Appendix F Removed

USMC

MCTP 3-32F

Deception

U.S. Marine Corps

Limited Dissemination Control: None. Approved for Public Release.

PCN 147 000094 00

USMC

A non-cost copy of this document is available at:
https://www.marines.mil/News/Publications/MCPEL/

Report urgent changes, routine changes, and administrative discrepancies by letter or email to the Doctrine Branch at:

Commanding General
United States Marine Corps
Training and Education Command
ATTN: Policy and Standards Division, Doctrine Branch (C 466)
2007 Elliot Road
Quantico, VA 22134-5010

or by email to: USMC_Doctrine@usmc.mil

Please include the following information in your correspondence:

Location of change, publication number and title, current page number, paragraph number, and if applicable, line number
Figure or table number (if applicable)
Nature of change
Addition/deletion of text
Proposed new text.

UNITED STATES MARINE CORPS

31 May 2024

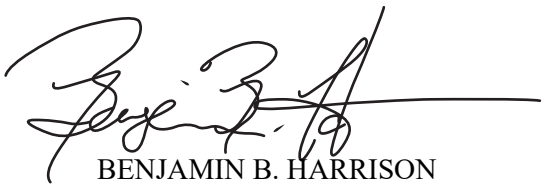
FOREWORD

Marine Corps Tactical Publication (MCTP) 3-32F, *Deception*, is designed to assist Marines while planning, preparing, executing, and assessing Marine Corps deception activities. It is also intended to inform the force of the relevance and importance of deception as a means to accomplish military objectives throughout the competition continuum. As such, this publication applies to Marines and civilians across the total force, at all echelons of command. It is primarily intended for practical use by commanders and deception planners at the tactical level (i.e., Marine expeditionary forces and below).

This publication provides a brief overview of deception theory and methodology, outlines responsibilities across the Marine Corps, and integrates the deception planning process with the Marine Corps Planning Process. As with all doctrine, while this publication reflects current best practices, considerations for application varies based on circumstance, authorities, and available resources.

Without Appendix F, this publication is approved for public release.

Reviewed and approved this date.



BENJAMIN B. HARRISON
Colonel, U.S. Marine Corps
Branch Head, G-39, Deputy Commandant Plans, Policy, and Operations

Publication Control Number: 147 000094 00

Limited Dissemination Control: None. Approved for public release.

Table of Contents

CHAPTER 1. FOUNDATIONS: DECEPTION AS A CAPABILITY

CHAPTER 2. METHODOLOGY: DECEPTION AS A PROCESS

CHAPTER 3. TACTICAL DECEPTION PLANNING

CHAPTER 4. TACTICAL DECEPTION EXECUTION

CHAPTER 5. DECEPTION IN SUPPORT OF OPERATIONS SECURITY

CHAPTER 6. DECEPTION ASSESSMENT

CHAPTER 7. ORGANIZATIONS, ROLES, RESPONSIBILITIES, AND ASSOCIATED AUTHORITIES

Appendices

NOTE: Appendix F contains classified information.

CHAPTER 1.
FOUNDATIONS: DECEPTION AS A CAPABILITY

WHAT IS DECEPTION?

Deception is a deliberate distortion of reality imposed on another where the deceiver gains an advantage. Military, deception refers to "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" (*DoD Dictionary of Military and Associated Term*, hereafter referred to as, *DoD Dictionary*). The Department of Defense (DoD) identifies the following three categories of activities that comprise DoD deception activities:

- Joint military deception (MILDEC) involves DoD deception activities planned and executed by combatant commanders and task force commanders in support of military campaigns and major military operations to cause adversary decision makers or commanders to take actions or inactions that are favorable to the commander's objectives and support military campaigns and major operations.
- Tactical deception (TAC-D) involves DoD deception activities planned and executed in support of tactical operations to cause adversary decision makers to take actions or inactions that are favorable to the commander's immediate tactical objectives.
- Deception in support of operations security (DISO) is a deception activity that is planned and executed to protect the security and secrecy of friendly operations, personnel, programs, equipment, and other assets from foreign intelligence entity (FIE) collection. See Department of Defense Instruction (DoDI) S-3604.1, *(U) Department of Defense Military Deception*, for more information.

WHY DO MARINES USE DECEPTION?

Marines conduct deception activities to achieve military ends—to gain or preserve an advantage linked to their assigned mission. Marines primarily use deception to achieve surprise or maintain security of an operation. These two effects support mission accomplishment by reducing the overall risk of an operation.

Security

Security conceals key indicators of friendly activity from adversary observation and exploitation. It includes operational, physical, and communications security, along with other disciplines. Security measures conceal the timing, location, intent, strength, and capabilities of friendly operations. Marines combine deception activities and security measure to reveal false indicators of activity to confuse the adversary.

Surprise

Surprise is closely linked to—and can result from—effective security. Surprise refers to an adversary's emotional reactions (i.e., shock or confusion) and their inability to effectively react to friendly actions. Whether it takes the form of misallocating forces, space and time constraints, improper weapons-to-target match, or lack of countermeasures, this inability to react is often caused by the adversary's misapprehension of friendly operational aspects. Operational aspects (i.e., timing, location, intent, strength, capabilities) are typically key intelligence questions for any opponent. Deception activities help achieve surprise by providing the adversary with false information, which leads them to take actions that place them at a disadvantage to planned friendly operations.

Risk Reduction

Achieving surprise or maintaining effective security ultimately reduces risk for the commander. The history of deception provides examples of small forces overcoming larger forces or achieving greater success than the initial balance of forces indicated, such as during Operation BERTRAM in 1942. Deceptions only need to be plausible enough to disrupt an adversary's decision-making process during a finite window of advantage for the commander, thereby reducing risk for friendly operations. This disruption gives friendly forces time and space to achieve the commander's objective. In a competition environment, deception enhances security to reduce the risk to the force throughout the course of operations. In a conflict environment, deception might be a critical enabler to achieve mission success by using surprise to create a decisive advantage, thereby reducing risk to friendly forces.

DECEPTION AS AN INFORMATION ACTIVITY IN MARINE CORPS OPERATIONS

As outlined in Marine Corps Doctrinal Publication 8, *Information*, information is one of seven Marine Corps warfighting functions. Like all the warfighting functions, information encompasses a grouping of similar activities that aid in planning and executing operations. Marines apply the information warfighting function to create and exploit information advantages in pursuit of mission objectives.

An information advantage is an exploitable condition resulting from an actor's ability to generate, preserve, deny, and project information more effectively than another. Marines create and exploit information advantages—through rapid, flexible, and opportunistic maneuver. The three information advantages are systems overmatch, prevailing narrative, and force resiliency; however, there are also other decision, temporal, spatial, or psychological advantages.

Marines apply the four functions of information (i.e., generate, preserve, deny, project) to create and exploit information advantages; however, deception activities typically use information denial and information projection. Information denial disrupts or destroys the information needed by the opponent. Information projection is the dissemination of information to inform, influence, or deceive an observer or targeted system.

A skilled and creative deception planner can combine information denial and projection to generate other information-based advantages, namely surprise. Marines combine security and deception operations, along with all other available capabilities, to conceal their locations, capabilities, and intent. Additionally, they create false impressions, which can lead to the adversary taking a specific action or inaction.

Marines apply the information warfighting function to leverage the attributes of both competition and war by exploiting the cognitive and functional components of threat systems (human and machine) to create relative advantages. Deception, as part of the information warfighting function, provides the commander a key capability to influence the environment to enable lethality, survivability, and operational effects.

DECEPTION AS AN INFORMATION ACTIVITY IN JOINT OPERATIONS

Marine Corps information doctrine is similar to joint doctrine; however, there are several differences that are important to note since Marine tactical units are employed within joint formations. Most notably, according to Joint Publication (JP) 3-04, *Information in Joint Operations*, joint force commanders leverage information in two ways. First, they plan and conduct all operations, activities, and investments to deliberately leverage the inherent informational aspects of such actions; and second, they conduct operations in the joint information environment (OIE). Unlike many other information capabilities, deception uses both ways of leveraging information to support military objectives.

Marine air-ground task force (MAGTF) deception planners must be conversant with Marine Corps and joint concepts and terminology as they apply to the deception capability. The MAGTF deception planners are responsible for maintaining liaison between joint organizations and Marine Corps formations to effectively plan and execute deception activities. For further information, refer to JP 3-04 and JP 3-13.4, *Military Deception*. The interaction between joint OIE and deception activities are discussed further in the following sections.

