary deception effort could involve destroying or degrading the adversary's deception capabilities and resources so they are unable to sustain their portrayal of the deception story. Like the other potential COAs, this outcome should include a wargaming step to identify possible second- and third-order effects and associated risk.

Intentionally Blank

APPENDIX A
MILITARY DECEPTION MAXIMS

MILDEC maxims are derived by the military from game theory, historical evidence, social science, and decision analysis theory and are offered to enhance the MILDEC concepts provided in this publication. These maxims provide additional insight that can be used by commanders and their staffs to develop their plans. There are 11 deception maxims.

1. "Magruder's Principle"

It is generally easier to induce a deception target to maintain a preexisting belief than to deceive the deception target for the purpose of changing that belief. The German Army did this to the US Army in their Operation "WACHT AM RHEIN," meaning "Watch on the Rhine." Even the code name for their winter offensive in the Ardennes in 1944 connoted a defensive operation, which is what US forces believed would occur.

2. "Limitations to Human Information Processing"

There are two exploitable limitations to human information processing. First, the "law of small number" suggests not making conclusions based on a small set of data: there is no statistical certainty in doing so. Second, there is a frequent inability of deception targets to detect small changes in friendly force indicators, even if the cumulative change over time is large. This is the basis for using conditioning (crying wolf) as a deceptive technique.

3. "Multiple Forms of Surprise"

Achieve surprise in the following categories: size, activity, location, unit, time, equipment, intent, and style (the manner in which and/or intensity with which missions are executed).

4. "Jones' Dilemma"

MILDEC generally becomes more difficult as the number of sources available to the deception target to confirm the real situation increases. However, the greater the number of sources that are deceptively manipulated, the greater the chance the deception will be believed.

5. "Choice of Types of Deception"

Ambiguity-reducing deceptions are employed to make the adversary quite certain, very decisive, and wrong. Ambiguity-enhancing deceptions are designed to cause the deception target (adversary decision maker) to become increasingly uncertain of the situation.

6. "Husbanding of Deception Assets"

It may be wise to withhold the employment of MILDEC capabilities until the stakes are high. The adversary knows US forces are revitalizing MILDEC capabilities, so let adversary intelligence collection and decision-cycle assets continually contend with US threat capabilities, while friendly commanders employ it at the time and place of their choosing.

7. "Sequencing Rule"

Sequence MILDEC activities to maximize the portrayal of the deception story for as long as possible. Mask (OPSEC) unit activities indicating the true mission to the last possible instant. These activities must be sequenced and coordinated in both time and space to be effective.

8. "Importance of Feedback"

An assessment plan should be developed to determine if the MILDEC is being adopted, rejected, or deceptively countered. Nominate MILDEC-related PIRs and establish named areas of interest to facilitate feedback on and exploitation of the MILDEC.

9. "Beware of Possible Unwanted Reactions"

MILDEC may produce subtle, unwanted reactions from the deception target and friendly forces. Proper coordination can reduce the chance that deceptions will result in unfavorable enemy action. The deception objective should be framed in terms of what you want the target to do, rather than think. In W.W. Jacob's story, "The Monkey's Paw," the 23rd Headquarters-Special Troops was a top secret organization attached to the US 12th Army Group Headquarters in World War II. This 1,100-man unit conducted 21 MILDEC operations from 1944 to 1945. In Operation BREST, it portrayed an armor attack buildup that was apparently believed by the German Army, but because of a lack of US coordination, an actual US armored unit tried to attack in that area. In another similar operation, the weakened German army division opposite the phony armor buildup believed the story, but the German army commander, believing he was about to be overrun by US armor, launched a spoiling attack, which was definitely not what US forces wanted.

10. "Care in the Design of Planned Placement of Deceptive Material"

Generally, if the deception target's intelligence collection assets have to work for the deception to be believed, the greater the likelihood the adversary will accept them as truth. US forces cannot boldly announce what they are doing or the adversary will be suspicious.

11. "Integrated Planning"

MILDEC planning must begin with the initial operational planning for the military operation supported and should continue throughout all phases of planning and execution.

Intentionally Blank

APPENDIX B
SUGGESTED BACKGROUND READINGS

1. MILDEC planning is a creative process that requires imagination and creativity on the part of its practitioners. Additionally, MILDEC plans should be carefully tailored for each situation. For these reasons, this publication has not provided a list of possible MILDEC schemes or otherwise attempted to suggest potential deception COAs for particular situations.

