# FM 3-13.4

## Army Support to Military Deception




**FEBRUARY 2019**

**DISTRIBUTION RESTRICTION:**
Approved for public release; distribution is unlimited.

**HEADQUARTERS, DEPARTMENT OF THE ARMY**

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil/) and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

Field Manual
No. 3-13.4

Headquarters
Department of the Army
Washington, DC, 26 February 2019

# ARMY SUPPORT TO MILITARY DECEPTION

## Contents

Page

**PREFACE** ..... **iii**

**INTRODUCTION** ..... **v**

**Chapter 1 FUNDAMENTALS** ..... **1-1**
Overview of Army Military Deception Planning ..... 1-1
Functions of Military Deception ..... 1-1
Categories of Deception ..... 1-1
Key Terms of Military Deception ..... 1-3
Principles of Deception ..... 1-5
Types of Military Deception ..... 1-6
Tactics ..... 1-7
Techniques ..... 1-8
Deception Maxims ..... 1-8
Deception Means ..... 1-11
Information Quality ..... 1-13
Roles and Responsibilities ..... 1-13

**Chapter 2 PLANNING** ..... **2-1**
Preplanning ..... 2-1
The Army Tactical Deception Planning Process ..... 2-4
Deception Plan Approval ..... 2-14
Intelligence Support to Deception Planning ..... 2-14
Legal Considerations ..... 2-17
Operations Security and Deception ..... 2-19
Military Deception as an Information-Related Capability ..... 2-20
Integration with Other Information-Related Capabilities ..... 2-21
Coordination Requirements ..... 2-23
Risk Assessment ..... 2-23

**Chapter 3 PREPARATION AND EXECUTION** ..... **3-1**
Preparation ..... 3-1
Execution ..... 3-1
Managing the Execution of the Deception Plan ..... 3-3
Terminating Military Deception Operations ..... 3-5

**Chapter 4 ASSESSMENT** ..... **4-1**
Assessment Responsibilities ..... 4-1
Assessment Plan ..... 4-2
Measures of Effectiveness and Measures of Performance Development ..... 4-2

**Appendix A COUNTERDECEPTION** ..... **A-1**

**DISTRIBUTION RESTRICTION**: Approved for public release; distribution is unlimited.

**Appendix B** **INPUT TO OPERATION PLANS AND ORDERS** ..... **B-1**
**Appendix C** **DECEPTION EVALUATION CHECKLIST** ..... **C-1**
**SOURCE NOTES** ..... **Source Notes-1**
**GLOSSARY** ..... **Glossary-1**
**REFERENCES** ..... **References-1**
**INDEX** ..... **Index-1**

# Figures

Figure 2-1. Planning steps ..... 2-12
Figure 3-1. Monitoring activities ..... 3-4
Figure B-1. Sample Appendix 14 (Military Deception) to Annex C (Operations) ..... B-1

# Tables

Table 1-1. Deception differences ..... 1-2
Table 1-2. Sample deception techniques ..... 1-8
Table 2-1. The Army tactical deception planning process in the military decisionmaking process 2-4
Table 2-2. Sample terminations ..... 2-14

# Preface

This field manual aims to provide techniques to assist planners in planning, coordinating, executing, synchronizing, and assessing military deception (MILDEC). While the means and techniques may evolve over generations, the principles and fundamentals of deception planning remain constant.

FM 3-13.4 applies to all members of the Army profession: leaders, Soldiers, Army Civilians, and contractors. The principal audience for this publication is Army commanders, staffs, and all leaders. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should refer to applicable joint or multinational doctrine concerning joint or multinational planning. Trainers and educators throughout the Army also use this publication as a guide for teaching MILDEC.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 27-10.)

FM 3-13.4 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text, the term is italicized, and the number of the proponent publication follows the definition.

FM 3-13.4 applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the United States Army Reserve unless otherwise stated.

The proponent for this publication is the United States Army Information Operations Proponent (USAIOP) Office. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send written comments and recommendations on a Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCD (FM 3-13.4), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by email to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

# Introduction

When properly resourced and integrated, deception has the potential to deter or induce actions that are favorable to the force and can increase the success of friendly activity. In the same way that operations transition from one phase to the next, deception plans integrated into each phase and through each transition will strengthen the ability of commanders to retain initiative throughout the operation. Successfully planned deceptions give commanders the ability to act faster than the enemy can make decisions, creating positions of relative advantage.

Deception, as part of a broader strategy, is present in military case studies. While deception has its roots in the earliest military strategies, the modern day practical study of deception relies largely on case studies from World War I to present day. The availability of actual participants for interviews combined with detailed after action review reporting provides an in-depth understanding of deception tactics and techniques.

Deception can play a pivotal role in achieving the commander's objectives and significantly reduce risk. Deception can conceal, protect, reinforce, amplify, minimize, distort, or otherwise misrepresent friendly technical and operational capabilities, intentions, operations, and associated activities. Deception can be a critical enabler to achieving operational surprise and maintaining the initiative during large-scale combat operations in highly contested, lethal environments.

This publication is the proponent for the new Army term, *tactical deception*.

This page intentionally left blank.

# Chapter 1
# Fundamentals

## OVERVIEW OF ARMY MILITARY DECEPTION PLANNING

1-1. *Military deception* 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 (JP 3-13.4). Deception applies to all levels of warfare, across the range of military operations, and is conducted during all phases of military operations. When properly integrated with operations security (OPSEC) and other information-related capabilities (IRCs), deception can be a decisive tool in altering how the enemy views, analyzes, decides, and acts in response to friendly military operations.

1-2. Deception is a commander-driven activity that seeks to establish conditions favorable for the commander to achieve objectives. It is both a process and a capability. As a process, deception employs an analytic method to systematically, deliberately, and cognitively target individual decision makers. The objective is to elicit specific action (or inaction) from the enemy. As a capability, deception is useful to a commander when integrated early in the planning process as a component of an operation focused on causing an enemy to act or react in a desired manner. Deception greatly enhances the element of surprise. Deception aligns with surprise and the displacement of critical threat capabilities away from the friendly point of action. Due to the potentially sensitive nature of deception activities and selected means, planners must implement appropriate security and classification measures to properly safeguard deception tactics, techniques, and procedures.

## FUNCTIONS OF MILITARY DECEPTION

1-3. Planners must have a thorough understanding of the functions and the scope of what deception can and cannot accomplish. A deception plan serves as a part of the overall mission. Every deception plan must clearly indicate how it supports the commander's objectives. The functions of deception include, but are not limited to—

- Causing delay and surprise through ambiguity, confusion, or misunderstanding.
- Causing the enemy to misallocate personnel, fiscal, and materiel resources.
- Causing the enemy to reveal strengths, weaknesses, dispositions, and intentions.
- Causing the enemy to waste combat power and resources with inappropriate or delayed actions.

## CATEGORIES OF DECEPTION

1-4. Deception activities support objectives detailed in concept plans, operation plans (OPLANs), and operation orders (OPORDs) associated with approved military operations or activities. Deception applies during any phase of military operations to establish conditions to accomplish the commander's intent. The Army echelon that plans a deception activity often determines its type. The levels of war define and clarify the relationship between strategic and tactical actions. The levels have no finite limits or boundaries. They correlate to specific authorities, levels of responsibility, and planning. The levels help organize thought and approaches to a problem. Decisions at one level always affect other levels. Table 1-1 shows the three types of deception.

**Table 1-1. Deception differences**

| | *Military deception* | *Tactical deception* | *Deception in support of operations security* |
|---|---|---|---|
| ***Focus*** | Influence the action or inaction of enemy decision makers | Gain a tactical advantage over an enemy | Make friendly force intentions harder to interpret |
| ***Level*** | Strategic or operational | Tactical | Any |
| ***Support to*** | Military campaigns and major operations | Army commanders | All in support of an approved operations security plan |
| ***Headquarters*** | Combatant command and joint task forces | Joint task forces, Army Service component command, division, and below | All |
| ***Approval from*** | In accordance with CJCSI 3211.01 or DODI 3604.01 | Two levels higher (as per combatant command instruction) | Two levels higher (as per combatant command instruction) |
| ***Target*** | Adversary or enemy | Enemy | Foreign intelligence entity |

CJCSI Chairman of the Joint Chiefs of Staff instruction
DODI Department of Defense instruction

## MILITARY DECEPTION

1-5. Military deception (MILDEC) is planned, trained, and conducted to support military campaigns and major operations. MILDEC activities are planned and executed to cause adversaries to take actions or inactions that are favorable to the commander's objectives. The majority of MILDEC planned for and executed by the combatant command (CCMD) to create operational-level effects. MILDEC is normally planned before, and conducted during, combat operations. CCMD instructions add guidelines, policies, and processes that must be adhered to in their respective commands. MILDEC is a joint activity to which the Army, as the primary joint land component, contributes. Army forces do not unilaterally conduct MILDEC. MILDEC must adhere to the regulatory requirements found in Army policy and regulations, CJCSI 3211.01 series, and applicable CCMD instructions.

## TACTICAL DECEPTION

1-6. ***Tactical deception*** **is an activity planned and executed by, and in support of, tactical-level commanders to cause enemy decision makers to take actions or inactions prejudicial to themselves and favorable to the achievement of tactical commanders' objectives**. Commanders conduct tactical deception (TAC-D) to influence military operations to gain a relative, tactical advantage over the enemy, obscure vulnerabilities in friendly forces, and enhance the defensive capabilities of friendly forces. In general, TAC-D is a related subset of deception that is not subject to the full set of MILDEC program requirements and authorities. In most circumstances, Army commanders can employ TAC-D unilaterally if certain criteria are met. In description, TAC-D differs from MILDEC in four key ways:

- MILDEC is centrally planned and controlled through CCMD-derived authorities, but TAC-D is not. TAC-D can be employed unilaterally by tactical commanders with an approved plan.
- TAC-D actions are tailored to tactical requirements of the local commander and not always linked or subordinate to a greater MILDEC plan.
- The TAC-D approval process differs from the MILDEC approval process in that it is only required to be approved at two echelons higher, provided that it adheres to the joint policy for MILDEC addressed in CJCSI 3211.01. CCMD instructions add guidelines, policies, and processes that must be adhered to in their respective commands.
- Planning for TAC-D is usually more abbreviated, but still focuses on influencing the action or inaction of enemy decision makers, to gain a tactical advantage over an enemy. TAC-D gains this relative advantage using deception activities that affect the enemy's perceptions of friendly activities and possibly targeting lower-echelon enemy combatants to affect their operations.

### DECEPTION IN SUPPORT OF OPERATIONS SECURITY

1-7. Deception in support of operations security (DISO) is a deception activity that conveys or denies selected information or signatures to a foreign intelligence entity (FIE) and limits the FIE's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets. The intent of DISO is to create multiple false, confusing, or misleading indicators to make friendly force intentions harder to interpret by FIE. DISO makes it difficult for FIEs to identify or accurately derive the critical information and indicators protected by OPSEC. Deception and OPSEC are mutually supporting activities. DISO prevents potential enemies from accurately profiling friendly activities that would provide an indication of a specific course of action (COA) or operational activity. DISO differs from joint MILDEC and TAC-D plans in that it only targets FIEs and is not focused on generating a specific enemy action or inaction. Because a DISO does not target a specific enemy decision maker, the DISO approval process differs from the MILDEC approval process. A DISO can be approved at two levels higher, provided that it adheres to the joint policy for MILDEC in CJCSI 3211.01 series and is developed in support of an approved OPSEC plan. CCMD instructions add guidelines, policies, and processes that must be adhered to in their respective commands.

## KEY TERMS OF MILITARY DECEPTION

1-8. Military deception officers (MDOs) must have a comprehensive understanding of deception terms and definitions. Deception refers to those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. The following are terms and definitions associated with deception that deception will use throughout the planning process—

- Deception goal.
- Deception objective.
- Deception target.
- Desired perceptions.
- Conduits.
- Indicator.
- Filter.
- Node.
- Link.
- Deception event.
- Observable.
- Competing observable.
- Patterns.
- Deception story.

1-9. The *deception goal* is the commander's statement of the purpose of military deception as it contributes to the successful accomplishment of the assigned mission (JP 3-13.4). It is always written from the perspective of the friendly force commander. In initial planning guidance, a deception goal may be general in nature, requiring refinement during the development of the deception estimate. The deception goal is usually stated as a positive friendly advantage or condition such as: "Deception will create a decisive combat power advantage for the coalition main effort attack along AXIS MONTANA." Like any other form of military operation, the measure of success for deception is its direct contribution to the accomplishment of the mission. Deception plans often require investments in effort and resources that would otherwise be applied against the enemy 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. Some additional examples include—

- "I want to use deception to improve the friendly force advantage."
- "I want to use deception to increase freedom of maneuver."

1-10. The *deception objective* is 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 3-13.4). It is the action or inaction that directly leads to the advantage or condition stated in the deception goal. For example, "Cause the enemy to hold its armored reserve in a position or status unable to impact friendly forces along AXIS MONTANA through H+36 hours."

1-11. The *deception target* is the adversary decision maker with the authority to make the decision that will achieve the deception objective (JP 3-13.4). The target thus directs the action or inaction of the military capability described in the deception objective. The deception target or target set is key individuals on whom planners focus the deception plan. Understanding the target's process for receiving and processing information, assessing a situation, and deciding a COA is critical to a successful deception plan. For more information on deception targets, see chapter 2.

1-12. In military deception, *desired perception* is what the deception target must believe for it to make the decision that will achieve the deception objective (JP 3-13.4). They are personal conclusions, official estimates, and assumptions that the deception target must believe in order to make the decision that will achieve the deception objective. These enemy perceptions will form from both objective (observation and analysis) and subjective (intuition and experience) analysis. They are also heavily impacted by biases, preconceptions, predispositions, and filters applied in the collection, analysis, delivery, and reception of information.

1-13. Within military deception, *conduits* are information or intelligence gateways to the deception target, such as foreign intelligence entities, intelligence collection platforms, open-source intelligence, and foreign and domestic news media (JP 3-13.4). They are the pathways to the deception target. Collectively, they define how the enemy will observe activity in the information environment and how those observations are transmitted, processed, and ultimately delivered to the decision maker. For more discussion on conduits and conduit analysis, see discussion beginning in paragraph 2-33.

1-14. In operations security usage, an *indicator* is data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities (JP 3-13.3).

1-15. A filter is any node within a conduit that aggregates, synthesizes, or applies bias information on its path to the deception target. A *node* is an element of a system that represents a person, place, or physical thing (JP 3-0). Planners understand that filters make every conduit unique, affecting the way information is transmitted through them. To create the most effective portrayal of the deception story, planners assess each conduit and the filters involved, ensure redundancy with other conduits, and appreciate the relative value of each conduit as perceived by the target.

1-16. A *link* is a behavioral, physical, or functional relationship between nodes (JP 3-0). The key link between selected indicators and the deception story is the tentative identification of one or more enemy conduits to which the plan exposes the indicator. Observable activities and the threat conduits combine to produce indicators that can be seen or perceived to aid in collection and decision-making processes. Unless exposed to one or more active conduits, an indicator is ineffective in conveying the observable or indicator: the enemy cannot register or respond to what it cannot see. Executions are the tasks or activities that the friendly unit conducts to put an observable into action.

1-17. A *deception event* is a deception means executed at a specific time and location in support of a deception operation (JP 3-13.4). A deception event aims to portray an observable that contributes to desired perceptions in the deception target.

1-18. In military deception, an *observable* is the detectable result of the combination of an indicator within an adversary's conduit intended to cause action or inaction by the deception target (JP 3-13.4). Observables are often made up of executions, which can include events, activities, or elements of information that must be seen or sensed by the target to form the desired perceptions. Observables may gain credibility through the use of supporting observables. To enhance the probability that the target will receive or accept one or more of the required observables.

1-19. MDOs may need to develop supporting observables. Supporting observables enhance the deception story and help create a believable context for the required observables. Planners identify all the activities

normally associated with a specific activity or event (the required observable). From those activities, the planner analyzes which of those associated activities the target would normally collect against and use as a significant indicator of usual or consistent friendly behavior. The activities must be fully compatible with all elements of the deception story and carefully sequenced with other observables to have their desired effects.

1-20. Within military deception, a *competing observable* is any observable that contradicts the deception story, casts doubt on, or diminishes the impact of one or more required or supporting observables (JP 3-13.4). To minimize the impact of competing observables on enemy analysis, they must be mitigated as part of the deception plan. Examples of mitigation for competing observables include protection with OPSEC, including DISO; neutralization of the enemy conduit to which competing observables are likely to be exposed; or assumption of risk based on detailed analysis of minimal impact to the operation. The availability of resources and time are often limiting factors in preparing such supporting measures, but they can be extremely valuable in raising the credibility and verifiability of the deception story and the probability of deception success.

1-21. Patterns are multiple-repetitive indicators that give the enemy an operational profile. Enemies use their intelligence collection assets to analyze patterns to identify the unit and predict its mission. Changes in pattern can affect how an enemy perceives friendly actions.

1-22. 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 (JP 3-13.4). It is a succinct statement or narrative of exactly what the MDO wants the target to believe to be the true situation, then decide and act on that basis. It is usually made up of the deception observables and the deception desired perceptions in a specific sequence to create deception events. MDOs write the deception story from the perspective of the enemy so it reads like the enemy's intelligence estimate about friendly forces' actions and intentions.

# PRINCIPLES OF DECEPTION

1-23. Just as the principles of war provide general guidance for the conduct of military operations, the six principles of deception provide guidance to plan deception. The principles of deception are—

- Focus.
- Objective.
- Centralized planning and control.
- Security.
- Timing.
- Integration.

## FOCUS

1-24. The deception plan should focus on the thought process of the threat decision maker who has the authority and capability of causing the desired actions. The enemy's intelligence, surveillance, and reconnaissance is normally not the target; rather, it is a primary conduit used in the deception plan to convey selected information to the decision maker. Planners must clearly understand the difference between intermediate conduits and the intended target. Focused deception must cause an action or inaction of the enemy force. In order to do this, there must be existing conduits to the deception target or a reasonable expectation that conduits can establish.

## OBJECTIVE

1-25. Deception plans focus actions and resources that motivate an enemy to decide to take (or not to take) specific desired actions. The plan cannot focus solely on motivating the target to believe certain things; it must lead to the target making a specific decision to act or not act.

## CENTRALIZED PLANNING AND CONTROL

1-26. A centralized approach is necessary to avoid confusion and to ensure various elements portray the same story and do not conflict with other operational objectives or evolving conditions in an operational environment. Execution of the deception may, however, be decentralized as long as all participating

organizations adhere to a single plan. Once the commander approves the deception plan, the designated operational element monitors the situation and its effects on the target, as well as friendly and partnered forces. The MDO, working with the deception working group (DWG), ensures synchronization, deconfliction, and OPSEC.

### SECURITY

1-27. Successful deception requires strict security that begins before execution with measures to deny the enemy knowledge of the friendly force's intent to deceive. Successful planners apply strict need to know criteria to each aspect of the deception plan. Maintaining the security of the deception means limiting the number of informed planners and participants to those needed. The MDO must develop and maintain access rosters and other security controls to limit exposure of operational deception activities.

### TIMING

1-28. The most critical aspects of deception planning are beginning proper synchronization with the commander's intent and maintaining synchronization during execution. Timing in deception operations is crucial. The challenge is to get the deception target to act in accordance with the deception objective within the timelines required by the friendly operation. Planners must conduct a thorough conduit analysis to understand the amount of time required for an observable to pass through filters and nodes before reaching an enemy decision maker. This means that friendly deception executions must be completed in a manner that accounts for the time consumed by the enemy's intelligence collection and analysis process, the enemy's decision-making process, and the enemy's activity that is to be exploited by friendly forces. Timing must be synchronous among friendly deception actions taken, the assimilation and reaction processes of the enemy, and dependent friendly operations.

### INTEGRATION

1-29. Deception is an integral part of an operation that planners must integrate, at all levels, throughout the planning process. This integration includes developing a concept for deception that supports the overall mission as part of COA development. Planners must also integrate deception plans with higher headquarters plans. Deceptions must be consistent with Army doctrinal norms. The MDO assists the staff in integrating the deception operation throughout all phases of the operation. This begins with planning, continues through execution, and concludes with the termination of the deception.

## TYPES OF MILITARY DECEPTION

1-30. Any deception aims to either increase or decrease the level of uncertainty, or ambiguity, in the mind of the deception target. This ambiguity has the potential to compel the target to mistakenly perceive friendly motives, intentions, capabilities, and vulnerabilities thereby altering the target's assessment. Two generally recognized types of MILDEC exist:

- Ambiguity-increasing.
- Ambiguity-decreasing.

### AMBIGUITY-INCREASING DECEPTION

1-31. Ambiguity-increasing deception provides the enemy with multiple plausible friendly COAs. Ambiguity-increasing deception is designed to generate confusion and cause mental conflict in the enemy decision maker. Anticipated effects of ambiguity-increasing deception can include a delay to making a specific decision, operational paralysis, or the distribution of enemy forces to locations far away from the intended location of the friendly efforts. Ambiguity-increasing deception is often directed against decision makers known to be indecisive or risk-adverse.

1-32. These deceptions draw attention from one set of activities to another. They can create the illusion of strength where weakness exists, or create the illusion of weakness where strength exists. They can also acclimate the enemy to particular patterns of activity that are exploitable later. For example, ambiguity-increasing deceptions can cause the target to delay a decision until it is too late to prevent friendly mission

success. They can place the target in a dilemma for which no acceptable solution exists. They may even prevent the target from taking any action at all. This type of deception is typically successful with an indecisive decision maker who is known to avoid risk.

### AMBIGUITY-DECREASING DECEPTION

1-33. Ambiguity-decreasing deceptions manipulate and exploit an enemy decision maker's pre-existing beliefs and bias through the intentional display of observables that reinforce and convince that decision maker that such pre-held beliefs are true. Ambiguity-decreasing deceptions cause the enemy decision maker to be especially certain and very wrong. Ambiguity-decreasing deceptions aim to direct the enemy to be at the wrong place, at the wrong time, with the wrong equipment, and with fewer capabilities. Ambiguity-decreasing deceptions are more challenging to plan because they require comprehensive information on the enemy's processes and intelligence systems. Planners often have success using these deceptions with strong-minded decision makers who are willing to accept a higher level of risk.

## TACTICS

1-34. Deception tactics can be characterized as operational-level constructs that encompass a broad range of deceptive activity and information integrated as a component of the overall plan. Deception plans apply five basic tactics: diversions, feints, demonstrations, ruses, and displays. These tactics are often best employed in TAC-D to support the commander's objectives. The selection of tactics and their use depends on planners' understanding the current situation as well as the desired deception goal and objective.

### DIVERSION

1-35. A *diversion* is the act of drawing the attention and forces of an enemy from the point of the principal operation; an attack, alarm, or feint that diverts attention (JP 3-03). The goal of diversion is to induce the enemy to concentrate resources at a time and place that is advantageous to friendly objectives.

### FEINT

1-36. In military deception, 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 (JP 3-13.4). A feint is designed to lead the enemy into erroneous conclusions about friendly dispositions and concentrations. A series of feints can condition the enemy to react ineffectively to a future main attack in the same area.

### DEMONSTRATION

1-37. In military deception, a *demonstration* is a show of force similar to a feint without actual contact with the adversary, in an area where a decision is not sought that is made to deceive an adversary (JP 3-13.4). A demonstration's intent is to cause the enemy to select a COA favorable to friendly goals.

### RUSE

1-38. In military deception, a *ruse* is an action designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system (JP 3-13.4). A ruse deceives the enemy to obtain friendly advantage. A ruse in deception is normally an execution based on guile or trickery that contributes to the larger deception plan.

### DISPLAY

1-39. In military deception, a *display* is a static portrayal of an activity, force, or equipment intended to deceive the adversary's visual observation (JP 3-13.4). Displays include the simulation, disguise, or portrayal of friendly objects, units, or capabilities in the projection of the deception story. Such objects, units, or capabilities may not exist but are made to appear that they exist.