RELATIONSHIP OF DECEPTION ACTIVITIES TO JOINT OPERATIONS IN THE INFORMATION ENVIRONMENT

The joint force uses the term joint OIE to refer to the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and by protecting friendly information, information networks, and information systems. Information forces include—

- Psychological operations forces.
- Civil affairs teams.
- Communication strategy and operations (COMMSTRAT) and public affairs organizations.
- Electromagnetic spectrum operations (EMSO) elements.
- Cyberspace operations forces.
- Space operations elements.

When commanders leverage information, they expand their options for employing military capabilities beyond the use of, or threatened use of, physical force.

The JFC integrates and deconflicts joint OIE and deception activities to minimize the risk of mishandling information and ensure that the relevant capabilities are being employed in an effective manner to support the commander's objectives. Specific considerations relevant to each capability are outlined in the following sections. For additional information, refer to JP 3-13.4.

Military Information Support Operations

Military information support operations (MISO) are "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives" (*DoD Dictionary*). Deception targets can also be MISO target audiences. Planners should deconflict deception events used to deceive deception targets with MISO themes and messages to maintain believability and credibility. The MISO products and activities are generally truth based. This practice is not based upon legal or policy restrictions but is based on a requirement to maintain credibility with target audiences in order to execute future MISO.

Deception planners should be aware of MISO themes and messages that the intended deception target might receive. These themes and messages contain both objective and subjective truth and must be generally "verifiable" by the target audience. Deception events and deceptive information inserted into adversary conduits contain falsehoods that must believable. The two can be mutually beneficial, but they can also run counter to each other. Therefore, planners should coordinate MISO and deception activities.

Commanders can use MISO products—directed at specific adversary target audiences—in conjunction with deception techniques such as feints, demonstrations, ruses, and displays to add credibility to the deception story or event. Examples of combined MISO products and deception techniques include warning of impending multinational force arrival, providing surrender instructions, or attacking adversary military or paramilitary forces' morale. However, because MISO must retain credibility with its broader target audiences, commanders must consider the cost versus benefit and second- or third- order effects of combining MISO and deception techniques.

Civil Affairs

Civil affairs operations are "actions planned, coordinated, executed, and assessed to enhance awareness of, and manage the interaction with, the civil component of the operational environment; identify and mitigate underlying causes of instability within civil society; and/or involve the application of functional specialty skills normally the responsibility of civil government" (*DoD Dictionary*). Civil affairs forces execute civil affair operations and enable the commander's civil-military operations (CMO), engaging the civil component of the operational environment to support the JFC's CMO efforts.

Civil-military operations are the "activities of a commander performed by designated military forces that establish, maintain, influence, or exploit relations between military forces and indigenous populations and institutions, by directly supporting the achievement of objectives relating to the reestablishment or maintenance of stability within a region or host nation" (*DoD Dictionary*). Commanders conduct CMO to gain maximum support for US forces from the civilian population. Civil-military operations contribute to the success of military operations and project a favorable US image throughout the operational area. Commanders and their staff coordinate deception operations with CMO and with those MISO activities that support CMO to ensure deception operations do not inadvertently undermine the relationships with the civilian population or host-nation military authorities. Failure to consider CMO could compromise deception plans or cause other unintended consequences to the overall mission.

Communication Strategy and Operations

Communication strategy and operations personnel focus on informing domestic, international, and internal audiences. They help achieve these objectives by putting operations, activities, and policies in context; facilitating informed perceptions about military operations; countering disinformation and propaganda; and correcting misinformation through the dissemination of timely and accurate information. Additionally, COMMSTRAT personnel—

- Participate in staff planning.
- Lead the collaborative development of operational- and tactical-level narratives.
- Develop constraints and restraints.
- Identify potential intended and unintended consequences of planned actions.
- Develop an understanding of the nature and flow of information in varying contexts.

The COMMSTRAT planners advise the commander on the possible direct and indirect effects of military actions on public perceptions, attitudes, and beliefs and formulate and provide timely and culturally attuned messages. United States policy prohibits deception activities and COMMSTRAT operations from explicitly or implicitly targeting, misleading, misinforming, or attempting to influence any of the following:

- US Congress.
- US public.
- US news media.
- US Government.
- International media.
- US decision makers.
- Public opinion.

A COMMSTRAT officer reviews all deception operations to eliminate, minimize, or mitigate the possibility that such influence might occur. Additionally, the commander coordinates deception operations with COMMSTRAT officers to identify any problems with deception activities that are potentially visible to the media or the public. This coordination reduces the chance that the commander or COMMSTRAT officers inadvertently reveal information that could undermine ongoing or planned deception operations.

Electromagnetic Spectrum Operations

As part of a Marine staff, EMSO elements work to organize, execute, and oversee the conduct of electromagnetic warfare (EW) and spectrum management. The EMSO elements do this as part of information operations and, when tasked, in support of other operations. Because EMSO are enablers for other activities that communicate through or use the electromagnetic spectrum, such as MISO, public affairs, or cyberspace operations, EMSO elements work closely with information planners from other fields within the information planning cell (often designated the G-39 within a Marine expeditionary force general staff).

Electromagnetic warfare is essential for protecting friendly operations and denying adversary operations within the electromagnetic operating environment. The term EW refers to “military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy” (*DoD Dictionary*). Deception activities, in conjunction with OPSEC, support EW operations by protecting the development, acquisition, and deployment of sensitive EW capabilities. It also supports the employment of EW units and systems.

Additionally, EW supports the execution of feints, ruses, demonstrations, and displays and facilitates the insertion of deceptive information. Commanders employ EW against intelligence collection assets to shape and control the adversary’s ability to obtain information about certain activities. Friendly EW elements; deception, communications, cyberspace and space support elements; spectrum management personnel; and intelligence planners must coordinate to ensure EW does not disrupt any adversary communications system that friendly forces are using as deception conduits or that are providing intelligence feedback.

Electromagnetic deception uses deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an adversary or to their electromagnetic dependent weapons; thereby, degrading or neutralizing the adversary's combat capability. Electromagnetic deception includes manipulative, simulative, or imitative techniques. For further information, refer to JP 3-85, *Joint Electromagnetic Spectrum Operations*.

Cyberspace Operations

Cyberspace forces retained by the Services or assigned to the CCMDs conduct offensive and defensive missions in friendly, neutral, or enemy cyberspace. Mission-tailored force packages using cyberspace forces and cyberspace capabilities are established as required and can include small mission elements selected from one or more teams up to joint task forces.

Deception and cyberspace operations can be mutually supportive in numerous ways. For example, because the adversary might also be resident in cyberspace and leverage the same systems and processes as friendly forces, cyberspace operations are an effective conduit for placing or delivering material to affect adversary military decision making and subsequent action or inaction. Deception planners 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 can include constructing false servers, communications nodes, and other hardware associated with a tactical computer network to include replicating information-system traffic and false data storage. Adversary collection assets can be redirected toward deceptive events (such as presenting a false "weakness" in friendly information systems) and then targeted for destruction or exploitation by friendly forces. For further information, refer to JP 3-12, *Joint Cyberspace Operations*.

Space Operations

Space officers assigned as planners ensure commanders and their staffs have a common understanding of space operations, provide space domain awareness, and coordinate space capabilities for lethal and nonlethal effects. Space operations support the flow and protection of information and decision making and serve as a thoroughfare for other activities that communicate through or use space capabilities. Deception activities can use space capabilities to present observables to adversary sensors, disrupt the ability of adversary perception of reality, or to coordinate aspects of the activity.

CHAPTER 2.
METHODOLOGY: DECEPTION AS A PROCESS

Of the three DoD deception activities categories, the Marine Corps only plans and conducts tactical deception and DISO, which can directly lead to achieving surprise and security. Marine Corps forces do not plan or conduct MILDEC; rather, Marine Corps component commands and Fleet Marine Forces contribute to this joint activity.

HOW DO MARINES DECEIVE?

Effective deception relies on two complementary functions: concealing facts and revealing fiction. These are woven together through skillful misdirection to influence the adversary's reaction. This process is called deception and it depends not only on the deceiver but also on the target (see Figure 2-1).