2. Commanders, MILDEC planners, and others can benefit, however, from the experiences of earlier MILDEC operations and from the theoretical work being done by academicians on the topics of MILDEC and surprise.

3. The following is a selected bibliography of books and periodicals that deal with the subject of MILDEC.

a. *The Art of War*, by Sun Tzu (Dover Publications, 2002).

b. *The Art of Deception in War*, by Michael Dewar (David and Charles, 1989).

c. *War, Strategy and Intelligence*, edited by Michael I. Handel (Frank Cass, 1989).

d. *Strategic and Operational Deception in the Second World War*, edited by Michael I. Handel (Frank Cass, 1989).

e. "Military Deception in War and Peace," by Michael I. Handel in *Jerusalem Papers on Peace Problems, Number 38* (The Leonard Davis Institute for International Relations, 1985).

f. *Soviet Military Deception in the Second World War*, by David M. Glantz (Frank Cass, 1989).

g. *The Double Cross System in the War of 1939 to 1945*, by J. C. Masterman (Yale University Press, 1972).

h. *Deception in World War II*, by Charles Cruickshank (Oxford University Press, 1979).

i. *Strategic Military Deception*, edited by Donald C. Daniel and Katherine L. Herbig (Pergamon, 1981).

j. *D-Day*, by Jock Haskell (Times Books, 1979).

k. *Practice to Deceive*, by David Mure (William Kimber, 1977).

l. *Master of Deception*, by David Mure (William Kimber, 1980).

m. *Soviet Operational Deception: The Red Cloak*, by LTC Richard N. Armstrong (Combat Studies Institute, US Army Command and General Staff College, 1989).

n. *Pastel: Deception in the Invasion of Japan*, by Dr. Thomas M. Huber (Combat Studies Institute, US Army Command and General Staff College, 1988).

o. "British Intelligence in the Second World War," by Sir Michael Howard, in *Strategic Deception*, Volume 5 (Cambridge University Press, 1989).

p. *The War Magician*, by David Fisher (Coward-McCann, 1983).

q. *The Wizard War*, by R. V. Jones (Coward, McCann, and Geoghegan, 1972).

r. *Masquerade*, by Seymour Reit (NAL Books, 1978).

s. *Codeword BARBAROSSA*, by Barton Whaley (MIT Press, 1973).

t. *The Art of Military Deception*, by Mark Lloyd (Cooper, Leo Books, 1997).

u. *The Art of Darkness: Deception and Urban Operations*, by Scott Gerwehr and Russell Glenn (Rand, 2000).

v. *Bodyguard of Lies*, by Anthony Cave Brown (Harper Collins, 1975).

w. The 1991 Intelligence Authorization Act.

x. *Secret Soldiers*, by Phillip Gerard (Dutton/Plume, 2002).

y. *Secret Soldiers: The Story of World War II's Heroic Army of Deception*, by Philip Gerard (Penguin Group, 2002).

z. *Fortitude: The D-Day Deception Campaign*, by Roger Hesketh (Woodstock, 2002).

aa. *The Man Who Never Was*, by Ewen Montagu (United States Naval Institute, 2001).

bb. *Deception Game, Czechoslovakian Intelligence in Soviet Political Warfare*, by Ladislav Bittman (Syracuse University Research Corporation, 1972).

cc. *Desperate Deception: British Covert Operations in the United States, 1939-44*, by Thomas Mahl (Brassey's Inc., 1999).

dd. *Deception in War: The Art of the Bluff, the Value of Deceit, and the Most Thrilling Episodes of Cunning in Military History, from the Trojan Horse to the Gulf War*, by Jon Latimer (Overlook Press, 2003).

cc. *Strategic Denial and Deception: The Twenty-First Century Challenge*, 5th ed., by Roy Goodson and James J. Wirtz (National Strategy-Information Center, Washington, DC, 2006).

ff. *Operation Mincemeat: How a Dead Man and a Bizarre Plan Fooled the Nazis and Assured an Allied Victory*, by Ben Macintyre (Crown; first edition May 4, 2010).

Intentionally Blank

APPENDIX C
SUPPLEMENTAL GUIDANCE

This appendix is a classified supplement provided under separate cover. The classified appendix expands on information contained in this publication.

Intentionally Blank

APPENDIX D
REFERENCES

The development of JP 3-13.4 is based upon the following primary references.