# TECHNIQUES

1-40. The application of techniques varies with each operation depending on time, assets, and objectives. Planners assess which techniques to apply based on feasibility, availability, and effectiveness. Table 1-2 provides sample deception techniques.

**Table 1-2. Sample deception techniques**

| *Technique* | *Deception created* |
|---|---|
| **Amplifying signatures** | To make a force appear larger and more capable or to simulate the deployment of critical capabilities. |
| **Suppressing signatures** | To make a force appear smaller and less capable or to conceal the deployment of critical capabilities. |
| **Overloading enemy sensors** | To confuse or corrupt their collection assets by providing multiple false indicators and displays. |
| **Repackaging known organizational or capability signatures** | To generate new or deceptive profiles that increase or decrease the ambiguity of friendly activity or intent. |
| **Conditioning the enemy** | To desensitize to particular patterns of friendly behavior and to induce enemy perceptions that are exploitable at the time of friendly choosing. |
| **Reinforcing the impression** | To mislead by portraying one course of action when actually taking a different course of action. |
| **Conditioning the target by repetition** | To believe that an apparently standard routine will be pursued, whilst in fact preparing a quite different course of action. |
| **Leading the enemy by substitution** | To believe that nothing has changed by covertly substituting the false for the real, and vice versa. |
| **Leading the enemy by mistake** | To believe that valuable information has come into their possession through a breach of security, negligence, or inefficiency. |

# DECEPTION MAXIMS

1-41. The military derives deception maxims from game theory, historical evidence, social science, and decision analysis theory. These maxims are offered to enhance the deception concepts provided in this publication. They provide additional insight that commanders and their staffs can use to develop their plans.

***Note.*** These deception maxims originated in *Deception Maxims: Fact and Folklore*. See the Source Notes.

## MAGRUDER'S PRINCIPLE

1-42. Magruder's principle states that it is generally easier to induce the deception target to maintain a pre-existing belief than to deceive the deception target for the purpose of changing that belief. Magruder's principle exploits target biases and the human tendency to confirm exiting beliefs. Magruder's principle alludes to two paths. A path of the deceiver changing the belief of a target and a path of maintaining a present belief. The principle then advises the better of the two paths. Magruder's principle is named for Major General John Magruder. During the Civil War, he was tasked with impeding Major General George McClellan's advance on Richmond with a numerically superior force. Magruder deceived McClellan by encouraging McClellan's belief that he faced a larger enemy than he actually faced. In using Magruder's principle, MDOs provide the targeted decision makers with information that reinforces their expectations for what they believe to be true. This reinforces the target's pre-existing perceptions. Any bias is potentially exploitable. Most targets are unaware of how deeply their biases influence their perceptions and decisions. Most people resist letting go of existing opinions and tend to seek information that reinforces their own bias.

1-43. An example of this principle occurred with the selection of the invasion site and its cover plan for the D-Day invasion of France. Using reconnaissance and communications intercepts, the Allies learned that Hitler and his senior military advisors believed that the most likely place for the Allied invasion would be in the Pas de Calais region. This was a viable plan as it provided better air cover and a shorter transit time from England; in fact, it was a reverse of their plan to invade England in 1940. The Allies were able to exploit and reinforce the enemy's expectations to the extent that the Germans had a difficult time reacting to the actual landings in Normandy.

## LIMITATIONS TO HUMAN INFORMATION PROCESSING

1-44. The human brain can only process so much information and only so fast; it is susceptible to inherent limitations or tricks of the mind. There are two primary exploitable limitations to human information processing: the law of small numbers and the susceptibility to conditioning. The law of small numbers is the tendency to generalize from a small sample set. Exploiting this law means that it does not necessarily take many observables for the target to draw a conclusion. Susceptibility to conditioning is the repeated presentation of stimuli to elicit a specific response from the target. In deception, it is the frequent inability of deception targets to detect small changes in friendly force indicators, even if the cumulative change over time is large.

1-45. An example of this principle was the breakout of the German ships Scharnhorst, Gneisenau, and Prinz Eugen from Brest on February 12, 1942. The Germans facilitated the breakout by jamming British radars. Ordinarily this would have been a significant tip-off that something was amiss, but British radar operators dismissed it as being caused by atmospheric disturbance. This error was the result of a carefully orchestrated German ruse directed by General Wolfgang Martini, the head of the Luftwaffe Signals Service. The Germans jammed the British radar sites every day at the same time to build the British radar operators' belief that the atmosphere was interrupting the receipt of any signals. The British became so accustomed to the so-called atmospheric problems that the ships were able to escape.

## MULTIPLE FORMS OF SURPRISE

1-46. A strong correlation exists between deception and surprise. The more forms of surprise built into the deception plan, the more likely it will overwhelm the target. These forms of surprise include size, activity, location, unit, time, equipment, intent, and style. One effect of surprise is the cry-wolf syndrome in which repeated false alarms have the potential to desensitize an enemy. A pattern of behavior lulls an opponent into a sense of normal behavior to allow a friendly action to occur without an immediate counteraction.

1-47. An example occurred when Egypt successfully deceived Israel into a false sense of security in 1973 by mobilizing reservists twenty-three times before actually acting. Many times over one year, the same source provided information that the war would break out on a specific date. Each time, that day would come and go without an attack. This happened so often that when the source actually provided the date of the real attack, no one believed him.

## JONES' DILEMMA

1-48. This principle is named after Reginald Victor Jones, a British professor heavily involved in solving science and technology intelligence challenges. In this deception, the target receives information through multiple means and methods, from many angles, throughout an operational environment. Deception generally becomes more difficult as the number of conduits available to the deception target to confirm the real situation increases. However, the greater the number of conduits that are deceptively manipulated, the greater the chance the target will believe the deception. Planners must balance the need to disrupt or deny enemy capabilities with the need to preserve select deception conduits to the enemy decision maker.

## CARE IN THE DESIGN OF PLANNED PLACEMENT OF DECEPTIVE MATERIAL

1-49. Windfalls (unexpected gains) of information or plans are usually second-guessed, and the target or the target's intelligence assets usually doubt the authenticity of any windfall if it comes too easily. The target will likely view deceptive materials or information as credible if it uncovers the information in a seemingly

natural manner. The harder the target has to work to acquire it, the more likely the target will believe it as credible.

1-50. Important military information that is too easy to obtain is usually suspect. Information that falls into the enemy's hands must appear to be the result of legitimate collection activities. People naturally tend to believe information earned more than information given. An example of this technique could be feeding mission information to the enemy through a trusted source instead of making the information general knowledge.

1-51. A common characteristic of successful deceptions is that they were designed to co-opt skepticism by requiring the target to participate either by physically obtaining the evidence or analytically by interpreting it. However, if the deception is too subtle, it risks that the target will fail to perceive the deception story at all.

1-52. An example of this principle is from early in World War II, when a German aircraft heading for Cologne became lost and made a forced landing near Malines in Belgium. Belgian authorities soon arrested the three passengers, two Wehrmacht officers and a Luftwaffe major. They were taken to the police station and left alone briefly. They attempted to burn some documents they were carrying. They were top secret documents containing attack plans for Holland and Belgium. However, the documents failed to burn and fell into the hands of Belgian authorities. The authorities believed that the documents were a part of a deception plan because the Germans could not be careless enough to allow actual war plans to fall into the hands of the Allies. This example shows a misclassification error in which a real windfall was dismissed as false because it was too easy to obtain.

## LEVERAGE THE TRUTH

1-53. In this instance, truth means reality based on facts or precedence. As a rule, the deception should not portray a reality that would come as a surprise to the target. A deception that conforms to proven or predictable patterns of behavior is more likely to succeed than a deception that violates these norms. Because the target has access to Army doctrine and probably understands how the Army operates (to include its core values), the target will see deceptions as false if they fail to align with foundational Army tenets or historical patterns of behavior. In this instance, the deception will fail. Planners can provide meaning to actual events, activities, and operations that support the deception plan.

## MINIMIZE FALSEHOOD

1-54. The less the deception relies on false information, the greater the chance of success. Although deception, by its nature, implies the use of false information to shape the target's perceptions, each portrayal of falsehood increases the risk of failure by increasing susceptibility to competing observables. This deception principle resembles the principle of economy of force—use only the amount of false information needed to produce the desired perceptions. Any falsehoods should be supported by elements of truth. This way the target discovers that, everywhere it turns, it finds verifiable information that makes any questionable part of the deception more believable.

## HUSBANDING OF DECEPTION ASSETS

1-55. This maxim suggests that it may be wise to withhold the employment of deception capabilities until the stakes and the benefits are high. Put another way, a planner conserves deception assets and activities until forces can employ them to achieve the greatest impact at the most opportune time. This principle considers that employment of an asset will cause it to become valueless after it has been used once.

1-56. An example of holding deception assets in reserve until the right moment involves the use of double agents by Britain in connection with the Normandy deception in World War II. The British had captured all known German agents operating in Britain and decided to use them against Germany. While Britain was certain that it was in control of the German's espionage system, it waited to use the agents against Germany until the Normandy invasion.

### SEQUENCING RULE

1-57. Planners must sequence deception activities and maintain them for as long as possible to maximize the deception story. OPSEC measures can help planners mask unit observables that would otherwise reveal the unit's mission and intent until the last possible instant. To be effective, deception and OPSEC activities must be sequenced and coordinated in both time and space, and in conjunction with adjacent or pre-existing operations.

### IMPORTANCE OF FEEDBACK

1-58. Planners must develop indicators that will determine the success or failure of the deception. An assessment plan uses measures of effectiveness (MOEs) to determine if the enemy has adopted, rejected, or countered the deception plan. Assessing MOEs gives the commander the necessary feedback to continue, adjust, or terminate a deception plan. When developing the deception plan, planners should build associated MOEs for key events.

1-59. An example of the importance of feedback happened during World War II. The British developed a top-secret cryptographic tool called ULTRA that enabled the British to read German codes. The information that ULTRA provided to the Allies was a critical element to the success of the Allied invasion of Normandy. The Allies knew through ULTRA that the German troops remained in Norway and concluded through feedback that the deception was successful.

### BEWARE OF POSSIBLE UNWANTED REACTIONS

1-60. Deceptions may produce unintended, often unwanted consequences. Believing that a threat is real, an enemy can act unpredictably. Proper planning and coordination and knowing the enemy can reduce the chance that deceptions will result in unfavorable action. Successful planners consider second- and third-order effects of the deception plan to mitigate unintended consequences. The risk inherent to a deception operation is measured by the losses that can result from its failure. The possibility of failure stems from the uncertainties surrounding how the target receives and interprets information intended for the target and, eventually, how it affects the target's desired perceptions. If discovered, resources used for the deception may be in jeopardy. As with any military operation that puts forces at risk, planners decide to use deception after a deliberate assessment that weighs opportunity against need and cost against benefit. The deception planner must advise the commander of the risk, benefit, and cost of the deception operation relative to both success and failure.

## DECEPTION MEANS

1-61. *Deception means* are methods, resources, and techniques that can be used to convey information to the deception target (JP 3-13.4). There are three basic categories of deception means: physical, technical, and administrative. An individual deception means may have multiple attributes that allow it to be characterized in more than one category. Planners normally employ deception means in complementary variety to mislead multiple types of enemy sensors to increase credibility and the likelihood of creating the desired perception. Means provide the signatures, associations, and profiles of friendly purported activities to the enemy. For additional deception means and the authorities to employ them, refer to CCMD instructions and request guidance from the CCMD.

### PHYSICAL MEANS

1-62. Physical means are resources, methods, and techniques used to convey or deny information or signatures normally derivable from direct observation or active sensors by the deception target. Most physical means also have technical signatures visible to sensors that collect scientifically or electronically. Planners typically evaluate physical means using characteristics such as shape, size, function, quantity, movement pattern, location, activity, and association with the surroundings. Examples might include—

- Movement of forces.
- Exercises and training activities.
- Decoy equipment and devices.
- Tactical actions.

- Visible test and evaluation activities.
- Reconnaissance and surveillance activities.

## TECHNICAL MEANS

1-63. Technical means are resources, methods, and techniques used to convey or deny selected information or signatures to or from the deception target. These means manipulate electromagnetic, acoustic, or other forms of energy or through olfaction. Technical means often use technical equipment.

1-64. Technical means may be applied with corresponding physical means or alone to replicate something physical that is absent from direct visual observation. As with any use of friendly military material resources, any use of technical means to conduct deception must comply with U.S. and international law. Planners integrate technical means with other technical activities of the operation. Examples of technical means might include—

- The establishment of communications networks and interactive transmissions that replicate a specific unit type, size, or activity.
- The emission or suppression of chemical or biological odors associated with a specific capability or activity.
- Multispectral simulators that replicate or mimic the known electronic profile of a specific capability or force.
- Selected capabilities that disrupt an enemy sensor or affect data transmission.

1-65. Electromagnetic deception is the deliberate change of electromagnetic energy intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons. The misinformation results in degrading or neutralizing the enemy's combat capability. Types of electromagnetic deception include manipulative, simulative, and imitative deception. Manipulative deception involves actions to eliminate revealing—or to convey misleading—electromagnetic telltale indicators that an enemy can use. Simulative deception involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces. Imitative deception introduces electromagnetic energy into enemy systems that imitate enemy emissions. For more information on electromagnetic deception, see FM 3-12. For more information on acoustic, other energy, or olfactory means, see ATP 3-53.1.

## ADMINISTRATIVE MEANS

1-66. Administrative means are resources, methods, and techniques to convey or deny selected written, oral, pictorial, or other documentary information or signatures to or from the deception target. They normally portray information and indicators associated with coordination for ongoing or planned military activity to the deception target. Examples of administrative means normally visible to an enemy at some level might include—

- Movement, transit, or overflight requests including flight planning, port call, or traffic control coordination.
- Basing inquiries or construction requests.
- Other preparatory coordination associated with a military operation normally done through unclassified channels.

## CAMOUFLAGE, CONCEALMENT, AND DECOYS

1-67. Camouflage and concealment are OPSEC measures and survivability operations tasks used to protect friendly forces and activities from enemy detection and attribution. Camouflage makes friendly capabilities or activities blend in with the surroundings. Concealment makes friendly capabilities or activities unobservable or unrecognizable to the enemy. Concealing the location, movement, and actions of friendly forces can delay hostile attack and assist commanders in retaining the tactical advantage. Both use physical, technical, and administrative means to deceive the enemy and protect the deception story. Deception measures use the same signatures for simulating friendly forces and activities.

1-68. A *decoy* is an imitation in any sense of a person, object, or phenomenon that is intended to deceive enemy surveillance devices or mislead enemy evaluation (JP 3-13.4). Decoys may be used in conjunction

with other deception activities to mislead enemy intelligence collection and direct the enemy's attention away from actual forces. Decoys must appear realistic to the enemy sensors to be effective. See ATP 3-37.34 for additional information on camouflage, concealment, and decoys.

# INFORMATION QUALITY

1-69. Information quality refers to the accuracy, completeness, relevance, and believability of information available for decision making. Deception should affect the quality of information available for enemy decisions in the following ways:

- Portray to the enemy true information that supports the deception story.
- Deliberately present misleading information and indicators to enemies to degrade the accuracy of enemy information.
- Give enemy decision makers a false sense of completeness of their understanding about friendly forces or intentions.
- Cause enemy forces to misjudge the relevance of available information and misallocate operational or intelligence resources.
- Cause enemies to doubt the veracity of their own intelligence assessments.

1-70. MDOs protect the quality of information available for friendly decisions and public dissemination by instituting internal processes to identify and isolate information generated as a by-product of any deception activity. This protection helps prevent the commander from reaching erroneous conclusions because the staff unknowingly integrated the content or output of the deception efforts as accurate information. This also ensures the information made public is not part of any deception plan that would result in a loss of public trust.

# ROLES AND RESPONSIBILITIES

1-71. Army commanders and their staffs have distinct and coordinating roles and responsibilities in deception. All planners must understand the roles and responsibilities of everyone involved with deception planning and execution and then tailor each planning team accordingly.

## COMMANDERS

1-72. The commander's role is critical in planning deception. The commander determines the utility of deception's contribution to achieving objectives. Commanders decide to develop a deception plan after evaluating the analysis and recommendations from the MDO. Commanders should guide applicable deception executions while understanding their potential importance during planning and execution. The commander has explicit and inherent responsibilities for the deception effort. The commander—

- Assesses higher headquarters' plans and orders for stated and implied deception tasks.
- Considers the ways deception can support every operation, mindful of deception maxims to gain maximum impact.
- States the tentative deception objective in the initial planning guidance.
- Approves the deception objective.
- Allocates necessary resources.
- When required, seeks appropriate approval to employ certain deception means.
- Determines when to exploit deception or counterdeception.

## G-2

1-73. The G-2 assists the commander by identifying deception objectives to complement operational objectives. With the commander leading the efforts, the G-2 identifies deception objectives that apply to operations, intelligence, and counterintelligence resources. The G-2—

- Analyzes the threat and the enemy's capability to process, filter, and evaluate intelligence on the friendly situation.
- Provides assessments on the threat's vulnerabilities to deception.
- Assesses threat targets, sensors, most dangerous and most likely COAs, acceptance of the deception story, and MOEs.
- Provides comprehensive assessments and continual feedback to the MDO in support of deception planning, execution, and deception termination.
- Supports counterdeception operations to protect friendly deception operations and to expose threat deception attempts.
- Responds to MDOs' requests for information (RFIs) concerning analysis data for behavioral influences or human factors for threat military, paramilitary, or violent extremist organizations.
- Helps to prevent reporting of unintentionally collected deception information to the commander as valid facts.

## G-3

1-74. The G-3 recommends the use of resources including those required for deception. For deception, the G-3—

- Recommends the deception objective, story, and plan to the commander.
- Coordinates the deception effort through the information operations cell.
- With the staff judge advocate, ensures that the deception effort is planned and conducted in accordance with the U.S. laws, rules of engagement, and the law of war.
- Supervises execution of the deception plan.
- Submits detailed and clear RFIs to the G-2 for information and intelligence that is key to deception planning, execution, and assessment.
- Provides feedback to the G-2 on intelligence products to include clarification or additional RFIs if needed.

### INFORMATION OPERATIONS OFFICER

1-75. The information operations (IO) officer is the staff officer responsible for the integration and synchronization of IRCs in support of the deception plan. These responsibilities include coordinating and deconflicting deception planning and integration into the scheme of IO (a clear, concise statement of where, when, and how the commander intends to employ and synchronize IRCs). The IO officer monitors the implementation and execution of the deception portion of IO. Since military deception is an IRC and fundamentally cognitive in nature, IO officers typically possess deception-related training and experience for effectively using TAC-D.

### MILITARY DECEPTION OFFICER

1-76. The MDO is responsible for coordinating military deception assets and operations. An MDO is authorized at corps and theater army levels as the command military deception officer (also known as CMDO). At division and lower echelons, the commander designates an MDO. Generally, the most suitable staff officer designated as the MDO is the IO officer because of experience and training. In the absence of a trained or experienced IO officer, the commander typically designates the individual trained in using Army IRCs to influence an enemy decision maker. MDOs ensure that staff classify plans in accordance with DODM 5200.01. The security classification guides establish parameters for planning, coordinating, and executing deception plans at appropriate levels.

1-77. MDO responsibilities include, but are not limited to—

- Providing programmatic oversight and compliance with security requirements.
- Developing Appendix 14 (Military Deception) to Annex C (Operations).
- Exercising staff supervision over deception activities.
- Maintaining program integrity through maintenance of strict OPSEC measures.

- Providing expertise in deception planning.
- Managing information required to develop deception plans and cultural analysis to determine the effects of ambiguity.
- Determining requirements or opportunities for deception operations (with the G-2) by red teaming the enemies' most probable COAs.
- Coordinating with other staff sections for support to the deception targets, deception objectives, and deception story.
- Ensuring themes, messages, and actions conveyed to the enemy decision maker enable the deception plan.
- Producing, distributing, briefing, and coordinating the deception plan on a need to know basis.
- Assessing the execution and effects of deception plans.
- Coordinating with unit operations planners to review and analyze plans for deception requirements.
- Understanding deception authorities and coordinating with designated officials at higher echelons to gain concept of operations approval.

### CYBERSPACE ELECTROMAGNETIC ACTIVITIES SECTION

1-78. The cyberspace electromagnetic activities (known as CEMA) section coordinates and synchronizes cyberspace and electronic warfare operations across staff elements from brigade to corps. The cyberspace electromagnetic activities section is key to the collaboration of cyberspace and electronic warfare operations to include the planning of electromagnetic deception.

## G-5

1-79. The G-5 has staff planning and supervisory responsibility for—

- Maintaining contingency plans and initiating crisis action planning efforts.
- Coordinating to ensure deception planning is included in OPLANs, concept plans, and campaign plans.
- Incorporating deception planning at the beginning of the planning process.

### DECEPTION WORKING GROUP

1-80. The MDO oversees all deception planning and execution. For successful deception integration, a deception planning team, appointed by the command, is formed. In most circumstances, the team then forms a DWG to facilitate the planning, coordination, integration, and assessment of deception. At a minimum, a DWG includes representatives from the G-2, G-3, the G-3 IO cell, G-5, and the OPSEC planner. The DWG often includes representatives from IRCs that are pertinent or relevant to the deception concept of operations being developed. The DWG plans, directs, monitors, and assesses deception plans. It may also provide planning, execution, and termination support for deception operations undertaken by higher command echelons in their operational area. Members of the DWG typically writes Appendix 14 (Military Deception) to Annex C (Operations) for the OPORD. Other responsibilities include—

- Interfacing and working closely with operational planners to review and analyze deception plan requirements.
- Responding to higher headquarters' deception tasking.
- Coordinating with higher headquarters on proposed deception efforts to solve potential conflicts.
- Providing resource requirements to higher headquarters for deception program development and sustainment.
- Looking for opportunities to implement deception in support of military objectives.

This page intentionally left blank.

# Chapter 2
# Planning

## PREPLANNING

2-1. The complexity and sensitivity of deception requires detailed planning that begins with preplanning. MDOs have three preplanning considerations: capability development, planning guidance, and mission analysis. A successful deception plan incorporates preplanning considerations as well as flexibility to lessen the risk of failure. When preplanning, MDOs create a baseline analysis, prepare deception planning guidance, and complete mission analysis.

### BASELINE ANALYSIS

2-2. Baseline analysis is preplanning that ensures the organization has the requisite staff, methods, and tools to plan deception. Baseline analysis entails acquiring basic information on available deception means. This includes information on friendly doctrine and tactics as well as technical characteristics of employed combat systems. It also includes basic data on friendly intelligence and counterintelligence resources and operations.

### DECEPTION PLANNING GUIDANCE

2-3. When preplanning, MDOs consider how to develop deception activities within the framework of the commander's intent and planned operations. They consider the commander's initial deception guidance that often arrives as a separate written or verbal deception-planning directive. Deception planning efforts must be synchronized and integrated with traditional unit planning efforts at all times. The importance of the relationship between the MDO and the G-5 cannot be overstated. Early in mission analysis, MDOs begin to determine a potential deception goal. Commanders verbalize the deception goal as specific contributions to mission accomplishment (see paragraph 1-9).

2-4. During mission analysis, planners identify potential deception objectives that enable forces to reach the deception goal. The deception objective is a concise statement of how the commander plans the enemy to act or not act (see paragraph 1-10). This objective provides the MDO with a clear aim. The objective is usually stated in a positive result, such as "deception will cause the enemy to delay commitment of reserve forces in the rear." Having decided the deception objective, the planners formulate a detailed plan.