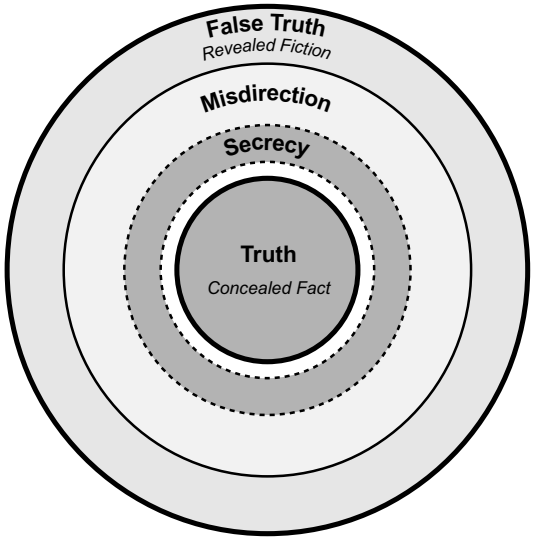


Figure 2-1. Layers to Deception.

Truth and Secrecy

Central to any successful deception is thorough knowledge of the truth. Deception planners must know the goal of the deception operation (i.e., the truth). If not, they might inadvertently reveal the operation—or cause an adversary to take unintended actions that are harmful to friendly interests. At the core of deception operations are the central truths of timing, location, intent, strength, or capability. Deception planners identify key indicators of friendly activity and use various security disciplines to hide them (i.e., secrecy). This is the passive component of deception.

Lies and Misdirection

After deception planners conceal aspects of the truth, they must produce alternative facts to confuse the adversary (i.e., lying). This is the active component of deception. Deception planners identify additional key indicators of activity and create false indicators of activity to present to the target. (i.e., misdirection). The deception planners must then communicate these alternative facts to the intended target, using a method that is both seen and believed by the adversary or enemy (i.e., the deception story).

The deception story must contain some truth, although it should misdirect the target's attention away from the essential facts, and towards the alternative facts. This misdirection should either lead to the target being more certain about certain "facts" or less certain because of multiple, plausible realities.

For a deception operation to be successful, either outcome must lead the target to a desired action or inaction. This is the objective of deception—influencing what the adversary must do.

DECEPTION METHODOLOGY

While deceptions unfold as a "SEE-THINK-DO" methodology, they are planned in the reverse sequence—as "DO-THINK-SEE." Before this planning process can begin, however, the commander must decide upon the overall purpose of the deception.

Deception Goal

Fundamentally, deception is used to gain or preserve an advantage. 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" (*DoD Dictionary*). It is usually stated as a positive friendly advantage or condition such as successful deception "creates a decisive combat power advantage for the main effort attack along AXIS MONTEZUMA."

Deception is not an end to itself. Like other military operations, the success of deception is measured by its direct contribution to mission accomplishment. Deception often requires substantial investments in effort and resources that would otherwise be applied against the adversary in a more direct fashion. Consequently, the commander should first envision the deception goal in terms of its specific contribution to accomplishing the designated mission.

Deception Objective

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" (*DoD Dictionary*). For example, a deception objective could be for "the adversary to hold their armored reserve in a position or status unable to impact forces along AXIS MONTEZUMA through D+36 hours." Other outcomes suitable for deception objectives include—

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

Deception Target

The deception target is "the adversary decision maker with the authority to make the decision that will achieve the deception objective" (*DoD Dictionary*). The target's mental state must be affected, through a set of desired perceptions, to achieve the objective(s).

In DISO, the deception target is an FIE, not the adversary decision maker. The intent of targeting FIE is more general to increase or decrease ambiguity to the adversary's overall intelligence apparatus.

Desired Perceptions and the Deception Story

Desired perceptions lead the deception target to make the decision that achieves the deception objective. They can include personal conclusions, official estimates, or assumptions formed from both objective (observation and analysis) and subjective (intuition and experience) approaches. Perceptions are affected by biases, preconceptions, predispositions, and filters applied in the collection, analysis, delivery, and reception of information. This is why most successful deceptions reinforce existing perceptions; it is far more challenging to change or create a perception than reinforce one.

Humans process reality through narratives, and deception is fundamentally a process of communication. Thus, a narrative structure is used as a deception story, which is "a scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception" (*DoD Dictionary*). The deception story must be believable, verifiable, consistent, and executable. It is primarily communicated to the target through indirect means, which lets the individuals see pieces of the puzzle and piece them together into their own narrative.

Deception Events

The deception story is told through deception means, which are the "methods, resources, and techniques that can be used to covey information to the deception target" (*DoD Dictionary*). Deception means are used in concert with truthful indicators of friendly activity, leading to information or a detectable action (specific facts or evidence) for the adversary to interpret or piece together and form assumptions and assessments about friendly activity, capability, and intent.

Although the deception target is typically a single decision maker, deception means typically focus on conveying information to the adversary's intelligence apparatus or other information sources that inform the deception target. The path information flows through is called a conduit. The conduit consists of a sensor that observes, nodes or filters through which information passes or is changed, and links connecting these nodes. Deception conduits are discussed in more detail later in this chapter.

By matching detectable indicators with a particular conduit, an observable is achieved that supports the deception story. Conversely, competing observables comprise observable that contradict the deception story. Deception planners should mitigate competing observable to avoid negatively affecting deception events. Observables, either singly or in groupings, are termed deception events, and can be performed using one or more of the following tactics: feints, demonstrations, displays and ruses. (See Figure 2-2.)

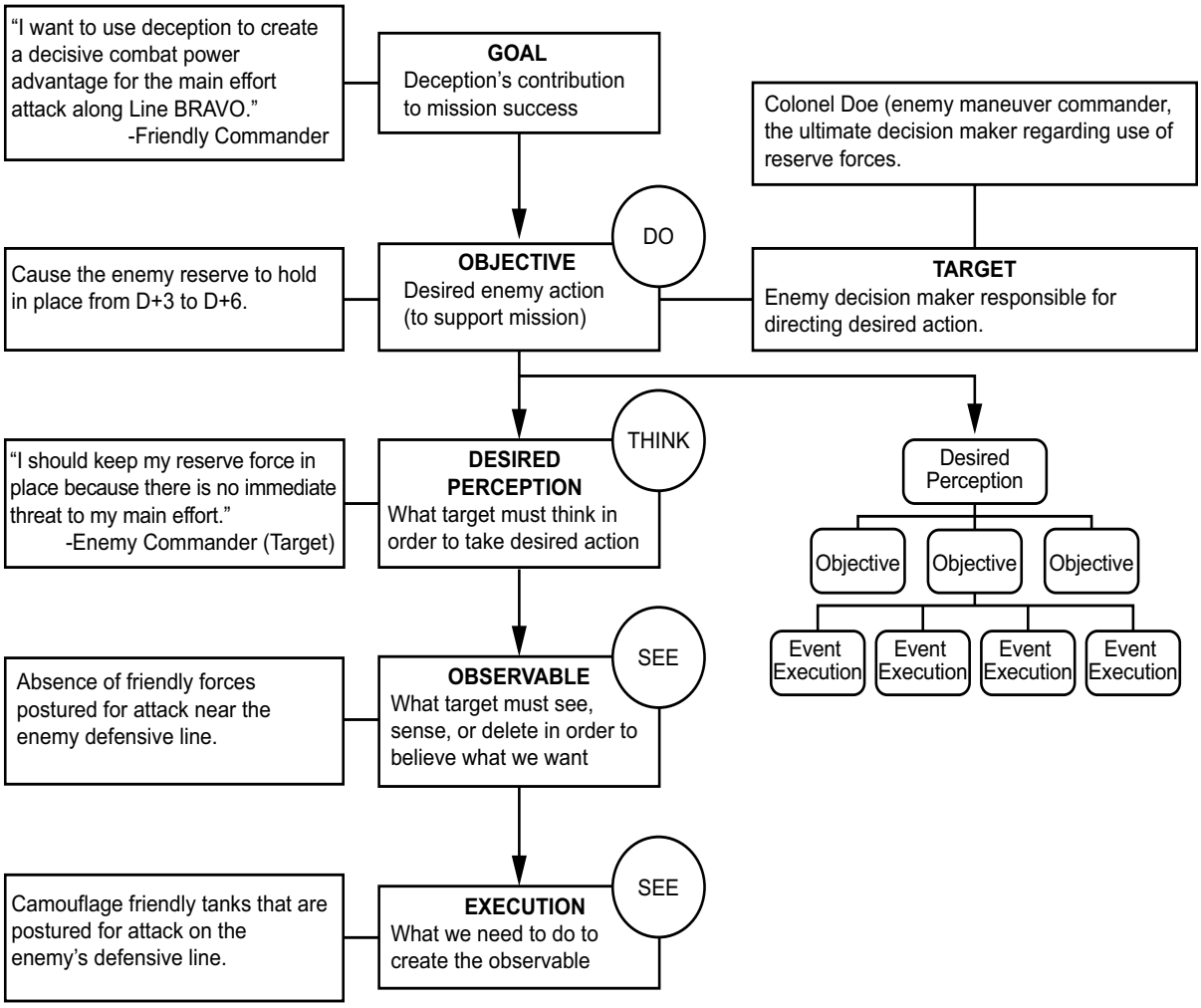


Figure 2-2. Deception as a Process.