1. Department of Defense Issuance

a. DOD Directive 3600.01, *Information Operations (IO).*

b. DOD Instruction S-3604.01, *(U) Department of Defense Military Deception.*

2. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 3210.01C, *Joint Information Operations Proponent.*

b. CJCSI 3211.01F, *(U) Joint Policy for Military Deception.*

c. CJCSI 3213.01D, *Joint Operations Security.*

d. CJCSI 3320.01D, *Joint Electromagnetic Spectrum Operations (JEMSO).*

e. CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND).*

f. CJCSM 3122.01A, *Joint Operation Planning and Execution System (JOPES) Volume I, Planning Policies and Procedures.*

g. CJCSM 3122.02D, *Joint Operation Planning and Execution System (JOPES) Volume III, Time-Phased Force and Deployment Data Development and Deployment Execution.*

h. CJCSM 3130.03, *Adaptive Planning and Execution System (APEX) Planning Formats and Guidance.*

i. *DOD Dictionary of Military and Associated Terms.*

j. JP 1, *Doctrine for the Armed Forces of the United States.*

k. JP 2-0, *Joint Intelligence.*

l. JP 2-01, *Joint and National Intelligence Support to Military Operations.*

m. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment.*

n. JP 3-0, *Joint Operations.*

o. JP 3-05, *Special Operations.*

p. JP 3-08, *Interorganizational Coordination.*

q. JP 3-13, *Information Operations.*

r. JP 3-13.1, *Electronic Warfare.*

s. JP 3-13.2, *Military Information Support Operations.*

t. JP 3-13.3, *Operations Security.*

u. JP 3-16, *Multinational Operations.*

v. JP 3-33, *Joint Task Force Headquarters.*

w. JP 3-57, *Civil-Military Operations.*

x. JP 3-60, *Joint Targeting.*

y. JP 3-61, *Public Affairs.*

z. JP 5-0, *Joint Planning.*

aa. JP 6-0, *Joint Communications System.*

bb. Joint Doctrine Note 1-15, *Operation Assessment.*

3. Army Publication

US Army Field Manual 27-10, *The Law of Land Warfare*, with Change 1.

APPENDIX E
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Supersession

This publication supersedes JP 3-13.4, *Military Deception*, 26 January 2012.

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: Deputy Director, Joint Education and Doctrine (DD JED), Attn: Joint Doctrine Division, 7000 Joint Staff (J-7), Washington, DC, 20318-7000 or email:js.pentagon.j7.list.dd-je-d-jdd-all@mail.mil.

b. Routine changes should be submitted electronically to the Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697, js.dsc.j7.list.dd-je-d-jdad-all@mail.mil, and info the lead agent, the joint staff doctrine sponsor, and the JDD AO who manages the JP that is impacted by the recommended change.

c. When a Joint Staff directorate submits a proposal to the CJCS that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Lessons Learned

The Joint Lessons Learned Program (JLLP) primary objective is to enhance joint force readiness and effectiveness by contributing to improvements in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. The Joint Lessons Learned Information System (JLLIS) is the DOD system of record for lessons learned and facilitates the collection, tracking, management, sharing, collaborative resolution, and dissemination of lessons learned to improve the

development and readiness of the joint force. The JLLP integrates with joint doctrine through the joint doctrine development process by providing lessons and lessons learned derived from operations, events, and exercises. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Lessons and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Website can be found at https://www.jllis.mil or http://www.jllis.smil.mil.

6. Distribution of Publications

Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be IAW DOD Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification*, and DOD Manual 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information*.

7. Distribution of Electronic Publications

[redacted]

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (NIPRNET) and [redacted] (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine.

[redacted]

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. [redacted] may request classified JPs by sending written requests to Defense Intelligence Agency (DIA) [redacted] 200 MacDill Blvd., Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

c. JEL CD-ROM. Upon request of a joint doctrine development community member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs. This JEL CD-ROM will be updated not less than semi-annually and when received can be locally reproduced for use within the combatant commands, Services, and combat support agencies.

