Joint Publication 3-13.4

Military Deception

26 January 2012

PREFACE

1. Scope

This publication provides joint doctrine for the planning, execution, and assessment of military deception (MILDEC) in support of joint operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military coordination with other US Government departments and agencies during operations and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes doctrine for MILDEC operations and training supporting joint operations. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. 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 the overall mission.

3. Application

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

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 for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, 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 United States, 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:

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-13.4
DATED 13 JULY 2006

- **Modifies the definition of military deception (MILDEC).**
- **Codifies the term Joint MILDEC.**
- **Deletes terms strategic MILDEC and operational MILDEC.**
- **Modifies definition of deception in support of operations security and tactical deception.**
- **Updates the MILDEC planning process.**
- **Revises the roles and responsibilities of the command MILDEC officer.**
- **Revises the roles and responsibilities for MILDEC planner.**
- **Updates reference and acronyms.**

Intentionally Blank

TABLE OF CONTENTS

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides an Overview of Military Deception (MILDEC) and the Goals, Objectives, Functions, and Principles**
- **Describes the Relationship between MILDEC and Information Operations**
- **Explains MILDEC Planning Methodology and Planning Steps**
- **Discusses Execution of MILDEC Operations**

Military Deception and Its Goals, Objectives, Functions, and Principles

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.

Specific guidance from the joint force commander (JFC) or higher authority during planning will determine the military deception (MILDEC) role in a joint operation. **MILDEC is intended to deter hostile actions, increase the success of friendly defensive actions, or to improve the success of any potential friendly offensive action.** Use of MILDEC during any phase of an operation should help to mislead adversaries as to the strength, readiness, locations, and intended missions of friendly forces. In combat situations, the focus is on driving the adversary to culmination and achieving the objectives defined by the JFC. In noncombat situations, the JFC seeks to dominate the situation with decisive operations designed to establish conditions for an early, favorable conclusion.

MILDEC and Information Quality

Care should be taken to protect the quality of information available for friendly decisions and public dissemination. This will help ensure the JFC has accurate information by not allowing staffs to unknowingly perceive the joint task force's MILDEC efforts as accurate information. This will also ensure the information made public by the JFC is not part of any MILDEC action and lose the public's trust.

MILDEC Goals and Objectives

The **MILDEC goal** is the commander's statement of the purpose of the MILDEC as it contributes to the successful accomplishment of the assigned mission. It is important for the commander to first envision the deception goal in terms of its specific contribution to accomplishing the designated mission. The **MILDEC objective** is a concise statement of what the MILDEC will cause the adversary to do or not do. It is expressed in terms of the adversary's action or inaction

that directly leads to the purpose or condition stated in the MILDEC goal.

MILDEC Targets

The **deception target is the adversary decision maker** with the authority to make the decision that will achieve the deception objective. The deception target or targets are the key individuals on whom the entire deception operation will be focused.

Conduits to Targets

Within MILDEC, **conduits are information or intelligence gateways to the deception target.** Conduits may be used to control flows of information to a deception target.

Deception Story

The cornerstone of any deception operation is the deception story.

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.

Functions of MILDEC

Function of MILDEC include:

- Causing ambiguity, confusion, or misunderstanding in adversary perceptions of friendly critical information.
- Causing the adversary to misallocate personnel, fiscal, and material resources in ways that are advantageous to the friendly force.
- Causing the adversary to reveal strengths, dispositions, and future intentions.
- Conditioning the adversary to particular patterns of friendly behavior to induce adversary perceptions that can be exploited by the joint force.
- Causing the adversary to waste combat power with inappropriate or delayed actions.

Principles of MILDEC

The six principles of MILDEC provide guidance for planning and executing MILDEC operations. The six principles are:

- **Focus.** The deception must target the adversary decision maker capable of causing the desired action(s) or inaction(s)

- **Objective.** To cause an adversary to take (or not to take) specific actions, not just to believe certain things

- **Centralized Planning and Control.** MIDEC operations should be centrally planned and directed

- **Security.** Deny knowledge of a force's intent to deceive and the execution of that intent to adversaries

- **Timeliness.** A deception operation requires careful timing

- **Integration.** Fully integrate each MILDEC with the operation that it is supporting

MILDEC Means, Tactics, Techniques, and Procedures

MILDEC employs three basic means: physical, technical, and administrative. Employ these means independently or in collaboration depending on the situation. The applications of tactics vary with each operation depending on variables such as time, assets, equipment, and objectives and are assessed for feasibility accordingly. MILDEC operations apply four basic deception techniques: feints, demonstrations, ruses, and displays. MILDEC procedures vary with each MILDEC operation and are conducted in accordance with the commander's guidance and the processes used to synchronize the tactics and techniques in real time.

Military Deception and Information Operations

MILDEC as a Capability of Information Operations

MILDEC and other information operations (IO) capabilities must be planned and integrated to support the commander's campaign and/or operation. Collectively, these capabilities target adversary decision makers to affect their information systems and decision-making processes.

Counterdeception as an Element of MILDEC

Counterdeception contributes to situational understanding and IO by protecting friendly command and control systems and decision makers from adversary deception. Friendly decision makers must be aware of adversary deception activities so they can formulate informed and coordinated responses.

Information Operations Planning

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 and is

responsible for incorporating and deconflicting MILDEC with other IO.

MILDEC and Camouflage and Concealment

Camouflage and concealment provide protection for MILDEC, particularly at the tactical level, by manipulating the appearance or obscuring the deceiver's actual activities.

MILDEC's Relationship to Legal Support

Staff judge advocate personnel assist in planning the operation to meet the objective while complying with legal requirements, such as providing training to deception planning cell (DPC) personnel on the law of armed conflict, foreign law, and ethics as applied to MILDEC operations.

Roles, Coordination, and Considerations for Military Deception

Roles and Responsibilities of MILDEC Planners

Commander. While MILDEC may not be appropriate to every joint operation, each JFC determines whether MILDEC could contribute to the achievement of assigned objectives. Commanders should guide and support applicable MILDEC operations and should also be readily available to the MILDEC planners. The conduct of MILDEC is the responsibility of the commander.

Operations Directorate of a Joint Staff (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 J-3 normally supervises the execution of MILDEC. The J-3 normally establishes a staff deception element to manage MILDEC operations as part of the IO cell. The IO cell chief is also responsible for monitoring the implementation and execution of the MILDEC portion of IO.

Command MILDEC Officer (CMDO). The CMDO is the primary designated officer with overall oversight and management responsibility for each MILDEC program within the combatant commands, agencies, and Service components which support joint military operations.

MILDEC Planner. The MILDEC planner is the commander's lead agent responsible for drafting the MILDEC objectives for various courses of action.

Intelligence Directorate of a Joint Staff (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 resources. The J-2 is a primary participant in this process.

Coordination Requirements

The Joint Staff has the authority and responsibility to plan, coordinate, and integrate Department of Defense IO capabilities that cross areas of responsibility or that directly support national objectives. For those MILDEC plans, the Joint Staff J-3 serves as the coordinating authority for the planning of MILDEC and the integration of Joint MILDEC with other elements of IO. The JFC-designated IO coordination officer normally is 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.

MILDEC Considerations

JFCs should ensure that their staffs and units receive training in MILDEC. Additionally, joint operation and MILDEC planners should receive appropriate MILDEC training.

Military Deception Planning

MILDEC Planning and the Joint Planning Processes

As with all joint planning, MILDEC planning is an iterative process that requires continual reexamination of its goals, objectives, targets, stories, and means. MILDEC planning can be deliberate planning (used normally during peacetime to develop operation plans and operation plans in concept format), or during crisis action planning (during time-sensitive situations to rapidly develop campaign plans and orders).

MILDEC Planning Methodology – "See, Think, Do"

Successful deception operations are those that do more than make the target "believe" or "think" that the deception is true. MILDEC must end in an action, or inaction, that supports the JFC operational plan. The following interrogatories describe the process:

- **See:** What does the target see from friendly operations?

- **Think:** What conclusions does the target draw from those observations?

- **Do:** What action may the target take as a result of the conclusions based upon those observations?

The MILDEC Planning Process

Deception planning is an iterative process that requires continual reexamination of its objectives, target, stories, and means throughout the planning and execution phases. A key factor that must be considered during MILDEC planning is risk. The overriding consideration in risk analysis is the comparison between the risk taken and the possible benefits of the deception. **The MILDEC planning process consists of six steps:** deception mission analysis, deception planning guidance; staff deception estimate; commander's deception estimate; Chairman of the Joint Chiefs of Staff estimate review; deception plan development; and deception plan review and approval.

MILDEC Capabilities, Limitations, and Risks

Capabilities in MILDEC operations vary with the mission type, adversary, location, assets available, and even the political climate. 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 our ability to measure the effectiveness of the MILDEC. **Risk** is a key factor that must be reexamined during every phase of MILDEC planning and execution. Fully integrate risk management into planning, preparing, executing, and assessing. The failure or exposure of the deception can significantly affect the friendly commander's operational activities.

Execution of Military Deception Operations

Execution of MILDEC Events and Actions

The MILDEC plan is normally executed as a component of the operation order. As with all military operations, the process of execution involves two basic functions, assessing and control. Assessing involves the receipt and processing of information concerning the MILDEC operation, and control entails making iterative decisions and issuing instructions until termination. The deception plan is the basis for execution, but execution may take place in conditions that are more dynamic than the plan anticipated.

Deception Execution Coordination

Once the planning process is complete, it is critical that constant coordination at the strategic, operational, and tactical level continues to ensure success. The potential for a tactical or operational level deception to have strategic implications is high. With this in mind, a continual process of coordination, called the deception execution cycle, must take place.

Terminating MILDEC Operations

The termination of a MILDEC is concerned with ending the MILDEC in a way that protects the interests of the deceiver. The objective of a successful termination is to conclude the MILDEC without revealing the MILDEC to the adversary. The DPC is concerned about terminating the overall MILDEC, as well as the termination implications embedded in each MILDEC event. Planning how to end an individual deception event in a way that does not leave suspicious traces of the MILDEC operations is an inherent aspect of MILDEC event preparation.

CONCLUSION

This publication provides joint doctrine for the planning, execution, and assessment of MILDEC in support of joint operations.

Intentionally Blank

CHAPTER I
GENERAL

"I make the enemy see my strengths as weaknesses and my weaknesses as strengths while I cause his strengths to become weaknesses and discover where he is not strong…I conceal my tracks so that none can discern them; I keep silence so that none can hear me."

Sun Tzu
***The Art of War*, c. 500 BC**

1. Policy

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3211.01E, *Joint Policy for Military Deception*, provides joint policy guidance for military deception (MILDEC). Refer to that document for information concerning responsibilities relating to MILDEC and for specific guidance and restrictions relating to MILDEC planned and conducted in support of joint operations.

2. Definition

MILDEC is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization (VEO) decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

3. Applicability

MILDEC is applicable at all levels of war, across the range of military operations, and can be conducted during all phases of military operations. Specific guidance from the joint force commander (JFC) or higher authority during planning will determine the MILDEC role in a joint operation. During the planning of an operation, MILDEC should be integrated into the early phases of an operation. The MILDEC role during the early phases of an operation will be based on the specific situation of the operation or campaign to help set conditions that will facilitate phases that follow.

a. MILDEC is intended to deter hostile actions, increase the success of friendly defensive actions, or to improve the success of any potential friendly offensive action. Use of MILDEC during any phase of an operation should help to mislead adversaries as to the strength, readiness, locations, and intended missions of friendly forces. MILDEC, as an element of an integrated information operations (IO) plan, can be a viable flexible deterrent option. In combat situations, the focus is on driving the adversary to culmination and achieving the objectives defined by the JFC. In noncombat situations, the JFC seeks to dominate the situation with decisive operations designed to establish conditions for an early, favorable conclusion. 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 military operations. Joint MILDEC activities are planned and executed by, and in support of, combatant commanders (CCDRs), 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 planned and executed MILDEC will be Joint MILDEC with operational-level effects. Joint MILDEC is normally planned prior to, and conducted during, combat operations.