Assessment

Friendly forces must monitor the reception and actions of the adversary to assess the effectiveness of a deception. The end goal is to achieve a friendly force advantage at the expense of adversary actions or inactions.

Termination

Successful or not, every deception must eventually terminate. Termination can merge with follow-on operations, leverage success or failure into a successive branching deception, or simply cease with appropriate security actions.

TENETS OF DECEPTION

The six tenets of deception, which are linked to the deception methodology, are overarching considerations that help inform deception planners in both planning and executing deception operations (see Table 2-1 for the six tenets).

Table 2-1. Tenets of Deception.

Tenet	Notes
Focus	Targets the adversary decision-maker capable of taking the desired action(s).
Objective	Causes an adversary to take (or not to take) specific actions, not just to believe certain things.
Centralized Planning and Control	Deception operations should be centrally planned and directed.
Security	Denies knowledge of a force's intent to deceive and the execution of that intent to adversaries.
Timeliness	A deception operation requires careful timing.
Integration	Integrates each deception activity with the operation that it is supporting.

Focus

The deception plan focuses on the thought process of the threat decision maker who has the authority and capability of causing the desired actions. The adversary's intelligence, surveillance, and reconnaissance capabilities are not typically the target; rather, they are the primary conduit used in the deception plan to convey selected information to the decision maker. Planners must understand the difference between intermediate conduits and the intended target. Focused deception must cause an action or inaction of the adversary force. To do this, there must be existing conduits to the deception target or a reasonable expectation that conduits can establish.

Objective

Deception plans focus actions and resources that motivate an adversary to decide to take (or not to take) specific desired actions, known as the objective. The plan cannot solely focus on motivating the target to believe certain things; it must also lead the target to act or not act.

Centralized Planning and Control

A centralized approach is necessary to avoid confusion and to ensure various elements portray the same deception story and do not conflict with other operational objectives or evolving conditions in an operational environment. Although core Marine Corps tenets include centralized command and decentralized execution, effective Marine Corps deception activities (MCDA) must be synchronized and centralized throughout the process because of the risk associated with the adversary learning of a deception. Execution of the deception can, 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 military deception officer (MDO), working with the deception activities working group (DAWG), ensures synchronization, deconfliction, and OPSEC. If the command does not have an MDO, the lead operational planner (military occupational specialty 0505) or advanced information staff planner (military occupational specialty 0550) should work with adjacent and higher-level commands to synchronize deception activities.

Security

Successful deception requires strict security that begins before execution with measures to deny the adversary 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 security of the deception means limiting the number of informed planners and participants to those with need to know. The MDO must develop and maintain access rosters and other security controls to limit exposure of operational deception activities. Additional information on security is discussed in Chapter 5.

Timing

Critical aspects of deception planning begin with synchronizing with the commander's intent and maintaining synchronization during deception execution. Timing in deception operations is crucial; the deception target must act or not act in accordance with the deception objective within the timelines. 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 adversary decision maker. This means that deception execution planning must account for the time the adversary will spend on intelligence collection and analysis, decision making, assimilation and reaction, and the activity to be exploited.

Integration

Deception is an integral part of an operation that planners must integrate at all points throughout the planning process. This includes developing a deception concept that supports the overall mission as part of course of action (COA) development. Planners must also integrate deception plans with higher headquarters plans. Deception activities must be consistent with Marine Corps 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.

DECEPTION MEANS

Deception means create convincing observables for an adversary and increase credibility and likelihood of success. There are three basic categories of deception means: physical, technical, and administrative. An individual deception operation can have multiple attributes that allow it to be characterized in more than one category.

A convincing deception incorporates multiple deception means to provide reinforcing indicators to the adversary. Planners typically employ deception means in complementary and synchronized ways to mislead multiple types of adversary sensors to increase credibility and the likelihood of creating the desired perception (refer to Jones' Lemma in Appendix D for deception means).

Physical Means

Marines use physical means to convey information or signatures—typically through direct observation or active sensors—to the deception target. Most physical means also have technical signatures visible to sensors that collect electronically. Planners typically evaluate physical means using characteristics such as shape, size, function, quantity, movement pattern, location, activity, and association with the surroundings. Examples of physical means include—

- Movement of forces.
- Exercises and training activities.
- Presence of specific equipment (real or decoy).
- Conducting tactical actions.
- Visible test and evaluation activities.
- Reconnaissance and surveillance activities.

Technical Means

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, cyber, acoustic, or other forms of energy, or olfaction.

Technical means can be applied alone, with corresponding physical means, or integrated with other technical aspects to replicate something physical that is absent from direct visual observation. As with other friendly military material resources, using technical means to conduct deception operations must comply with US and international law. Technical means include—

- Establishing communications networks and interactive transmissions that replicate a specific unit type, size, or activity.
- Emitting or suppressing chemical or biological odors associated with a specific capability or activity.
- Using multispectral simulators to replicate or mimic the known electronic profile of a specific capability or force.
- Using selected capabilities to disrupt an adversary sensor or affect data transmission.

Administrative Means

Administrative means are resources, methods, and techniques used to convey or deny selected written, oral, pictorial, or other information or signatures to or from the deception target. They generally portray information and indicators associated with coordination for ongoing or planned military activity to the deception target. Administrative indicators are often derived from OPSEC-related topics; therefore, the contents of administrative means are considered “high importance.” Administrative means visible to an adversary 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 typically done through unclassified channels.

TACTICS AND TECHNIQUES OF DECEPTION

Marine Corps deception activities apply the three deception means using deception tactics to achieve various deception effects. Planners consider the time, place, and adversary when selecting which deception method to use. Table 2-2 lists common deception tactics.

Table 2-2. Deception Tactics.

Tactic	Description
Feints	"In military deception, an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action" (*DoD Dictionary*). A feint is designed to lead the adversary into erroneous conclusions about friendly dispositions and concentrations. A series of feints can condition the adversary to react ineffectively to a future main attack in the same area.
Demonstrations	"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" (*DoD Dictionary*). A demonstration's intent is to cause the adversary to select a COA favorable to friendly goals.
Ruses	"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" (*DoD Dictionary*). A ruse deceives the adversary to obtain a friendly advantage. A ruse in deception generally contributes to the larger deception plan.
Displays	"In military deception, a static portrayal of an activity, force, or equipment intended to deceive the adversary's visual observation" (*DoD Dictionary*). 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.

Table 2-3 lists techniques used to accomplish deception tactics. These can be employed singly or together using available resources and are only limited by the creativity of the deception planner.

Table 2-3. Deception Techniques.

Technique	Deception Created
Amplifying signatures	A force appears larger and more capable to simulate the deployment of critical capabilities. Amplifying signatures can mislead the adversary into anticipating a force ratio that is not in their favor. This can cause them to commit finite resources to a space and time intended by the deception planner, or discard COAs that are deemed infeasible because of the perception of a much larger and capable friendly force.
Suppressing signatures	A force appears smaller and less capable or to conceal the deployment of critical capabilities. Conversely, suppressing signatures can result in an adversary that discounts seemingly inconsequential friendly capabilities.
Dazzling	Confuses or corrupts an adversary's collection assets by providing multiple false indicators and displays that can overload sensors.
Repackaging known organizational or capability signatures	Generates new or deceptive profiles that increase or decrease the ambiguity of friendly activity or intent.
Conditioning the adversary	Desensitizes the adversary to particular patterns of friendly behavior and induces adversary perceptions that are exploitable at the time of friendly choosing.
Reinforcing the impression	Misleads the adversary by portraying one COA but tasking a different COA.