GLOSSARY

PART I—ABBREVIATIONS, ACRONYMS, AND INITIALISMS

BCT	brigade combat team
CCDR	combatant commander
CCMD	combatant command
CI	counterintelligence
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMDO	command military deception officer
CMO	civil-military operations
CO	cyberspace operations
COA	course of action
CONOPS	concept of operations
CONPLAN	concept plan
CWG	counterdeception working group
DES	deception event schedule
DIE	deception intelligence estimate
DISO	deception in support of operations security
DOD	Department of Defense
DOWG	deception operations working group
DPC	deception planning cell
EM	electromagnetic
EMS	electromagnetic spectrum
EW	electronic warfare
FIE	foreign intelligence entity
IC	intelligence community
IO	information operations
IRC	information-related capability
IS	information system
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-4	logistics directorate of a joint staff
J-5	plans directorate of a joint staff
J-6	communications system directorate of a joint staff
JFC	joint force commander
JIPOE	joint intelligence preparation of the operational environment
JP	joint publication
JPG	joint planning group

JPP	joint planning process
JTF	joint task force
LNO	liaison officer
LOO	line of operation
MDO	military deception officer
MILDEC	military deception
MISO	military information support operations
MOE	measure of effectiveness
MOP	measure of performance
OODA	observe, orient, decide, act
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PA	public affairs
PIR	priority intelligence requirement
RFI	request for information
ROE	rules of engagement
SJA	staff judge advocate
TAC-D	tactical deception

PART II—TERMS AND DEFINITIONS

competing observable. Within military deception, any observable that contradicts the deception story, casts doubt on, or diminishes the impact of one or more required or supporting observables. (Approved for inclusion in the DOD Dictionary.)

conduits. Within military deception, information or intelligence gateways to the deception target, such as foreign intelligence entities, intelligence collection platforms, open-source intelligence, and foreign and domestic news media. (Approved for incorporation into the DOD Dictionary.)

counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. (Approved for incorporation into the DOD Dictionary.)

deception action. A collection of related deception events that form a major component of a deception operation. (DOD Dictionary. SOURCE: JP 3-13.4)

deception concept. The deception course of action forwarded to the Chairman of the Joint Chiefs of Staff for review as part of the combatant commander's strategic concept. (DOD Dictionary. SOURCE: JP 3-13.4)

deception event. A deception means executed at a specific time and location in support of a deception operation. (DOD Dictionary. SOURCE: JP 3-13.4)

deception goal. Commander's statement of the purpose of military deception as it contributes to the successful accomplishment of the assigned mission. (Approved for inclusion in the DOD Dictionary.)

deception means. Methods, resources, and techniques that can be used to convey information to the deception target. (Approved for incorporation into the DOD Dictionary.)

deception objective. The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (DOD Dictionary. SOURCE: JP 3-13.4)

deception story. A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (DOD Dictionary. SOURCE: JP 3-13.4)

deception target. The adversary decision maker with the authority to make the decision that will achieve the deception objective. (DOD Dictionary. SOURCE: JP 3-13.4)

decoy. An imitation in any sense of a person, object, or phenomenon that is intended to deceive enemy surveillance devices or mislead enemy evaluation. Also called **dummy**. (Approved for incorporation into the DOD Dictionary.)

demonstration. In military deception, a show of force similar to a feint without actual contact with the adversary, in an area where a decision is not sought that is made to deceive an adversary. (Approved for incorporation into the DOD Dictionary.)

desired perception. In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (DOD Dictionary. SOURCE: JP 3-13.4)

display. In military deception, a static portrayal of an activity, force, or equipment intended to deceive the adversary's visual observation. (DOD Dictionary. SOURCE: JP 3-13.4)

dummy. None. (Approved for removal from the DOD Dictionary.)