(2) Deception in Support of Operations Security (DISO). DISO is a MILDEC activity that protects friendly operations, personnel, programs, equipment, and other assets against foreign intelligence and security services (FISS) collection. The intent of a DISO is to create multiple false indicators to confuse or make friendly force intentions harder to interpret by FISS, limiting the ability of FISS to collect accurate intelligence on friendly forces. DISOs are general in nature, they are not specifically targeted against particular adversary military, paramilitary, or VEO decision makers, but are, instead, used to protect friendly operations and forces by obfuscating friendly capabilities, intent, or vulnerabilities. Joint commanders may conduct approved DISOs pre-execute order, or as part of an operation plan (OPLAN), operation plan in concept format (CONPLAN), or operation order (OPORD).

(3) Tactical Deception (TAC-D). TAC-D is deception activities planned and conducted to support battles and engagements. TAC-D is planned and executed by, and in support of, tactical-level commanders to cause adversaries to take actions or inactions that are favorable to the US commanders' objectives. TAC-D is conducted to influence immediate military operations in order to gain a temporary tactical advantage over an adversary, to mask vulnerabilities in friendly forces, or to enhance the defensive capabilities of friendly forces.

b. **Termination and Strategic End State.** In later phases of an operation, prior to termination, MILDEC should support the transition of responsibility to civil control or other authority. The complexity of joint operations in later phases is compounded by the attempt to disengage the joint force; support for host nation, other government agencies, and nongovernmental organizations as they assume responsibility; the nonlinear nature of the operating area; and the possible lack of sequential timing in the transfer of responsibilities for control of the area. Thus, MILDEC planning and execution during later phases of a campaign may involve selected nonmilitary members, complicating operations security (OPSEC) concerns, and should focus on national objectives and end state, not just the military termination. During this time, the JFC focuses on synchronizing and integrating joint force actions with the activity of the other instruments of national power to bring operations to a successful conclusion, typically characterized by self-sustaining peace and the establishment of the rule of law. MILDEC may be conducted to: support redeployment or withdrawal operations; protect sensitive operational capabilities from being revealed; establish favorable conditions for subsequent military operations; support possible counterinsurgency operations; defend or rebuild critical infrastructure; and aid in the transition of responsibility to civil control or other authority.

4. Military Deception and Information Quality

Information quality refers to the accuracy, completeness, relevance, and believability of information available for decision making. Care should be taken to protect the quality of information available for friendly decisions and public dissemination. This will help ensure the JFC has accurate information by not allowing staffs to unknowingly perceive 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 and lose the public's trust. MILDEC by design should affect the quality of information available for adversary decisions in the following ways:

a. Deliberately presents misleading information to adversaries to degrade the **accuracy** of adversary information.

b. Seeks to give adversary decision makers a false sense of **completeness** about friendly forces or intentions.

c. May cause the adversary to misjudge the **relevance** of available information and misallocate operational or intelligence resources.

d. May cause adversaries to **doubt the validity** of their own intelligence gathering systems.

5. Military Deception Goals and Objectives

The MILDEC plan should clearly delineate both the goal and the objective of the MILDEC. This provides the commander with a solid understanding of how the deception supports the overall operation and establishes a firm foundation for planning and executing MILDEC operations.

a. **The MILDEC Goal.** The MILDEC goal is the commander's statement of the purpose of the MILDEC as it contributes to the successful accomplishment of the assigned mission. The goal of a MILDEC is usually stated in a positive result, such as: "Successful MILDEC will improve the friendly force advantage on a designated axis of advance." 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.

b. **The MILDEC Objective.** The MILDEC objective is a concise statement of what the MILDEC will cause the adversary to do or not do. It is expressed in terms of the adversary's action or inaction that directly leads to the purpose or condition stated in the MILDEC goal. An example of a MILDEC objective is: "Cause the adversary to misdirect reconnaissance and surveillance assets away from the friendly attacking force and to defend the wrong sector." Further MILDEC objectives may include:

(1) Cause the adversary commander to employ forces and assets in ways that are advantageous to the joint force.

(2) Cause the adversary to reveal strengths, dispositions, and intentions.

(3) Cause the adversary to withhold strategic reserves until friendly forces have achieved mission success.

(4) Condition the adversary to particular patterns of friendly behavior to induce adversary perceptions that are exploitable at a time chosen by the joint force.

(5) Cause the adversary to waste combat power with inappropriate or delayed actions.

6. Military Deception Targets

The deception target is the adversary decision maker with the authority to make the decision that will achieve the deception objective. The deception target or targets are the key individuals on whom the entire deception operation will be focused. In selecting the deception target, several factors should be considered.

a. The deception target must be capable of causing the desired action(s) or inaction(s) to occur. The target has the authority to make decisions that will aid US forces in achieving the desired deception objective.

b. There must either be existing conduits to the deception targets, or there must be a reasonable expectation that conduits to the deception targets can be established.

c. During development of the deception, sufficient intelligence regarding the deception target should exist to determine what (if any) preconceived perceptions the deception target may have. History has shown that deception operations that play upon the preconceived perceptions of a deception target have been very successful. The MILDEC planner should submit request for information (RFI) inputs to the intelligence community (IC) requesting behavioral influence analysis (BIA)/human factors analysis (HFA) data on adversary military, paramilitary, and VEO decision makers.

7. Conduits to Targets

Within MILDEC, conduits are information or intelligence gateways to the deception target. Conduits may be used to control flows of information to a deception target. It is rare that a deceptive message is sent directly to the deception target itself. Most often, deception messages are sent to intelligence collectors (conduits) with the expectation that the deceptive message will systematically make its way to the deception target.

a. Examples of conduits include FISS, intelligence collection platforms, open-source intelligence, and individuals through whom information reaches the deception target.

b. The development and utilization of conduits should be approached systematically. A path should be discernable from the initial input to the conduit to the deception target. Ideally, conduits are part of a closed loop system which facilitate and enable feedback regarding receipt of the deceptive message by the intended deception target and whether or not the desired adversary actions are occurring or will occur. Factors to be considered include: Are there stop gaps between the initial receptor and the final desired end point (the deception target)? Are there filters that might skew the desired perception? Are there conduits that might potentially validate or contradict the desired message? In the case of FISS, could the conduit potentially serve as a feedback mechanism?

8. Deception Story

The cornerstone of any deception operation is the deception story. 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. In other words, the deception story parallels what the deception would want the opponent's intelligence estimate to say about your own commander's intentions and your own unit's actions. 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.

a. An exact understanding of the perceptions and observables required for the deception provides a concrete basis for crafting the deception story. The deception story weaves these elements together into a coherent depiction of the situation the target will reconstruct from the information provided. Ideally, the deception planner wants the deception story to be the exact mental picture of the target forms as the deception unfolds. The deception story should read like the adversary's own intelligence estimate. The deception story is, in effect, the equivalent of a completed puzzle. As such, it serves as a means of checking the logic and consistency of the internal elements of the deception. This allows the deception planner to identify desired perceptions, observables, and executions that may need refinement, and to add supporting observables as needed to strengthen certain elements of the deception story or diminish the impact of troublesome competing observables. Each element of the deception story should have associated deception means that can credibly portray the data, plus identified conduits that transfer this information into the enemy's information processing system. Unavoidably, various nodes in this line of communications also become filters of the information conveyed, allowing the target to introduce their own predispositions and biases that the MILDEC planner must anticipate. As the story is developed and elaborated, the MILDEC planner continuously monitors changes in the situation and validates the deception story against other friendly plans and/or actions.

b. The story should be believable, verifiable, consistent, and executable.

(1) Believable. The story must correspond to the deception target's perceptions of the friendly force's mission, intentions, and capabilities.

(2) Verifiable. The adversary should be able to verify the veracity of the deception story through multiple channels and conduits. The deception story, therefore, takes into account all of the adversary's intelligence sources and is made available through all or many of those sources.

(3) Consistent. Deception stories should be consistent with the deception target's understanding of actual friendly doctrine, historical force employment, campaign strategy, battlefield tactics, and the current operational situation. This calls for the MILDEC planner to have as complete a picture as possible of the deception target's level of knowledge and belief in these areas.

(4) Executable. As with any course of action (COA), the MILDEC option that forms the deception story should be within the capabilities of the friendly force as the deception target perceives it. The deception target must believe that the friendly force has the capability to execute the operations that are being portrayed by the deception story.

9. Functions of Military Deception

The functions of MILDEC include:

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

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

c. Causing the adversary to reveal strengths, dispositions, and future intentions.

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

e. Causing the adversary to waste combat power with inappropriate or delayed actions.

10. Principles of Military Deception

Just as the principles of war provide general guidance for the conduct of military operations, the six principles of MILDEC (see Figure I-1) provide guidance for planning and executing MILDEC operations.

a. **Focus.** MILDEC should target the adversary decision maker capable of causing the desired action(s). The adversary's intelligence, surveillance, and reconnaissance (ISR) 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.

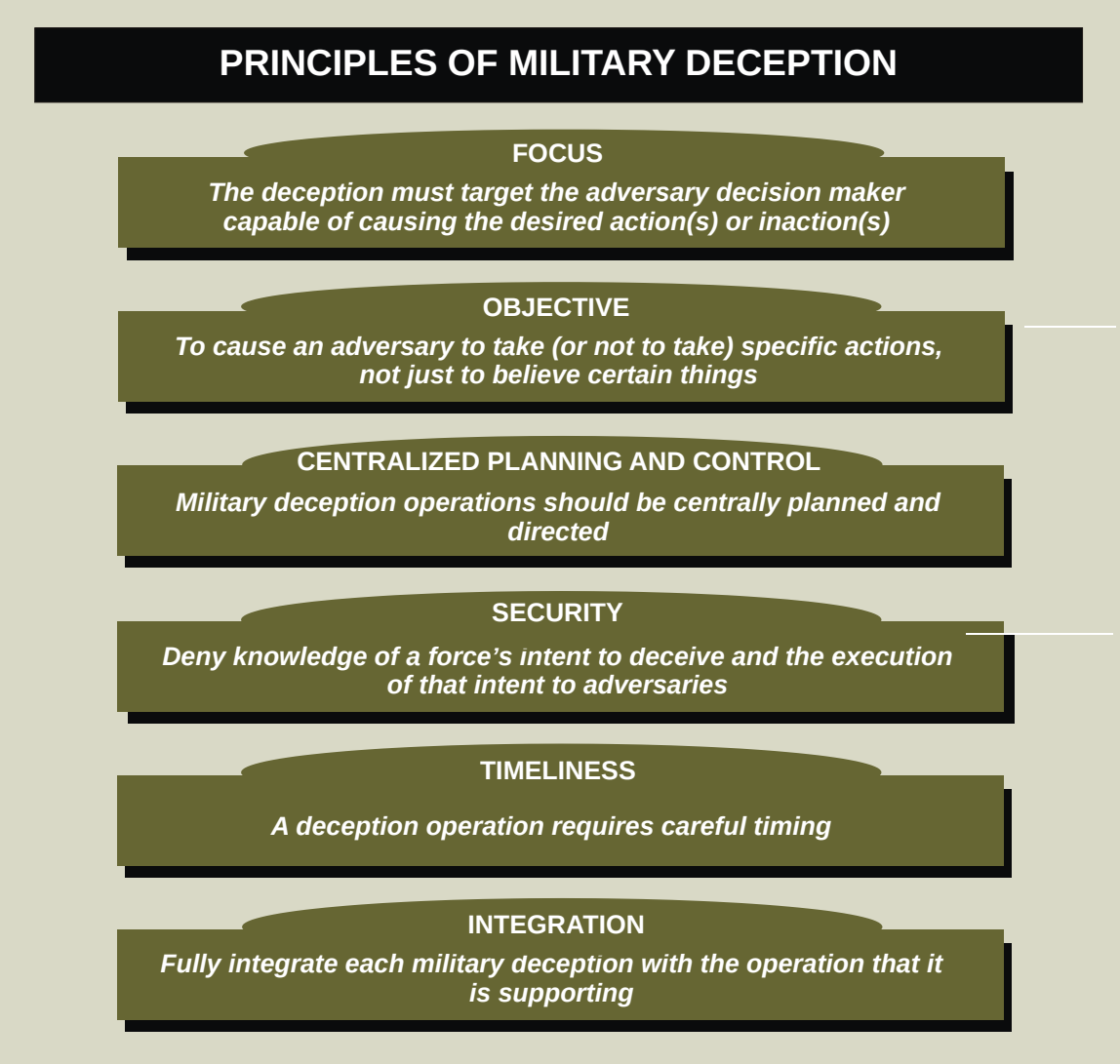


Figure I-1. Principles of Military Deception

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 that the various elements involved in MILDEC portray the same story and are not in conflict with other operational objectives. 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 information must be correctly classified and handled in accordance with the current *Joint MILDEC Security Classification Guide.*

e. **Timeliness.** A MILDEC operation requires careful timing. Provide sufficient time for its portrayal; for the adversary's ISR system to collect, analyze, and report; for the adversary decision maker to react; and for the friendly ISR 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 that subordinate deception plans are integrated within higher-level plans.