2-5. Sometimes the commander's initial guidance contains no specific guidance for deception planning to occur. In that case, the MDO uses the commander's intent informed by the results of mission analysis to evaluate whether deception can or should play a role in the overall operation. That role, when identified, is then stated as a proposed deception goal and its associated deception objectives. Sometimes multiple deception goals exist based on such considerations as operational phasing, duration, or complexity.

2-6. Deception is never conducted as an end in itself; it must support real plans, operations, and objectives. Correspondingly, the success of an operation cannot be contingent on the success of a deception. Policy prohibits deception from deliberately targeting anyone outside the enemy military decision-making process without further legal review (see paragraph 2-89 for more on legal considerations).

### MISSION ANALYSIS

2-7. All military planning includes mission analysis. Mission analysis involves gathering, analyzing, and synthesizing information to get oriented on current conditions of an operational environment. MDOs in conjunction with staff planning efforts conduct mission analysis to better understand the situation and problem and to identify *what* deception the unit can accomplish, *when* and *where* it should be done, and *why*

to do it—the purpose of the deception operation. Deception mission analysis begins before the Army tactical deception planning process and is always properly informed by current operations and planning efforts.

2-8. The deception goal and its associated deception objectives are key outputs of deception mission analysis, and the foundation for subsequent deception planning. They provide the commander and MDOs with a solid understanding of how the deception supports the overall operation and establishes the conceptual framework for the deception plan. An effective deception does not have to be elaborate or complex. Simplicity is often preferred.

2-9. MDOs need to participate in and have their efforts informed by conventional planning efforts. Conventional and deception planning horizons occur simultaneously in parallel. During mission analysis, the MDO begins with analyzing and assessing an operational environment and information environment. Deception may be a feasible option, if appropriate to the mission, and if there is a possibility of success. Issues that planners consider when determining if deception is a viable COA include—

- Availability of assets.
- Understanding any potential deception targets.
- Suitability.
- Time.
- Risk.

## Availability of Assets

2-10. MDOs consider the availability of assets to determine if sufficient assets exist to support both the operation and the deception. There are few assets specifically designed and designated for deception. This means plans may require shifting assets from supporting the operation to the deception plan. Commanders consider the risks to ascertain that shifting assets to support deception does not adversely affect the operation or prevent mission success. Resource development includes collecting potential target data sources, identifying potential conduit systems, and cataloging potential deception means. Resource development also includes the collection of essential foreign and friendly situation and background information needed to initially to organize operations and assess general capabilities.

## Understanding the Deception Target

2-11. MDOs consider the potential deception target to determine if sufficient information exists on how the target acquires information and makes decisions, what knowledge the target has of the situation, and how the target views the friendly force. Planners also determine if sufficient information exists to reveal the biases, beliefs, and predispositions of the deception target. If necessary, the staff can make assumptions about the deception target, but it must avoid mirror imaging, which is the tendency to assume a person sees the world and makes decisions in a manner similar to oneself. It is for this reason that MDOs rely heavily on human factors analysis (see paragraph 2-37).

## Suitability

2-12. MDOs consider suitability. Some missions are better suited to deception than others are. When a unit has the initiative and has some control over the area of operations, then deception is more suitable. In some situations, specific personnel or organizations are better suited to execute deception operations than others are. Deception planners determine if conditions are appropriate to conduct deception and make a recommendation to commander. The decision ultimately resides with the commander. Conditions in which deception are appropriate include the following:

- The enemy has an advantage that cannot be overcome without using deception, for example, advantageous force strength, capability, agility, or situational awareness.
- The enemy has known preconceptions that can be exploited.
- The enemy has known flaws in its decision-making process.
- The enemy is under pressure to act.
- The enemy is susceptible to suggestion.

- Deception will enhance OPSEC.
- Deception will enhance the effectiveness and likelihood of success of a conventional plan.

### Time

2-13. MDOs consider time available. Time is a key element to consider when developing the deception story. MDOs determine how much time they have to present the deception story and to estimate how much time the deception target will use make a decision and direct the desired action. The available time may determine the scope and depth of the story. MDOs carefully time deception events to synchronize them with the approved plan.

### Risk

2-14. An important planning consideration is the mitigation of identified risk. Risk is a key factor that must be reexamined during all phases of deception planning and execution (see paragraph 2-126). The MDO must evaluate any substantial risk which may include—

- Risk of deception failure.
- Risk of compromise.
- Risks associated with a successful deception.
- Exposure of means or feedback channels.

### Information Environment Analysis

2-15. An information environment analysis is an extension of mission analysis. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). The information environment is a subset of an operational environment. The MDO, working with IO planners, must identify the key aspects of the information environment relevant to the deception target and decision making. To influence the behavior of the deception target, the planner must understand how the target views the environment, processes information, and makes decisions. This understanding includes an analysis of the political, military, economic, social, information, and infrastructure variables of the target's environment.

### Deception Running Estimate

2-16. Once created, a mission analysis provides information that helps produce a deception running estimate. The deception running estimate is a specialized product derived from the intelligence preparation of the battlefield and from responses to situation-specific RFIs submitted by MDOs. Most information in the estimate originates from mission analysis, but much of the detail required is unique to deception. MDOs collaborate with intelligence analysts to build the running estimate. MDOs work with the G-2 to obtain information critical to effective deception planning. This information forms the basis of the deception running estimate that feeds the development of a viable deception concept.

2-17. The deception running estimate identifies deception opportunities, detects information and capability requirements, and recommends a feasible deception goal and its objectives. The MDO presents this estimate during the mission analysis briefing. The estimate considers current capabilities based on enemy susceptibilities, preconceptions, and biases; available time; and available deception means. A key outcome of the running estimate is the determination of whether or not there is a viable deception opportunity.

2-18. Preparing the deception estimate involves developing alternative approaches to reaching the deception goal. It first determines the objective of the deception and then the desired perceptions that likely lead to that objective. Developing the estimate is a critical process to prepare for a deception operation. Depending on the nature of the commander's guidance, the deception estimate may be integrated in the operation's running estimate, may stand alone, or may not be appropriate at that time. In the latter case, the role of deception is limited to OPSEC activities or simply to supporting one or another component of the operation.

2-19. The deception running estimate is a living product. Planners refine it as additional information and intelligence become available, or as conditions evolve and change within an operational environment and information environment. During the initial planning, MDOs and intelligence analysts often make

assumptions that later require validation to continue with planning. Planners track these assumptions, align them with an open RFI, and consider them during risk analysis. During the unit's COA analysis (war gaming), planners help refine the estimate and may add support to key planning assumptions about probable enemy responses to planned friendly activity. The greater the number of assumptions underpinning a deception plan, the higher the risk that one or more assumptions will prove false and threaten the plan's success.

2-20. The deception running estimate identifies key enemy decision makers and develops individual or group profiles. The analysis of the enemy military decision-making structure includes identifying key decision makers who exercise some level of direct control over the enemy capabilities. These individuals or groups are potential deception targets. As such, the MDO works with the G-2 to collect as much available information relating to their backgrounds, psychological profiles, personal relationships, key influencers, known biases, predispositions or vulnerabilities, current perceptions, and previous behavior in similar circumstances. With that information, the planner identifies the enemy's most probable and most dangerous COAs related to the deception goal.

2-21. The MDO briefs the initial running estimate to the commander in private during mission analysis to seek approval of the deception goal and its objectives, receive refined commander's planning guidance for deception, and ensure nesting within the supported plan. The commander may provide additional guidance concerning specific deception COAs the staff should address when preparing estimates. Once approved, the deception goal and its objectives become the focus for all subsequent deception planning.

# THE ARMY TACTICAL DECEPTION PLANNING PROCESS

2-22. The Army tactical deception planning process nests in the steps of the Army's military decisionmaking process (known as MDMP). The deception plan supports the OPLAN. Planners nest and integrate the deception plan with the OPLAN to achieve the deception's desired effect. A successful deception plan unfolds logically and realistically. Deception planning is an iterative process that requires continual reexamination of its goals, objectives, targets, and means. The early integration of deception in the planning cycle ensures optimum application of resources and maximizes the potential for overall success. Table 2-1 shows the Army tactical deception planning process nesting in the military decisionmaking process.

**Table 2-1. The Army tactical deception planning process in the military decisionmaking process**

| ***Army tactical deception planning process*** | | ***Military decisionmaking process*** |
|---|---|---|
| Deception preplanning. | → | Step 1: Receipt of mission |
| Step 1: Determine the deception goal and the deception objective. | → | Step 2: Mission analysis |
| Step 2: Identify and analyze the deception target.<br>Step 3: Identify desired perceptions of the deception target.<br>Step 4: Develop deception observables and means.<br>Step 5: Develop the deception story.<br>Step 6: Develop the deception event schedule.<br>Step 7: Develop OPSEC and other protection measures.<br>Step 8: Develop feedback criteria.<br>Step 9: Develop a termination plan. | → | Step 3: Course of action development<br>Step 4: Course of action analysis and war gaming<br>Step 5: Course of action comparison |
| | | Step 6: Course of action approval |
| Step 10: Produce Appendix 14 (Military Deception) to Annex C (Operations) | → | Step 7: Orders production, dissemination, and transition |
| OPSEC operations security | | |

2-23. Because of its inherent sensitivity, MDOs usually need to protect access to deception planning. As a result, deception planning occurs in an access-controlled area rather than through open discussion in the plans shop. Key staff members and leadership who are part of the deception planning effort plan discretely to integrate and deconflict deception planning outputs into the overall planning effort. Planners balance the need

to conduct adequate coordination with a parallel planning process during deception planning against the need to maintain the secrecy required for effective deception operations. MDOs establish and use strict need to know criteria to determine which specific staff members will participate in deception planning. The criteria may specify separate levels of access to facilitate coordination, thus allowing more individuals access to the less sensitive aspects of the deception plan.

## DECEPTION PLANNING METHODOLOGY

2-24. MDOs use the see-think-do planning methodology to guide deception planning, execution, and assessment. Successful deception operations are those that do more than make the target believe or think the deception is true. The deception target must make a decision to act or not act in a way that favors friendly operations.

### Enemy Cognitive or Action Process (See-Think-Do)

2-25. Deception focuses on the decision making of an enemy. Deception must end in a decision to act or not act in a way that supports an operation. MDOs emulate the cognitive process by identifying what they want the enemy to *do*, determining what the enemy must *think* in order to act as desired, and then establishing what the deception target must *see* to encourage thinking that way. The enemy cognitive or action process occurs in the see-think-do order:

- **See**: What significant indicators of something does the enemy see, sense, or detect?
- **Think**: Do these indicators lead the enemy to believe what it sees, senses, or detects?
- **Do**: Has the enemy decided on an action or inaction based on what it believes?

### Deception Planning Process (Do-Think-See)

2-26. The deception planning process follows the reverse of the enemy cognitive process. This reverse planning uses do-think-see:

- **Do**: What action or inaction do friendly forces want the enemy to take?
- **Think**: What must the deception target believe to take the desired action or inaction?
- **See**: What deception must friendly forces show to or hide from the deception target that will cause the target to develop the desired perception?

## STEPS OF THE ARMY TACTICAL DECEPTION PLANNING PROCESS

2-27. Planning for deception follows the reverse planning sequence of activities; it determines how to cause sequential events that lead to success but in the reverse order of their occurrence. The goal and its objectives of the deception operation start this process by specifying the operational effects of the deception and the decision of the target that provide the desired operational effect.

2-28. Deception planning comes together during COA development, analysis, war gaming, and comparison. Planners produce a deception plan to support each COA as they develop each COA. The level of analysis and detail for a deception plan needs to suffice for an MDO to effectively portray a viable concept to the commander. The planner must present a high level of confidence that friendly forces can successfully execute the deception plan with available assets, continued planning, and detailed coordination. As with the overall COA, the doctrinal evaluation criteria is that a COA must be adequate, feasible, acceptable, distinguishable, and complete. Planners brief each deception plan as a subset of the overall COA.

2-29. Each COA briefing contains the following information:

- Previously developed deception goal and objectives.
- Identification of deception target (position, relation to enemy capabilities to affect, goals, decision process, potential vulnerabilities to deception, and accessibility).
- Desired perceptions.
- Narrative statement describing concept or deception story (may include deception type, techniques, and tactics).
- Identification of tentative means or capabilities, conduits, and feedback.

- Identification of execution shortfalls concerning intelligence, means, capability, or authority).
- A concept sketch.

2-30. The MDO ensures that each deception plan is properly constructed. Using the approved COA or concept as a base, the MDO integrates any revised commander's guidance, updated intelligence analysis, and revisions to the primary COA to refine and complete the deception plan. The initial step in this process is to review all previous planning products and adjust them as required. From this point, the planner begins the ten-step Army tactical deception planning process:

- Step 1—Determine the deception goal and the deception objective.
- Step 2—Identify and analyze the deception target.
- Step 3—Identify desired perceptions of the deception target.
- Step 4—Develop deception observables and means.
- Step 5—Develop the deception story.
- Step 6—Develop the deception event schedule.
- Step 7—Develop OPSEC and other protection measures.
- Step 8—Develop feedback criteria.
- Step 9—Develop a termination plan.
- Step 10—Produce Appendix 14 (Military Deception) to Annex C (Operations).

## Step 1—Determine the Deception Goal and the Deception Objective

2-31. The deception goal is the desired contribution of the DWG to friendly mission success. The deception goal is usually recommended in the running estimate and confirmed by the commander's planning guidance at the conclusion of mission analysis. The commander is responsible for providing the deception goal. The MDO or DWG often develops a deception objective based on that goal.

2-32. The deception objective is the purpose of the deception expressed as the enemy's actions or inactions at a critical time and location. Like the deception goal, the running estimate contains the deception objective. The commander confirms the deception objective in the commander's planning guidance at the conclusion of mission analysis.

## Step 2—Identify and Analyze the Deception Target

2-33. The deception target is the enemy decision maker who has authority to make the decision to achieve the deception objective. During mission analysis, MDOs identify potential deception targets. The target directs the action or inaction of the enemy force or capabilities. Friendly forces need existing conduits to the deception target or a reasonable expectation to establish conduits.

2-34. To fully analyze a target for deception, planners—

- Characterize enemy decision making.
- Analyze the human factors affecting a deception.
- Conduct conduit analysis of the deception target.
- Understand the enemy's intelligence and counterintelligence organizations and capabilities.
- Analyze the enemy's potential vulnerability to deception.
- Understand enemy deception and counterdeception doctrine and resources.

### *Characterize Enemy Decision Making*

2-35. To affect enemy decision making, planners must first understand and characterize its functional components by analyzing and describing the enemy's decision-making structure and style. Decision-making structure refers to how the enemy organizes relevant information to collect, transmit, analyze, and deliver to support decision making. Decision-making structure provides the basis for conduit analysis. Planners select a model that is conducive to rapid understanding. This type of model enables intelligence analysts and MDOs to better understand the overall enemy decision-making structure and subsequently communicate the reason for a certain operational approach or series of deception events.

2-36. Decision-making style refers to the deliberative process that a selected decision maker uses to reach a conclusion. The selection and use of a common framework allows intelligence analysts and planners to focus their analysis and discussions to best support achievement of objectives. Many formal and informal decision-making styles exist. Once an enemy selects a framework, intelligence analysts and planners work to identify what conditions might cause adjustments to that base style.

### *Analyze the Human Factors Affecting a Military Deception*

2-37. Enemy goals and operational objectives provide the "why" behind enemy decision making and subsequent actions or inaction. Understanding and predicting enemy behavior is the first step planners take. *Human factors* are the physical, cultural, psychological, and behavioral attributes of an individual or group that influence perceptions, understanding, and interactions (JP 2-0). Human factors affect decision making, the flow of information, and the interpretation of information by individuals or groups at any level in any state or organization. MDOs analyze the human factors that influence decision making that also include feelings and emotions that influence cognitive functions. MDOs also use a cognitive approach to understand the thought processes and functions of the enemy, such as attention, perception, memory, reasoning, problem solving, and decision making. Cognitive functions combine to help individuals make sense of their environments.

2-38. Planners analyze factors that affect enemy decision making by conducting emulative analysis. This analytical process reproduces what or how the enemy thinks, to include the socio-cultural lenses through which the enemy's thinking occurs. Emulative analysis provides the basis for the friendly assessment of what the target must see or not see. It anticipates the enemy's response to changes in the environment created by friendly forces. It also studies the enemy's predispositions, biases, patterns of receiving information, and priorities, among other factors. Emulative analysis is crucial to deciding what must be shown; where, when, and by whom it must be shown; how it must be packaged; and how it must be transmitted to create the desired reaction within the target's control system. Systematically applying emulative analysis comes before evaluating the target's range of possible reactions to observables and the alternative conclusions the target could draw from them.

2-39. Cognitive biases and preconceptions might subjectively influence enemy decision making. This is important to any attempt to predict future behaviors. The study of psychology and decision making recognizes numerous potential types of bias. For purposes of illustration, a commonly recognized summary of bias types includes—

- **Cultural biases** caused by the interpretation of information through one's own cultural knowledge, beliefs, morals, customs, habits, and cognitive styles acquired as a member of a specific social environment or group.
- **Organizational biases** stemming from a potential outcome of the goals, norms, policies, and traditions that characterize the specific organizations in which individuals affiliate.
- **Personal biases** that come from personality traits, education, and firsthand experiences that affect a person's worldview over the course of a lifetime.

2-40. Preconceptions are conceptions or assumptions formed beforehand. In addition to being highly influenced by bias, people form preconceptions by sustained observation and perceived recognition of patterns. This is particularly relevant to deception planning because known biases and preconceptions can be exploited.

2-41. MDOs have other considerations when analyzing a target. They consider answers to the following questions:

- Is all information equally important to the target?
- Does the target rely more on certain sources?
- Does the target receive influential analysis or advice from someone within or supported by the same information conduit?
- Does the presence of an intermediate-level decision maker in the conduit affect the deception story or the observable?
- What enemy vulnerabilities can be exploited?

### *Conduct Conduit Analysis of the Deception Target*

2-42. Conduit analysis is the detailed mapping of individual conduits or information pathways to the potential deception targets. The MDO chooses and deconflicts access to specific conduits to deliver a synchronized portrayal of selected information and indicators. In general terms, an individual conduit consists of a sensor that registers a signature, a transmission means from the sensor to an intermediate node or nodes that might act on the information in a variety of ways, and a delivery to the deception target.

2-43. Conduit analysis usually depicts the conduit and the method of transmitting information between two nodes. Conduit analysis begins with the initiation of planning and continues to be refined through the COA development, COA selection, and finalization of the deception plan. MDOs normally identify potential conduits using one of two methods: working outward from the deception target and their inner circle of information sources or working inward by visualizing the presentation of a potential indicator to known enemy collection capabilities up through the process flow to the deception target.

2-44. Some key terms associated with conducting conduit analysis include the following:

- **Conduit**: An information or intelligence gateway to the deception target. Conduits can include a FIE, an intelligence collection platform, an open-source intelligence, and foreign and domestic news media.
- **Observable**: The detectable result of the combination of an indicator within an enemy's conduit intended to cause action or inaction by the deception target. Observables are events, activities, or elements of information that must be seen or sensed by the target to form the desired perceptions.
- **Transmission time**: The average time for an observable transmission to move from sensor to deception target. Estimating and anticipating transmission time for conduits is critical to synchronizing a deception plan execution.

2-45. Planners consider information on any risks incurred by using a conduit. Risks might include exposure of friendly means, forces, or sensitive capabilities. Risks can also include potential awareness by the enemy that a selected means might be part of a friendly deception, causing the conduit to lose credibility. The selection of appropriate conduits is a critical part of developing a successful plan. When selecting conduits, the MDO considers—

- How the information enters the conduit.
- The information that can be conveyed through the conduit.
- The time the conduit is available to transmit information.
- The amount of time the information needs to reach the target.
- The degree of control the relevant nodes have over the conduit.
- The credibility of the conduit to the decision maker.
- The filters likely to affect information as it moves through the conduit.

2-46. Whatever method (or combination of methods) the MDO uses, the more conduits that the planner and supporting G-2 intelligence analysts can identify and map, the greater the chance of synchronizing friendly deception operations to feed multiple conduits simultaneously, and the increased potential success of the deception. Additionally, when the MDO classifies conduits as simple or complex, then the planning team can share the context more effectively. A simple conduit transmits data to the intended decision maker without applying an intermediate filter. A complex conduit includes one or more filters that might substantially alter the content, add context to the observable, or alter the timeframe for delivery.

2-47. Ideally, the MDO selects multiple conduits to deliver information to the deception target and sequences the delivery in a manner that builds and confirms the deception story. Such delivery can cause information about the same observable to be delivered at multiple differing times and from many sources. This technique can reinforce the desired ambiguity-increasing or ambiguity-decreasing effect. To enhance the believability of the deception story, the MDO works with OPSEC and other IRCs to manage competing observables (any indicator that might contradict the deception story) and to limit the function of conduits that might register and report them.

2-48. While the initial discussion of a given conduit might address the relevant information flow in simple terms, planners cannot actually fully exploit that conduit until they analyze it in detail. Intelligence analysts

and MDOs must understand and subsequently collaborate to diagram key elements and complete a worksheet or other planning template that corresponds to each conduit for use in future planning.

### *Understand the Enemy's Intelligence and Counterintelligence Organizations and Capabilities*

2-49. Enemy decision making stems from its intelligence and counterintelligence organizations and capabilities that support them (to include external intelligence sources). To manipulate or augment the information available to a deception target, the MDO needs detailed knowledge of the enemy's ability to see and interpret all relevant friendly activities and indicators. Traditionally, the G-2 analyzes enemy intelligence and counterintelligence capabilities, organizations, and functions. By leveraging the full scope of resources, the G-2 provides the enemy's perception of friendly goals and objectives, the enemy's perception of friendly technical estimates, and the enemy's intelligence process.

2-50. The G-2 provides the enemy's perceptions of friendly capabilities. This analysis includes an enemy perspective analysis of friendly probable goals and objectives, friendly most probable and dangerous COAs, a blue center of gravity analysis, and any other fundamental assumptions or perceptions the enemy has developed about friendly activities, capabilities, or intent.

2-51. The G-2 provides detailed technical estimates of the enemy's collection capabilities, intelligence networks, and reporting channels. Ideally, this analysis includes the capabilities of FIEs that share intelligence with the enemy. The G-2 can capture this information within the deception running estimate by organizing threat capabilities under the intelligence disciplines: geospatial intelligence, human intelligence, signals intelligence, measurement and signature intelligence, open-source intelligence, technical intelligence, and counterintelligence. Deception planners need the scope of this analysis to identify a particular threat's collection capabilities anywhere that they provide potential knowledge of friendly plans.

2-52. The G-2 also provides knowledge of the enemy's intelligence process: planning and direction, collection, processing and exploitation, analysis and production, and dissemination and integration. The MDO needs to understand every sensor, link, node, and potential filter in the conduit through which that event's execution was transmitted. This knowledge enables planners to inject deceptive information into the enemy's intelligence system as a deception event, track its delivery to the decision maker, and evaluate whether the execution produced the desired perception or effect. Knowledge of the enemy's intelligence process requires sufficient fidelity of intelligence in the deception running estimate to conduct a reasonably accurate enemy conduit analysis with minimal assumptions later in the planning process.

### *Analyze the Enemy's Potential Vulnerability to Deception*

2-53. To fully analyze a target for deception, planners analyze the enemy's vulnerability to deception and conditions that might favor the enemy in protecting against deception. MDOs use the framework of physical, informational, and cognitive dimensions of the information environment. Sample vulnerabilities in the physical dimension include shortfalls in collecting or processing capability and vulnerabilities in force structure or capability. Examples of vulnerabilities in the informational dimension might include such things as poor information management or data processing capability and overdependence on vulnerable or non-redundant communications networks. Cognitive vulnerabilities to deception can include such things as predisposition or bias, an overly burdensome decision-process model, poor decision quality (group think, single point of failure, or lack of subordinate autonomy), or poor decision timeliness (a leader who cannot come to a decision quickly). Enemy strengths in the areas mentioned above are normally inverse statements to examples provided.