Table 2-3. Deception Techniques (Continued).

Technique	Deception Created
Conditioning the target by repetition	Leads the adversary to believe that an apparently standard COA will be pursued, when in fact a different COA will be executed.
Leading the adversary by substitution	Leads the adversary to believe that nothing has changed by covertly substituting the false for the real, and vice versa.
Leading the adversary by mistake	Leads the adversary to believe that valuable information has come into their possession through a breach of security, negligence, or inefficiency.

TYPES OF DECEPTION

Deception aims to either increase or decrease the level of uncertainty or ambiguity in the mind of the deception target and is categorized by two styles:

- Ambiguity-increasing.
- Ambiguity-decreasing (misleading).

Ambiguity-Increasing

Ambiguity-increasing deception provides the adversary with multiple plausible friendly COAs. It is designed to generate confusion and cause mental conflict in the adversary decision maker. Examples of anticipated effects of ambiguity-increasing deception include causing the adversary to—

- Delay making a specific decision.
- Develop operational paralysis.
- Reroute their forces 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. Ambiguity-increasing deceptions divert attention from one set of activities to another. It can create the illusion of strength where weakness exists or create the illusion of weakness where strength exists. Additionally, it can acclimate the adversary or enemy to patterns of activity that friendly forces can later exploit. 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 where no acceptable solution exists or even prevent the target from taking action. This type of deception is typically successful with an indecisive decision maker who is known to avoid risk.

Ambiguity-Decreasing (Misleading)

Ambiguity-decreasing deceptions manipulate and exploit an adversary decision maker's pre-existing beliefs and bias by displaying observables that reinforce and convince the decision maker that their pre-held beliefs are true. Ambiguity-decreasing deceptions cause the adversary decision maker to be certain—and wrong—about particular facts. Ambiguity-decreasing deceptions aim to direct the adversary 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 adversary's processes and intelligence systems. Planners often have success using these deceptions with decision makers who are willing to accept a higher level of risk.

DECEPTION CONDUITS

Deception conduits are information or intelligence pathways to the deception target. Collectively, they define how the adversary registers or "sees" activity in the information environment and how those observations are transmitted, processed, and ultimately delivered to the decision maker. The deception planner chooses and deconflicts access to specific conduits, to provide a synchronized portrayal of selected information and indicators. Typically, 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 various ways, and delivery to the deception target(s).

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

LEGALITY

Marine Corps deception activities must comply with applicable US law; the law of armed conflict; treaties and agreements to which the US is a party; Presidential, DoD, and Department of Navy policy and regulations; and rules of engagement. Deception planners must ensure deception plans are developed lawfully and consistent with applicable policies to avoid creating unnecessary risk for commanders and broader US Government efforts. Determining legality of a deception operation is a complex process, as some activities or techniques are prohibited by domestic or international law, while others might be legal but are prohibited by various policies. General guidelines that assist the deception planner in understanding of these considerations are discussed in the following sections.

Overall, deception activities cannot—

- Mislead the US public, US Congress, or US news media.
- Partake in perfidy. Perfidy includes acts that invite the confidence of enemy persons to lead them to believe that they are entitled to or that the friendly forces are obligated to accord protections under the law of war with the intent to betray that confidence to secure a military advantage to kill or wound the enemy.

The key element in perfidy is the false claim to protections under the law of war to secure a military advantage to *kill or wound*. It is therefore not perfidy to invite the confidence of the adversary and imply an obligation to accord them protection under the law of war to accomplish certain purposes (e.g., to facilitate spying, sabotage, capturing enemy personnel, or evading enemy forces). Such deception, however, may not rely on certain protected signs and symbols. Moreover, persons who use deception to engage in spying and sabotage might forfeit prisoner of war status or be liable to certain penalties under the domestic law of enemy states. Examples of perfidy include the following:

- Feigning an intent to negotiate under a flag of truce and then attacking an opponent.
- Feigning surrender and then attacking to gain an immediate tactical advantage over enemy forces.
- Feigning that one is wounded, sick, or dead, and then attacking an opponent.
- Feigning civilian status to obtain an advantage over enemy forces to kill or wound them.

The law of war prohibits misusing certain protected signs, symbols, signals, or emblems such as the Red Cross or Red Crescent and feigning non-hostile relations to seek a military advantage. A deception plan must follow the commander's limitations and agreements, and planners must consider legal implications throughout the planning, execution, and assessment processes. Staffs should always consult with the judge advocate when developing a deception plan.

Per DoD policy, deception operations cannot target or mislead the US public, the US Congress, US news media, or any open-source (unclassified or generally available to the public) publications. All DoD missions and activities are governed by federal statute or, in the absence of statutory authority, through delegation or exercise of executive branch powers. The President, under constitutional and statutory authority, may issue documents that provide direction to the executive branch, which is further promulgated into policy applicable to deception activities.

Deception operations are constrained, but not forbidden, by international agreements. Ruses of war and the employment of measures necessary measures for obtaining information about the enemy and country are permissible. Ruses of war are acts that are intended to mislead or to induce the adversary to act recklessly, but that do not infringe upon any rule of international law applicable in armed conflict. Ruses of war are permissible so long as they do not involve treachery or perfidy, or contravene domestic law, policy, or international legal obligations of the United States. Ruses, as used here, is a legal term to mean deceptions that are not prohibited by the law of war, and are distinguished from the common, factual use that describes both lawful and unlawful ruses.

The line of demarcation between legitimate and illegitimate ruses sometimes blurs. Although each particular deception activity must be evaluated on a case-by-case basis for compliance with law and policy, the following provides typically acceptable examples of permissible ruses:

- Surprises, ambushes, feigning attacks, retreats, or flights.
- Simulated quiet and inactivity.
- Using small forces to simulate a large unit.
- Transmitting false or misleading radio or telephone messages.

- False orders purporting to have been issued by the adversary commander.
- Using the adversary's signals and passwords.
- Communications with non-existing troops or reinforcement.
- Deceptive supply movements.
- Planting of false information.
- Moving landmarks.
- Assembling dummy guns and vehicles or laid dummy mines.
- Establishing dummy installations and airfields.
- Removing unit identifications from uniforms.
- Using signal deceptive measures.
- Using MISO messages and actions for psychological effects.

Refer to Chapter 7 for the specific roles a staff judge advocate (SJA) performs in the review of deception plans.

POLICY

Beyond legal review and considerations tied to the law of armed conflict, US law and the DoD Law of War Manual, legal and policy reviews are necessary throughout the process to appropriately identify and mitigate risks. For example, policy prohibits deception from deliberately targeting anyone outside the adversary's military decision-making process without further legal review. The commander and staff must understand that current policy might prohibit otherwise lawful deception because of risk or policy considerations.

In addition, there are multiple distinctions within the operational environment that affect applicability of policy instruments. Two examples include differences between international and non-international armed conflicts, and status of combatants.

Policy governing application of DoD deception activities can undergo major changes with little or no notice. Because of the complexities of US, DoD, Service, and international policy, the deception planner should view legal and policy considerations within a rubric of risk management. Deception planners can mitigate risk by establishing early communication and engagement with legal advisors and including them throughout the deception activity planning process.

CHAPTER 3.
TACTICAL DECEPTION PLANNING

OVERALL PLANNING CONSIDERATIONS

As outlined in Marine Corps Warfighting Publication (MCWP) 5-10, *Marine Corps Planning Process*, Marine Corps units conduct three levels of planning: conceptual, functional, and detailed. Conceptual planning is the highest level of planning, which addresses developing tactical, operational, or strategic concepts for the overall conduct of military actions. Functional planning addresses developing and integrating supporting plans for discrete functional activities, to include information activities. Detailed planning addresses translating the broad concept into a complete and viable plan.

Marines conduct planning using one of the following four planning processes: the troop leading steps, the Marine Corps Planning Process (MCPP), the joint planning process, or the rapid response planning process (R2P2). Selecting the appropriate planning process is dictated by the echelon of command, relationship to the joint force, and the time available for planning.