11. Military Deception Means, Tactics, Techniques, and Procedures

a. **MILDEC Means.** MILDEC employs three basic means: physical, technical, and administrative. Employ these means independently or in collaboration depending on the situation.

(1) **Physical Means.** Activities and resources used to convey or deny selected information to an adversary. Physical means include operational activities and resources such as:

(a) Movement of forces.

(b) Exercises and training activities.

(c) Dummy and decoy equipment and devices.

(d) Tactical actions.

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

(f) Test and evaluation activities.

(g) Reconnaissance and surveillance activities.

(2) **Technical Means.** Those military material resources and their associated operating techniques used to convey or deny selected information to an adversary. As with any use of US military material resources, any use of technical means to achieve MILDEC must comply with domestic and international law. A variety of technical means include:

(a) Deliberate emission, alteration, absorption, or reflection of energy.

(b) Emission or suppression of chemical or biological odors.

(c) Multimedia (radio, television, sound broadcasting, computers, computer networks, smart phones, and personal digital assistants).

(3) **Administrative Means.** Administrative means include resources, methods, and techniques designed to convey or deny oral, pictorial, documentary, or other physical evidence.

b. **MILDEC Tactics.** The applications of tactics vary with each operation depending on variables such as time, assets, equipment, and objectives and are assessed for feasibility accordingly. The tactics of MILDEC may:

(1) Mask an increase in or redeployment of forces or weapons systems spotted by the adversary.

(2) Shape the adversary's perception and/or identification of new forces or weapons being introduced into combat.

(3) Reinforce the adversary's preconceived beliefs.

(4) Distract the adversary's attention from other activities.

(5) Overload adversary ISR collection and analytical capabilities.

(6) Create the illusion of strength where weakness exists.

(7) Desensitize the adversary to particular patterns of friendly behavior to induce adversary perceptions that are exploitable at the time of friendly choosing.

(8) Confuse adversary expectations about friendly size, activity, location, unit, time, equipment, intent, and/or style of mission execution, to effect surprise in these areas.

(9) Reduce the adversary's ability to clearly perceive and manage the battle.

c. **MILDEC Techniques.** 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 US goals.

(3) **Ruses.** A ruse is a cunning trick 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).

d. **Unlawful Deceptions.** Certain deception techniques may amount to "perfidious acts" due to their treacherous nature. Perfidious acts are prohibited under the law of armed conflict (LOAC) because they undermine the effectiveness of the law of war and thereby jeopardize the safety of civilians and noncombatants and/or the immunity of protected structures and activities. Acts of perfidy are deceptions designed to invite the confidence of the enemy to lead him to believe that he is entitled to, or is obliged to accord, protected status under the LOAC, with the intent to betray that confidence. Under this deception technique, the deceiving unit intends to use the enemy's compliance with the law of war to gain an advantage with respect to the enemy. Acts of perfidy include, but are not limited to, feigning surrender or waving a white flag in order to lure the enemy into a trap; misuse of protective signs, signals, and symbols in order to injure, kill, or capture the enemy; and using an ambulance or medical aircraft marked with the Red Cross, Red Crescent, or Red Crystal to carry armed combatants, weapons, or ammunition in order to attack or elude enemy forces.

AMPHIBIOUS DEMONSTRATION—OPERATION DESERT STORM

During the early days of DESERT SHIELD, a powerful 18,000-man amphibious task force steamed into the North Arabian Sea to add an important element to the allied arsenal. Within less than a month after the Iraqi invasion of Kuwait, more than 20 amphibious ships from ports in Virginia and California completed the roughly 10,000-mile trip to the Gulf of Oman, where nearly 8,000 Marines and 10,000 Sailors commenced full-scale preparations to "hit the beach" to eject Iraq's army from Kuwait. The task force, with Marines from the 4th Marine Expeditionary Brigade (MEB) and 13th Marine Expeditionary Unit embarked, included air, land, and sea assets tailor-made for coastal assault—Harrier attack jets and assault support helicopters to provide air cover for infantry, and armor that would hit the beach aboard high-speed landing craft, aircushion vehicles. The Task Force, quickly forged from several amphibious ready groups, represented the largest amphibious assault force assembled in more than 30 years. They also completed demanding shipboard drills and amphibious assault training on coalition beaches. That training grew more intense as the amphibious forces performed high-visibility exercises off the coast of Saudi Arabia to heighten the enemy wariness of an invasion from the sea. The amphibious presence grew larger following President Bush's 8 November decision to nearly double US forces in theater.

The 13 ships of Amphibious Group Three arrived from three west coast ports with nearly 15,000 Marines of the 5th MEB embarked to join the amphibious task force. As the ground war commenced, nearly 17,000 Marines stood ready aboard the largest combined amphibious assault force since the Inchon landing in Korea. Only then did the Sailors and Marines of the amphibious force learn that their warfighting skills would not be immediately required as they had expected. But their preparation had not been in vain. It was at the core of the deceptive tactics which played a major role in the quick allied victory.

Amphibious operations focused enemy attention on the threat from seaward and tied down at least seven Iraqi divisions, even after the coalition ground campaign was well under way.

SOURCE: Department of the Navy, Naval Historical Center

e. **MILDEC Procedures.** MILDEC procedures vary with each MILDEC operation and are conducted in accordance with the commander's guidance and the processes used to synchronize the tactics and techniques in real time. Consequently, they are specific (unique or changing) with regard to each operation. For more detailed information, refer to Marine Corps Reference Publication 3-40.4A/Navy Tactics, Techniques and Procedures, 3-58.1/Air Force Tactics, Techniques and Procedures (Instruction) 3-2.66, *Multi-Service Tactics, Techniques and Procedures for Military Deception Operations*.

Intentionally Blank

CHAPTER II
MILITARY DECEPTION AND INFORMATION OPERATIONS

"It is very important to spread rumors among the enemy that you are planning one thing; then go and do something else…"

The Emperor Maurice
***The Strategikon,* c. 600 AD**

1. Information Operations

IO is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.

For further guidance on IO, refer to Joint Publication (JP) 3-13, Information Operations.

2. Military Deception as a Capability of Information Operations

MILDEC and other IO capabilities must be planned and integrated to support the commander's campaign and/or operation. Collectively, these capabilities target adversary decision makers to affect their information systems (ISs) and decision-making processes. Deception requires a thorough knowledge of adversaries and their decision-making processes. During the formulation of the commander's concept, particular attention is placed on defining how the commander would like the adversary forces to act at critical points in the operation. Those desired adversary actions then become the objectives of MILDEC operations. MILDEC is focused on desired behavior, not simply misleading an adversary's thinking. The intent is to cause adversary commanders to form inaccurate impressions about friendly force dispositions, capabilities, vulnerabilities, and intentions; misappropriate their ISR collection assets; and/or fail to employ combat or support units to their best advantage. MILDEC operations identify and focus on selected deception targets; develop and portray a credible deception story; and assess and modify, as needed, the MILDEC plans to termination.

3. Counterdeception as an Element of Military Deception

Counterdeception contributes to situational understanding and IO by protecting friendly command and control (C2) systems and decision makers from adversary deception. Friendly decision makers must be aware of adversary deception activities so they can formulate informed and coordinated responses. Counterdeception strives to identify and exploit adversary attempts to mislead friendly forces. Activities that contribute to understanding adversary posture and intent serve to identify adversary deception attempts. Countering deception is difficult. Knowing deception methods an adversary has used successfully is important. Properly balancing tactical and operational indicators with strategic assumptions is also important. The chance of surprise might be reduced if estimates weigh tactical indicators more heavily than strategic assumptions. Dismissing tactical indicators because they conflict with preconceptions may allow a hostile deception operation that plays on those

preconceptions to succeed. Counterdeception includes actions taken to force adversaries to reveal their actual and deception intentions and objectives. It 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 them. Counterdeception includes actions taken to thwart adversary attempts to capitalize on deception tactics, thus affecting adversary decision-making processes.

a. **ISR.** ISR is a capability that provides awareness of an adversary's posture or intent and identifies an adversary's attempt to deceive friendly forces. Continual analysis of an adversary's deception operations and activities provide commanders and staffs with an understanding of the adversary's deception doctrine, techniques, capabilities, and limitations. Armed with this knowledge, MILDEC planners can assist others to identify and respond to adversary deception measures. Trained MILDEC analysts should be postured and have access to intelligence data, information, and products during the deployment and execution of friendly operations. If intelligence reveals or suggests adversary deception during the deployment or execution, planners should ensure that this intelligence and its potential impact on the friendly operation is considered. Counterdeception relies on coordination between the operations and ICs. Identifying an adversary's MILDEC attempts is the responsibility of the IC, but how this information is acted upon is the responsibility of the commander.

For further guidance on joint intelligence and the operational environment, refer to JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

b. **Countering Adversary Deception.** After an adversary's deception operation is revealed, commanders can adopt one of several COAs. Commanders can ignore, expose, exploit, or eliminate adversary deception efforts. Each COA involves a different level of risk. For example, 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. Commanders might choose to publicly expose the deception to cause embarrassment or to increase confusion within an adversary's information environment and systems. The intent here is to illustrate to the adversary that his or her deception operations are futile, and to discourage further attempts. Exposure techniques could include the use of print and broadcast media to garner support among allies and influence the adversary's population. Another COA is to exploit the adversary's deception effort. An example of exploitation might involve friendly forces pretending to be deceived until the culminating point of the adversary's deception, and then reacting in an unexpected manner to turn the adversary's deception against himself. Eliminating the adversary deception effort could involve destroying or degrading the adversary's deception capabilities and resources.

c. Knowledge of an adversary's deception plan enables a commander to take appropriate action against the deception, gain valuable insight into the perceptions of the adversary (the means used to portray the deception story that is passed, and the deception targets and objectives), and allows for increased force protection if required. The exposure of an adversary's deception operation reveals the way the adversary views friendly forces. This information can provide a tool for influencing those perceptions and subsequently be

used effectively against the adversary. Once friendly forces understand the deception and how the adversary is using it, they can begin to look at methods of exploiting the deception (as previously discussed). Other benefits may include utilizing the adversary's deception means to counter with our own deception.

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

Information-related capabilities can play a coordinated and interrelated role in the overall MILDEC effort. The purpose of employing other information-related capabilities in a coordinated effort is to achieve a common objective. Coordination and close cooperation supports the principle of unity of effort, which is not normally attained from independent application.

a. MILDEC and Military Information Support Operations

(1) Military information support operations (MISO) are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motivate objective reasoning, and ultimately the behavior of foreign governments, organizations groups, and individuals.

(2) MISO and MILDEC potentially engage the same target audiences simultaneously in support of commander's objectives. Themes and messages used to engage target audiences must remain consistent throughout operations 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 truth and must be credible. MILDEC themes and messages contain falsehoods and need only be believable. The two can be mutually beneficial, but they may also run counter to each other; therefore, MISO and MILDEC should be carefully coordinated.

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

b. MILDEC and Operations Security

(1) OPSEC is the process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify actions that can be observed by adversary intelligence systems; determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. OPSEC is a methodology that denies critical information to an adversary. Unlike security programs that seek to protect classified information, OPSEC measures identify, control, and protect generally unclassified evidence that is associated with

sensitive operations and activities. This unclassified information is called OPSEC indicators, which are friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. OPSEC measures are methods and means to gain and maintain essential secrecy about critical information. Critical information is specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

(2) OPSEC and MILDEC have much in common because both seek to limit an adversary's ability to detect or derive useful information by observing friendly activities. MILDEC also seeks to create or increase the likelihood of detection of certain indicators to cause an adversary to derive a predicted/predictable conclusion.

(3) DISO can directly support OPSEC by creating numerous false indicators, making it more difficult for adversary intelligence analysts to identify the real indicators that OPSEC is seeking to control. Cover stories, for example, provide plausible explanations for activities that are impossible to hide. False vehicle or aircraft markings can disguise the deployment of specific forces.