### *Analyze Enemy Deception and Counterdeception Doctrine and Resources*

2-54. Planners fully analyze a target for deception by exploring an enemy's deception and counterdeception doctrine and capability. Knowing an enemy's deception doctrine and capability is critical to deception planning. It can enable analysts and MDOs to understand the emphasis the enemy places on deception and thus vigilance in its detection. This knowledge also provides the necessary awareness to help friendly forces identify when the enemy might use deception to influence friendly decision making.

## Step 3—Identify Desired Perceptions of the Deception Target

2-55. After the MDO has determined how the enemy thinks, the planner identifies *what* the enemy wants friendly forces to think. The deception target perceptions are what the deception target must believe in order to make the decision that will achieve the deception objective. This perception of friendly force actions is based on the deception objective and exploits the deception target's information processing cycle. This includes the supporting information and network-enabled systems, decision-making processes, beliefs, biases, and preconceptions regarding friendly forces and the situation. Once the desired perceptions are determined, the MDO begins to sequence them. These perceptions become the required perceptions for a successful deception. Required perceptions are those that are essential, pre-eminent above others in the enemy's analysis. Referring to them as required conveys the criticality of focus, resourcing, and feedback to a perception's formation by the deception target.

## Step 4—Develop Deception Observables and Means

2-56. The MDO takes the initial sequence of required perceptions and starts to determine how to portray the deception using observables and means. Deception observables resemble the pieces of a puzzle presented to the target over time. The target—usually aided by supporting information and intelligence systems—assembles the pieces of the puzzle, gradually reconstructing the picture of a constructed military situation. Observables that must be "seen" and accepted as true by the enemy to form the desired perceptions sometimes called required observables. As with perceptions, required observables may be given greater credibility using supporting observables. Observables are portrayed to the target (and target information and intelligence systems) through executions, often referred to as deception events.

2-57. The deception means are the methods, resources, and techniques used to create required observables (things the deception target needs to see in order to deduce the desired perceptions) and act out the deception story. The nature of the desired perception—with the indicators needed to convey the perception to the deception target—determines the deception means employed. Physical means are observable physical activities of forces, systems, and individuals that present visual indicators. Technical means could include cyber-based messaging and information-sharing venues, smart phone and mobile wireless communications, radio broadcasts, radar emissions, and electromagnetic deception. Administrative means convey oral, pictorial, documentary, or other material evidence to a deception target. While many available means may exist, the means employed must be consistent.

## Step 5—Develop the Deception Story

2-58. The deception story outlines friendly actions portrayed to cause a deception target to take action (or inaction) as designed in a deception objective. The deception story should be a summarized statement of our deception portrayal stated as a logical enemy conclusion derived from all available observables. The core elements of the story are the desired perceptions that we wish to create within the enemy decision maker. The deception story consists of observables and desired perceptions. It also addresses competing observables. The MDO uses the intelligence estimate and writes the deception story as a narrative from the perspective of the enemy.

2-59. A well-developed deception story presents an overview of the entire deception as seen from the target's point of view. As such, it serves as a valuable means of checking the logic and consistency of the internal elements of the deception and identifying areas that need refinement or may call for the addition of supporting observables. An exact understanding of the perceptions and observables required for the deception provides a concrete basis for creating the deception story. The deception story weaves these elements together into a coherent whole that describes the picture of the situation that the target will reconstruct from the information the deception provides. An effective deception story must be verifiable, executable, believable, and consistent.

### *Verifiable*

2-60. A target can verify an effective deception story through multiple channels and by using all intelligence sources. When making sure that the deception story is verifiable, deception planners avoid single-source inputs that would provide the whole story. Multiple conduits provide pieces of a puzzle that combine to create

the deception story. Employing various conduits in a timely and believable manner is of the utmost importance. This dynamic clearly underscores the value and importance of the IO officer in the deception process.

***Executable***

2-61. A supported commander has the resources and authority to execute a deception story and the time available. Time, and echelon when it is employed, may limit the scope and depth of the deception story, which is why planners continually assess the synchronization and deception event schedule.

***Believable***

2-62. A believable deception story corresponds to the deception target's perceptions of the friendly force's mission, intentions, and capabilities. An enemy will likely discount notional plans or forces that grossly distort actual friendly capabilities. An enemy often meets unverifiable deception with suspicion and doubt. Additionally, enemies will not believe stories that closely copy past and already exposed deception operations. The deception story must be believable both in its parts and as a whole. If one or more of the parts do not fit into the complete picture, they may create enough suspicion to reveal the deception.

***Consistent***

2-63. An effective deception story matches the target's understanding of actual friendly doctrine, historical force employment, campaign strategy, tactics, current operational situation, and conditioned patterns of friendly activity. The deception element must have as complete a picture as possible of the deception target's level of knowledge and belief in these areas.

## Step 6—Develop the Deception Event Schedule

2-64. A *deception event* is a deception means executed at a specific time and location in support of a deception operation (JP 3-13.4). The deception event schedule is the tool used to sequence deception events for a logical progression of the deception story and to synchronize the deception with the broader plan. This schedule requires identifying when the MDO employs specific deception events. The schedule aims to influence the deception target's perceptions in time and space so the target completes the desired action (the deception objective) at the most operationally advantageous moment. The deception event schedule captures what will occur, when it will take place, where it will occur, and who will control the execution. Each planned deception event has a unique number to facilitate coordination and execution tracking. It is imperative that MDOs synchronize and deconflict the deception event schedule with the unit's operations synch matrix. Figure 2-1 on page 2-12 depicts the steps leading up developing the event schedule.

2-65. Deception events are activities conducted through deception means at a specific time and location to convey the deception story to the target. Deception events build observables that create desired perceptions. The observables and desired perceptions are two key elements of the deception story. To convey the story, the enemy needs to sense and observe the events. If the enemy's intelligence system can see, sense, or detect the deception event, then it can collect the information it needs to piece together the deception story. The systematic, yet seemingly random, projection of deception story elements by multiple means at varied times also makes the deception more believable. The MDO carefully ensures that information appears as legitimately collected. The enemy usually suspects important military information that is too easy to obtain.

2-66. Based on the commander's final decision as to how to portray the story, the MDO develops the deception event schedule in a time-ordered sequence. This schedule captures all friendly actions (deception events), executing elements, and execution reporting and coordination requirements involved in the deception operation. It also directly supports the tasking of friendly resources, coordination with other staff elements, and identification of administrative and logistics requirements. MDOs consider the following factors when building the deception event schedule:

- The overall plan.
- The timing of actual friendly activities in the operations synch matrix.
- The time required for friendly forces to conduct the deception activity.

- The location a particular activity fits in the normal sequence of events for the type of operation being portrayed.
- The time required for the enemy intelligence collection assets to collect, analyze, and report on the activity.
- The time required for the deception target to process, decide, and execute the desired action.
- The time required to execute the desired action or inaction.
- The impact of filters on the timeliness of observables.

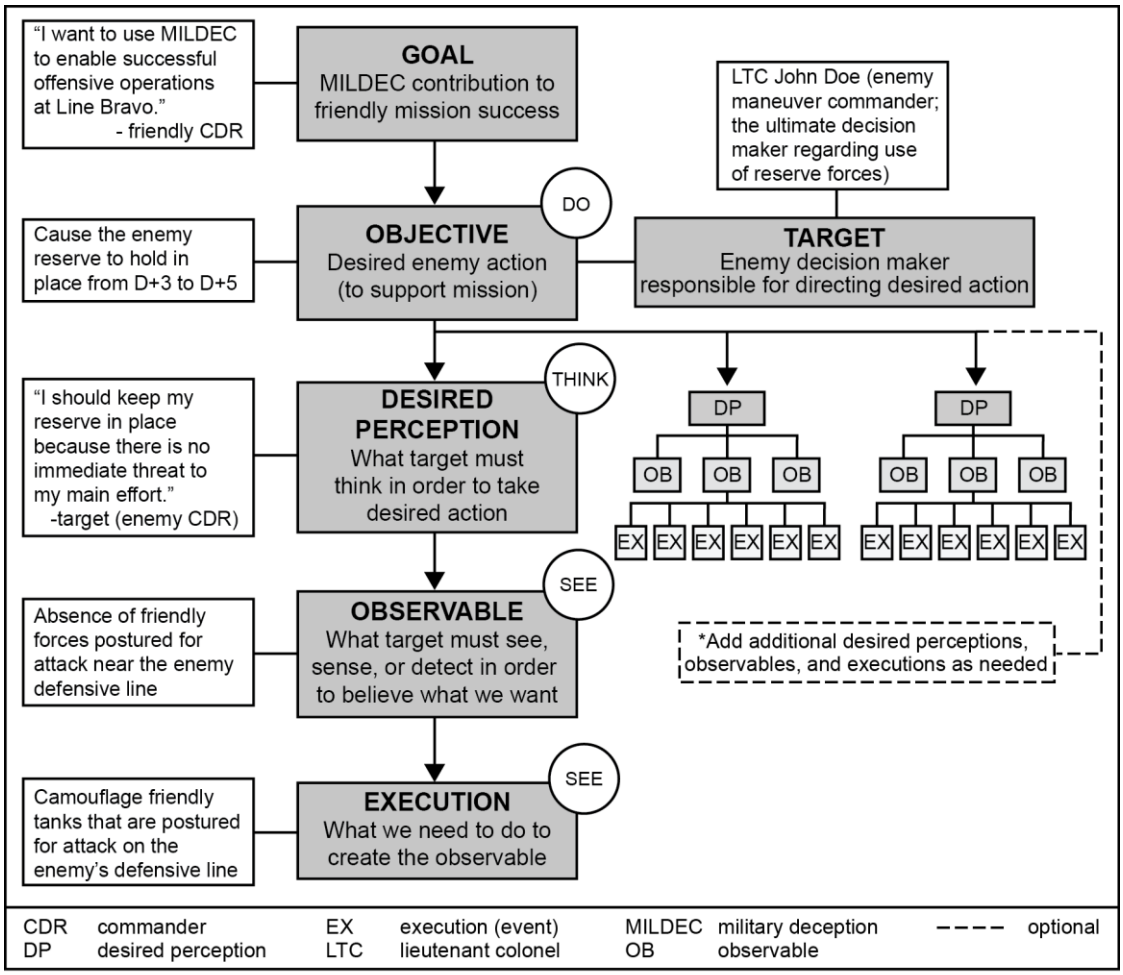



**Figure 2-1. Planning steps**

## Step 7—Develop Operations Security and Other Protection Measures

2-67. OPSEC and other protection measures are employed with deception to ensure that only the desired deception events reach the enemy and that actions in support of operations are concealed. Without OPSEC, the enemy may observe preparations for the supported operation. Deception activities may not convince the enemy to believe the deception story if the enemy observes preparations. Equally important is risk assessment. All deception involves risk and cost. Commanders base the decision to conduct a deception on a deliberate assessment that weighs costs (including risk) against benefits. MDOs can mitigate risk by ensuring the success of the supported operation does not hinge upon the success of the deception, anticipating conditions that could compromise the deception, and developing responses in the event of unintended effects.

### Step 8—Develop Feedback Criteria

2-68. Identifying (or in some cases, establishing) channels for feedback is a continuous and integral part of deception planning. Feedback is information that reveals how the target or information systems respond to the deception. The essence of feedback planning is expressed in three steps. The MDO first envisions the target's response to each desired perception or observable. Then the MDO analyzes the target's actions associated with the response (response indicators) that friendly resources can detect. Lastly, the MDO coordinates with or tasks appropriate friendly resources for reports on those indicators within a given period.

2-69. Although a high level of feedback is a desirable planning goal, staffs do not need dedicated feedback mechanisms for every perception or observable. Carefully designed feedback at key times during the deception can often provide information on the enemy's reaction to multiple observables. Additionally, friendly intelligence, surveillance, and reconnaissance efforts often collects response indicators related to enemy operations as a part of unit intelligence collection. Where feedback relies on such information, early coordination with the intelligence officer's collection plan can help eliminate redundant feedback mechanisms and reduce unnecessary tasking.

2-70. Feedback demonstrates that the deception story is being assembled by the targeted decision maker in the desired manner. An effective MDO plans and incorporates these feedback mechanisms into the deception event schedule to gather necessary information at critical times in the deception story's development. Feedback enables the commander to determine whether to continue the deception story, adjust the deception events, or terminate the deception. These determinations depend on the target's reaction to the deception events conducted by friendly forces. Feedback-related tasks and activities are also noted in the deception event schedule. Chapter 4 discusses feedback in detail.

### Step 9—Develop a Termination Plan

2-71. Deception does not just simply end. A commander-approved termination plan guides a coherent, structured, and implementable exit strategy. This is important because the commander terminates a deception after it meets its termination criteria, which may include success, failure, compromise, or a combination of the three. Like the deception story, the deception target must also believe the exit strategy and friendly operational profiles. Additionally, the termination plan keeps the target unaware of the deception means, techniques, and events. Otherwise, the next deception operation may not have the desired effect if the enemy gained insights into friendly tactics, techniques, and procedures. Various circumstances might create a requirement to terminate the deception completely or in part.

2-72. Termination planning ensures the controlled, orderly cessation of planned deception events, protects means and resources, and sets the parameters for any release of information relating to the deception. Planning the termination of a deception operation requires the same care and attention to details that went into planning the deception's execution. Ideally, termination planning includes contingencies for unforeseen events such as the deception's premature compromise. In the event of compromise, termination planning for deception includes a notification to rapidly inform forces that may be affected. The termination concept provides initial planning considerations to implement and should include the following:

- A brief description of each termination scenario circumstance included in the plan.
- Steps for initiating termination operations in each scenario circumstance included in the plan.
- The identification of the first commander who has termination authority.

2-73. The MDO anticipates that, as the plan proceeds in execution, circumstances of termination will change. A termination concept entirely suited to the initial set of conditions often differs from what is required as the deception matures. The termination concept identifies the timing to release information about the deception. It may provide a cover story should questions arise about the role of deception in a particular operation. Controlling the exposure of the existence of a deception operation or of elements of a deception may be difficult because of the nature of the operation. A termination concept should also include classification and dissemination instructions for deception-related information.

2-74. Potential termination scenarios are illustrated in table 2-2 on page 2-14.

**Table 2-2. Sample terminations**

| *Scenario* | *Criteria and Events* |
|---|---|
| Successful deception operation | The deception has run its natural course, achieved its objectives, and termination will not expose or affect the deception. |
| Change of mission | The overall operational situation has changed and circumstances that prompted the deception no longer pertain. |
| Prudent risk: a decreased probability of success | Some elements of the deception estimate have changed, increasing the risk and costs to friendly forces and prompting the commander to end the deception component of the course of action. |
| Synchronization issues | • The deception is proceeding and may succeed but is no longer synchronized with other aspects of the operation or campaign.<br>• The deception is proceeding and may succeed but it becomes evident that the window of opportunity for exploiting certain conduits or the target itself has closed.<br>• Deception events cannot be synchronized or executed at the required times or locations for any number of reasons. |
| New opportunity | It becomes apparent that if forces modify some elements of the deception (choice of conduits, objectives, or targets), then the probability of success will increase, risks will be reduced, or the impact of the deception will be greater. In this case, the commander may want to terminate some deception events and activities while reorienting other elements of the deception. |
| Compromise | The commander has cause to believe that all or some elements of the deception have become known to the enemy. |

### Step 10—Produce Appendix 14 (Military Deception) to Annex C (Operations)

2-75. Following completion of the deception event schedule and the termination plan, the MDO has everything required to complete Appendix 14 (Military Deception) to Annex C (Operations) of the OPLAN or OPORD. Exhibits, worksheets, and templates used to develop the deception plan can add clarity and detail to a plan so personnel who were not part of the original planning process can rapidly grasp its contents. In most cases, the Appendix 14 to Annex C is classified at or above the classification of the supported plan. Care must be taken in the classification of the deception appendix (to include in training and exercise environments).

## DECEPTION PLAN APPROVAL

2-76. After completing, coordinating, and reviewing the deception plan for consistency, the MDO presents it to the commander for tentative approval. To ensure its synchronization at all levels, approval authority for deception resides two echelons above the originating command. After the approving authority has approved the deception plan, it becomes a part of the OPLAN or OPORD. It is important that deception plans are not widely distributed. To ensure every opportunity to succeed and to protect the deception from compromise, planners strictly limit access to the deception operation to those with a need to know. Deception staffing and approval must adhere to the regulatory requirements found in CJCSI 3211.01 and applicable CCMD instructions. The need to know criteria is essential, and only a limited number of personnel participate in the deception plan review and approval process.

## INTELLIGENCE SUPPORT TO DECEPTION PLANNING

2-77. Intelligence support is critical to a successful deception plan. Deception requires the timely collection, evaluation, analysis, integration, and interpretation of all relevant information and intelligence that is immediately, or potentially, significant to the deception. A lack of accurate information and intelligence database and an inadequate time to rectify a situation can limit the range of viable deception options available to the commander. These deficiencies can also increase the associated risk and significantly reduce the probability of success. Adequate emphasis on timely and in-depth development of information resources

during the capability development phase of the deception plan can go a long way toward alleviating deficiencies. For information on development of data collection plans, see chapter 4.

## INTELLIGENCE SUPPORT

2-78. MDOs frequently make informed assumptions on various topics to continue planning. In addition to RFIs associated with completing the deception event schedule, MDOs often require a high level of detail and predictive analysis. Information on potential deception conduits comes from many sources and must be collected and available so a commander can execute a deception plan with confidence. Once combat operations have begun and U.S. forces have disrupted or neutralized enemy pre-conflict military decision-making structure and flow, access to sensors, and decision-making support networks, the conduits should be reassessed. Rapid enemy adaptation to new conditions in an operational environment requires equally agile friendly intelligence support. Unless deception RFIs are aligned with the priority intelligence requirements, or the deception plan is supported with dedicated intelligence analysis and resources, the deception plan is at risk of becoming desynchronized or ineffective.

2-79. Focused intelligence support is essential to the successful planning, execution, and assessment of any deception. A well-constructed deception plan requires substantive intelligence support. Intelligence supports the execution of effective deception in five ways:

- Identifies enemy decision makers and the information conduits associated with them.
- Helps complete the deception estimate. Begun during mission analysis, the deception estimate is the foundation for effective deception planning as well as subsequent execution and assessment.
- Supports the conduit analysis step of the deception planning process.
- Ensures the collection plan supports the development, collection, and analysis of planned deception measures of performance (MOPs), MOEs, and indicators.
- Identifies and confirms instances of enemy deception and supporting counterdeception exploitation.

2-80. Deception plans employed at any level of conflict (tactical, operational, and strategic) impose special requirements for information collection and intelligence production. Examples of such specialized intelligence production include—

- Studies of the enemy's decision-making responsibilities, logic, processes, and procedures.
- Technical and operational assessments of the enemy's intelligence collection, processing, production, and dissemination systems (strategic, operational, and tactical).
- Emulative assessments of how the enemy sees an operational environment and perceives U.S. forces, including expectations about intentions and capabilities.

2-81. MDOs thoroughly analyze and anticipate intelligence support requirements, making information needs and commander's critical intelligence requirements known to supporting intelligence collection and production organizations.

2-82. The planning and execution of deception operations demands a highly responsive system for managing relevant information collection and intelligence support. Because of the often highly specialized nature of the information and intelligence required, the sensitivity of the operation, and its special security requirements, the MDO must develop internal information and intelligence synch matrixes. Although the specific content and subject matter of these matrixes may fundamentally differ from the types of information required of more traditional military operations, the basic objective is the same in all cases: to ensure the timely, sufficient, and reliable flow of information and intelligence throughout all phases of the planning and execution of the operation. Each deception operation requires a deception matrix. The matrix is a detailed catalog of the specific information required to accomplish every element of the deception. The deception matrix identifies when that information is required and establishes the criticality of the information to deception planning and execution.

2-83. A deception plan is important to the overall success of the operation. MDOs prepare it in a comprehensive and systematic manner and follow a format that facilitates the coordination and integration of all supporting information sources and agencies. The plan is a dynamic tool that is continuously refined and adapted as the operation proceeds.

## INTELLIGENCE REQUIREMENTS

2-84. After performing functional analysis and developing threat models, the intelligence staff assists the MDO in refining selected intelligence requirements into information categories that prioritize and ensure their collection. These categories typically include deception target information, conduit information, military decision-making information, and military capabilities information. Several intelligence entities can compile this type of information, but an MDO will typically coordinate requests through the theater S-2, G-2, or J-2 elements.

### Deception Target Information

2-85. MDOs collect and develop the following on key target decision makers in areas of interest:

- General biographic data and career summary.
- Level of target's decision-making authority.
- Personal decision-making style.
- Biases, predispositions, and range of knowledge.
- Primary or favored sources of information.
- Relationships with and degree of influence with political authorities, key advisors, and known personalities.
- Experience in and attitudes toward friendly and enemy use of deception.
- Historical patterns of decisions.

### Conduit Information

2-86. MDOs collect and develop the following information on the potential means of conveying information to key target decision makers in areas of interest:

- Intelligence system and capabilities such as—
  - Signals intelligence capabilities that include systems and processes for collection, processing, and dissemination.
  - Human intelligence capabilities that include systems and processes for collection, processing, and dissemination.
  - Measurement and signature intelligence capabilities that include systems and processes for collection, processing, and dissemination.
- Operational staff structure, staff process, and information filters.
- Communications and automated information systems structure and process.
- Other information sources (open source, commercial satellite, third-country intelligence, or personal contacts) and the process for integrating them into the military information system.

### Military Decision-Making Process Information

2-87. MDOs have a unique requirement to understand how targeted decision makers actually make decisions, what logical processes that they employ, and how their staff supports this process by analyzing and presenting information to them. Automated, heuristic, prescriptive norms, and simple quantitative methods might be employed in various combinations. There are many ways decisions can be made, and these methods can change within each level of headquarters depending on the mission, time available, and other circumstances. This type of required information includes—

- Command and staff process for military situation assessment (by echelon), including—
  - Required elements of information for situation assessment.
  - Assessment factors and biases.
  - The analytical process, to include human reasoning and automated system support.

- Command and staff process for analyzing and determining COAs (by echelon), including—
  - Required elements of information for COA analysis.
  - Assessment factors and biases.
  - The analytical process, to include human reasoning and automated decision aids.
- Command and staff process for developing OPLANs and issuing orders (by echelon).

### Military Capabilities Information

2-88. Friendly intelligence routinely collects information on the military capabilities of potential threats. Access to all information regarding military capabilities is crucial to effective planning and execution of deception. The more MDOs know about actual capabilities of the threat, the more accurately they can assess the ability of a designated target to achieve a specific deception objective in time for the actions (or inaction) of its forces to be exploited by friendly forces. Typical classes of information about threat capabilities that may prove useful to the MDO include—

- Doctrinal "ways of war" data.
- Force structure, systems, and capabilities.
- Military mobilization systems.
- Force training priorities and proficiencies.
- Force mobility and maneuver capabilities.
- Force deployments and reserves.
- Force reconnaissance, intelligence and target acquisition systems, and capabilities.
- Technical and operational characteristics of key weapons systems.
- Logistic support systems, techniques, and capabilities.
- Command and control procedures, systems, and capabilities.
- Standard operating procedures and practices.
- Strategic, theater, and tactical communications systems, procedures, and capabilities.
- Information warfare and command and control warfare doctrine, systems, and capabilities.
- Military space systems, operations, and capabilities.
- Nuclear forces and weapons.

## LEGAL CONSIDERATIONS

2-89. A number of U.S. and international legal and policy restrictions governs the conduct of deception operations in wartime and contingency operations. MDOs ensure that they are knowledgeable on such matters and able to reliably advise the commander. This means coordinating with the higher command echelon deception staff element to determine applicable guidelines. MDOs also work with the command's legal officer to ensure that the commander's legal responsibilities are properly reflected in deception planning and execution.