Joint MILDEC is planned in conjunction with the joint planning process. Marine units plan for TAC-D within joint operations using the MCPP. Marines typically plan TAC-D using the R2P2, which is primarily used by Marine expeditionary units (MEUs) conducting maritime operations. At the lowest tactical level, particularly for small units without a staff, Marines use the troop leading steps to execute deception tactics.

Processes result in either a plan or an order, depending on whether they are used to support deliberate or crisis planning, or to support the execution of ongoing operations. The deception plan is a tab contained with the plan or order, following the formats provided in the Chairman of the Joint Chiefs of Staff (CJCS) Manual 3130.03A, *Planning and Execution Formats and Guidance*, or MCWP 5-10. While these formats are similar, the numbering conventions adopted by the Marine Corps in the current MCWP differ from CJCS Manual 3130.03A. Planners should carefully evaluate each format when conducting joint operations to avoid confusion with other Services.

The TAC-D planning process is considered a form of functional planning, bridging the gap between conceptual and detailed planning. Deception in support of operations security is planned as part of OPSEC functional planning (measure and countermeasure development) and is discussed further in Chapter 5. For joint MILDEC support planning, refer to JP 3-13.4.

TACTICAL DECEPTION PLANNING DURING THE MARINE CORPS PLANNING PROCESS

The MCPP is guided by three tenets: top-down planning, single-battle concept, and integrated planning. To ensure TAC-D planning is integrated with the commander's objectives and desired end state, planners conduct it as part of the MCPP. The early integration of deception in the planning cycle ensures optimum application of resources and maximizes the potential for overall success. The deception tenets of centralized control and focus correspond with the top-down planning tenet of the MCPP. However, Marines must consider the unique security requirements for deception, such as the tension that arises in keeping everyone involved in the planning while still maintaining security (see Figure 3-1).

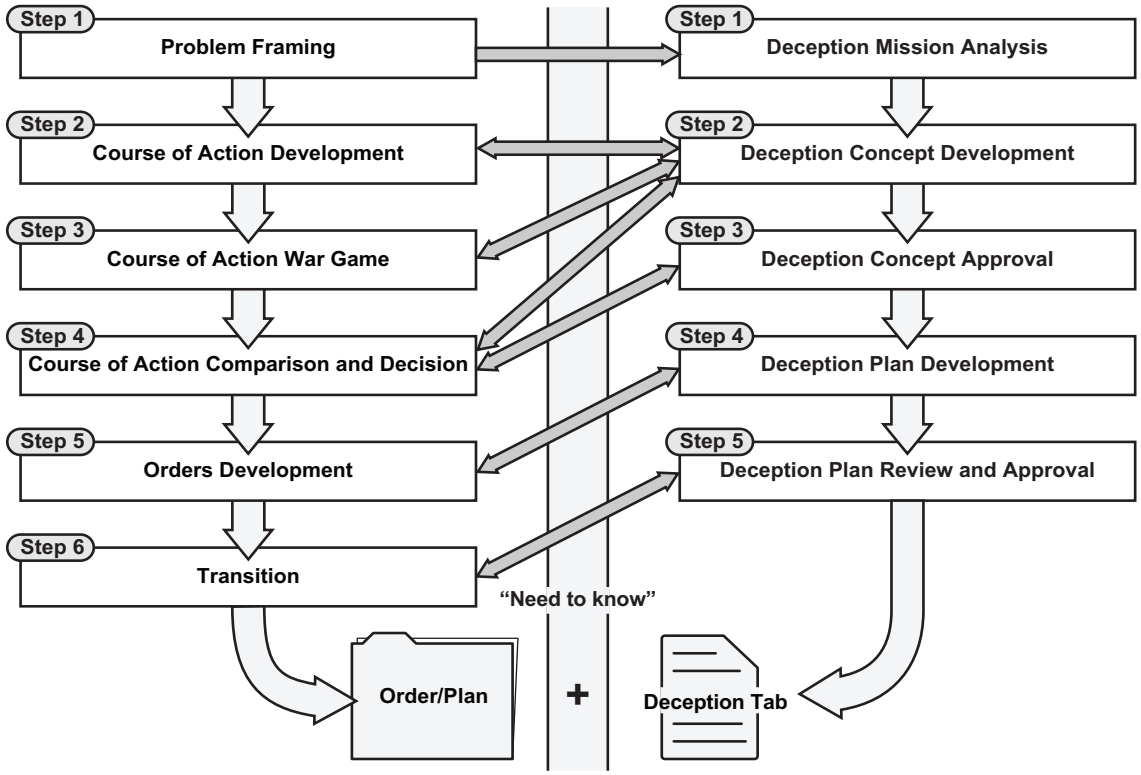


Figure 3-1. Marine Corps Planning Process and the Tactical Deception Planning Process.

Because of deception planning's inherent sensitivity, access to it is usually protected. As a result, TAC-D planning requires an access-controlled, parallel planning process rather than open discussion in an operational planning team (OPT). Key staff members and leadership that have access to the TAC-D plan discretely integrate and deconflict TAC-D planning outputs into the overall planning effort. Marines balance the need to coordinate TAC-D planning with the need to maintain secrecy for effective TAC-D operations.

The MCPP is conducted using six steps:

- Problem framing.
- COA development.

- COA war game.
- COA comparison and decision.
- Orders development.
- Transition.

These steps, while generally sequential, are interactive and require iterative development. The TAC-D planning process parallels the MCPP, but consists of five steps:

- Deception mission analysis.
- Deception concept development.
- Deception concept approval.
- Deception plan development.
- Deception plan review and approval.

These steps are informed by, and interact with, the MCPP steps as mediated by the need-to-know security considerations.

The following four considerations apply to deliberate TAC-D planning:

- Reexamine Planning Criteria. As with all planning, TAC-D planning is an iterative process in which planners must continually reexamine goals, objectives, targets, stories, and means. Commanders and staffs must respond to dynamics of the situation and to their headquarters.
- Organize for TAC-D Planning Success. At the MAGTF level, the MDO oversees functional planning for deception operations. Expertise is provided by one or more deception planners from the Marine expeditionary force (MEF) G-3 fires and effects coordination center (FECC) or the MEF information group. The MAGTF's deception planning cell (DPC) consists of personnel from the MEF G-3 FECC, the MEF information group, and deception planners from MSCs or MSEs. The MDO is typically a core member of the OPT or crisis action team. The OPT or crisis action team is formed by either the G-5 or G-3 as dictated by the commander and chief of staff. Additionally, the MDO generally forms a DAWG comprising key, cleared staff members who perform the parallel steps of the TAC-D planning process. The DAWG consists of the DPC, the G-3 OPSEC planner, and representatives from G-2, G-3, G-39, G-4, G-5, G-6, G-9, and SJA. In accordance with the commander's guidance and under the authority of the G-3, the DPC (supported by the broader DAWG) plans, directs, monitors, and assesses TAC-D operations. If directed, the DPC also provides planning, execution, and termination support for joint MILDEC operations undertaken by higher command echelons in the DPC's operational area. The DPC is typically tasked to develop the deception tab of the overall order or plan. Other DPC responsibilities include—
  - Directing and coordinating deception planning activities.
  - Interfacing and working with unit operations planners to review and analyze deception plan requirements.
  - Responding to higher headquarters' deception tasking.

- Coordinating with higher headquarters on proposed deception efforts to resolve potential conflicts.
- Looking for opportunities to implement deception in support of military objectives.

- Plan TAC-D Operations from the Top Down. Subordinate deception plans must support higher-level plans. Commanders at all levels can plan TAC-D operations but must coordinate their plans with their senior commander to ensure overall unity of effort. Operations security might dictate that only a select group of senior commanders and staff officers know which actions are deceptive in nature. To avoid confusion, commanders and their staffs closely monitor planning actions.
- Coordinate Deception and OPSEC Planning Efforts. Deception and OPSEC are complementary capabilities. In addition to the primary planning goal of unifying what is visible to adversary decision makers into a holistic and managed denial and deception effort, TAC-D and OPSEC planning intersect at multiple points in the MCPP. In execution, deception activities frequently require OPSEC measures and countermeasures to protect sensitive means and resources, and ultimately enhance believability to the adversary.