(4) OPSEC supports MILDEC. An OPSEC analysis of a planned activity or operation identifies potential OPSEC vulnerabilities. Those vulnerabilities are useful to MILDEC planners as possible conduits for passing deceptive information to an adversary. The OPSEC process identifies key characteristics about friendly capabilities and intentions, which adversary commanders need. OPSEC can complement MILDEC by denying the adversary information required to both assess a real plan and disprove a deception plan. MILDEC planners set out to provide the adversary with plausible incorrect information that can induce certain desired actions.

(5) MILDEC actions often require specific OPSEC protection. The existence of a MILDEC operation in and of itself may convey OPSEC indicators that reveal to the opposing commander the actual friendly intentions. An OPSEC analysis of the planned MILDEC is needed to protect against an inadvertent or unintentional outcome. Failure to maintain good OPSEC can lead to identification of the operation as a deception effort and cause the adversary's intelligence services to refocus their attention on the actual friendly operation.

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

c. **MILDEC and Electronic Warfare**

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

(a) **EA** involves the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is a form of fires.

(b) **EP** involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EM spectrum that degrade, neutralize, or destroy friendly combat capability.

(c) **ES** involves actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.

(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 ISR systems and assets can facilitate the insertion of deceptive information. EW targeted against ISR 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 that EW does not disrupt any adversary communications systems that are used as MILDEC conduits or that are providing intelligence feedback.

(4) EM deceptive techniques are a form of EA and a technical means of MILDEC. EM deception is the deliberate radiation, reradiation, 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 EM Deception.** This type of deception involves actions to eliminate revealing, or convey misleading, EM telltale indicators that may be used by hostile forces.

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

(c) **Imitative EM Deception.** This type of deception introduces EM energy into enemy systems that imitates enemy emissions.

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

d. **MILDEC and Cyberspace Operations**

(1) **Integration of Cyberspace Operations (CO) and MILDEC.** MILDEC and CO can be mutually supportive in a variety of ways. A few examples are noted below:

(a) CO and OPSEC can act as a supporting effort to an overall MILDEC objective by luring intruders to "honey pots" as conduits to the deception targets.

(b) MILDEC planners can help prevent physical destruction of critical nodes by ensuring that the IS is replicated as part of the MILDEC operation just as are combat forces. Such an operation may include the construction of false servers, communications nodes, and other hardware associated with a tactical computer network.

(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.

(2) **Planning Considerations for Integrated CO and MILDEC.** Given the highly technical knowledge required for successful friendly CO, and the specialized planning experience needed for MILDEC, integration of the two areas is critical for mission success.

(a) Any MILDEC plan must consider the abilities and limitations of friendly and adversary CO. Careful and detailed planning is required to ensure that MILDEC executions using CO assets are tracked, recorded, and deconflicted with real CO.

(b) The MILDEC plan should be protected as highly sensitive material and not exposed to unprotected computer networks or sent via unsecured email. 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 is 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? Is time better utilized by performing other executions?

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

e. **MILDEC and Physical Attack/Destruction**

(1) Physical attack/destruction refers to the use of lethal weapons against designated targets as an element of an integrated IO effort. The relationship of MILDEC and physical attack/destruction is very similar to that of deception and EW. MILDEC, used in conjunction with OPSEC, can protect the deployment and use of physical attack or

destruction systems. It can mislead an adversary as to the true capabilities and purpose of a weapon system.

(2) Physical attack/destruction can support MILDEC by shaping an adversary's intelligence collection capability through destroying or nullifying selected ISR capabilities or sites. Attacks can mask the main effort from the adversary.

(3) MILDEC planners should be an integral part of developing the integrated target priority list to ensure gain versus loss assessments are conducted prior to destroying potential MILDEC conduits such as ISR or radar sites.

f. **MILDEC and Information Assurance.** Information assurance (IA) 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, IA serves to detect, protect, and overcome adversary deception attempts while at the same time safeguarding information and indicators that may reveal friendly deception operations.

g. **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 principle of MILDEC. Without adequate physical security, a MILDEC plan can be compromised. Physical security measures contribute directly to the success of MILDEC and counterdeception operations. Commanders should ensure physical security measures are integrated into every phase of the deception planning process.

h. **MILDEC and Public Affairs (PA).** MILDEC operations should be coordinated with PA to avoid potential compromise of the deception operation and to work out other details of planning such as compliance with Department of Defense (DOD) policies and procedures that affect MILDEC. MILDEC activities, including planning efforts, do not explicitly or implicitly target, mislead, or attempt to influence the US Congress, the US public, or the US news media. All MILDEC activities eliminate, minimize, or mitigate the possibility that such influence might occur. Using PA to misinform the media about military capabilities and intentions in ways that influence US decision makers and public opinion is contrary to DOD policy. 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.

i. **MILDEC and Civil-Military Operations.** Civil-military operations (CMO) are conducted as part of the overall US diplomatic, military, economic, and informational effort and may occur before, during, or subsequent to other military operations. 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 that 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.

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

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

5. Information Operations Planning

a. IO planning is accomplished within the JFC's overall joint operation planning and should begin at the earliest stage of a campaign or operation planning efforts. The organizational structure to plan and coordinate IO should be sufficiently flexible to accommodate a variety of planning and operational circumstances. To be successful, IO should be an integral part of all phases of joint operations. This requires extensive planning and coordination among many elements of the joint headquarters and component staffs to ensure that IO are fully integrated with other phases and operations.

b. The JFC normally establishes an IO cell. Joint force staffs effectively plan integrate and synchronize IO efforts through the IO cell. 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 and is responsible for incorporating and deconflicting MILDEC with other IO. Because MILDEC plans are close hold, some MILDEC details may be compartmentalized due to OPSEC.

c. The IO cell is the coordination entity for the MILDEC representative and other government agencies and 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 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 and Concealment

Camouflage and concealment are related to MILDEC but they are distinctly different. Camouflage is the use of natural or artificial material on personnel, objects, or tactical positions with the aim of confusing, misleading, or evading the adversary. Concealment is the protection from observation or surveillance. MILDEC, as previously described, are those

actions executed to deliberately mislead adversary military decision makers. Camouflage and concealment provide protection for MILDEC, particularly at the tactical level, by manipulating the appearance or obscuring the deceiver's actual activities.

7. Military Deception's Relationship to Legal Support

MILDEC and Legal Support. Staff judge advocate (SJA) personnel are included in coordination efforts to ensure compliance with US law and international law. SJA personnel assist in planning the operation to meet the objective while complying with legal requirements, such as providing training to deception planning cell (DPC) personnel on LOAC, foreign law, and ethics as applied to MILDEC operations.

THE 5TH WIRELESS GROUP—ELECTRONIC DECEPTION

During the period just prior to the allied invasion of German-held territory at Normandy, a special electronic unit, the 5th Wireless Group, was formed to help with the deception plan for the invasion. By this point in the war the Germans had no air cover available for aerial reconnaissance and were relying completely on wireless transmissions. The 5th Wireless Group utilized a newly developed transmitter, which allowed a group of people to effectively simulate an entire network of people taking part in exercises.

Before writing the scripts for transmission, the 5th Wireless Group observed genuine exercises, both land and amphibious, taking place in Yorkshire and off the coast of Scotland. Scripts were then prepared, rehearsed, and "performed" using troops stationed in the area to record the exercises. Great care was taken in ensuring authenticity including, interestingly enough, taking care that it was not "too perfect." In real conversation, script writers noticed, there were phrases missed, requests for repetition, conversations overlapping, etc. Every attempt was made to make the exercises seem genuine, even if it meant adding a little confusion.

These exercises were an integral part of FORTITUDE SOUTH, the operation designed to convince the German command of the invasion from the Pas de Calais. Once the deception was completed and the invasion of Normandy proven successful, the 5th Wireless Group was also deployed to Europe to assist in deception regarding troop movements. It continued to serve as an important factor in deception until the defeat of the German forces.

SOURCE: Martin Young and Robbie Stamp
Trojan Horses: Deception Operations in the Second World War

Intentionally Blank

CHAPTER III
ROLES, COORDINATION, AND CONSIDERATIONS FOR MILITARY DECEPTION

"In his movements the general should act like a good wrestler; he should feint in one direction to try to deceive his adversary and then make good use of the opportunities he finds, and in this way he will overpower the enemy."

The Emperor Maurice
***The Strategikon,* c. 600 AD**

1. Roles and Responsibilities of Military Deception Planners

Due to MILDEC's dynamic role in joint operations, JFCs can use any of their forces and all feasible and available methods subject to the rules of engagement (ROE) and LOAC to accomplish their MILDEC objective.

a. **Roles**

(1) **Commanders.** While MILDEC may not be appropriate to every joint operation, each JFC determines whether MILDEC could contribute to the achievement of assigned objectives. This determination is usually made after the analysis that goes on in the Adaptive Planning and Execution (APEX) process. JFCs make the determination to use MILDEC after evaluating the analysis and recommendations that occur during joint planning. Commanders should guide and support applicable MILDEC operations and should also be readily available to the MILDEC planners.

(2) **Operations Directorate of a Joint Staff (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 COAs to the JFC that may include various options for IO (including MILDEC). Once the JFC has selected a particular 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 the execution of MILDEC.

(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 the MILDEC planning as part of the overall IO plan. The IO cell chief is also responsible for monitoring the implementation and execution of the MILDEC portion of IO.

(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 combatant commands, 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 combatant command. The CMDO also provides support to the approved MILDEC plans and operations of other combatant commands as required. Specific duties and responsibilities of the CMDO are specified in CJCSI 3211.01E, *Joint Policy for Military Deception*.

(5) **MILDEC Planner.** The MILDEC planner is the commander's lead agent responsible for drafting the MILDEC objectives for various COAs. Once a particular COA that requires MILDEC has been approved, MILDEC planners work with other planners (internal and external to the IO cell) as necessary to develop detailed plans.

(6) **Other Planners.** All joint staff planners should consider using MILDEC when developing COAs. Because of the classified and close hold nature of MILDEC, 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 other planners outside the IO cell that may benefit from the addition of MILDEC actions to their part of the plan.

b. **Responsibilities**

(1) **Commander.** The conduct of MILDEC is the responsibility of the commander. Not all staff elements have an active role in MILDEC operations; however, each staff element contributes to the overall effort. 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 the 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 higher approval for employment of certain technical deception means.

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

(2) **Intelligence Directorate of a Joint Staff (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 insights into the adversary, and the adversary's capability to process, filter, and evaluate ISR 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 measurements of deception effectiveness.

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

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

(f) Responds to MILDEC planners RFI inputs that solicit BIA/HFA data on adversary military, paramilitary, or VEOs.

(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 or synchronized as part of the lethal or nonlethal effects as part of the joint targeting process.

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

(e) Supervises execution of the deception plan.

(f) Develops measures of effectiveness (MOEs) to assess the deception operation.

(g) Controls termination of the deception effort.

(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 standing war plans and initiates deliberate planning efforts.

(a) Coordinates with the CMDO to ensure deception planning is included into standing 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 serves as the coordinating authority for the planning of MILDEC and the integration of Joint MILDEC with other elements of IO. The Joint Staff J-3 supports the CCDRs in development, assessment, coordination, and recommendation of MILDEC planning and operations COAs. The MILDEC planner forwards any plan that has transregional effects or that directly supports national objectives to the Joint Staff. The Joint

Staff J-3 then conducts a review of the plan and ensures combatant command MILDEC requirements do not conflict with MILDEC operations occurring in other areas of responsibility. If a conflict is detected, the Joint Staff J-3 recommends possible allocation solutions and forwards these to the Joint Staff. When MILDEC operations support operations falling under the auspices of Campaign Plan 7500, coordination with United States Special Operations Command (USSOCOM) is required. The Joint Staff determines the appropriate actions to be taken to resolve any conflicts which cannot be resolved by USSOCOM.

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 government 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 coordination officer normally is 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, restrict knowledge of information relating to planned and ongoing MILDEC operations to only those personnel who meet the strictly defined need-to-know criteria.

(1) The JFC is responsible for providing 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 members.

(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 Enclosure F of CJCSI 3211.01E, 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. In some situations, a joint force may lack the capability to convey certain types of deceptive information to the adversary. Other organizations, however, may have the required capability. MISO organizations can discreetly convey tailored messages to selected target audiences through appropriate "key communicators" back channel networks.

PLANNED DECEPTION—BATTLE OF EL ALAMEIN

General Charles Richardson, a member of General Montgomery's staff given responsibility for planning deception before the Battle of El Alamein, considered several factors in executing the operation.