2-90. Supporting IRCs such as public affairs activities, civil affairs operations, cyberspace operations, and military information support operations (MISO) are controlled and regulated by their respective policies and practices. A compliant MDO knows these policies and practices while ensuring that no aspect of the deception plan or its execution conflicts with the governing policies of other agencies or activities. Coordination and planning ensure an adherence to all policies and their integration in a synchronous manner. While deception operations may leverage the resources, activities, and operations of such parallel activities and operations, they cannot do so in a way that violates governing policy and legal responsibilities. This is why sufficient training and experience are critical attributes of an MDO. MDOs must possess discreet capabilities in a legally sufficient manner that insulates risk to the commander.

### UNLAWFUL DECEPTIONS

2-91. Certain deception activities or techniques are prohibited because they violate the law of war, including killing or wounding the enemy by resorting to perfidy. Acts of perfidy are acts that, by design, invite the

confidence of an enemy to lead it to believe that the enemy is entitled to, or obliged to accord, protection under the law of war, with intent to betray that confidence. Moreover, the law of war prohibits misusing certain protected signs such as the Red Cross or Red Crescent, fighting in the enemy's uniform, and feigning non-hostile relations in order to seek a military advantage. These actions are prohibited because they undermine the protections afforded by the law of war to civilians, persons who are hors de combat, or other protected classes of persons and objects; impair non-hostile relations between opposing belligerents; and may damage the basis for the restoration of peace. A deception plan must follow the commander's limitations and agreements, and planners must consider legal implications. Staffs should always consult with the judge advocate when developing a deception plan.

2-92. Deception operations are constrained, but not forbidden, by international agreements. Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible. Ruses of war are legitimate so long as they do not involve treachery or perfidy on the part of the belligerent resorting to them. They are, however, forbidden if they contravene any generally accepted rule. The line of demarcation between legitimate and illegitimate ruses sometimes blurs, but the following examples indicate the correct principles. Improper practice to secure an advantage over the enemy includes deliberate lying or misleading conduct that involves a breach of faith or a moral obligation to speak the truth. For example, it is improper to feign surrender so as to secure an advantage over the opposing belligerent.

2-93. The *Department of Defense Law of War Manual* states deception operations will not intentionally target or mislead the U.S. public, the U.S. Congress, U.S. news media, or any open-source (unclassified or generally available to the public) publications. Traditionally, all Department of Defense (DOD) missions and activities have either been determined by federal statue or, in the absence of statutory authority, through the broad constitutional powers of the President. The President, under constitutional and statutory authority, may issue documents that provide direction to the executive branch that apply to this field. Specific regulatory guidance pertaining to the conduct of deception operations is promulgated by DOD and the Services. Misinforming the media about military capabilities and intentions in ways that influence U.S. decision makers and public opinion is contrary to DOD policy. Deceptions will comply with U.S. law, applicable international treaties and agreements to which the U.S. is a party, DOD and Service regulations and policies, and established rules of engagement for U.S. forces. See the *Department of Defense Law of War Manual* and DODD 2311.01E.

2-94. It is expressly forbidden to make improper use of a flag of truce, of the national flag, or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention. Flags of truce must not be used surreptitiously to obtain military information or merely to obtain time to affect a retreat or secure reinforcements, or to feign a surrender in order to surprise an enemy. In practice, it has been authorized to make use of national flags, insignia, and uniforms as a ruse. Hague Regulation (Article 23) does not prohibit such employment but does prohibit their improper use. It is certainly forbidden to employ them during combat, but their use at other times is not forbidden.

2-95. Legitimate ruses can include the following examples:

- Surprises, ambushes, feigning attacks, retreats, or flights.
- Simulated quiet and inactivity.
- The use of small forces to simulate a large unit.
- The transmission of false or misleading radio or telephone messages:
  - False orders purporting to have been issued by the enemy commander.
  - The use of the enemy's signals and passwords.
  - Fake communication with troops or reinforcement that do not exist.
- Deceptive supply movements.
- Deliberate planting of false information.
- The use of spies and secret agents.
- The movement of landmarks.
- Assembled dummy guns and vehicles or laid dummy mines.
- Erected dummy installations and airfields.

- Removal of unit identifications from uniforms.
- The use of signal deceptive measures.
- The use of MISO messages and actions for psychological effects.

### LEGAL SUPPORT TO MILITARY DECEPTION

2-96. MDOs include legal support personnel in coordination efforts to ensure compliance with applicable U.S. and international laws, treaties, and agreements to which the United States is a party; Presidential and DOD policy and regulations; rules of engagement; and applicable component policy. Legal personnel assist in planning the operation to achieve the objective while complying with legal requirements. They also provide training to MDOs on law and policy applicable to deception operations.

## OPERATIONS SECURITY AND DECEPTION

2-97. OPSEC is the process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to—

- Identify those actions that can be observed by enemy intelligence systems.
- Determine indicators that enemy intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to enemies.
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to enemy exploitation.

2-98. The purpose of OPSEC is to reduce the vulnerability of U.S. and multinational forces from successful enemy exploitation of critical information. Deception is typically active, while OPSEC is more passive in nature. OPSEC is a concealment aspect for all deceptions, affecting both the plan and its execution. (See JP 3-13.3 for a detailed discussion of OPSEC.)

2-99. Deception and OPSEC are mutually supporting activities and complementary IRCs. Planners fully integrate them at all levels to maximize effective support to operations. They contribute to the elements of surprise, security, and freedom of maneuver. Deception and OPSEC planners cooperate to manage visible indicators to influence how the enemy perceives friendly capabilities, actions, or intent, so to affect enemy subsequent action or inaction in a manner conducive to the operation.

2-100. OPSEC incorporates countermeasures to reduce the risk of an enemy exploiting vulnerabilities. OPSEC is not an administrative security program but an activity to conceal and protect the operationally significant information from the enemy's collection assets. Limiting the number of personnel who know the actual operation is often key to maintaining OPSEC.

2-101. Deception plans can benefit from normally occurring activity provided the normal activity fits the deception story. Conversely, actual operations have the potential to create OPSEC indicators that pose a threat to the effectiveness of deception plans. These real indicators may conflict with the deception story. Deception and OPSEC planners have to coordinate with organizations that create these indicators to limit potential adverse effects or to maximize their deception potential. Critical information is the specific facts about friendly intentions, capabilities, and activities needed by enemies to plan and act effectively against friendly mission accomplishment. *Operations security vulnerability* is a condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making (JP 3-13.3).

2-102. In addition to the primary planning goal of unifying what is visible to the enemy military decision makers into a holistic and managed denial and deception effort, deception and OPSEC planning intersect at multiple points in the planning process. In execution, deception activities themselves frequently require OPSEC measures and countermeasures to protect sensitive means and resources, and ultimately enhance their believability to the enemy.

2-103. As trained OPSEC practitioners analyze friendly information and planned activities, they understand what information or observable activity rises to the level of critical information and indicators. If the enemies can collect that critical information or those indicators, they can potentially derive an accurate operational

picture of key friendly aspects. Those aspects can include presence, capability, strength, intent, readiness, location of future operations or activity, timing, and method of operations.

2-104. MDOs consciously and continuously analyze and manage friendly operational profiles so what the enemy can see is no more or less than what the MDOs deliberately plan. OPSEC focuses primarily on identifying and protecting critical information and indicators associated with the planned COA. Deception leverages the visible aspects of friendly operations and combines them with a deceptive activity to create plausible alternative facts and conditions in an operational environment to which targeted decision makers feel they must respond.

2-105. OPSEC planners, with the intelligence community, use OPSEC to—

- Identify critical information and indicators by phase, type of operation, or mission.
- Determine how the enemy collects (sees).
- Determine how the enemy perceives potentially visible friendly critical information and indicators.
- Measure the enemy's ability to collect, analyze, and respond to the critical information and indicators to a level that generates an unacceptable risk (time and operational ability to respond).
- Develop and apply OPSEC measures and countermeasures to protect and deny critical information and indicators that enable the enemy to accurately determine and subsequently interdict planned operations.

2-106. To achieve the desired level of control over enemy perceptions, OPSEC planners and MDOs coordinate activities across a spectrum of influence that includes—

- **Truth**: factual information and actions visible to all.
- **Denial**: critical information and indicators protected by OPSEC.
- **Misdirection**: DISO and other activities designed to confuse enemy analysts and decision makers.
- **Deceit**: deceptive activity and information delivered as part of the approved deception plan.

2-107. While OPSEC identifies and protects critical information and indicators about the actual COA, deception actively generates what appears to be critical information and indicators supporting the deception story. Deception deliberately leads the enemy decision makers to the wrong conclusion, thus usurping their decision making and subsequent action.

2-108. Deception and OPSEC planners can save significant time and resources by collaborating during the military decisionmaking process. Enemy threat assessment in the OPSEC planning process to determine technical aspects of how an enemy sees and perceives friendly activity correlates directly with the MDO's identification of conduits necessary to deliver deceptive information to military decision makers. Both OPSEC and deception require a detailed knowledge of enemy decision making to project the impact of planned activities. In concept development, the OPSEC planner and MDO both require detailed knowledge of friendly indicators (signature, association, profile, contrast, and exposure). They use OPSEC to identify and protect critical information and indicators and use deception to replicate desired indicators that effectively portray the deception story.

2-109. OPSEC also supports deception directly during planning, preparation, and execution. The existence of a deception plan in and of itself is critical information, and indicators require protection. Planners need an OPSEC analysis of the planned deception to protect against an inadvertent or unintentional disclosure of deception existence, techniques, or particular means being used. Failure to maintain good OPSEC can enable the enemy to identify the operation as a deception effort with resulting second- and third-order effects such as the refocusing of enemy intelligence collection and combat power against actual friendly force dispositions and intent.

# MILITARY DECEPTION AS AN INFORMATION-RELATED CAPABILITY

2-110. An *information-related capability* is a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions (JP 3-13). A properly planned and executed deception is one of the most effective IRCs available to the

commander. It can directly influence, corrupt, disrupt, and usurp the enemy's decision-making process and the subsequent direction of its forces.

# INTEGRATION WITH OTHER INFORMATION-RELATED CAPABILITIES

2-111. IRCs play a coordinated and interrelated role in the overall deception effort. In many cases, IRCs provide the sole means for accomplishing a deception task. Just as MDOs integrate deception with the overall plan, they also coordinate and deconflict it with IRC plans to eliminate potentially counterproductive activities. This is normally accomplished through the integrating and synchronizing function of IO. Not all planners know the existence or extent of deception activity since access to the plan remains strictly on a need to know basis.

## MILITARY INFORMATION SUPPORT OPERATIONS

2-112. *Military information support operations* are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives (JP 3-13.2). Deception targets differ from MISO target audiences; however, a deception target might also be included as part of a broader MISO target audience. MDOs deconflict deception observables used to deceive deception targets with MISO themes and messages to maintain believability and credibility.

2-113. MISO actions and messages are generally truth based. This practice is not based upon legal or policy restrictions but a requirement to maintain credibility with target audiences in order to execute future MISO. Informed MDOs know the MISO themes and messages that the intended deception target may receive. MISO actions and messages contain both objective and subjective truth, and must be generally "verifiable" by the target audience. Deception events and deceptive information inserted into enemy conduits may contain falsehoods and need only be believable to the target. The two can be mutually beneficial, but they may also run counter to each other; therefore, planners carefully coordinate MISO and deception.

2-114. Commanders can use MISO actions and messages directed at specific enemy target audiences with deception techniques such as feints, demonstrations, ruses, and displays to add credibility to the deception story or event. MISO messages warning of impending multinational force arrival, providing surrender instructions, or attacking the morale of enemy military or paramilitary forces are examples of this type of cooperation. However, because of the requirement for MISO to retain credibility with its broader target audiences, MDOs carefully evaluate any use of MISO in this manner (and proposed themes) for potential costs, benefits, and second- and third-order effects of its use.

## ELECTRONIC WARFARE

2-115. Electronic warfare is essential for protecting friendly operations and denying enemy operations within the electromagnetic spectrum throughout an operational environment. The term *electronic warfare* refers to military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). Deception, in conjunction with OPSEC, supports electronic warfare operations by protecting the development, acquisition, and deployment of sensitive electronic warfare capabilities.

2-116. Electronic warfare can support feints, ruses, demonstrations, and displays. Positioning electronic warfare systems in a particular location, and the electromagnetic signatures the systems present, can create an indicator of the command's intended main effort. By disrupting enemy communications, and other enemy systems using the electromagnetic spectrum, electronic warfare can introduce or increase ambiguity, confuse enemy operations, or affect the enemy's ability to obtain and pass information about certain activities. Close coordination is required between friendly electronic warfare, deception, communications, cyberspace and space support elements, frequency management, and intelligence planners to ensure electronic warfare does not disrupt enemy communications systems that are used as deception conduits or that are providing intelligence feedback.

2-117. Electromagnetic deception is the deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Using electromagnetic deception is not exclusive to deception but can provide potent effects for aspects of deception operations related to the electromagnetic. Among the types of electromagnetic deception are the following:

- Manipulative involves actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces.
- Simulative involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.
- Imitative involves actions to imitate enemy emissions to mislead hostile forces.

## CYBERSPACE OPERATIONS

2-118. Deception and cyberspace operations can be mutually supportive in many ways. Since an enemy can reside in cyberspace and leverage the same systems and processes, cyberspace operations serve as an effective conduit for placing or delivering deceptive material to affect enemy military decision making and subsequent action or inaction. MDOs can help protect friendly use of information systems by applying deceptive activities similar to those used in the physical dimension for maneuver forces. Such an operation may include constructing false servers, communications nodes, and other hardware associated with a tactical computer network to include the replication of traffic and false data storage.

2-119. Enemy intelligence and targeting systems, which make a priority of attacking or subverting a friendly information system, can be dissuaded from doing so via a successful deception plan. MDOs can redirect enemy collection assets toward deceptive events (such as the presentation of a false "weakness" in friendly information systems) and then target those assets for destruction or exploitation by friendly forces. Any deception plan must consider the abilities and limitations of friendly and enemy cyberspace operations. Careful and detailed planning ensures deception executions using cyberspace operations assets are tracked, recorded, and deconflicted with other nondeceptive cyberspace operations. Planners properly classify and avoid exposing the deception plan to unprotected computer networks or sending it via unsecured email. Any exposure can lead to plan failure.

## SPACE OPERATIONS

2-120. Space operations capabilities offer many options to influence deception activities to include satellite-based imagery and signals intelligence collection systems against friendly forces. These collection satellites generally operate in predetermined orbits, and thus the time they are in position to collect intelligence on friendly forces is predictable. MDOs can use this information to portray to the enemy a desired observable or use it to camouflage or take appropriate OPSEC measures to avoid providing indicators to enemy intelligence operations. Additionally, the posturing of friendly force satellites capabilities may also assist in deception efforts. For instance, the use of a friendly force intelligence, surveillance, and reconnaissance, or the positioning of a communications satellite both illustrate methods that may help mislead the enemy regarding friendly force intentions.

## PUBLIC AFFAIRS

2-121. Deception activities, including planning efforts, are prohibited from explicitly or implicitly targeting, misleading, or attempting to influence the U.S. Government, U.S. Congress, the U.S. public, or the U.S. news media. Legal staff review all deception activities to eliminate, minimize, or mitigate the possibility that such influence might occur. Planners coordinate deception plans that have activities potentially visible to the media or the public with appropriate public affairs officers to identify any potential problems. Coordination reduces the chance that public affairs officers inadvertently reveal information that could undermine an ongoing or planned deception.

### CIVIL-MILITARY OPERATIONS

2-122. Civil-military operations are the activities of a commander performed by military forces to establish, maintain, influence, or exploit relationships between military forces and indigenous populations and institutions. These operations support national objectives for host-nation and regional stability. Civil-military operations may include military forces conducting activities and functions normally done by the local, regional, or national government. Conducted to gain maximum support for U.S. forces from the civilian population, civil-military operations contribute to the success of military operations and project a favorable U.S. image throughout the operational area. MDOs coordinate deception with civil-military operations and with MISO efforts that support civil-military operations to ensure deception plans do not inadvertently undermine the relationships with the civilian population or with host-nation military authorities. Failure to consider civil-military operations could compromise deception plans or have other unintended consequences.

## COORDINATION REQUIREMENTS

2-123. MDOs coordinate both deception and its supporting actions with higher, adjacent, subordinate, and supporting staffs. Within a staff, coordination is required between MDOs and other planners and analysts on the staff. Coordination with U.S. Government department and agency personnel prevents destabilizing civil-military relationships and an unintentional compromise of deception plans. This coordination has increased importance in situations in which the media or general public view deception.

2-124. It is important to restrict knowledge of information relating to planned and ongoing MILDEC operations to only those personnel who need to know. The commander provides guidance concerning the dissemination of deception-related information. During multinational operations, the staff informs the commander of information requirements and concerns of the non-U.S. partners. During planning, MDOs 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.

2-125. When deception plans incorporate or involve multinational partners, the command's foreign disclosure officer helps determine appropriate access to deception information and operations. For further information on multinational personnel access to deception plans, refer to CJCSI 3211.01.

## RISK ASSESSMENT

2-126. The evaluation of the risks associated with conducting a deception does not end with the commander's decision to adopt a particular COA. In planning, commanders use risk assessment to determine the potential consequences of deception failure or compromise and the consequences of unintended effects of the deception.

2-127. As planning progresses, the MDO refines the risk assessment as each element of the plan is detailed and aligned with the current situation. For example, the execution of a required observable by an electronic ruse instead of by a demonstration conducted by a combat unit may reduce the risk to command resources. Throughout the course of the deception planning process, MDOs must note significant changes in risk to the commander and staff so their impacts can be assessed and accounted for in operational planning. The staff records results of risk analysis during planning. The MDO then develops risk mitigation measures to ensure risk remains within acceptable levels to the commander.

2-128. The MDO develops a risk assessment for the finalized deception plan under conditions prevailing at that time. That risk assessment must be clearly presented during the approval process so the commander can make a well-informed decision on whether to approve and execute the deception operation or not. If the deception plan is not immediately implemented, the MDO continues to monitor risk to account for implications of changes in the situation.

This page intentionally left blank.

# Chapter 3
# Preparation and Execution

## PREPARATION

3-1. During preparation, planners take every opportunity to refine the deception plan based on updated intelligence and friendly information. Deception plans are not static and are continually adjusted. As assumptions prove valid or invalid, staffs confirm enemy perceptions, or the status of friendly units change, the MDO adjusts the deception for the commander or recommends aborting it if the deception can no longer significantly influence the situation and achieve the deception goal. As part of the plan, OPSEC activities also continue during preparation for the deception. OPSEC is a dynamic effort that anticipates and reacts to enemy collection efforts.

3-2. MDOs coordinate the deception plan with every other aspect of the OPLAN. This coordination still occurs with those only who have a need to know. The complexity of deception, its secrecy, and its many witting and unwitting links within the staff and across operational forces requires careful coordination of the deception plan with overall planning. Coordination also occurs with specific staff entities. Close coordination with operations and intelligence planners is driven by the essential nature of their contribution to the deception planning process, but most other elements of the staff have a less direct relationship.

3-3. During deception planning, OPSEC is a necessary condition and a critical planning requirement. The planning process itself must be secure, with no inadvertent disclosures due to carelessness in staff work or coordination. At the same time, planning must ensure that security is built into and maintained throughout the deception operation. This security reduces the risk of compromise and protects activities and units involved in the deception, particularly unwitting participants.

## EXECUTION

3-4. The deception plan forms the basis for execution, but execution may occur in conditions more dynamic than anticipated. Consequently, the deception plan is subject to continual reassessment and refinement. By its nature, little flexibility exists in the concept of operations for deception. Successful monitoring involves knowing precisely when to take the next step in conveying the deception story. MDOs often identify specific operational feedback events identified in the plan to provide these cues. IO officers are critical in assessing and deciding the timing, frequency, and means through which an observable is transmitted to achieve the desired cognitive effect on the deception target.

### DECEPTION EXECUTION

3-5. Deception execution includes the following activities:

- Adjust the deception plan as necessary for changed conditions.
- Sustain deception synchronization with an approved COA and OPSEC plan.
- Sustain internal deception synchronization between the planning team and commander.
- Sustain intelligence collection during deception execution.
- Monitor, assess, and mitigate risk.
- Keep the commander informed.
- Maintain strict security and access controls throughout.

## Adjust the Deception Plan as Necessary for Changed Conditions

3-6. The cycle begins with a review of the plan. In this step, the MDO analyzes the situation and operational environment, and reviews anticipated conditions and planning assumptions against which the plan was developed. Existing RFIs are reemphasized, and new RFIs are developed to address shortfalls in necessary intelligence.

3-7. During this step, the MDO reviews and identifies any changes to the enemy situation. Changes can include—

- Adjustments to the enemy decision-making process or key military decision makers.
- Changes in enemy force structure, capabilities, disposition, and intelligence collection efforts (conduits or information pathways) to best facilitate the effective delivery of the deception story.
- Changes in third-party intelligence support.
- Potential new sources of open-source intelligence based on rapidly evolving social media or other networks.

3-8. The MDO also reviews and identifies changes to the friendly plan. Changes can include—

- Revised strategic or commander's guidance.
- Changes to allocated forces.
- Changes to relationships with multinational partners.
- Changes to basing or adjustments to operational phasing or timing.

The MDO coordinates with the G-3 on initial deception and operations execution timing to ensure a synchronous, supporting relationship exists that will aid the deception, the operation, or both.

3-9. Once the MDO has updated knowledge of the enemy and friendly situations, all key elements of the plan—from the deception goal and objectives through the final deception event schedule—are validated or adjusted as required. While this is the first step in deception execution, this process of analysis and adjustment continues as conditions evolve and change over the course of mission execution.

## Sustain Deception Synchronization with the OPSEC Plan

3-10. The MDO continuously coordinates vertically and horizontally with commanders and staffs to synchronize real-world operations and deception operations. This coordination helps portray a credible, believable, and realistic deception. Changes to any operational aspect—such as presence, capability, strength, intent, readiness, future location, timing, or method of planned friendly operations—require accountability in the scheduled execution of deception activities. Such accountability requires the MDO to maintain situational awareness, participate in meetings that address targeting and assessments, and provide routine updates and operational analysis to the commander. The MDO works with the OPSEC planner to monitor critical information and indicators throughout the operations as well as recommend changes to DISO plans.

3-11. MDOs have a special responsibility to keep deception and OPSEC closely synchronized. Both deception and OPSEC work closely together in the holistic portrayal of friendly activities. Deception activities often receive support from focused OPSEC measures and countermeasures that protect their existence. This support includes close cooperation in the targeting or exploitation of enemy conduits so they are either neutralized or available as required to create the desired OPSEC and deception effects.

## Sustain Internal Deception Synchronization Between the Planning Team and Commander

3-12. Deception executions, while planned in detail, do not remain static activities on an access-controlled deception event schedule or operational-level synch matrix. The MDO maintains constant communication with internal components, capability owners, and other resource providers tasked to execute or support each event so the portrayal of the deception story proceeds as planned. This includes operational-level tasks—such as synchronizing different deception lines of effort and balancing or shifting lines of effort as appropriate—to sustain the desired story progression. Based on feedback, the MDO may adjust, repeat, postpone, or cancel some planned executions or event series.

### Sustain Intelligence Collection during Deception Execution

3-13. Working with the G-2 collection manager enables internal synchronization of the deception plan. This helps ensure information collection assets are in position to collect MOPs and monitor MOEs and indicators as outlined in the plan. This synchronization also informs the commander on its status, current levels of success, and revised risk. During combat operations in particular, the MDO actively monitors intelligence collection.