The following sections consists of a detailed examination of the TAC-D planning process as conducted during the MCPP, and highlights the considerations, estimates, and products that support the development of the plan or order. The TAC-D planning process is derived from the joint MILDEC planning process provided in JP 3-13.4.

Step 1: Tactical Deception Mission Analysis.

Step 1 parallels the problem framing step of the MCPP. Figure 3-2 outlines the primary key injects, DAWG activities, and key results for this planning step. Since deception is a protected effort, the commander's initial deception guidance may come in a separate written or verbal deception planning directive.

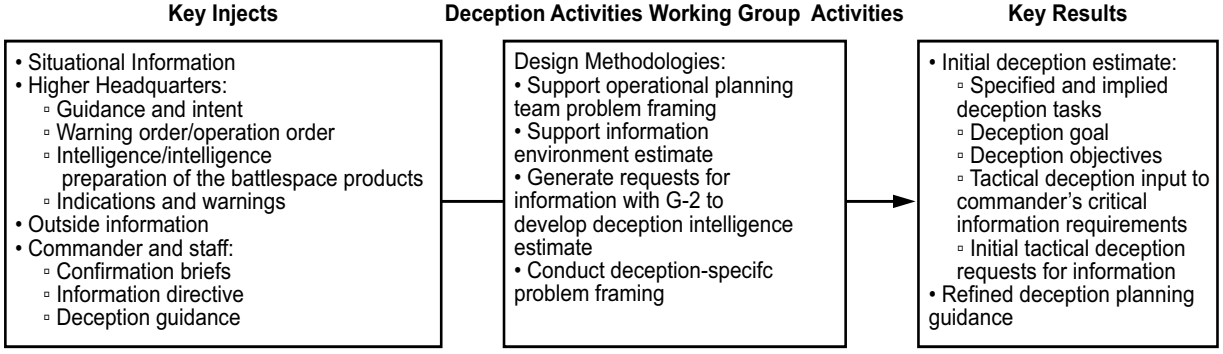


Figure 3-2. Tactical Deception Mission Analysis.

In the absence of specific guidance for inclusion of deception in the commander's initial operational approach, the DPC uses mission analysis to evaluate all appropriate planning references and guidance to determine whether TAC-D can or should have a role in the overall campaign. The role, when identified, is stated as a proposed deception goal(s) and associated deception objectives. There can be multiple deception goals based on considerations such as operational phasing, duration, or complexity.

Deception planners participate in the OPT and information working group, which use design methodologies to conduct problem framing per MCWP 5-10. Deception planners integrate, refine, and contribute to the outputs from other staff sections, such as planning facts and assumptions, information environment estimates, operational limitations, initial risk determinations, and developing overall success criteria.

During the deception mission-analysis step, deception planners work with the G-2 through the request for information (RFI) process, wherein they obtain analysis of the adversary that might be critical to effective deception planning. This information forms the basis of the deception intelligence estimate (DIE), which supports the development of a viable deception concept in the next TAC-D planning step.

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

Step 2: Tactical Deception Concept Development

Step 2 parallels the COA development, COA war game, and the first half of the COA comparison and decision steps of the MCPP. During TAC-D concept development, deception planners combine operational art with the TAC-D planning process to develop a viable concept of how TAC-D can achieve the commander's approved deception goals and objectives. This involves developing one or more distinct operational approaches based on the complexity and various COAs developed by the OPT. The primary planning inputs and outputs for deception concept development are shown in Figure 3-3.

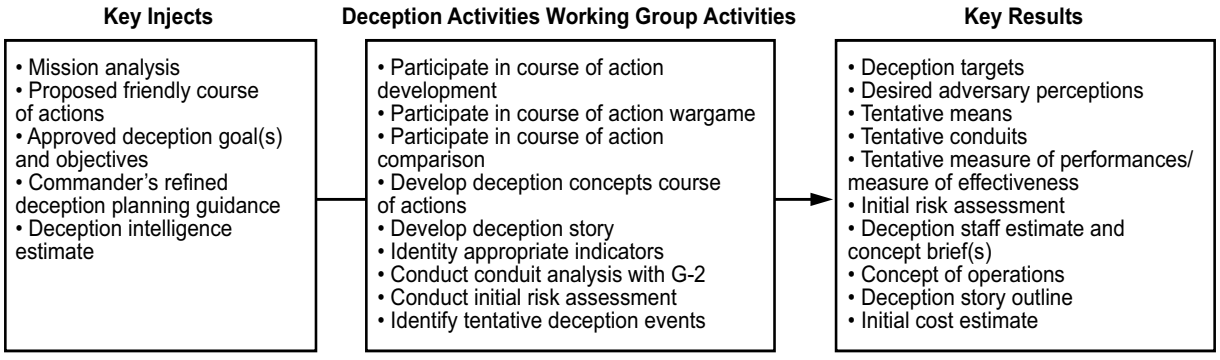


Figure 3-3. Tactical Deception Concept Development.

Using the initial staff estimate, any revised commander's planning guidance, and a detailed knowledge of the adversary contained in the DIE, deception planners in the DAWG develop one or more deception concepts or COAs. The actual number is determined by considerations such as the number of deception-suitable COAs developed by the OPT and time and personnel available for deception planning.

The DAWG develops TAC-D COAs using the same baseline operational sequencing and phasing as the OPT. Depending on the scope and complexity of the planned operation, TAC-D plans can range from simple and short duration to complex and long duration, although typically not as complicated as joint MILDEC. Based on the approved TAC-D goals and objectives, the TAC-D COA might include multiple lines of operation (LOOs). Deception planners might also be asked to support branch and sequel planning once the base COA is selected and finalized.

Each proposed deception concept or COA must be capable of accomplishing the commander's deception goal(s) and meet requirements for COA sufficiency. The proposed concept or COA must be adequate, feasible, acceptable, distinguishable, and complete. In some cases, actual COAs developed by the main OPT provide the basis for TAC-D COAs. For example, portraying the operational indicators associated with COA "A" in support of COA "B" or vice versa. The OPT develops alternative COAs to ensure the deception COAs are feasible, practical military operations. Additionally, the proposed deception COAs should seek to promote actions the adversary is already conducting or considering.

Each TAC-D COA developed in parallel with the MCPP contains, at a minimum, the following information:

- Deception target(s).
- Desired perceptions arranged in a preliminary deception story.
- Proposed deception types, techniques, or tactics.
- Tentative conduits.
- Draft measures of performance (MOPs) and measures of effectiveness (MOEs).
- Preliminary sequencing, concept sketches, and accompanying narrative for presentation in the COA selection brief.
- Initial risk assessment.

Additionally, deception planners observe the OPT wargaming process for each COA to incorporate the action, probable reaction, counteraction, assets, and time used into the TAC-D COA.

The first step in creating the desired action or inaction, as defined in the deception objective, is identifying the deception target with the authority to make that action or inaction. Key considerations in the appropriate selection of the deception target include—

- Understanding the target's relationship to the TAC-D objective's action or inaction; their position relative to adversary goals, aims, and strategy.
- Current perceptions.
- Decision-making process.
- Key advisors.
- Primary means of collecting information.

As planning progresses, intelligence analysts supporting TAC-D planning might be asked to develop individual target folders on specific deception targets to aid in later completion of the plan.

The design considerations reflected in the development of the deception goals and associated objectives, and their alignment with potential LOOs, determine the number of TAC-D targets across phased operations. For example, multiple avenues of advance for the ground combat element supports an ambiguity-increasing TAC-D targeted at the commander controlling the adversary's operational reserve; simultaneously, an ambiguity-decreasing TAC-D supporting aviation freedom of movement during a key portion of the operation targets the adversary commander's air defense unit.

In some cases, deception planners and supporting intelligence analysts identify key individuals who, by virtue of their position or personal relationships with a decision maker, influence the TAC-D target's decision making without formal or direct participation. These individuals are stakeholders and can either be conduits or filters depending on how they are used within the TAC-D plan. For example, stakeholders may affect the TAC-D's target's decision through the addition of aggregation, synthesis, or bias to an observable on the way to the deception target, or influence the deception target without participating in the formal decision process generating the action or inaction.