Richardson's first priority was to create a deception to convince General Rommel that the attack would be coming from the south; secondly, that it would occur later than the actual target date. To that end, Richardson put together a plan of concealment and deception. In order to create the illusion of a southern attack, "spoof" assembly areas were put together in rear areas, while preparations in the forward area such as petrol and ammunition dumps were camouflaged. Petrol, which was provided in tins of two feet by ten inches square, was brought up at night and arranged to resemble fire trenches rather than lying on the ground in a dump as usual. Water pipelines played a major role in clouding the time factor. Richardson knew that the enemy would be watching such construction and using it to judge for when work would be completed; in order to use this observation to their advantage, the camouflage crew used empty petrol tins to create the effect of a pipeline gradually being completed. To enemy surveillance cameras it appeared that construction on the water pipelines would not be completed until ten days after D-Day.

Other deception plans were being carried out simultaneously. A dummy petrol, food, and ammunition dump was placed in the rear in the south in order to bolster Rommel's impression of a southern attack; meanwhile, ammunitions dumps at the front were enlarged and camouflaged. Legitimate armored formations were moved to the front at night, where they were concealed from detection by sunshields. They were replaced by dummy formations. Dummy artillery units placed in the south not only served in the initial deception but, when they were discovered to be shams during the battle, were promptly replaced with genuine artillery and mounted a surprise counterattack.

In addition to the planned deception, the Royal Air Force kept the Luftwaffe's Technical Reconnaissance from gaining a clear picture of the ground operations. The German command was so completely fooled by the deceptions that Rommel was away when the battle started. It was several days before reinforcements could be moved up from the northern sector.

SOURCE: Martin Young and Robbie Stamp
Trojan Horses: Deception Operations in the Second World War

MILDEC planners should conduct the coordination required to obtain the necessary support from those organizations and to integrate, coordinate, and deconflict MILDEC and actual operations.

i. Assign liaison officers (LNOs) from the appropriate intelligence staffs and CI 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.

3. Military Deception Considerations

JFCs should ensure that their staffs and units receive training in MILDEC. Additionally, joint operation and MILDEC planners should receive appropriate MILDEC training. Accomplish staff training during command post exercises, wargames, and conceptual exercises during the preparatory and execution periods of field exercises or routine forward deployments. Seminars, briefings, and other such activities can also provide training for individuals and staffs. Conduct unit training during exercises.

a. **JFCs and Staffs.** To effectively plan and execute MILDEC, commanders and their staffs should be trained to understand:

(1) The role of MILDEC in IO.

(2) MILDEC's value as a force multiplier and as a cost effective tool for achieving operational objectives.

(3) What is required to plan and execute effective MILDEC.

(4) The policies that govern the use of MILDEC.

(5) Legal constraints in the use of MILDEC.

b. **Joint Operation Planners.** Those assigned as joint operation planners should understand:

(1) The process for addressing MILDEC during preparation of staff and commanders' estimates and COA development.

(2) The broad range of what can and cannot reasonably be executed as MILDEC.

(3) How the other IO capabilities support MILDEC.

(4) How MILDEC supports other IO capabilities.

(5) Deception's role in military history.

c. **MILDEC Planners.** The selection and training of MILDEC planners are critical. The Services currently have MILDEC courses that are available for potential planners to

attend. The Office of the Secretary of Defense, Defense Military Deception Program Office (OSD/DMDPO) also offers a Joint MILDEC training course. Additionally, OSD/DMDPO provides mobile training teams that provide on-site MILDEC training to deploying units. It is essential that MILDEC planners possess fertile imaginations, because the ability to create and execute an effective MILDEC often depends upon the creativity used to develop and maintain a story. MILDEC planners must:

(1) Understand each component's deception and other IO capabilities.

(2) Be intimately familiar with their command's assigned missions and operational area.

(3) Understand the concepts of centers of gravity, calculated risk, initiative, security, and surprise.

(4) Understand friendly and adversary intelligence systems and how they function.

(5) Possess technical understanding of intelligence sensors, the platforms on which they deploy, their reporting capabilities, and associated processing methodologies.

(6) Understand the psychological and cultural factors that might influence the adversary's planning and decision making.

(7) Understand potential adversaries' planning and decision-making processes (both formal and informal).

(8) Understand the assets that are available to support the deception.

CHAPTER IV
MILITARY DECEPTION PLANNING

"To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds."

Mao Tse-Tung
***On Protracted War,* 1938**

1. Military Deception Planning and the Joint Planning Processes

MILDEC planning is conducted in conjunction with the APEX system. It is part of effective joint operations planning and is not an "add on" to the existing planning processes.

a. MILDEC planning can be deliberate planning (used normally during peacetime to develop OPLANs and CONPLANs), or during crisis action planning (CAP) (during time-sensitive situations to rapidly develop campaign plans and orders). See JP 5-0, *Joint Operation Planning*, and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122 Series, *Joint Operation Planning and Execution System (JOPES)* for discussion on deliberate planning and CAP.

b. **The CAP Process.** Use CAP during time-sensitive situations to rapidly develop campaign plans and OPORDs. MILDEC planning relates to the APEX CAP process.

c. **The Campaign Planning Process.** Campaign planning may begin during deliberate planning when the actual threat, national guidance, and available resources become evident, but it is normally not completed until after the President and Secretary of Defense select the COA during CAP. After the COA is approved by the President and Secretary of Defense, the supported commander provides specific guidance to the staff. That COA becomes the basis for the development of an OPORD.

2. 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" that the deception is true. MILDEC must end in an action, or inaction, that supports the JFC operational plan. 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 IV-1). The following interrogatories describe the process:

(1) **See:** What does the target see from friendly operations?

(2) **Think:** What conclusions does the target draw from those observations?

(3) **Do:** What action may the target take as a result of the conclusions based upon those observations?

c. A perfect example of the methodology at work was Operation BODYGUARD in 1944, the deception plan in support of Operation OVERLORD (the D-Day invasion). In that example, the Allies conducted air raids, broadcasted false communications, and even built an entire deceptive army to convince the German high command that the real objective of the invasion was Pas de Calais. The German high command saw these operations ***(See),*** drew the conclusion that Calais would be the initial objective of the invasion ***(Think),*** and took the action of reinforcing the area with an entire field army ***(Do).***

d. **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 their 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.

e. The DPC is a focal point for MILDEC planning and execution. The DPC may be formed using existing members of the IO cell or key planners that the commander or the DPC chief determine. At a minimum, the DPC should include representatives from J-2, J-3, J-4, J-5, and J-6. In accordance with the JFC's guidance, the DPC plans, coordinates, and monitors MILDEC operations. With the JFC's approval, the DPC also may 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 A (Military Deception) to appendix 3 (Information Operations) to annex C

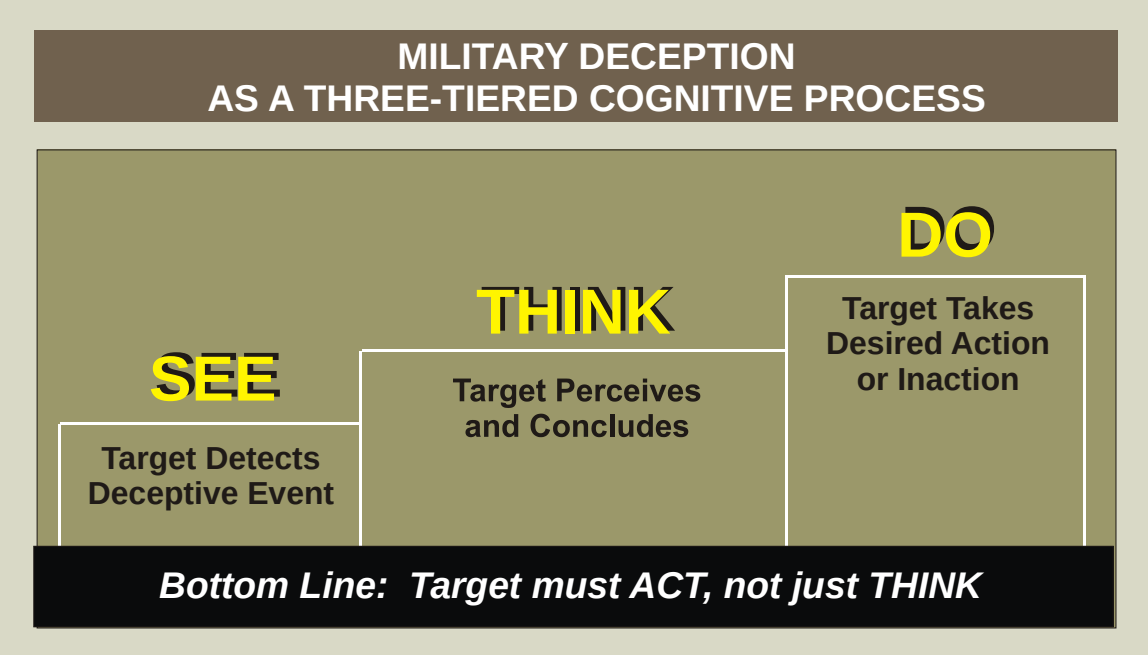


Figure IV-1. Military Deception as a Three-Tiered Cognitive Process

(Operations) for the OPORD. Other responsibilities of the DPC include:

(1) Directing and coordinating deception planning activities.

(2) Interfacing and working closely with unit operations planners to review and analyze plans for deception requirements.

(3) Responding to higher headquarters' deception tasking and ensuring appropriate coordination.

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

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

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

3. The Military Deception Planning Process

Deception planning is an iterative process that requires continual reexamination of its objectives, target, stories, and means throughout the planning and execution phases. MILDEC planners must be prepared to respond to the dynamics of the adversary as well as friendly situations. A key factor that must be considered during MILDEC planning is risk. At each stage of deception planning, the MILDEC planners must carefully consider the risks involved with using deception. The overriding consideration in risk analysis is the comparison between the risk taken and the possible benefits of the deception. Major determining factors include the following: deception failure, exposure of means or feedback channels, and unintended effects and consequences. The MILDEC planning process consists of six steps (see Figure IV-2).

a. **Step 1: Deception Mission Analysis.** MILDEC mission analysis is conducted as part of the overall mission analysis that is done by a JFC. During this analysis, the JFC establishes a deception goal that describes how the MILDEC is expected to support the accomplishment of the mission. Next, the JFC identifies deception objectives that clearly identify adversary action (or inaction) that directly supports the deception goal. MILDEC is not applicable to every situation, but commanders and planners should consider it, especially at the operational level. Even in situations where Joint MILDEC or TAC-D is inappropriate, there is normally a role for DISO.

b. **Step 2: Deception Planning Guidance.** After completion of the mission analysis, the commander issues planning guidance to the staff. In addition to other guidance, the commander may include the deception goals and objectives for the operation. The commander may go on to provide additional guidance concerning specific deception COAs that the staff should address when preparing estimates. MILDEC should be planned and executed as part of the overall concept of the operation from its inception. Even if a

MILDEC operation is well executed, an adversary may detect the MILDEC operation if it is

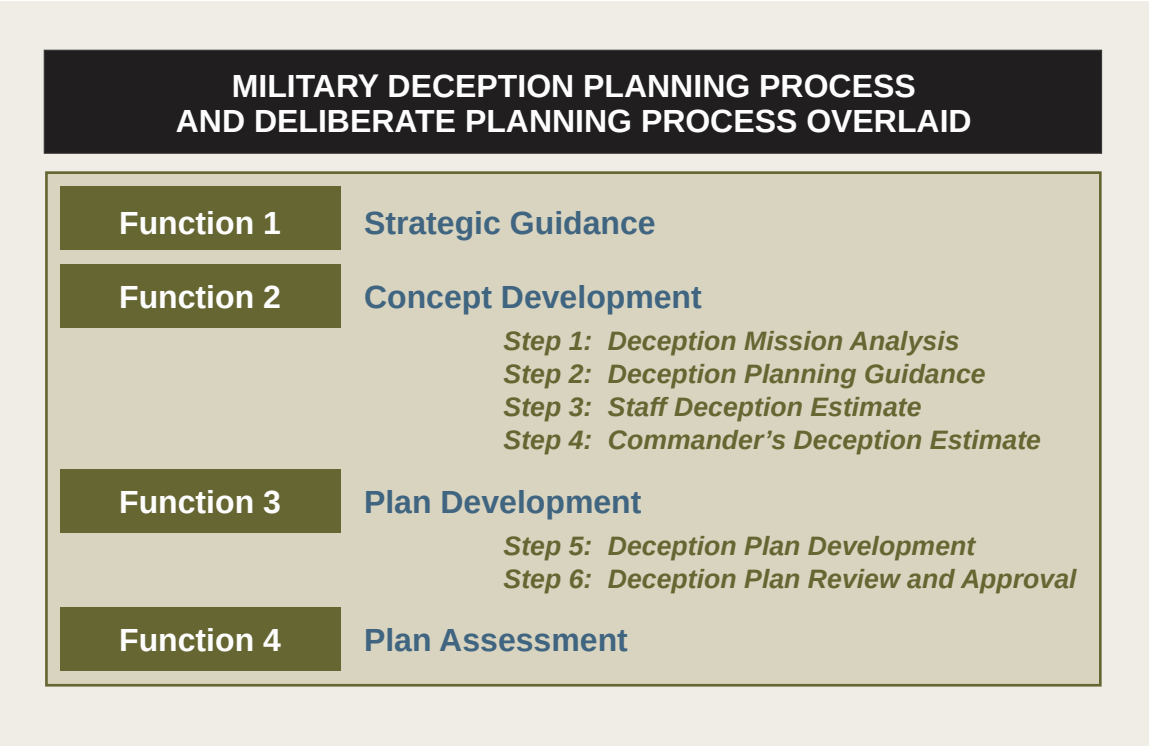


Figure IV-2. Military Deception Planning Process and Deliberate Planning Process Overlaid

not consistent with the rest of the perceived overall operation.

c. **Step 3: Staff Deception Estimate**

(1) The deception estimate is conducted as part of the operations estimate. Working with operational planners and intelligence analysts, MILDEC planners:

(a) Gather and analyze information relating to the adversary.