### Monitor and Assess for Compromise and Counterdeception

3-14. Using the target feedback provided by MOEs collection, in conjunction with the assessment process, the MDO determines the current progression and success of the deception plan. Specially trained intelligence analysts, supported by MDOs, remain alert for indicators of compromised components of a deception story. Compromise includes the identification of any possible enemy counterdeception efforts. Deception compromise, when detected, may lead to one or more termination or exploitation scenarios.

### Keep the Commander Informed

3-15. The status of the deception operation is part of the commander's routine battlefield update and assessment processes. As the principal authority for the execution of the plan, the commander has responsibility for any decision to alter, terminate, or change the deception or primary COA to exploit changing conditions. Deception also factors largely in the overall computation of operational risk. Increased risk might generate a requirement for adjustment to the plan in other areas.

### Maintain Strict Security and Access Controls Throughout

3-16. Effective forces practice tight security throughout execution to protect the deception plan and its execution. While commanders make many decisions in the planning process on a need to know basis, situations can arise that require external expertise or input, such as legal and policy interpretations. The commander decides who has a need to know and applies appropriate controls to limit the compromise of any deception. To decide, the commander, informed by the MDO, balances mission against prudent risk to determine security limits and parameters. In the intense and fluid activity of managing complex military operations, it becomes even more critical for all involved personnel to apply appropriate classification, handling, and access controls on a daily basis. Staffs should immediately report any OPSEC or other security violations of the deception plan at any level (strategic, operational, or tactical) to the MDO and OPSEC planner. They will evaluate the violation for potential impact.

## MANAGING THE EXECUTION OF THE DECEPTION PLAN

3-17. Once the commander orders the execution of the deception, staffs begin implementing the plan in a dynamic environment. The implementing order can require immediate execution, or it may provide an effective start date in coordination with other operations or events.

3-18. The MDO is the controlling planner for its execution. Continuity of key personnel as the deception moves from a plan to an actual operation ensures that the people executing the deception understand all its conceptual nuances, the inherent risks, and the underlying intentions and techniques behind each planned deception event. The controlling planner oversees the implementation of the specific deception events in accordance with the deception event schedule and continuously monitors the deception operation as part of the developing situation, evaluating the deception at each stage. The planner responds to developments with recommendations as to how the operation should proceed. As a result of the recommendations on the actual situation, the commander can add, delete, or modify scheduled deception events.

3-19. Because of the extreme sensitivity of deception plans, if the plan requires more than minor adjustments, the original approving authority must approve the revised plan before execution begins. Changes that impact the deception goal, the deception objective, or the commander's guidance should not be considered as minor. Before initiating the plan, planners refer any requirements for plan changes that affect earlier assessments of the probability of deception success or alter the degree of risk initially associated with the operation to the commander. However, planners can consider minor changes that involve the timing or sequence of individual

deception events based on actual operational conditions so long as they do not significantly alter the basic operational flow of the deception.

3-20. Once planners review and validate the deception event schedule and supporting worksheets, the controlling planner synchronizes the implementation of the plan. During implementation, participating units and resources normally receive tasks through traditional command operational and intelligence tasking channels. Occasionally, the controlling planner may directly engage participants outside the normal tasking channels when special communications channels are required to protect sensitive means and sources that reside outside normal command channels.

3-21. The controlling planner monitors feedback indicators at each stage and regulates the scheduling and intensity of deception operations. At times, the controlling planner may need to delay or accelerate planned deception events or, if the situation requires, add measures to achieve desired enemy perceptions in the time indicated by the commander's overall plan. The controlling planner informs the commander and the chief of operations of the status of all synchronization requirements associated with the execution of the deception. An inability to execute the deception with timing needs of other operations may prompt termination of a deception operation.

## Monitoring the Deception Operation

3-22. As with most plans, the quality of a deception plan directly relates to the validity of assumptions concerning the situation at the start of the operation. Validating such assumptions with current information is essential to any monitoring activity. Before starting the operation, staffs continually monitor the general situation and submit RFIs to confirm or deny assumptions concerning the conditions under which forces initiate the deception operation. Such pre-operational monitoring may prompt the start time for execution.

3-23. Four types of monitoring activities occurs for a deception operation (see figure 3-1). Monitoring the developing situation to ensure that the deception concept continues to correspond to actual conditions is the first activity. A second type of monitoring involves observing the effects of the deception operation at each stage of execution. This monitoring consists of obtaining the necessary feedback to trace the progress of the deception in line with the deception event and execution schedule. The third type of monitoring provides the means for assessing the need to terminate the deception operation for reasons other than mission accomplishment. The fourth type of monitoring activity detects and traces unintended consequences of the deception operation. Such consequences can be positive or negative and may involve either the deception itself or other operations. MDOs may use data on unintentional effects to adjust the deception or take advantage of new opportunities.

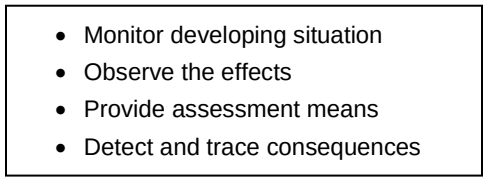



**Figure 3-1. Monitoring activities**

3-24. To achieve the level of synchronized activity that the deception operation demands, the controlling planner monitors the general military situation together with the systematic execution of the deception. The controlling planner also understands and evaluates the status of the deception operation in the full context of the overall operation as well as how deception activities are proceeding. At the same time, MDOs keep higher command echelons that direct and coordinate theater-wide and strategic deception operations informed regarding the execution of the command's deception.

## Controlling the Deception Operation

3-25. Although monitoring requirements are extensive, control remains the central issue of execution. Control involves making decisions to conduct each activity as specified by the plan or to change the plan to

align it to changes in the situation or the target's responses. Terminating the deception is the final control action in the execution of the operation.

3-26. Control consists of the series of implementing decisions and actions undertaken during the course of a deception operation. MDOs project many of these activities during the planning stage as a part of the natural progression of events envisioned in the deception event and execution schedule. Other decisions are dictated by the course of events revealed during monitoring. Centralized control over deception activities is imperative to ensure synchronous operations and the integration of deception in a manner that does not conflict with other operations. This principle requires close coordination among deception support elements operating at various levels of command. Authority to implement changes to various aspects of the deception operation must be specified in the deception plan.

3-27. Throughout the execution of the deception plan, the controlling planner remains prepared to support the commander with sound recommendations when operations reach decision points. If the deception plan has a progression of specific phases, with each new phase contingent on the success of the preceding phase, and the commander's approval is required for the execution of each phase, then the commander will need to know the specific status of the deception operation at each approval phase. If it becomes apparent that the deception story is not being successfully transmitted, the deception story is not eliciting the desired action from the target, or the deception is not synched with larger operational requirements, then the controlling planner may recommend to the commander to adjust the operation to fit alternative opportunities or to terminate it. If the assessed operational risk increases during the execution, the controlling planner addresses this change with the commander and provides a recommendation as to how the operation should proceed.

## TERMINATING MILITARY DECEPTION OPERATIONS

3-28. The termination of a deception is concerned with ending the deception in a way that protects both the short- and long-term interests of the command. Planners rarely know in advance the exact circumstances that will require termination of a deception plan. Consequently, termination preparations are a continuous process that span the planning and execution of the deception. When the commander decides to terminate, the termination concept that planners developed and refined during previous phases becomes the basis for a deliberate series of termination actions. These actions are designed to advantageously end the operation while protecting employed means and techniques.

3-29. The actions involved in termination include—

- The organized cessation of deception activities.
- The protected withdrawal of deception means.
- After action assessments and reports.

All three actions of termination occur whether or not the operation achieves its objective and whether or not the deception plan remains concealed. In developing the deception plan, planners determine conditions and provisions for the termination of the operation. The termination concept outlines alternative reasons and methods for terminating the operation, such as indications that the deception objective will not be reached or operational situations indicating that the goal is no longer valid. Termination planning anticipates the commander's need to avoid the compromise of deception means and methods, and it anticipates the levels of risk acceptable to sources and means before recommending termination.

3-30. When the commander orders termination, 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. Termination of a deception also encompasses evaluation and reporting. After action assessment should be conducted by the MDO. This assessment provides the commander with an objective basis for determining the degree of mission success and for improving future deception plans. Because important information on various elements of the deception may continue to become available over a long time, a series of interim after action reports may be required before making a final assessment. The after action report provides a comprehensive overview of the deception as it was planned to work and actually conducted.

This page intentionally left blank.

# Chapter 4
# Assessment

## ASSESSMENT RESPONSIBILITIES

4-1. One primary responsibility of the MDO involves assessing the effectiveness of deception and DISO in achieving supported command objectives. Assessment is the continuous monitoring—throughout planning, preparation, and execution—and evaluation of the current situation to measure the overall effectiveness of the operation. An essential and resource-intensive aspect of any successful deception, MDOs consider assessment from the initiation of planning. Planners avoid developing deception objectives that cannot be associated with a progressive and observable enemy response into a more detailed deception concept or subsequent execution. Deception is assessed in the same manner as other operations: using MOPs to determine if a deception event was executed according to plan and using MOEs to determine if the event created the desired impact or effect. In deception, MOPs involve everything up to and including delivery of the observable (filtered or unfiltered) to the deception target.

4-2. Accurately assessing MOEs for deception is complicated by the fact that MDOs need to measure desired changes in perception, as well as the action or inaction manifested by their success. MDOs develop MOEs that measure effectiveness, efficiency, and adaptability using the following guide:

- **Appropriate**: MOEs should correlate to the target's objectives.
- **Mission-related**: MOEs must correlate to the mission.
- **Measurable**: Quantitative MOEs reflect reality more accurately than qualitative MOEs, and hence, are generally the measure of choice when the situation permits their use.
- **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.

4-3. Because of this complexity, a detailed assessment plan accompanies each planned deception event. A detailed assessment plan includes MOPs, MOEs, and coordination with the G-2 for information collection assets to collect and report indicators in real time. Every assessment plan begins with a baseline—the point from which assessments are measured. Planners can generate a baseline from an initial survey, poll, or estimate or establish a baseline from a specific time or event.

4-4. The MDO also has responsibility for continually reassessing the deception objective, target, story, and events to ensure they are still important to the achievement of the mission objectives. Monitoring activities include, but are not limited to—

- Monitoring and evaluating the deception to ensure it continues to support operations.
- Evaluating how the target is acting or not acting in response to the deception story.
- Monitoring for unintended consequences resulting from the deception.
- Determining when termination criteria are met.

4-5. Planners consider how to assess a deception plan at the start of the planning process. A plan to assess a deception informs the commander if the operation is being executed as planned and achieving the desired results. As part of the evidence-based approach to decision making, assessment is integral to the planning process, and it must be designed as part of the initial planning process once the commander's intent has been articulated. By integrating assessment into the planning cycle, staff can identify potential second- and third-order effects and unintended consequences.

# ASSESSMENT PLAN

4-6. An MDO develops an assessment plan using the following steps:

- Design an assessment plan.
- Develop a data collection plan and an analysis plan.
- Collect and treat data.
- Analyze, interpret, and make recommendations.

## DESIGN AN ASSESSMENT PLAN

4-7. An MDO designs an assessment plan at the initial planning phase of the operation. This should be integral to the planning process. Assessment design typically uses two types of feedback:

- **Target feedback**: information, analytical determinations, and evidence (MOEs) that the target is acting or preparing to act on the deception.
- **Conduit feedback**: information and evidence (MOEs) that the conduits receive, process, and transmit to elements of the deception. This feedback is also referred to as operational feedback.

An effective design includes indicators of whether the target is receiving the deception story as planned. It also includes indicators of whether the target is acting in accordance with the deception objective.

## DEVELOP A DATA COLLECTION PLAN AND AN ANALYSIS PLAN

4-8. An MDO designs a collection plan during the planning phase of the operation. This not only articulates the procedure by which indicators should be collected, but also the time-sensitive monitoring of indicators as they relate to the measurable outcome. Alongside the collection plan, MDOs design an analysis plan at the initial stage of deception planning. This analysis plan identifies the analytical techniques used to analyze the collected evidence.

## COLLECT AND TREAT DATA

4-9. The DWG continuously collects and treats data during the execution phase of the operation. First, the group establishes a baseline prior to the execution phase beginning and continuously monitors the collection plan. All assessments require a baseline. A pre-operation baseline is used to gauge progress during the operation against eventual outcomes post-operation. If the deception plan does not establish a baseline, the staff cannot determine what has changed as part of the deception plan or understand eventual success or failure.

## ANALYZE, INTERPRET, AND MAKE RECOMMENDATIONS

4-10. The DWG continuously analyzes, interprets, and makes recommendations during the execution phase of the operation, but a final assessment after the operation is required. If the MDO designed the deception plan correctly—with a robust analysis plan based on a mixed methods approach to collect and monitor the necessary evidence—then the final assessment should be robust. This is important as the final assessment informs the realization of the effect being sought as part of the overall OPLAN. The deception assessment contributes to the overall evidence that informs the commander's decision-making process.

# MEASURES OF EFFECTIVENESS AND MEASURES OF PERFORMANCE DEVELOPMENT

4-11. The development of deception MOEs and MOPs differs slightly from similar processes for other capabilities. One way to easily conceptualize MOEs and MOPs for deception involves using the see-think-do methodology. MOEs are associated with *think* and *do*: what perceptions and conclusions did the enemy draw from a particular observable (alone or in the context of other observations)? Are those perceptions leading toward the desired action or inaction captured in a deception objective? MOPs are most closely associated with *see*: did friendly forces portray the planned indicator? Did the enemy see the execution and transmit the desired message to the deception target creating an observable?

4-12. MOE development and collection for deception focuses on the current cognitive state of the deception target. The enemy's cognitive state can be measured in one of two ways. First, it uses the evaluation of known comments or public statements by the decision maker. Second, it identifies and monitors the flow of enemy (particularly the target's) activity to determine patterns of behavior that indicate the deception target's susceptibility to being moved toward the desired perception and subsequent action or inaction. The baseline provides the first indication that friendly forces can affect the target in the manner that meets the desired effect. However, the knowledge of this activity occurring or not occurring may not be easily available or discernible. Sometimes, it will manifest itself at the very moment a particular effect in the deception plan is required; thus, the controlling planner remains vigilant to indicators that suggest the current cognitive state of the target has in some manner changed.

4-13. MOP collection for deception involves two conceptual steps:

- Determining that the tasked friendly unit or capability employed the desired means to create an indicator at the appropriate time and location.
- Verifying that the intended enemy conduits cued on the friendly signature, transmitted the collected data, and delivered the information to the deception target in a discernable context.

These two steps define the difference between a deception MOP and a traditional MOP (one that asks if friendly forces performed the directed action). Part of every successful deception execution involves action by the enemy. The conduit that the deception seeks to exploit must function.

4-14. MDOs determine a deception event schedule from reporting channels. The MDO coordinates this reporting with the element controlling a particular execution as a part of finalizing the plan for appropriate access and security controls. Verifying that the enemy conduit functioned as planned and that the desired information reached the deception target requires focused and coordinated intelligence, surveillance, and reconnaissance support. Using their previous conduit analysis work, MDOs, supporting intelligence analysts, and the intelligence collection manager collaborate. They identify points at which the information transmission might fall susceptible to enemy monitoring and analysis. The presence of filters in the conduit pathway makes this verification process difficult because predicting the level of data aggregation or synthesis with other friendly observables is subjective at best. In some cases, the appearance of an anticipated MOE might be the only validation that a persuasive observable was accurately received and perceived.

4-15. To provide the commander with the information to adjust plans as needed based on timely MOEs, the G-2 and MDO coordinate. For example, if one deception objective is for the enemy to hold the armored reserve away from the decisive point of ground action, then MDOs develop MOEs related to achieving that objective. MOE examples related to the action or inaction of the reserve might include such things as—

- An increase or decrease in preparation of defensive positions (implying a period of static activity).
- An increase or decrease in enemy intelligence collection in the vicinity of a friendly main axis of advance at the expense of other sectors (is the enemy "telegraphing" an interest?).
- An increase or decrease in route reconnaissance toward the friendly sector by armored reserve units or leadership (is this pending or an active branch plan?).
- An increase or decrease in battle drill or movement rehearsal by the enemy reserve.

4-16. Without the close support of the G-2 and a deliberate focus on the development of viable MOEs and MOPs as part of the deception plan, the success or failure of the deception might not be known until the moment that a planned enemy action or inaction is turned against friendly forces. This could result in a loss of initiative or increased friendly loss of life.

This page intentionally left blank.

## Appendix A

# Counterdeception

## COUNTERDECEPTION PLANNING

A-1. Enemies can use deception to mislead friendly analysts and decision makers about their activities, capabilities, or intent to offset a friendly superiority or gain some other operational advantage. *Counterdeception* is efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation (JP 3-13.4). Successful friendly decision makers know of enemy deception activities to formulate informed and coordinated responses and, more importantly, avoid placing friendly forces at an operational disadvantage. Counterdeception contributes to situational awareness by protecting friendly systems and decision makers from responding to deceptive manipulation or faulty analysis of an operational environment. Counterdeception applies across the range of military operations in which enemies might use deception in an attempt to alter friendly activities or even achieve operational surprise during hostilities.

A-2. Knowledge of an enemy's deception plan enables a commander to act appropriately against the deception. It provides friendly forces an opportunity to gain valuable insight into the means used to portray the deception. It also provides friendly forces a chance to analyze enemy deception targets and objectives as indicators of the broader context in which the enemy views friendly forces and operations. Counterdeception becomes a tool for influencing those perceptions and could subsequently be turned effectively against the enemy.

## DETECTING ENEMY DECEPTION

A-3. The intelligence warfighting function plays a central role in identifying enemy deception operations. MDOs can assist in this effort. Trained deception personnel should be postured and have access to information, intelligence data, analytical support, and intelligence products during the deployment and execution of friendly operations. To identify enemy deception, trained deception personnel must first understand the enemy's deception doctrine, techniques, capabilities, and limitations. Knowing previous methods the enemy has used deception is also important. The MDO collaborates with the G-2 to collect and provide this information as part of the deception running estimate. Understanding the enemy's operational objectives; normal operational profiles; posture; tactics, techniques, and procedures; and intent are also crucial to identifying tactical or operational indicators of possible deception. The MDO can use the friendly OPSEC doctrinal construct of signature, association, profile, contrast, and exposure to assess enemy activity for its congruency with known patterns or expectations based on the evolving operational situation. Indicators of potential deception can range from a dedicated analyst's intuitive sense that "something is amiss" to the outright compromise of deceptive means, methods, or activity by friendly intelligence collection assets. Properly balancing tactical and operational indicators with strategic assumptions is also important. Planners can reduce potential surprise if their estimates weigh tactical indicators more heavily than strategic assumptions in some phases of the operation. Dismissing tactical indicators or other minor contrasts because they conflict with friendly biases and preconceptions may allow a hostile deception to succeed.

## CONFIRMING ENEMY DECEPTION

A-4. If intelligence reveals or suggests an enemy deception activity, the staff must fully analyze the situation and ensure that this intelligence and its potential impact on the friendly operation are presented to the commander. One method to analyze the situation involves forming a working group to analyze, review, and determine the deceptive activity. This working group could include the MDOs, G-2 analysts, red team members, G-3 planners, and others with knowledge of suspected enemy deception means or methods. If it has not already been done, the working group analyzes vulnerability to enemy deception using the physical, informational, and cognitive dimensions. The group then uses information and intelligence available through

the intelligence enterprise to determine the enemy deception plan. Using the deception planning methodology of see-think-do, the working group might use an abbreviated war-gaming process to construct enemy deception goals and objectives, targets, desired perceptions and deception story narrative, probable events and means, conduits, and anticipated MOEs. Deception planners then use outputs of this technique to focus friendly intelligence collection assets that confirm or deny the existence and scope of an actual enemy deception plan and related executions.

# COUNTERING OR EXPLOITING ENEMY DECEPTION

A-5. After confirming an enemy's deception operation, the working group has two primary functions. It first examines past information collection, intelligence production, and intelligence analysis to determine the impact the deception may have had on friendly planning, decision making, or current operational activities. The outputs of the working group inform future COAs or counterdeception planning. Second, the working group develops and presents proposed counterdeception COAs to the commander. Each COA involves a different level of risk or opportunity that must be weighed in the overall context of the operation and commander's desired end state. Based on risks, commanders can ignore, expose, exploit, or defeat enemy deception efforts.

A-6. Commanders ignore the deception if acknowledging the deception compromises friendly deception identification capabilities. Such a compromise of friendly capabilities might lead to future improvements in enemy deception capabilities. This scenario requires a working group to continue to identify deceptive indicators and base the friendly force operational decision making and subsequent activity on actual enemy capability, activity, or intent.

A-7. Commanders might choose to publicly expose the deception to embarrass the enemy or increase risk within an enemy's operational cost and benefit analysis. Through exposure, the enemy might be persuaded that its deception operations are futile, too costly, or too risky to continue. Exposure of a deception prior to combat operations might also serve to weaken the enemy's political or military position with allies or domestic audiences.

A-8. An exploitation of enemy deception focuses on forcing an enemy to expend resources and continue deception operations by reinforcing the perception that friendly forces are unaware of the deception. In this scenario, friendly forces provide positive MOEs that the deception is having the desired effect until the culminating point of the enemy's deception (their desired "do or not do" for one friendly operational capability) and then reacting in an unexpected manner that turns the enemy's anticipated advantage against itself.

A-9. Defeating the enemy deception effort could involve destroying or degrading the enemy's deception capabilities and resources so it cannot sustain its portrayal of the deception story. Like the other potential COAs, this outcome ideally includes a war-gaming step to identify possible second- and third-order effects and associated risk.

# Appendix B
# Input to Operation Plans and Orders

## APPENDIX 14 (MILITARY DECEPTION) TO ANNEX C (OPERATIONS) DIRECTIONS

B-1. Appendixes are information management tools. They simplify orders by providing a structure for organizing information. FM 6-0 discusses the organizational structure for appendixes to Army to OPLANs and OPORDs. Staffs list appendixes under an appropriate heading at the end of the document they expand. For example, Appendix 14 (Military Deception) is to Annex C (Operations). This appendix describes how deception supports operations described in the base plan or order. Some additional considerations for writing the Appendix 14 include the following:

- Access to Appendix 14 is typically on a need to know basis, which means limiting access to those individuals who are involved in planning, approving, or executing deceptions and must have knowledge of the military deception to perform their duties.
- The deception appendix will normally be developed, published, distributed, and maintained separately.
- Staffs do not use normal administrative procedures to distribute or staff the deception appendix. Only positive control means, such as hand-to-hand delivery, will be used to distribute deception related material.

## APPENDIX TEMPLATE

B-2. Commanders and staffs use Appendix 14 (Military Deception) to Annex C (Operations) to OPLANs and OPORDs to describe how deception will support operations described in the base plan or order. See figure B-1 for a sample format instructions. The italicized font in figure B-1 explains the information that commanders and staffs complete.

**MILITARY DECEPTION**

**References**: List documents essential to this tab.
a. Maps and charts
b. Other relevant documents
Task Organization: (If applicable)

*Information and intelligence provided here must be focused and plan-specific. Do not reiterate information available in the base plan.*

**1. Situation**. *Summarize situational information relevant to the execution of the deception*.

a. General. *Identify the overall purpose of the deception plan. In one paragraph briefly identify the commander's intent in employing deception—what the deception plan is designed to accomplish. Specifically identify the friendly operation it will support. Identify any phasing for the conduct of operations. Briefly state the expected results if the plan is successful.*

b. Enemy.