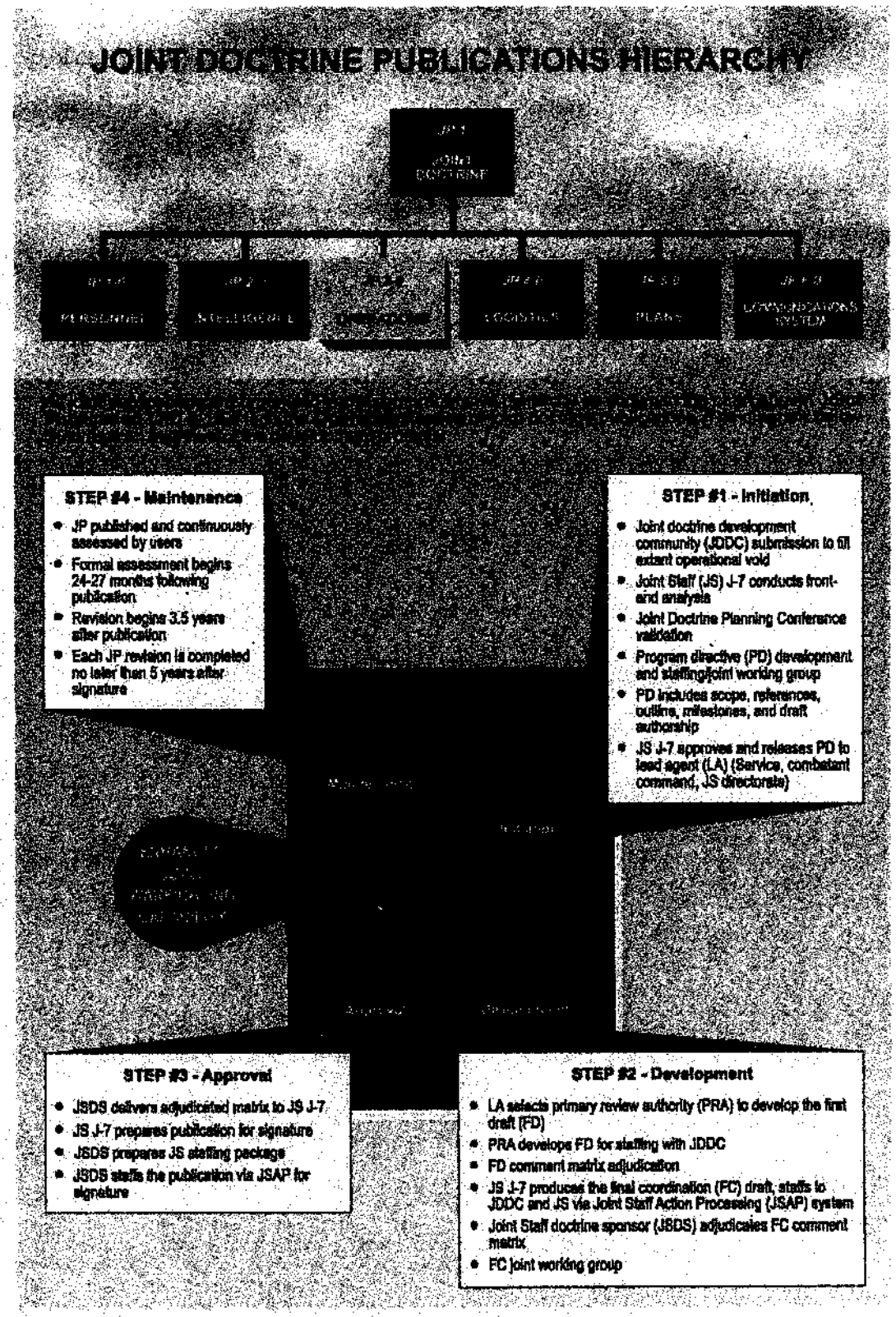
feint. In military deception, an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. (DOD Dictionary. SOURCE: JP 3-13.4)

honey pot. None. (Approved for removal from the DOD Dictionary.)

military deception. Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called **MILDEC**. (DOD Dictionary. SOURCE: JP 3-13.4)

observable. In military deception, the detectable result of the combination of an indicator within an adversary's conduit intended to cause action or inaction by the deception target. (Approved for inclusion in the DOD Dictionary.)

ruse. In military deception, an action designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. (Approved for incorporation into the DOD Dictionary.)


JOINT DOCTRINE PUBLICATIONS HIERARCHY
STEP #4 - Maintenance
• JP published and continuously assessed by users
• Formal assessment begins 24-27 months following publication
• Revision begins 3.5 years after publication
• Each JP revision is completed no later than 5 years after signature
STEP #1 - Initiation
• Joint doctrine development community (JDDC) submission to fill extant operational void
• Joint Staff (JS) J-7 conducts front-end analysis
• Joint Doctrine Planning Conference validation
• Program directive (PD) development and staffing/joint working group
• PD includes scope, references, outline, milestones, and draft authorship
• JS J-7 approves and releases PD to lead agent (LA) (Service, combatant command, JS directorate)
STEP #3 - Approval
• JSDS delivers adjudicated matrix to JS J-7
• JS J-7 prepares publication for signature
• JSDS prepares JS staffing package
• JSDS staffs the publication via JSAP for signature
STEP #2 - Development
• LA selects primary review authority (PRA) to develop the first draft (FD)
• PRA develops FD for staffing with JDDC
• FD comment matrix adjudication
• JS J-7 produces the final coordination (FC) draft, staffs to JDDC and JS via Joint Staff Action Processing (JSAP) system
• Joint Staff doctrine sponsor (JSDS) adjudicates FC comment matrix
• FC joint working group