(b) Identify the key decision makers and study all available information relating to their backgrounds, psychological profiles, and biometrics enabled intelligence.

(c) Identify preconceptions that adversary leadership may have about friendly intentions and capabilities.

(d) Consider the adversary's C2 system and decision-making process.

(e) Study adversary ISR collection and analysis capabilities.

(f) Study adversary CI collection and analysis capabilities, systems, networks.

(g) Identify COAs that the adversary may adopt or have under consideration.

(2) Intelligence analysts provide assessment of adversary vulnerability to MILDEC in the intelligence estimate.

(a) They determine the adversary's detection and collection capabilities. The first action in means selection is determining the adversary's detection and collection capabilities.

1. The intelligence staff can provide multidiscipline CI products that can identify a particular adversary's capabilities.

2. Most adversary surveillance and reconnaissance capabilities include at a minimum human intelligence, open-source intelligence, and some signals intelligence (SIGINT) and geospatial intelligence capabilities. More sophisticated surveillance and reconnaissance systems will include airborne and spaceborne systems that may include extensive SIGINT capabilities and organic or foreign commercial imagery collection systems. The adversary may have access to data collected from assets he does not control. These assets may include US or foreign commercial and foreign government ground, air, or space-based reconnaissance systems.

3. Study each adversary to determine its particular surveillance and reconnaissance capabilities. If possible, determine which surveillance and reconnaissance capabilities the deception target most relies upon for information during decision making.

4. Deception planners need to be aware of and consider the possibility of adversaries acquiring intelligence from commercial surveillance and reconnaissance systems. If the adversary does not maintain a formidable surveillance and reconnaissance capability, they may seek to purchase intelligence data available in the open market. Intelligence

General Eisenhower's thorough analysis of the German High Command was a crucial element of the deception planned in support of the Normandy Invasion.

analysis needs to include ISR organizations and systems that are not directed by the adversary but available for their use as a resource.

(b) They identify the current possible (and, when justified by the evidence, probable) adversary COAs and the adversary's rationale for taking those actions.

(c) Analysts help commanders and MILDEC planners understand how adversary decision makers, their staffs, and trusted advisors perceive friendly capabilities and intentions and how the adversary is likely to react to the deception.

(d) They identify key organizations and personnel who will either make decisions or take actions that impact on whether the deception story is accepted or rejected by the target. They identify known existing and potentially accessible, or required (yet unidentified or established), sensor-conduit networks that can carry the deception story to the target. They identify how the deception story will be received, interpreted, and acted on within the target's particular decision-making style.

(e) CI analysts provide expertise concerning the adversary's ISR collection capabilities and processes, which is required to select appropriate conduits for deceptive information and to determine time frames for deception events. They also advise on efforts the adversary is likely to take to verify collected information.

(3) On the basis of the information developed during the initial estimate process, the MILDEC planners, working directly with the operation planners and the other IO planners, develop several deception COAs. The proposed deception COAs must each be capable of accomplishing the commander's deception goal. Integrate the deception COAs with the operational COAs that are developed.

(4) Each MILDEC COA must support the JFC's deception goal and objectives. Each MILDEC COA will identify deception target(s), discuss required perceptions, evaluate possible deception means and conduits, and provide an outline of the proposed deception story.

(5) In many cases, actual COAs developed by the operational planners will provide the basis for MILDEC COAs. Using COAs developed by operational planners helps to ensure that the deception COAs are feasible and practical military options. Additionally, the proposed deception COAs should seek to promote actions that the adversary is already conducting or considering.

(6) When assessing COAs, determine what would be the effect if the adversary responded differently than expected. What is the risk of the adversary not responding favorably? For example, if a MILDEC was planned to launch a substantial number of aircraft to condition the adversary to their presence, in the hopes of disguising the actual attack when it did occur, what is the possibility of the adversary launching a preemptive strike when they see the friendly air formations?

(7) The strengths and weaknesses of each of the proposed MILDEC COAs are analyzed. 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.

(8) In the final phase of the estimate process, the MILDEC planners consider MILDEC during the comparison of the proposed friendly operational COAs. The ability of MILDEC along with the other IO tools to support a particular friendly COA is one of the factors considered when determining which proposed COA is recommended for adoption by the JFC.

d. **Step 4: Commander's Deception Estimate**

(1) Using the staff estimates as a basis, the JFC conducts an estimate. The JFC selects an operational COA for development into an OPLAN or OPORD and issues any necessary additional guidance. At the same time, the JFC selects the supporting deception COA.

(2) The JFC's decision becomes the basis for the development of the selected deception COA into a complete plan or order. As in the other steps in the process, the MILDEC planners work very closely with other planners to ensure that the deception plan and the OPLAN are mutually supporting.

(3) The component MILDEC planners, if not already participating, are brought into the planning process at this point to ensure that their units can support the plan, as well as to facilitate the integration of individual component MILDEC plans into the overall joint MILDEC plan.

e. **Step 5: Deception Plan Development.** Developing a complete MILDEC plan is the most time-consuming part of the planning process. **There are six major actions in this step:** complete the story, identify the means, develop the event schedule, identify feedback channels, determine MOES, and develop the termination concept.

(1) **Complete the Deception Story**

(a) During the estimate, planners develop a deception story outline. The planners now need to transform the outline into a fully developed story. MILDEC planners must identify all actions that the adversary's ISR systems would see and would not see if friendly forces were actually executing the deception story. MILDEC planners will require the assistance of operational, logistic, and communication system planners to ensure that all normal activities are identified.

(b) Time is a key element to consider in developing the deception story. The 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 the decision to take 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:

1. **Time of Maximum Disadvantage.** When is the adversary's action (or inaction) required: tomorrow, next week, or next month? The amount of time available for planning and executing the MILDEC plan may limit the scope of the MILDEC operation.

2. **The Deception Target.** Is the target cautious or bold? Will the target react to initial indicators, or will the target demand extensive confirmation through other ISR sources before reaching a decision? How long does it normally take the target to make a decision?

3. **Opposing Force Execution.** Once the decision is made, how long will the target need to formulate and issue an order? How long will it take the adversary to perform the desired action? For example, if the deception objective is the movement of an adversary squadron to some distant point, allow time for the deception target to issue the movement order and for the squadron to receive and execute the order.

4. **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.

5. **Execution of the Deception Tasks.** When must displays, demonstrations, feints, and other actions be detected or recognized by the adversary's ISR systems? How long should each last?

(2) **Identify the Deception Means.** Once the story is fully developed, MILDEC planners will identify the means used to portray the story. This action requires a detailed understanding of the adversary's ISR capabilities and of friendly force operations.

(a) **Identify Indicators.** The first action in means selection is to determine the specific indicators that are associated with the activities needed to portray the deception story. The collection of indicators associated with a particular unit or activity is commonly referred to as a unit profile. The profile is more than just a listing of equipment. The operational patterns (where, when, and how normal activities occur) associated with a unit or activities are also part of a profile.

1. This action requires detailed knowledge of friendly operations. If, for example, the plan calls for the electronic portrayal of a carrier task force, the MILDEC planners will need to determine what emitters are normally associated with that element and how they are normally employed.

2. If the main command post of an Army heavy maneuver brigade is portrayed electronically and visually, then the planner will need to know not only what communications systems are found in the command post but also how many vehicles and of what types, how many tents, and where and in what pattern the vehicles and tents are normally located.

3. Units of similar sizes can have very different profiles. Marine air-ground task forces and Army mechanized brigades have different profiles because of different equipment and communications systems.

4. Indicator and profile information is available from the component deception planners. An additional source is OPSEC program officers. They are also concerned about indicator and unit profiles.

5. To facilitate planning, joint deception planners, working with component planners and OPSEC program officers, should develop friendly unit indicator and profile databases.

(b) **Compare Capabilities to Indicators.** The next action is to compare the adversary's ISR collection capabilities, which were assessed during the staff deception estimate process, to the appropriate indicators. Those indicators that the adversary cannot collect will not require portrayal. If it is known that the adversary places a higher value on information received from certain intelligence sources than from others, then emphasize those indicators that are collected by the valued sources.

(c) **Select Means.** Using the results of the previous actions in this step, MILDEC planners now select the specific means that will portray the deception story.

1. In essence, the selection of deception means is the opposite of selecting OPSEC measures. While the goal of OPSEC is normally to reduce the adversary's ability to see certain indicators, deception normally seeks to increase the visibility of selected indicators. Both seek to manage what indicators are observed by the adversary. OPSEC and MILDEC planners must work closely to ensure coordinated indicator management.

2. During means selection, coordination is also required with the intelligence, EW, MISO, CO, and targeting planners to ensure unity of effort. If the deception story depends on the use of certain means, then the EW and targeting planners need to know not to target for destruction or disruption the particular adversary ISR systems that will collect against those means. For example, if the portrayal of the deception story is dependent upon false communications, then carefully coordinate attacks on the adversary's SIGINT system with the MILDEC planners. Similarly, coordinate MISO messages with the deception story to ensure that they are sending the same message to the deception target.

(3) **Develop the Deception Event Schedule**

(a) In this action, the deception means are developed into deception events. This requires identifying when specific means are employed. The objective is to ensure that the deception target's perceptions are influenced in time to complete the desired action (the deception objective) at the most operationally advantageous time.

(b) The MILDEC planners, in coordination with the other operational and intelligence planners, develop detailed execution schedules for the means identified in the previous action. The schedule identifies what will occur, when it will take place, where it will occur, and who will execute it.

(c) Consider the following factors during scheduling:

1. The timing of actual friendly activities.

2. The time required for friendly forces to conduct the deception activity.

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

4. The time required for the adversary ISR systems to collect, analyze, and report on the activity.

5. The time required for the deception target to make the desired decision and order the desired action.

6. The time required to execute the desired action.

(d) Group events to portray deception actions such as feints or demonstrations.

(e) The deception event schedule is published as part of the deception plan. Figure IV-3 is an example.

(4) **Identify the Deception Feedback Channels**

(a) MILDEC planners require two major types of feedback about their operations. Operational feedback identifies what deception information is reaching the deception target. Analytical feedback identifies what actions the deception target is taking because of that information.

DECEPTION EVENT SCHEDULE

ID#	OBJECTIVE	DATE/TIME TO INITIATE	ACTION	UNIT	DATE/TIME TO TERMINATE	REMARKS
29	Simulate preparation for movement south	131500	1. Establish traffic control points 2. Install radio nets 3. Pass scripted message traffic per scenario	Headquarters 2nd Division	131800	Initiate counter surveillance measures to prevent adversary visual photo reconnaissance of notional route

Figure IV-3. Deception Event Schedule

(b) All-source intelligence and CI about the adversary's intelligence interests and activities provide indications of the receipt of deception information.