**Figure B-1. Sample Appendix 14 (Military Deception) to Annex C (Operations)**

(1) Enemy Intent. *Identify the assessed enemy goal or condition (favorable or unfavorable, as perceived through the opponent's perspective) that this deception plan is designed to counter or exploit.*

(2) General Capabilities. *Identify significant enemy military capabilities that can affect the overall operations in general and the deception plan in particular.*

(a) Enemy Intelligence Organizations. *Identify intelligence organizations, missions, and capabilities for covert and clandestine operations. Include collection, processing, analysis, and dissemination. Specifically note those organizations most likely to provide intelligence to the targeted decision maker and those tasked with exposing deception.*

(b) Enemy Counterintelligence Organizations. *Identify enemy missions, capabilities, and operations.*

(c) Enemy Intelligence Sharing with Other Countries. *Identify other intelligence organizations available to the enemy, the nature of intelligence exchange, and the potential for using that relationship for the deception.*

(d) Other Sources and Related Matters. *Identify scientific, technical, diplomatic, or academic contacts that might act as information conduits.*

(e) Enemy Deception and Denial Activities. *Provide an analysis of the enemy's use of deception and denial supporting its political and military goals. Identify the enemy's deception and denial methods as well as current deception and denial activities.*

(3) Deception Targets. *Describe the decision maker targeted by the deception plan. Include personality, strengths, weaknesses, vulnerabilities, and people or factors known to influence decisions.*

(4) Target Biases and Predispositions. *Briefly describe those biases and predispositions of the target that the deception plan is targeting for exploitation.*

(5) Probable Enemy Course of Action. *Refer to Annex B.*

(6) Enemy Ability to Respond. *Discuss the ability of the target to respond to the deception. Discuss how the enemy has previously responded to similar events, conditions, and circumstances.*

(7) Probable Enemy Courses of Action without the Deception. *Discuss probable enemy courses of action and their possible results if deception is not used.*

c. Friendly. *Summarize the friendly situation, critical limitation, and concept of operations.*

(1) *Provide information on activities by unwitting friendly forces having an impact on the deception. Compare the time necessary to collect, process, report, and analyze intelligence (in support of deception) with the plan's operational timeline. Assess the impact here.*

(2) *Identify required capabilities and capacities for collection and identify shortfalls. Consider current collectors' actual capacities in relation to the projected volume of information requirements.*

d. Assumptions. *State the assumptions concerning friendly, enemy, or third-party capabilities, limitations, or courses of action. State conditions that the commander believes will exist during execution.*

e. Information Requirements.

**Figure B-1. Sample Appendix 14 (Military Deception) to Annex C (Operations) (*continued*)**

(1) *Identify requirements, including those of subordinate commanders, for pre-execution and execution phases of the planned operation.*

(2) *List questions and answers required for further planning and as a basis for decision on execution.*

(3) *List the additional priority intelligence requirements and other intelligence requirements that become relevant upon execution. (Use additional paragraphs if necessary to reflect differing requirements during planned phases of the operation.)*

**2. Mission**. *Identify the task and purpose for the deception.*

a. Operational Mission. *Briefly state the operational mission that the deception operation supports.*

b. Deception Mission. *Briefly identify the general purpose of the deception mission, including the desired actions that the deception target is expected to take. Identify how friendly capabilities, situations, conditions, or operations will be improved or protected if the target commits the desired actions.*

(1) Deception Goal. *Precisely state the commander's purpose of the deception operation as it contributes to the command's mission objectives.*

(2) Deception Objectives. *Precisely state the intended effect of the deception on the target in terms of the specific action or inaction the deception operation is expected to elicit from the target. State, exactly, what friendly forces want the target to do or not to do with its forces, capabilities, and operations.*

(3) Enemy Perceptions. *Precisely identify the key conclusions, estimates, or assumptions that the target will have to accept as being true in order for it to act in accordance with the deception objective.*

(4) Deception Story. *Briefly outline the friendly actions to portray to cause the deception target to acquire the desired perceptions. The deception story is presented in a style that replicates what the target would expect to read in his own intelligence estimates of the "enemy" situation (typically no more than a short paragraph).*

**3. Execution**.

a. Concept of Operations. *Identify how the deception operation supports the commander's overall concept of operations. Describe how the deception is integrated into the supporting plan. If applicable, list how the deception operation will be phased.*

(1) General. *Generally describe the framework for the operation. Include a brief description of the phases of the deception.*

(2) Other Capabilities or Activities. *Discuss the use of other capabilities and activities in support of the deception plan. Discuss all other capabilities and activities plans and operations pertinent to the deception. Include coordination required to deconflict if necessary.*

(3) Feedback and Monitoring. *Provide a general statement of the type of feedback expected, if any, and how it will be collected (monitored). Identify the effect of no feedback. Identify the friendly capability to identify and collect plan-specific feedback information.*

(a) Operational Feedback. *Identify specific intelligence operations and indicators that will be monitored to determine if deception events are being sensed by enemy intelligence collection, analytical, or dissemination systems.*

**Figure B-1. Sample Appendix 14 (Military Deception) to Annex C (Operations) (*continued*)**

(b) Analytical Feedback. *Identify specific expected actions or inactions.*

(4) Executions to be Conducted and Means. *Briefly outline the general framework for the deception operation and the means to employ. Identify and provide a general description of the types of executions and means used to portray them for each operational phase. If applicable, include the timelines for major phase executions. Use the deception event schedule to describe specific executions and events in order.*

(5) Risks. *Give a brief risk analysis in the categories given below. Rate risk as low, medium, or high in each category.*

(a) Deception is successful. *Include likely enemy response. Describe impact on friendly forces from enemy intelligence sharing.*

(b) Deception fails. *Describe the impact if the target ignores the deception or fails in some way to take the actions intended.*

(c) Deception is compromised to allies or enemies. *Describe impact on friendly forces from enemy intelligence compromise.*

(6) Termination. *Provide detailed instructions on conditions for termination, actions to be taken (must be reflected in Exhibit 2 (Execution Schedule)), or emergency if there is unintended disclosure or compromise. Focus on the termination "story" to be used if the deception succeeds, is compromised, or is ended by the friendly commander.*

b. Tasks. *Specify execution and feedback tasks to organizations participating in the deception operation. Identify how collection managers will support planners and analysts.*

c. Coordinating Instructions. *Identify any tasks or instructions pertaining to two or more of the units listed in the preceding subparagraphs. List the tentative D-day and H-hour, if applicable, and any other information required to ensure coordinated action between two or more elements of the command.*

**4. Administration and Logistics**. *State instructions regarding administrative and logistics support procedures used in developing, coordinating, and implementing the deception plan. Do not include those administrative, logistics, and medical actions or ploys that are an actual part of the deception operation.*

a. Administration.

(1) General. *Outline general procedures to be employed during planning, coordination, and implementation of deception activities.*

(2) Specific. *Detail any special administrative measures required for executing the deception plan.*

b. Logistics. *Detail logistics requirements required for executing such as the transportation of special material or provision of printing equipment and materials. Do not include executions conducted by logistics elements as part of the portrayal of observables.*

c. Costs. *Note if applicable.*

**5. Command and Control**.

a. Command Relationships.

**Figure B-1. Sample Appendix 14 (Military Deception) to Annex C (Operations) (*continued*)**

(2) Authority. *Designate supported and supporting commanders as well as supporting agencies as applicable.*

(3) Oversight. *Detail oversight responsibilities particularly for executions by nonorganic units or organizations outside the chain of command.*

(4) Coordination. *Identify coordination responsibilities and requirements related to deception events and execution feedback. Address in-theater and out of theater requirements.*

b. Command, Control, Communications, and Computer Systems. *Detail communications means and procedures to be used by control personnel and participants in the deception plan. Include all reporting requirements.*

**6. Security**.

a. General. *Outline general procedures to be employed during planning, coordination, and implementation of deception activities.*

b. Specific. *State access restrictions, handling instructions, and authority to grant access to the deception appendix or plan. Describe use of cover stories if applicable, code words, nicknames, and procedures for planning and execution documents. If required, place access rosters and other detailed security considerations in a separate document. As a general policy, any material related to planned, ongoing, or completed deception is accorded controlled access. Address essential elements of friendly information, indicators to be managed, and protective measures.*

**Figure B-1. Sample Appendix 14 (Military Deception) to Annex C (Operations) (*continued*)**

This page intentionally left blank.

## Appendix C

# Deception Evaluation Checklist

## G-3 EVALUATION CHECKLIST

C-1. The G-3 completes an evaluation after a deception. The evaluation checklist can include the following questions:

- What integration of deception operations into tactical maneuvers occurred?
- Did the OPSEC annex support the deception annex?
- Was the deception annex to the OPLAN written to support tactical operations?
- Were individuals at all echelons identified and aware of their responsibilities in relation to deception activities?
- What were the required unit tasks?
- How was the deception annex coordinated? Was it complementary?
- Did it address a common list of indicators that required either display or concealment?
- Did other supporting annexes contain option choices addressed in the deception annex without alluding to deceptive intent?
- Does the deception annex address main and alternate COAs in the basic operational concept?
- Were surveys conducted of both concealed sensitive indicators (OPSEC) and displayed deceptive indicators to access visibility?
- What was the deception objective?
  - Did the deception objective closely support the objective of the tactical operation?
  - Did the deception objective support corresponding OPSEC objectives?
  - Were phase-out actions planned to disguise that deception was used?
  - Was an implementing schedule prepared?
  - Did the implementing schedule identify the start and finish times of event, location, unit involved, and means to be used?
- What was the deception story?
  - Was it employed as planned?
  - Did the deception story provide adequate information to deter the enemy from taking undesirable actions?
  - Was the story flexible enough to allow changes during its execution to take advantage of unexpected enemy actions?
- Did compromise of intent of deception or OPSEC activity occur?
  - If yes, what was the compromise?
  - If yes, did the compromise degrade the overall success of the operation?
- What were the essential elements of friendly information and were they integrated into the plan as specific, inherently low-visibility options? What options were chosen?
- What deception technique was employed?
  - Were communications-electronics deception and electronic counter-countermeasures or command, control, and communications protection measures planned for and used? What was the desired effect?
  - Were non-communications-electronics deception and electronic counter-countermeasures planned for and used? What was the desired effect?

  - If non-electronics deception techniques (reconnaissance, engineer activities, and so forth) were used, what was the desired effect of the techniques?
- What resources (personnel, equipment, and time) were tasked to conduct operations with deceptive intent?
- Were sufficient resources available?
- What was the experience level of deception element personnel?
- What specific deception items (dummies, decoys, and so forth) were constructed, used, and how? How many were used?
- What other resources or services were required? Were they available?
- What real missions could not be accomplished because these resources were being used for deception?
- Do the benefits of deception justify any loss of operational resources?
- Were dedicated, secured communications lines and other means of transmission of the plan available? Were they adequate?
- Was sufficient time available to formulate, write, and execute the deception and OPSEC plans?
- What were the results of deception activities?
- Did the deception assist in the successful execution of the overall operation?

# G-2 EVALUATION CHECKLIST

C-2. The G-2 completes an evaluation after a deception. The evaluation checklist can include the following questions:

- Were deception and OPSEC annexes to the OPLAN written to support tactical operations?
- Does intelligence have an established enemy database and an understanding of enemy doctrine?
- Was there awareness of enemy intelligence capabilities and collection schedules?
- What were the priority intelligence requirements and information requirements for the deception and OPSEC plans?
- What intelligence activities were targeted at discovering deceptions in progress against friendly forces?
- What intelligence activities were targeted to determine enemy reaction to friendly deceptions?
- What enemy activities were identified as being deception related? Why?
- What was the deception story?
  - At what level of the enemy organization was it focused?
  - Did the deception story cause the enemy decision maker to make the desired decision?
  - Was the story consistent with the friendly unit's tactical doctrine, established patterns, and normal operational sequences?
  - Was the story consistent with the target's perception of the friendly unit's real capabilities?
  - Did the story permit verification by various enemy collection systems?
- What countersurveillance techniques were used to deny the enemy knowledge of true intentions and evaluate indicator visibility?
- What were the essential elements of friendly information and were they integrated into the plan as specific, inherently low-visibility options? What options were chosen?
- What deception steps were employed?
  - If communications-electronics deception and electronic counter-countermeasures or command, control, and communications protection measures were planned for and used, what was the actual effect of these measures?
  - If non-communications-electronics deception and electronic counter-countermeasures were planned for and used, what was the actual effect of these measures?
  - If non-electronics deception techniques (reconnaissance, engineer activities, and so forth) were used, what was the desired effect of the techniques?

- Did the enemy's intelligence estimate of friendly capabilities warrant the use of deception with the expected expenditure of personnel and equipment?
- Was there adequate time for the enemy to observe the deception and react in a desired manner?
- What were the results of deception activities?
- Were intelligence means and indicators established to measure enemy reaction to the friendly unit's deception?

This page intentionally left blank.

# Source Notes

This division lists the source by page number.

1-8 Examples given in paragraphs 1-42 through 1-60 originated in the Central Intelligence Agency, Office of Research and Development, *Deception Maxims: Fact and Folklore* (Washington D.C.: Government Printing Office, 1980), 9–40.

This page intentionally left blank.

# Glossary

The glossary lists acronyms and terms with Army or joint definitions. The proponent publication for terms is listed in parentheses after the definition. The term for which FM 3-13.4 is the proponent is marked with an asterisk (*).

## SECTION I – ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **ADP** | Army doctrine publication |
| **ATP** | Army techniques publication |
| **CCMD** | combatant command |
| **CJCSI** | Chairman of the Joint Chiefs of Staff instruction |
| **COA** | course of action |
| **DA** | Department of the Army |
| **DISO** | deception in support of operations security |
| **DOD** | Department of Defense |
| **DODD** | Department of Defense directive |
| **DODI** | Department of Defense instruction |
| **DODM** | Department of Defense manual |
| **DWG** | deception working group |
| **FIE** | foreign intelligence entity |
| **FM** | field manual |
| **G-2** | assistant chief of staff, intelligence |
| **G-3** | assistant chief of staff, operations |
| **G-5** | assistant chief of staff, plans |
| **IO** | information operations |
| **IRC** | information-related capability |
| **J-2** | intelligence directorate of a joint staff |
| **JP** | joint publication |
| **MDO** | military deception officer |
| **MILDEC** | military deception |
| **MISO** | military information support operations |
| **MOE** | measure of effectiveness |
| **MOP** | measure of performance |
| **OPLAN** | operation plan |
| **OPORD** | operation order |
| **OPSEC** | operations security |
| **RFI** | request for information |
| **S-2** | battalion or brigade intelligence staff officer |

| | |
|---|---|
| **TAC-D** | tactical deception |
| **U.S.** | United States |

## SECTION II – TERMS

**competing observable**

Within military deception, any observable that contradicts the deception story, casts doubt on, or diminishes the impact of one or more required or supporting observables. (JP 3-13.4)

**conduits**

Within military deception, information or intelligence gateways to the deception target, such as foreign intelligence entities, intelligence collection platforms, open-source intelligence, and foreign and domestic news media. (JP 3-13.4)

**counterdeception**

Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. (JP 3-13.4)

**deception event**

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

**deception goal**

Commander's statement of the purpose of military deception as it contributes to the successful accomplishment of the assigned mission. (JP 3-13.4)

**deception means**

Methods, resources, and techniques that can be used to convey information to the deception target. (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 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 3-13.4)

**deception target**

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

**decoy**

An imitation in any sense of a person, object, or phenomenon that is intended to deceive enemy surveillance devices or mislead enemy evaluation. (JP 3-13.4)

**demonstration**

In military deception, a show of force similar to a feint without actual contact with the adversary, in an area where a decision is not sought that is made to deceive an adversary. (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 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 3-13.4)

**diversion**

The act of drawing the attention and forces of an enemy from the point of the principal operation; an attack, alarm, or feint that diverts attention. (JP 3-03)

**electronic warfare**

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-13.1)

**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 3-13.4)

**human factors**

The physical, cultural, psychological, and behavioral attributes of an individual or group that influence perceptions, understanding, and interactions. (JP 2-0)

**indicator**

In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 3-13.3)

**information environment**

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

**information-related capability**

A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. (JP 3-13)

**link**

A behavioral, physical, or functional relationship between nodes. (JP 3-0)

**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. (JP 3-13.4)

**military information support operations**

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives. (JP 3-13.2)

**node**

An element of a system that represents a person, place, or physical thing. (JP 3-0)

**observable**

In military deception, the detectable result of the combination of an indicator within an adversary’s conduit intended to cause action or inaction by the deception target. (JP 3-13.4)

**operations security vulnerability**

A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. (JP 3-13.3)

**ruse**

In military deception, an action designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary’s intelligence collection system. (JP 3-13.4)

***tactical deception**

An activity planned and executed by, and in support of, tactical-level commanders to cause enemy decision makers to take actions or inactions prejudicial to themselves and favorable to the achievement of tactical commanders' objectives.

# References

All Websites were verified on 14 February 2019.

## REQUIRED PUBLICATIONS

Readers require these publications for fundamental concepts, terms, and definitions.

*DOD Dictionary of Military and Associated Terms*. January 2019.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

## RELATED PUBLICATIONS

These publications are referenced in this publication.

### JOINT PUBLICATIONS

CJCS issuances are available at https://www.jcs.mil/Library/. DOD issuances are available at https://www.dtic.mil/whs/directives/. Joint publications are available at https://jdeis.js.mil/jdeis/generic.jsp.

CJCSI 3211.01. *Joint Policy for Military Deception* (U). 14 May 2015. (This classified publication is available on the SIPRNET. Contact the preparing agency of this publication for access instructions.)

DODD 2311.01E. *DoD Law of War Program*. 09 May 2006.

DODI 3604.01. *Department of Defense Military Deception* (U). 11 March 2013. (This classified publication is available on the SIPRNET. Contact the preparing agency of this publication for access instructions.)

DODM 5200.01. *DoD Information Security Program: Overview, Classification, and Declassification Volume 1*. 24 February 2012.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-03. *Joint Interdiction*. 09 September 2016.

JP 3-13. *Information Operations*. 27 November 2012.

JP 3-13.1. *Electronic Warfare*. 08 February 2012.

JP 3-13.2. *Military Information Support Operations*. 21 November 2014.

JP 3-13.3. *Operations Security*. 06 January 2016.

JP 3-13.4. *Military Deception*. 14 February 2017.

### ARMY PUBLICATIONS

Army doctrine and training publications are available at https://armypubs.army.mil/.

ATP 3-37.34. *Survivability Operations*. 16 April 2018.

ATP 3-53.1. *Military Information in Special Operations*. 23 April 2015.

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.

FM 6-0. *Commander and Staff Organization and Operations*. 05 May 2014.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

### OTHER SOURCES

Geneva Convention and Hague Regulation (Article 23) at https://www.icrc.org/eng/assets/files/publications/icrc-002-0173.pdf.

Central Intelligence Agency, Office of Research and Development. *Deception Maxims: Fact and Folklore*. Washington DC: Government Printing Office, 1980.

*Department of Defense Law of War Manual*. 12 June 2015 at https://apps.dtic.mil/dtic/tr/fulltext/u2/1014128.pdf.

## PRESCRIBED FORMS

This section contains no entries.

## REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Website: https://armypubs.army.mil/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

## RECOMMENDED READINGS

Armstrong, LTC Richard N. *Soviet Operational Deception: The Red Cloak*. Fort Leavenworth, Kansas: Combat Studies Institute, U.S. Army Command and General Staff College, 1989.

Axelrod, Robert. "The Rational Timing of Surprise." *World Politics*, vol. 31, no. 2 (1979): 228–246.

Bittman, Ladislav. *Deception Game, Czechoslovakian Intelligence in Soviet Political Warfare*. Syracuse, New York: Syracuse University Research Corporation, 1972.

Brown, Anthony Cave. *Bodyguard of Lies*. New York: HarperCollins, 1975.

Cruickshank, Charles. *Deception in World War II*. New York: Oxford University Press, 1979.

Daniel, Donald C. and Katherine L. Herbig, editors. *Strategic Military Deception*. New York: Pergamon Press, 1982.

Dewar, Michael. *The Art of Deception in War*. New York: David & Charles, 1989.

Dunnigan, James F. and Albert A. Nofi. *Victory and Deceit; Dirty Tricks at War*. New York: Morrow, 1996.

Fisher, David. *The War Magician*. New York: Coward-McCann, 1983.

Gawne, Jonathan. *Ghosts of the ETO*. Havertown, Pennsylvania: Casemate Publishers, 2002.

Gerard, Philip. *Secret Soldiers: The Story of World War II's Heroic Army of Deception*. New York: Dutton, 2002.

Gerwehr, Scott and Russell Glenn. *The Art of Darkness: Deception and Urban Operations*. Santa Monica, California: Rand, 2000.

Glantz, David M. *Soviet Military Deception in the Second World War*. Totowa, New Jersey: Frank Cass, 1989.

Godson, Roy and James J. Wirtz. *Strategic Denial and Deception: The Twenty-First Century Challenge*. New Brunswick, New Jersey: Transaction Publishers, 2002.

Handel, Michael, editor. *Strategic and Operational Deception in the Second World War*. Totowa, New Jersey: Frank Cass, 1989.

Handel, Michael, editor. *War, Strategy and Intelligence*. Totowa, New Jersey: Frank Cass, 1989.

Hartcup, Guy. *Camouflage: A History of Concealment and Deception in War*. New York: Scribner's, 1980.

Haswell, Jock. *D-Day: Intelligence and Deception*. New York: Times Books, 1979.

Haswell, Jock. *The Tangled Web: The Art of Tactical and Strategic Deception*. Wendover: John Goodchild Publishers, 1984.

Hesketh, Roger. *Fortitude: The D-Day Deception Campaign*. Woodstock, New York: Overlook Press, 2002.

Holt, Thaddeus. *The Deceivers: Allied Military Deception in the Second World War*. New York: Scribner, 2004.

Howard, Sir Michael. *British Intelligence in the Second World War: Strategic Deception*. Vol. 5. New York: Cambridge University Press, 1989.

Huber, Dr. Thomas M. *Pastel: Deception in the Invasion of Japan*. Fort Leavenworth, Kansas: Combat Studies Institute, U.S. Army Command and General Staff College, 1988.

Jones, R. V. *The Wizard War: British Scientific Intelligence, 1939-1945*. New York: Coward, McCann, & Geoghegan, 1972.

Lloyd, Mark. *The Art of Military Deception*. London: L. Cooper, 1997.

Macintyre, Ben. *Operation Mincemeat: How a Dead Man and a Bizarre Plan Fooled the Nazis and Assured an Allied Victory*. New York: Harmony Books, 2010.

Mahl, Thomas. *Desperate Deception: British Covert Operations in the United States, 1939-44*. Washington D.C.: Brassey's Inc., 1998.

Masterman, J. C. *The Double-Cross System in the War of 1939 to 1945*. New Haven: Yale University Press, 1972.

Montagu, Ewen. *The Man Who Never Was*. Philadelphia: J.B. Lippincott Company, 1954.

Mure, David. *Master of Deception*: *Tangled Webs in London and the Middle East*. London: William Kimber, 1980.

Mure, David. *Practice to Deceive*. London: William Kimber, 1977.

Reit, Seymour. *Masquerade: The Amazing Camouflage Deceptions of World War II*. New York: Hawthorn Books, 1978.

Sun Tzu. *The Art of War*. New York: Oxford University Press, 1971.

The 1991 Intelligence Authorization Act.

Whaley, Barton. *Codeword BARBAROSSA*. Cambridge, Massachusetts: MIT Press, 1973.

Whaley, Barton. *Practise to Deceive: Learning Curves of Military Deception Planners*. Annapolis, Maryland: Naval Institute Press, 2016.

Whaley, Barton. *Stratagem: Deception and Surprise in War*. Boston: Artech House, 2007.

This page intentionally left blank.

# Index

Entries are by paragraph number.