(c) Observations by friendly surveillance and reconnaissance assets provide information about changes in the adversary's dispositions and actions. Those dispositions are normally the key determinant of the success of the MILDEC. Once operations commence, the adversary's reactions to friendly initiatives are indicators of whether the deception story is still believed by the deception target.

(d) MILDEC planners must coordinate with the intelligence planners to ensure that the intelligence needs of MILDEC are reflected in the command's priority intelligence requirements (PIRs). Additionally, MILDEC planners should work with the appropriate intelligence analysts to make them aware of the type of information that is sought. Establish reporting channels between the analysts and deception planners to facilitate the rapid passage of feedback information.

(e) MILDEC planners must also coordinate with other operational, intelligence, IO, and targeting planners to ensure that critical sources of deception feedback information are not targeted.

(5) **Measures of Effectiveness**

(a) MOEs are qualitative assessments based upon the aggregation of discrete, observable, and quantifiable indicators. MOEs provide commanders and higher authorities a means to evaluate the contribution of MILDEC efforts to the more encompassing and overarching desired end state. More importantly, MOEs facilitate the assessment of how well the deception achieves its specific goals. Such measures are situational dependent, often requiring readjustment as the situation changes and higher-level guidance develops.

(b) Developing MOEs for MILDEC can be the most difficult step in the deception planning process. Without MOEs, it is not possible to evaluate the effectiveness of the deception plan. MILDEC planners need to build MOEs into the plan to measure:

1. **Effectiveness.** Describes the relationship between outputs and objectives. Were the deception objectives achieved? If not, why not?

2. **Efficiency.** Describes the relationship of inputs and outputs. Although the deception plan was effective, were there ways to accomplish it quicker and with fewer resources?

3. **Adaptability.** Describes the ability of the deception plan to respond to changing demands. Was there sufficient flexibility to adjust the deception plan to react to an unexpected event?

(c) Develop MOEs and identify associated quantitative indicators as means to evaluate operations and guide decision making. Accurate and effective MOEs contribute to mission effectiveness in many ways. MOEs assist in identifying effective strategies and tactics and reveal points at which to shift resources, transition to different phases, or alter or

terminate the mission. There is no single all-encompassing checklist for MOEs; they vary according to the mission. However, commanders and staffs should keep the following factors in mind when developing and using MOEs.

1. **Appropriate.** MOEs should correlate to the audience objectives. If the objective is to present information to those outside the command, MOEs should be general and few in number. If the objective is to assist on-scene commanders, then MOEs should be more specific and numerous.

2. **Mission-related.** MOEs must correlate to the mission. If the mission is relief, MOEs should help the commander evaluate improvements in living standards, mortality rates, and other related areas.

3. **Measurable.** Quantitative MOEs reflect reality more accurately than non-quantitative MOEs, and hence, are generally the measure of choice when the situation permits their use. When using non-quantitative MOEs, clear measurement criteria should be established and disseminated to prevent misinterpretation.

4. **Reasonable in Number.** Avoid establishing excessive MOEs. They can become unmanageable or collection efforts will outweigh their value.

5. **Sensitive.** MOEs should be sensitive to force performance and accurately reflect changes related to joint force actions. Extraneous factors should not greatly affect established MOEs.

6. **Useful.** MOEs should detect situation changes quickly enough to enable the commander to immediately and effectively respond at decision points identified in the deception plan.

(d) MILDEC MOEs include indicators such as:

1. Adversary operational commander employs forces in ways advantageous to friendly forces.

2. Adversary commander reveals strengths, dispositions, and future intentions.

3. Overloading and confusion in adversary intelligence and analysis capability regarding friendly intentions.

4. Adversary conditioning to friendly patterns of behavior that are exploitable.

5. Adversary wastes combat power with inappropriate or delayed actions.

(6) **Develop the Termination Concept**

(a) Each MILDEC plan must address how to terminate the deception operation. Termination planning ensures the controlled, orderly 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 forcing its early termination.

(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. In some cases, 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. Most of the time, however, it is better not to reveal a MILDEC—either to the adversary or to friendly forces—to avoid deception exposure.

(c) There are numerous potential termination scenarios. They include:

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 parallel IO or other aspects of the 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 deceiver may want to terminate some MILDEC events and activities, while reorienting other elements of the MILDEC.

6. The *MILDEC compromise scenario*, in which the deceiver 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. Provide classification and dissemination instructions for deception-related information.

f. **Step 6: Deception Plan Review and Approval**

(1) Review and approval requirements and processes are stipulated in CJCSI 3211.01E, *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.

(2) The combatant command staff can further review any component, or subordinate joint force MILDEC plan.

4. Military Deception Capabilities, Limitations, and Risks

a. **Capabilities.** Successful military planners rely on deception to mask the real objectives of military operations. MILDEC remains a critical contributor to achieving surprise, 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.

b. **Limitations.** 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 our ability to measure the effectiveness of 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.

c. **Risks.** Risk is a key factor that must be reexamined during every phase of MILDEC planning and execution. Fully integrate risk management into planning, preparing, executing, and assessing.

(1) **Deception Failure.** MILDECs may fail for many reasons. It is possible that 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 may discover the deception. The failure or exposure of the deception can significantly affect the friendly commander's operational activities. 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 fail to design or implement the MILDEC operation carefully enough, or the intended target detects the deception.

(2) **Exposure of Means or Feedback Channels.** 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.

(3) **Minimize Risk to Third Parties.** Third parties (e.g., neutral or friendly forces not read into the deception) may receive and act on deception information intended for the deception target. MILDEC planners must ensure that 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.

5. Joint Planning Considerations

a. CJCSM 3122.01A, *Joint Operation Planning and Execution System (JOPES) Vol. I (Planning Policies and Procedures)*, contains the detailed requirements for preparing joint OPLANs, campaign plans, or OPORDs. JP 5-0, *Joint Operation Planning*, sets forth doctrine that guides planning by the Armed Forces of the United States in joint, multinational, or interagency operations. In planning, MILDEC is addressed as part of IO in the commander's overall CONOPS. The specific deception plan is located at tab A (Military Deception) to appendix 3 (Information Operations) to annex C (Operations) of any OPLAN or OPORD.

b. Balance the need to conduct adequate coordination during MILDEC planning 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, allowing more individuals access to the less sensitive aspects of the deception plan.

Intentionally Blank

CHAPTER V
EXECUTION OF MILITARY DECEPTION OPERATIONS

"Always mystify, mislead, and surprise the enemy, if possible; and when you strike and overcome him, never give up the pursuit as long as your men have strength to follow…"

Lieutenant General Thomas "Stonewall" Jackson, 1862

1. Execution of Military Deception Events and Actions

The MILDEC plan is normally executed as a component of the OPORD. As with all military operations, the process of execution involves two basic functions, assessing and control. Assessing involves the receipt and processing of information concerning the MILDEC operation, and control entails making iterative decisions and issuing instructions until termination. The deception plan is the basis for execution, but execution may take place in conditions that are more dynamic than the plan anticipated.

2. Deception Execution Coordination

Once the planning process is complete, it is critical that constant coordination at the strategic, operational, and tactical level continues to ensure success. The potential for a tactical or operational level deception to have strategic implications is high. With this in mind, a continual process of coordination, called the deception execution cycle, must take place.

During a Gulf War deception operation a simulated OH-58C Kiowa helicopter with simulated fuel blivets was used to portray a forward arming and refueling point.

a. The cycle begins with a leadership decision to terminate, alter, or plan new deception operations. The commander must be kept informed of the MILDEC success, failure, or the need to modify the plan.

b. 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.

c. The DPC must ensure the methods used to communicate the deception story are still appropriate and effective for the target audience. The methods should be assessed continually to see if they need to be modified or different ones implemented depending on successful or failed communications.

d. Among the MILDEC planner's most critical execution tasks is ensuring that the MILDEC is proceeding in synchronization with the commander's overall operational concept and is in line with the command's employment of IO.

e. Necessary coordination must occur 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 that the portrayal is credible, believable, and realistic.

f. Coordination with J-2 to monitor feedback from the MILDEC and comparison to current ROE, force protection issues, etc., allows the commander to determine if the MILDEC requires modification to meet changing operational requirements.

g. Compare termination concept criteria to current intelligence to see if the MILDEC requires termination.

h. Throughout the deception execution cycle it is imperative that tight security is practiced to protect the MILDEC and the operations that are supporting or being supported. Figure V-1 provides an example of this process.

3. Terminating Military Deception Operations

a. The termination of a MILDEC is concerned with ending the MILDEC in a way that protects the interests of the deceiver. The objective of a successful termination is to conclude the MILDEC without revealing the MILDEC to the adversary. The DPC is concerned about terminating the overall MILDEC, as well as the termination implications embedded in each MILDEC event. Planning how to end an individual deception event in a way that does not leave suspicious traces of the MILDEC operations is an inherent aspect of MILDEC event preparation. Reasons for termination can be seen in Figure V-2.

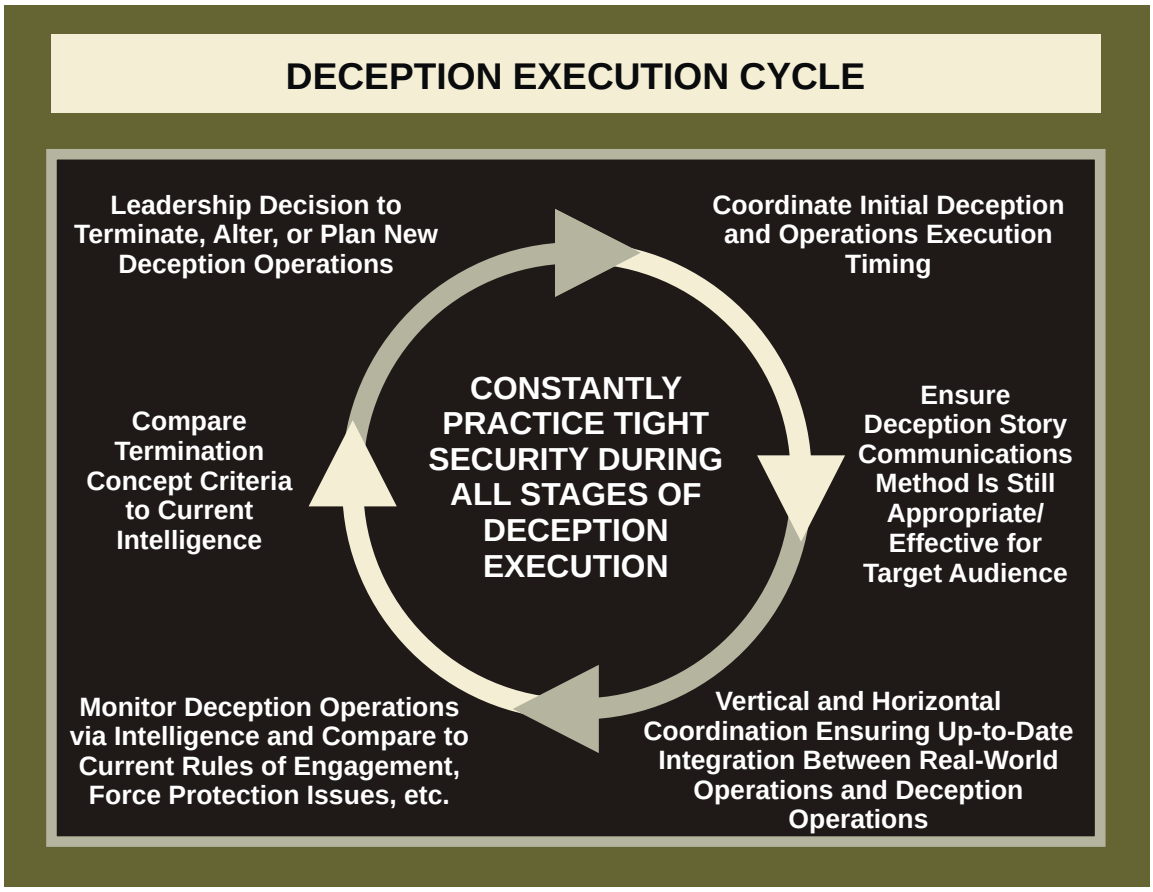


Figure V-1. Deception Execution Cycle

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 actions should reflect the predisposition and bias of the adversary. Termination actions are a presentation of what the deceiver wants the adversary to conclude with respect to the entire MILDEC. The range of termination may be expressed through silence, admission, denial, or a specialized MILDEC designed to mislead—a MILDEC within a MILDEC. As the MILDEC execution proceeds, some previously considered candidate termination options become unsuitable, while others become increasingly credible, warranting further planning requirements.

d. Termination of a MILDEC requires coordination. As a rule the commander retains the authority to terminate only when the operation is not part of a larger MILDEC operation and immediate termination is required to protect resources or more critical aspects of the larger operation. Otherwise, the initiating commander coordinates termination with the higher command prior to executing termination actions. This is necessary because aspects of the proposed termination plan, like the MILDEC itself, can place resources and operations at risk that lie beyond the purview of the initiating commander.

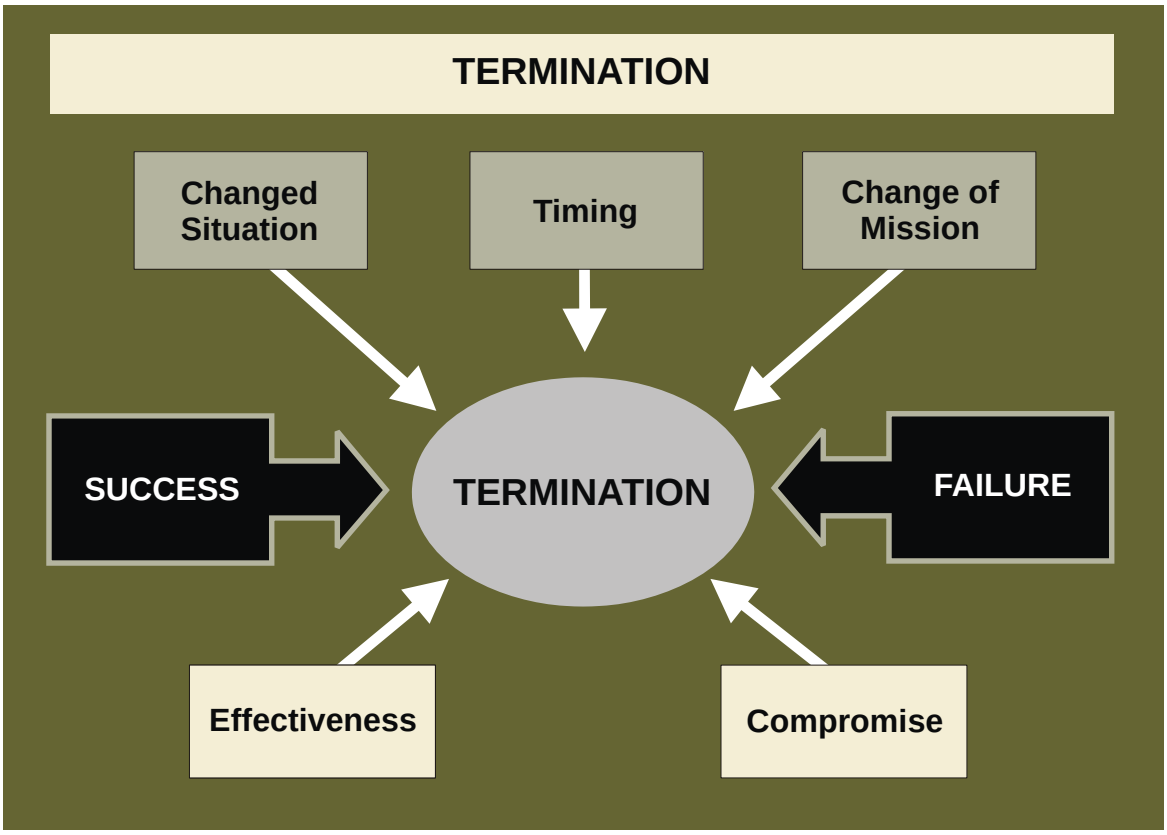


Figure V-2. Termination

e. Termination of a MILDEC also encompasses evaluation and reporting. After-action assessment should be conducted by the DPC. 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.

APPENDIX A
MILITARY DECEPTION MAXIMS

MILDEC maxims are derived by the military IC 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 limitations to human information processing that are deceptively exploitable. First, the "law of small number" suggests not to make conclusions based on a small set of data; there is no statistical certainty in doing so. Secondly, 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

surveillance and reconnaissance 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 ISR 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. It is necessary to effect proper coordination to ensure deceptions do not result in unit fratricide. 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 1100-man unit conducted 21 MILDEC operations from 1944-1945. In Operation BREST, it portrayed an armor attack build-up 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 build-up believed the story, but the German army commander, believing that 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 ISR 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.

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 deals 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. Glanz (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-McMann, 1983).

q. *The Wizard War* by R. V. Jones (Coward, McMann, 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).

ee. *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).

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

DOD Directive 3600.1, *Information Operations (IO).*

2. Chairman of the Joint Chiefs of Staff Issuances

a. CJCSI 3210.01B, *Joint Information Operations Policy* (U).

b. CJCSI 3210.03C, *Joint Electronic Warfare Policy* (U).

c. CJCSI 3211.01E, *Joint Policy for Military Deception* (U).

d. CJCSI 3213.01C, *Joint Operations Security.*

e. CJCSI 6510.01F, *Information Assurance (IA) and 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 3122.03C, *Joint Operation Planning and Execution System (JOPES) Volume II: (Planning Formats).*

3. Joint Publications

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

b. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms.*

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

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

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

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

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

h. JP 3-08, *Interorganizational Coordination During Joint Operations.*

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

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

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

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

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

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

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

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

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

r. JP 5-0, *Joint Operation Planning.*

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

4. Army Publication

US Army Field Manual 27-10, *The Law of Land Warfare*, w/Chg. 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 and Coalition Warfighting, Joint and Coalition Warfighting Center, ATTN: Joint Doctrine Support 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, 13 July 2006, *Joint Doctrine for Military Deception*.

4. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J39//
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//

b. Routine changes should be submitted electronically to the Deputy Director, Joint and Coalition Warfighting, Joint and Coalition Warfighting Center, Joint Doctrine Support Division and info the lead agent and the Director for Joint Force Development, J-7/JEDD.

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. 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 in accordance with DOD 5200.1-R, *Information Security Program*.

6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS at https://jdeis.js.mil (NIPRNET) and https://jdeis.js.smil.mil (SIPRNET) and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

b. Only approved JPs and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified JP to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA, Defense Foreign Liaison/IE-3, 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 and Services.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

APEX	Adaptive Planning and Execution
BIA	behavioral influences analysis
C2	command and control
CAP	crisis action planning
CCDR	combatant commander
CI	counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
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	operation plan in concept format
DISO	deception in support of operations security
DOD	Department of Defense
DPC	deception planning cell
EA	electronic attack
EM	electromagnetic
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
FISS	foreign intelligence and security services
HFA	human factors analysis
IA	information assurance
IC	intelligence community
IO	information operations
IS	information system
ISR	intelligence, surveillance, and reconnaissance
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
JP	joint publication
JTF	joint task force
LNO	liaison officer
LOAC	law of armed conflict
MILDEC	military deception
MISO	military information support operations
MOE	measure of effectiveness
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSD/DMDPO	Office of the Secretary of Defense, Defense Military Deception Program Office
PA	public affairs
PIR	priority intelligence requirement
RFI	request for information
ROE	rules of engagement
SIGINT	signals intelligence
SJA	staff judge advocate
TAC-D	tactical deception
USSOCOM	United States Special Operations Command
VEO	violent extremist organization

PART II—TERMS AND DEFINITIONS

conduits. Within military deception, conduits are information or intelligence gateways to the deception target. Examples of conduits include: foreign intelligence and security services, intelligence collection platforms, open-source intelligence, news media—foreign and domestic. (Approved for inclusion in JP 1-02.)

counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (JP 1-02. SOURCE: JP 3-13.4)

deception. None. (Approved for removal from JP 1-02.)

deception action. A collection of related deception events that form a major component of a deception operation. (JP 1-02. 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. (JP 1-02. SOURCE: JP 3-13.4)

deception course of action. None. (Approved for removal from JP 1-02.)

deception event. A deception means executed at a specific time and location in support of a deception operation. (JP 1-02. SOURCE: JP 3-13.4)

deception means. Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. **physical means.** Activities and resources used to convey or deny selected information to a foreign power. b. **technical means.** Military material resources and their associated operating techniques used to convey or deny selected information to a foreign power. c. **administrative means.** Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02. SOURCE: JP 3-13.4)

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. (JP 1-02. 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. (JP 1-02. SOURCE: JP 3-13.4)

deception target. The adversary decision maker with the authority to make the decision that will achieve the deception objective. (JP 1-02. SOURCE: JP 3-13.4)

decoy. An imitation in any sense of a person, object, or phenomenon which is intended to deceive enemy surveillance devices or mislead enemy evaluation. Also called **dummy.** (Approved for incorporation into JP 1-02 with JP 3-13.4 as the source JP.)

demonstration. 1. An attack or show of force on a front where a decision is not sought, made with the aim of deceiving the enemy. 2. In military deception, a show of force in an area where a decision is not sought that is made to deceive an adversary. It is similar to a feint but no actual contact with the adversary is intended. (JP 1-02. SOURCE: JP 3-13.4)

desired perception. In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (JP 1-02. 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. (JP 1-02. SOURCE: JP 3-13.4)

diversionary landing. None. (Approved for removal from JP 1-02.)

dummy. See decoy. (Approved for incorporation into JP 1-02 with JP 3-13.4 as the source JP.)

electromagnetic deception. None. (Approved for removal from JP 1-02.)

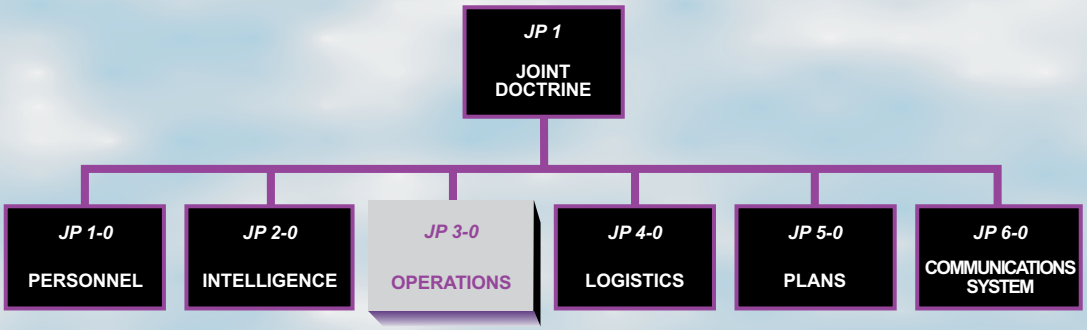
feint. In military deception, an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. (JP 1-02. SOURCE: JP 3-13.4)

honey pot. A trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers. (Approved for inclusion in JP 1-02.)

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.** (Approved for incorporation into JP 1-02.)

ruse. In military deception, a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. (JP 1-02. SOURCE: JP 3-13.4)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



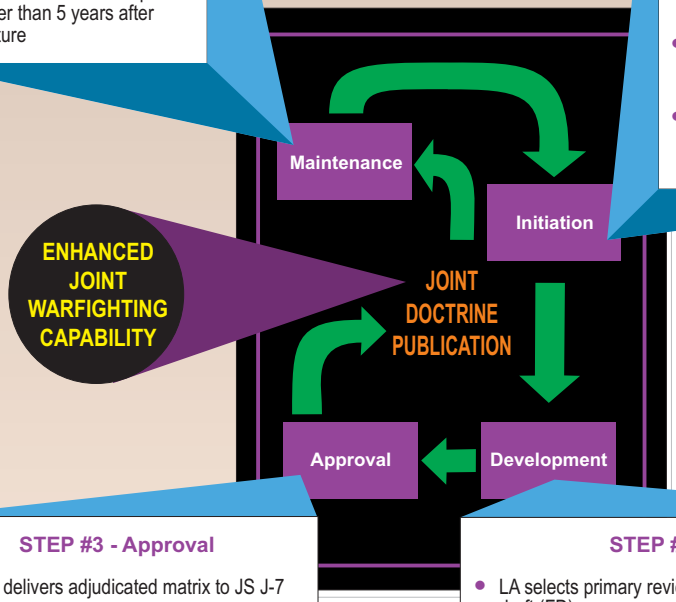
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-13.4** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

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


JOINT
CHIEFS OF STAFF