**A**

access, maintaining, 3-16
  multinational partners, 2-125
  protecting, 2-23
actions, cause, 1-24
activities. *See also* deception activities.
  coordinating, 2-106, 2-121
  deception execution, 3-5–3-16
  MILDEC, 1-5
  monitoring, 1-19, 2-103, 3-23, 4-4
  reverse planning, 2-27
  support from, 1-4
administrative means, 1-66
ambiguity-decreasing deception, 1-33, 2-47
ambiguity-increasing deception, 1-31–1-32, 2-47, 2-116
analysis. *See also* conduit analysis, mission analysis.
  baseline, 2-2
  emulative, 2-38
  information environment, 2-15
  intelligence, 2-50–2-52, 2-78–2-79, 2-84, A-5
  OPSEC, 2-109
analysis plan, developing, 4-8
appendix 14, B-1–B-2
  producing, 2-75
  template, B-2
approval, deception plan, 2-76
approval authority, deception plan, 3-19
assessment. *See also* risk assessment.
  DWG, 1-80
  feedback, 1-58, 3-14
  final, 4-10
  intelligence, 2-79
  responsibilities, 4-1–4-5
  termination, 3-30
assessment plan, 4-6–4-10
  deception event, 4-3
  developing, 4-6–4-10
  feedback types, 4-7
assets, availability, 2-10
  collection, 1-21, 2-119, 3-13
  coordinating, 1-77
  saving, 1-55
assumptions, making, 2-78
  planning, 2-19
  validating, 3-22

**B**

baseline analysis, 2-2
behavior, influencing, 2-15
  patterns of, 1-46, 1-53, 4-12
  understanding, 2-37, 2-39
beliefs, changing, 1-42
  credibility of, 1-33, 1-49–1-50
believable, deception story, 1-19, 1-31, 1-60, 2-24, 2-62
  information, 1-69, 2-55
bias, types of, 2-39
briefing, COA, 2-29
  mission analysis, 2-17
  running estimate, 2-21

**C**

camouflage, 1-67
capabilities, 1-2, 1-67, 2-62, 2-117, 2-120, A-6, A-9
  deception, 1-39, 1-55
  military, 1-11, 2-88
  understanding, 2-49–2-52, 2-54
caution, reactions and, 1-60
civil-military operations, 2-122
COA, briefing, 2-29
  providing, 1-31, 2-30, A-5
  support to, 2-28
COA development, planning, 2-9, 2-28
cognitive, bias, 2-37, 2-39
  process, 2-25, 2-26
  state, 4-12
  vulnerabilities, 2-53
collaboration, benefits, 2-108
  cyberspace operations, 1-78, 2-118
commander, approval from, 2-21, 2-76, 3-27
  brief to, 2-21
  compromising by, A-6
  considerations by, 1-72
  decisions by, 2-12, A-4
  guidance from, 2-5, 2-124
  information for, 4-15
  informing, 3-15
  responsibilities, 1-71–1-72, 3-16
  support to, 1-73, 3-27
  team and, 3-12
  termination plan, 2-71, 3-30
  understanding, A-2
commander's intent, guidance from, 1-4, 1-28
  mission analysis and, 2-5
communication, 2-116, 3-12
competing observable, defined, 1-20
complex conduit, 2-46
concealment, 1-67
  OPSEC and, 2-67, 2-98, 2-100
conditions, changing, 1-26, 2-19, 2-78, 3-6–3-9, 3-15
  establish, 1-2, 1-4
  suitability, 2-12, 2-53, 2-128, 3-4, 3-23, 3-29
conduit analysis, 1-15, 2-42
  conducting, 2-42–2-48
  terms, 2-44
conduits, complex, 2-46
  defined, 1-13
  exploiting, 2-48
  identifying, 2-43, 2-46
  information, 2-86
  manipulating, 1-48
  risk and, 2-45
  selecting, 2-47
  simple, 2-46
  verifiable, 2-60
considerations, analyzing, 2-13, 2-41, 2-72, B-1
  commanders, 1-72
  legal, 2-89–2-96
  MDO, 2-1, 2-3, 2-10, 2-11, 2-12, 2-41, 2-45, 2-66, 4-1
  planners, 1-60, 2-9, 2-45, 4-5
consistency, deception story, 2-63

**Entries are by paragraph number.**


control, centralized, 1-26
  criteria, 3-26
  execution, 3-25
controlling planner, execution, 3-18, 3-20–3-21
  responsibilities, 3-24
  support from, 3-27
coordination, 2-106, 3-10
  civil-military operations, 2-122
  deception event schedule, 4-14
  deception plan, 3-2
  electronic warfare, 2-116
  intelligence staff, A-3
  MDO, 1-76, 2-111, 3-2, 3-10, 4-14, A-3
  multinational, 2-125
  planning, 1-60, 2-23
  requirements, 1-71, 1-75, 2-89–2-90, 2-123–2-125
counterdeception, defined, A-1
  planning, A-1–A-2
course of action. *See* COA.
credibility, 2-45
  MISO, 2-114
criteria, feedback, 2-68–2-70
  termination, 2-71
cultural, bias, 2-39
cyberspace electromagnetic activities, 1-78
cyberspace operations, 2-118–2-119

**D**

data, 1-14, 2-77
  collecting and treating, 4-9
  collection plan, 4-8
deception, assessment of, 4-1
  categories, 1-4–1-7
  challenge, 4-2
  characteristics of, 1-51
  confirming enemy's, A-4
  detecting enemy's, A-3
  see-think-do, 2-26
  employment of, 1-61
  exposing, A-7
  focus, 2-25
  guidance for, 1-23
  integrating, 2-99
  MOP and, 4-13
  movement, 3-18
  OPSEC, 2-97–2-109, 3-10–3-11
  personnel, A-3
  planning process, 2-22–2-75
  principles, 1-23–1-29
  restrictions to, 2-89
  results, 4-16
  running estimate, 2-16–2-21
  support from, 2-6
  support to, 2-10
  synchronizing, 2-64
  unlawful, 2-91–2-95
  viable, 2-9
deception activities, 2-91, 2-121
  developing, 1-4, 1-7, 1-70, 2-3, 2-120
  enemy, A-1, A-4
  sequencing, 1-57
deception assets, husbanding, 1-55–1-56
deception event, 2-13, 2-65, 2-72, 3-18, 4-3
  assessment plan, 4-3
  defined, 1-17, 2-64
deception event schedule, 2-70, 3-12
  completing, 2-75, 2-78, 3-20
  considerations, 2-66
  developing, 2-64–2-66, 2-70, 4-14
  sequencing, 2-66
  support from, 2-66
deception execution, activities, 3-5–3-16
deception goal, alternatives, 2-18
  approval, 2-21
  defined, 1-9
  determine, 2-3–2-5, 2-31–2-32
  output, 2-8
  planning, 2-27
deception in support of operations security. *See* DISO.
deception means, 1-61–1-68, 2-64, 2-65
  categories of, 1-61
  defined, 1-61
  developing, 2-56–2-57
  perceptions and, 2-57
deception objective, 2-8, 2-55, 2-58, 4-1
  defined, 1-10
  determine, 2-32
  identifying, 1-73, 2-4
  planning, 2-27
  running estimate and, 2-18
deception observable, developing, 2-56–2-57, 2-112
deception operations, constraints, 2-92, 2-93
  controlling, 3-25–3-27
  information collection, 2-82
  monitoring, 3-22–3-24
  status, 3-15
  synchronizing, 3-24
  terminating, 3-28–3-30
deception plan, adjusting, 3-1, 3-6–3-9
  approving, 2-76
  assess, 4-5
  authority, 3-19
  benefits from, 2-101
  construction, 2-30
  coordination with, 3-13
  cyberspace operations, 2-119
  enemy, A-2
  executing, 3-4, 3-17–3-27
  identifying enemy's, A-3
  implementation, 3-20
  intelligence production from, 2-80
  protection of, 3-16
  quality, 2-83, 3-22
  requirements of, 2-79
  risk, 2-128
  support from, 2-22
  support to, 4-16
deception planning, creating, 2-28
  feedback and, 2-68
  guidance, 2-3–2-6
  methodology, 2-24–2-26
  security, 2-23
  steps of process, 2-27–2-75
  support to, 2-77–2-88
deception story, compromised, 3-14
  confirming, 2-47
  conveying, 2-64
  defined, 1-22
  developing, 2-58–2-59
  effective, 2-59
  supporting, 2-107
  time for, 2-13
deception target, 2-33–2-54
  analyzing, 2-42–2-48
  defined, 1-11
  identifying, 2-33
  information, 2-85
  perceptions of, 2-55
  understanding, 2-11
  versus MISO target, 2-112
deception task, completing, 2-111
deception working group. *See* DWG.
decision making, enemy, 2-49
  influencing, 2-39
decision-making process, 2-87
decision-making structure, 2-35
decision-making style, 2-36
decoy, defined, 1-68
demonstration, 2-114, 2-116
  defined, 1-37

**Entries are by paragraph number.**


desired perception, 1-22, 2-55, 2-58, 2-65
  defined, 1-12
DISO, 1-7
  assessment of, 4-1
display, 2-114, 2-116
  defined, 1-39
diversion, defined, 1-35
doctrine, enemy, 2-54
do-think-see, deception, 2-26
DWG. *See also* working group.
  data, 4-9
  deception goal, 2-31
  recommendations from, 4-10
  responsibilities, 1-80

**E**

electromagnetic deception, 1-65
  types, 2-117
electronic warfare, 2-115–2-117
  defined, 2-115
  support from, 2-116
emulative analysis, conducting, 2-38
enemy. *See also* target.
  analyzing, 2-51, 2-54
  assessing threat, 2-108
  capabilities, A-1
  cognitive state, 4-12
  deception plan, A-3
  decision making, 2-25, 2-35–2-36
  goals, 2-37
  identifying, 2-20
  intelligence, 2-49–2-52
  knowledge of, 2-11
  misleading, 1-8
  perspective, 2-59
  see-think-do, 2-25
  understanding, 2-49–2-52
  vulnerabilities, 2-53
enemy deception, confirming, A-4, A-5
  countering, A-5–A-9
  exploiting, A-5–A-9
estimate. *See also* running estimate.
  deception, 1-9, 2-18
  technical, 2-51
evaluation, G-2, C-2
  G-3, C-1
  risks, 2-126
event schedule, adjusting, 3-21
  validation, 3-20
execution, 3-4–3-16
  challenges to, 3-25
  deception plan, 3-4, 3-27
  deception story, 2-61
exploitation, 1-33, 2-48, 2-98
  enemy deception, A-5–A-8

**F**

feedback, assessment plan, 4-7
  criteria, 2-68–2-70
  developing, 2-68–2-70
  importance of, 1-58–1-59
  monitoring, 3-21
  results of, 2-70
  use of, 3-14
feint, defined, 1-36
filter, 1-15, 2-46
flags, deception and, 2-94
focus, deception plan and, 1-24, 4-16
foreign intelligence entity, analyzing, 2-51
  support to, 1-7
functions, military deception, 1-3

**G**

G-2, evaluating by, C-2
  perceptions and, 2-50
  responsibility, 1-73
G-3, evaluating by, C-1
  responsibilities, 1-74
G-5, responsibilities, 1-79, 1-80, 2-3
goal, enemy, 2-37
  feedback and, 2-69
guidance, 1-23, 2-30, 2-31, 2-124
  deception planning, 1-9, 2-3–2-6, 2-21

**H**

human factors, analyzing, 2-37–2-41
  defining, 2-37
human information processing, limitations to, 1-44–1-45

**I**

illusions, creating, 1-32
indicator, critical, 2-103
  defined, 1-14
  threats from, 2-101
information, accessing, 2-88
  analyzing, 2-103
  conduit, 2-86
  critical, 2-103
  deception target, 2-85
  decision-making process, 2-87
  delivering, 2-47
  enemy considerations, 2-11
  manipulating, 2-49
  processing, 1-44
  protecting, 2-104
  restricting, 2-124
information collection, 3-13, 4-3
  managing, 2-82
information environment, defined, 2-15
information operations, MDO and, 1-77
information operations officer, responsibilities, 1-75
information quality, 1-69–1-70
information-related capability. *See* IRC.
integration, deception and, 1-29, 1-64
intelligence, enemy, 2-49–2-52
  friendly, 2-88
  requirements, 2-84–2-88
  validity, 1-49
intelligence collection, 1-38, 3-13
intelligence estimate, deception story and, 2-58
intelligence process, enemy, 2-52
intelligence requirements, 2-81
  refining, 2-84
intelligence staff, 3-13
  MDO, 4-15
intelligence support, deception planning, 2-77–2-88
  managing, 2-82
  requiring, 2-79
IRC, 2-90, 2-99
  defined, 2-110
  integrating, 1-75, 2-111–2-122

**J**

Jones' dilemma, 1-48

**K**

knowledge, 3-9, A-2
  providing, 2-52
  restricting, 1-27, 2-124

**L**

law of war, adhering to, 2-91
legal, considerations, 2-89–2-96
leverage the truth, 1-53
link, defined, 1-16
location, 2-116
  deception planning, 1-31, 1-67, 2-23, 2-65

**M**

Magruder's principle, 1-42–1-43

**Entries are by paragraph number.**


material, 1-49, 1-64
maxims, deception, 1-41–1-60
MDO. *See also* planners.
  analyzing, 2-81, 2-104
  assessment plan, 4-6
  assistance from, 1-72
  considerations by, 2-1, 2-3, 2-10, 2-11, 2-12, 2-41, 2-45, 2-66, 4-1
  coordinating, 2-97, 3-2
  evaluation, 2-14
  information operations and, 1-77
  intelligence staff, 4-15
  intelligence support, 2-78
  mission analysis and, 2-7
  responsibilities, 1-76–1-77, 1-79, 2-1, 2-24, 2-30, 2-55, 2-56, 2-73, 2-85, 2-89, 2-123, 3-6–3-9, 3-26, 3-30, 4-1, 4-4, 4-8, 4-14
means. *See* deception means.
measure of effectiveness. *See* MOE.
measure of performance. *See* MOP.
message, 2-113–2-114
methodology, 2-43, 2-46, 2-87, A-4
  deception planning, 2-24–2-26
  see-think-do, 2-24, 4-11
military deception, 1-5
  defined, 1-1
  functions of, 1-3
  legal support to, 2-96
  planning, 1-1–1-2
  terms, 1-8–1-22
  types of, 1-30–1-33
  versus tactical deception, 1-6
military deception officer. *See* MDO.
military information support operations. *See* MISO.
minimize falsehood, 1-54
MISO, 2-112–2-114
  credibility, 2-114
  defined, 2-112
  message, 2-113
mission, 4-2, 4-4
  suitability, 2-12
  time for, 2-13
mission analysis, planners, 2-4, 2-33
  planning, 2-7–2-22
  running estimate for, 2-16
MOE, developing, 4-11–4-16
  focusing, 4-12
  using, 1-58, 3-14, 4-2
monitoring activities, feedback, 3-14
  types, 3-23
MOP, collection steps, 4-13
  developing, 4-11–4-16
  using, 4-1

**N**

node, 1-16, 2-43
  defined, 1-15

**O**

objective, conflict with, 1-26
  deception plan and, 1-25
  enemy, 2-37
observable, building, 2-65
  defined, 1-18
operation order. *See* OPORD.
operation plan. *See* OPLAN.
operations, coordinating, 1-77
operations security. *See* OPSEC.
OPLAN, 2-22, 3-2, B-2
  input to, B-1
  support to, 2-22
OPORD, 1-80, 2-75, 2-76, B-2
  input to, B-1
OPSEC, 1-67
  deception, 2-97–2-109, 2-115
  developing, 2-67
  DISO and, 1-7
  integrating, 1-1, 2-99
  planners, 2-105
  planning and, 1-57, 3-3
  purpose, 2-98
  synchronizing, 3-11
OPSEC analysis, using, 2-109
OPSEC plan, deception and, 3-10–3-11
organizational, bias, 2-39

**P–Q**

patterns, enemy and, 1-21
  of behavior, 1-53, 4-12
perceptions, believable, 2-62
  controlling, 2-106
  creating, 2-50, 2-65
  identifying, 2-55
  interpretations of, 4-11
  measuring, 4-2
personal, bias, 2-39
perspective, target, 1-9, 2-59–2-63
physical means, 1-62
plan, adjusting, 4-15
  implementing, 3-17
  revised, 3-19
  terminating, 2-71–2-74
  validating, 3-9
planners. *See also* MDO.
  activity, 1-19
  analyzing by, 2-38
  considerations by, 1-60, 2-9, 2-45, 4-5
  deception plan, 2-22
  integrating, 2-99
  OPSEC, 2-105
  preparation and, 3-1
  responsibilities, 2-34, 2-35
planning, assumptions, 2-19
  centralized, 1-26
  effort, 2-9
  military deception, 1-1–1-2
  reverse, 2-27
  risk, 2-126
  suitability, 2-12
  termination, 2-72
  time, 2-13
planning horizon, 2-9
planning process, deception, 2-102
  deception plan in, 4-5
  nesting, 2-22
  OPSEC, 2-102
  tactical, 2-22–2-75
preconception, 2-40
preparation, 2-18, 2-67, 3-1–3-3
preplanning, 2-1–2-22
  considerations, 2-1
protection, cyberspace operations, 2-118
  electronic warfare, 2-115
  measures, 2-67
public affairs, deception and, 2-121

**R**

reactions, unwanted, 1-60
recommendations, DWG and, 4-10
reporting channels, 4-14
resources, enemy, 2-54
  OPSEC, 2-108
  use of, 1-74
restrictions, legal, 2-89
risk, conduits and, 2-45
  deception and, 1-55
  deficiencies, 2-77
  planning, 2-14
  reducing, 2-100
risk assessment, 2-126–1-128
  developing, 2-128
  refining, 2-127

**Entries are by paragraph number.**

running estimate, deception, 2-16–2-21
preparing, 2-18
refining, 2-19
results, 2-17, 2-20
support from, 2-31–2-32
ruse, defined, 1-38
electronic warfare, 2-116
legitimate, 2-95
ruse of war, 2-92

**S**

security, deception and, 1-27
maintaining, 3-16
see-think-do, 4-11
enemy, 2-25
MDO, 2-24
sequencing rule, 1-57
signatures, physical means, 1-62
simple conduit, 2-46
space operations, 2-120
staff. *See also* G-2, G-3, G-5.
intelligence, 3-13
responsibilities, 1-71–1-80, 3-17, A-4
suitability, mission, 2-12
supporting observable, 1-19
surprise, forms of, 1-46–1-47
sustainment, 3-10–3-13
synchronization, 3-10–3-11, 3-24
conduits and, 2-46
internal deception and, 3-12
OPSEC plan, 3-10–3-11
timing and, 1-28

**T**

tactical deception, defined, 1-6
planning process, 2-22–2-75
versus military deception, 1-6
tactics, deception and, 1-34–1-39
target. *See also* enemy.
analyzing, 2-34, 2-41, 2-53
decision maker, 2-70
team, commander and, 3-12
technical means, 1-63–1-65
techniques, application of, 1-40
termination, actions of, 3-29
criteria, 2-71
deception plan, 3-28
evolving, 2-73
preparation of, 3-28
scenarios, 2-74
termination plan, completing, 2-75
developing, 2-71–2-74
terms, military deception, 1-8–1-22
time, deception story, 2-13
mission, 2-13
OPSEC and, 2-108
transmission, 2-44
timing, planning and, 1-28
tools, information management, B-1
transition, 3-18
transmission time, 2-44
truth, leverage of, 1-53

**U**

update, 3-15

**V**

validity, intelligence, 1-49
verifiable, sources, 2-60
vulnerabilities, analyzing, 2-53
exploiting, 2-100

**W–X–Y–Z**

working group. *See also* DWG.
analysis by, A-4
functions, A-5

This page intentionally left blank.

**FM 3-13.4**
**26 February 2018**

By Order of the Secretary of the Army:

**MARK A. MILLEY**
*General, United States Army*
*Chief of Staff*

Official:



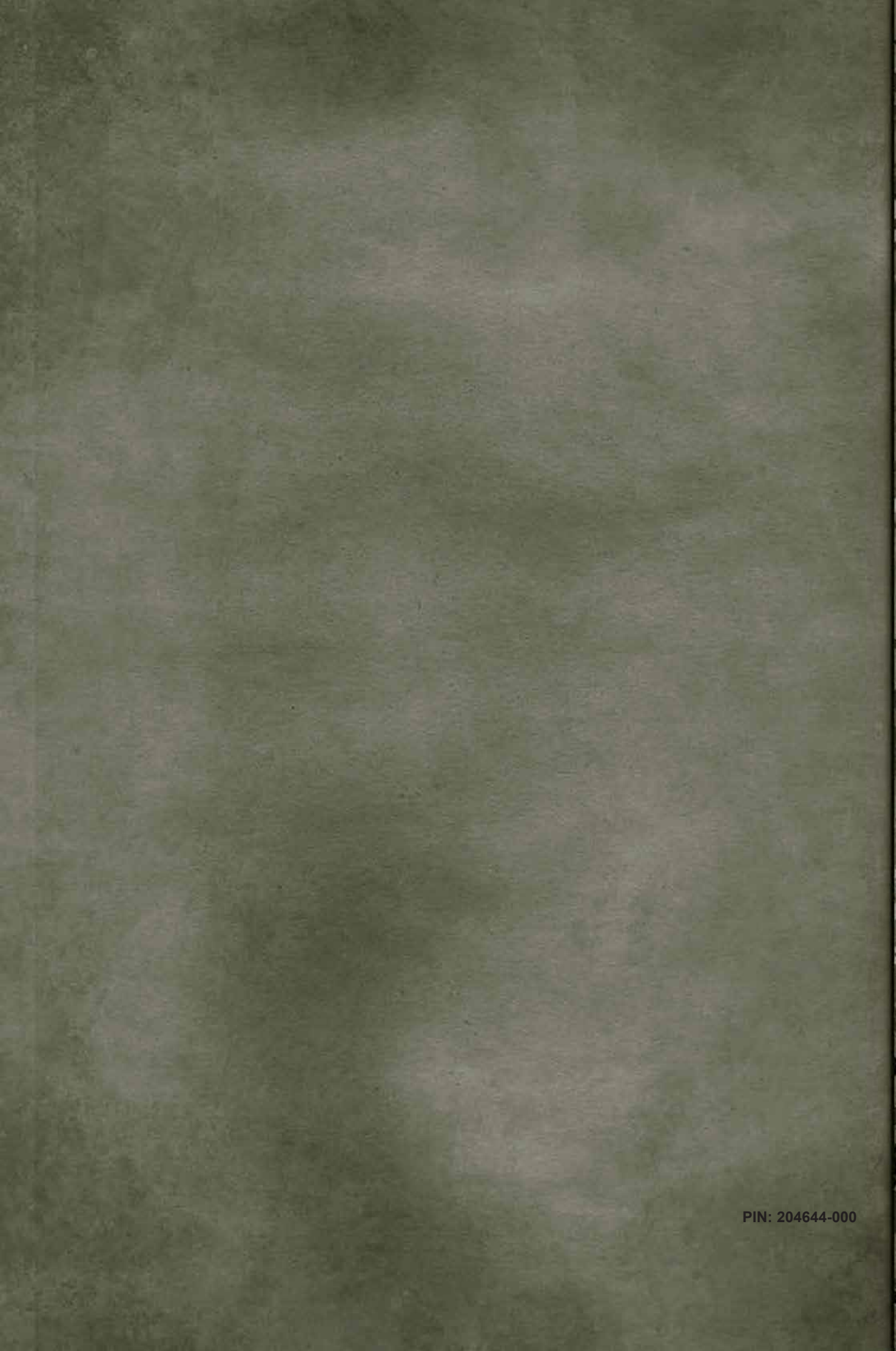
**KATHLEEN S. MILLER**
*Administrative Assistant*
*to the Secretary of the Army*
1905601

**DISTRIBUTION:**
*Active Army, Army National Guard, and United States Army Reserve:* To be distributed in accordance with the initial distrubution number (IDN) 116087, requirements for FM 3-13.4.

This page intentionally left blank.

This page intentionally left blank.

This page intentionally left blank.



PIN: 204644-000