After selecting the deception target(s), the deception planner establishes the desired perceptions that will focus future deception events. Desired perceptions are the conclusions, official estimates, and assumptions the TAC-D target uses in their assessment and decision-making process. These adversary perceptions are formed from both objective (observation and analysis) and subjective (intuition and experience) thought processes. They are also affected by biases, preconceptions, and filters applied in information collection, analysis, delivery, and reception. To construct a logical flow blending truthful and deceptive information and indicators (observable conditions) later in the plan, deception planners determine the target's current perceptions and assess the potential for change or reinforcement. Desired perceptions also exploit known adversary vulnerabilities in the physical, informational, and cognitive dimensions of the information environment.

Planners include desired perceptions in the preliminary deception story. It is stated as a series of logical adversary conclusions about friendly capability, activity, and intent derived from all available observable. Deception stories are usually arranged in chronological sequence to facilitate planning and synchronizing events across phases or LOOs. The deception story is the "think" in the "see, think, do" methodology.

Time is a key consideration when developing the deception story. Deception planners must determine how much time is available to present the deception story and estimate how much time is required for the deception target to make a decision and direct the desired action. The available time determines the scope and depth of the story. The following time-related issues can arise when developing the deception story:

- Time of Maximum Disadvantage. When does the adversary's action (or inaction) best suit the commander's objectives?
- The Deception Target. Is the target cautious or bold? Will the target react to initial indicators, or will the target require a series of events before reaching a decision? How long does it generally take the target to make a decision?
- Target Response Time. Once the decision is made, how much time does the target need to formulate and issue an order? For example, if the deception objective is the movement of an

adversary mobile reserve to some distant point, allow time for the deception target to issue the movement order and for the unit to receive and execute the order.

- Intelligence Processing. How much time is needed for the adversary's detection and collection systems to collect, analyze, and provide false intelligence created by the deception to the deception target? This varies depending on the target's level of command.
- Executing Deception Tasks. When should displays, demonstrations, feints, and other actions be detected or recognized by the adversary's intelligence collection methods and systems? How long should each last?

During concept development, the deception planner typically begins to refine their approach by selecting appropriate TAC-D types (ambiguity increasing or ambiguity decreasing), TAC-D tactics (feints, demonstrations, ruses, or displays), and applicable TAC-D techniques to help structure the development of key TAC-D events that will constitute the detail required to determine COA viability and desirability. Refer to Chapter 2 for a description of these terms.

The DAWG uses the preliminary deception story and proposed friendly COAs to identify indicators that most effectively portray the deception story. The DAWG then aligns those indicators with one or more adversary conduits to create an observable effect and begins selecting the deceptions means to activate those conduits. This creates the "see" in the "see, think, do" methodology. By analyzing which indicators most effectively portray the friendly activities and profiles that convey the deception story, the deception planner can better focus the selected techniques and apply limited or costly means in a more effective manner. Contrast and anticipated exposure must also be factored into the deceptive portrayal.

Indicators are the "puzzle pieces" the deception planner creates to lead the adversary to a desired perception and subsequent conclusion. This activity directly complements the denial and deception constructs by concealing critical information and indicators related to the commander's actual COA. Additionally, the TAC-D plan provides plausible alternatives that require the adversary to respond. Joint Publication 3-13.3, *Operations Security,* identifies five characteristics of an indicator that provide important understanding to the deception planner when selecting which indicators to portray the deception story (see Table 3-1).

Table 3-1. Characteristics of an Indicator.

Characteristics	Description
Signature	Characteristic that is unique and makes an indicator identifiable—causes it to stand out.
Association	Relationship of an indicator to other activities.
Profile	Sum of signatures and associations for an activity
Contrast	Difference or deviation between activity's standard profile and its most recent or current activities.
Exposure	When and for how long an indicator is observable.

To identify the indicators that effectively portray the deception story, planners must have detailed knowledge of friendly operational profiles and reliable, correct intelligence on how the adversary "sees" the operational environment. An operational profile is everything that a friendly force does to prepare, conduct, and sustain operations. Creating observable in this step aligns key indicators with adversary collection conduits and processes identified in the DIE. For example, if the

deception plan calls for creating the perception that an additional infantry battalion in located on alternate axis of advance, planners must create an effect that is observable by adversary signals and human intelligence. To create that observable effect, deception planners need to know what communications systems are in the dispersed units and how they typically operate, vehicle types and quantity, where and in what pattern the vehicles are typically employed, and the supporting logistical infrastructure footprint. Although the unit supporting such an execution finalizes the details, the DAWG uses the details outlined during COA development to assess concept feasibility.

The MSC and MSE planners develop indicator and profile information. To increase planning efficiency, deception planners, working with OPSEC planners at each MSC and MSE, develop friendly profile databases prior to the initiation of planning. This is particularly helpful when planning is time constrained. Such a database might contain profile data (e.g., all physical, technical, and administrative signatures and typical associations) for each service, capability, or function (e.g., information, logistics, intelligence collection) by mission-essential task, activity, or any other logical conceptual boundary that facilitates analysis and subsequent ease of reference.

Once the deception planner understands the indicators and available adversary conduits that will be used to create the observables required for each perception in the deception story, the planners determine which are already visible to the adversary as part of the planned base COA and identify observables that must be altered or created as part of the deception plan. An example of this blending would be leveraging the actual logistical staging of the assault force in a way that supports the deception story versus using deceptive means to portray equivalent actions at an equally advantageous location. As with other steps in deception planning, this requires a detailed and current understanding of the OPT's plan, as well as the activities of various information forces coordinated by information planners (e.g., FECC, FSCC, MEF information group).

Another key aspect of this step is identifying and mitigating competing observable conditions. Planners use OPSEC measures to hide competing observable conditions If the observation of the competing conditions cannot be mitigated, planners use other deceptive means to creates plausible explanations.

Once the DAWG identifies which observables convey the deception story, the process of aligning specific means to create them begins (see Chapter 2 for more information). The DAWG develops tentative events for each proposed COA to facilitate the COA analysis and wargaming, comparison, and COA approval (selection) steps of the MCPP.

Planners must consider several factors when developing and planning deception events. One of the first considerations in potential means selection is sensor-conduit linkage. For example, what adversary sensors are positioned to observe the selected indicator in the location and timeframe it would logically occur? Marines should employ complementary physical, technical, and administrative means that activate various sensor types to process information through both simple and complex conduits to the deception target. Considerations include the following:

- How will Marines know the sensor is active and transmitting information through the conduit?
- What is the anticipated reaction of adversary forces when the means are employed?
- What risks are associated with the means of employment (in terms of risk to force or risk to mission)?

Selecting which tentative deceptions means to employ has substantial implications for friendly forces and operations. The DAWG coordinates with other planning groups to address considerations such as who will control employment of the deception means and what are the preparatory steps and associated timeline. Considerations include the following:

- What is the breadth of need to know for the unit conducting the deceptive activity?
- How long or frequently will this indicator need to appear (exposure) to make sure it is observed?
- What is the concept for employing the deception means and what are the operational conditions and criteria that need to be established to optimize effectiveness in portraying the desired indicator?
- How will the employment of deception means be terminated and under what conditions?
- What is the estimated cost (in dollars, other resources, and operational efficiency) associated with this event?

When developing tentative deception events, the deception planner must consider MOPs and MOEs (see Chapter 6). Proposed events that cannot be aligned with viable assessment criteria are not suitable for further development. Deception planners should identify at least one MOP and MOE for each proposed event or event series.

As the deception planner begins aligning deception means with selected indicators to generate observables, they must sequence events that supports completing and briefing the concept or COA. Planners can sequence and align tentative events by various typographies to include LOO, desired perception, phase, component, geography, time, or any combination of the above. The DAWG uses this initial sequencing and alignment to build a more detailed product called the deception event schedule (DES) in TAC-D planning process step 4 (deception plan development).

Once the DAWG completes the above steps, they prepare sketches and an associated narrative that the salient concept elements. Sketches should graphically represent information such as the timing, relationship, and control of key proposed events or groups of related events (i.e., deception series); the conduits used to transmit the planned observables to the adversary decision maker; the location and function of key filters; the time for processing the observable and any subsequent decision or order by the deception target; and any competing observables, along with their proposed mitigation plan. The narrative links the illustrative COA sketches and provides additional detail necessary to facilitate understanding. A sample sketch, one of several that might be part of a final COA briefing, is depicted in Figure 3-4.

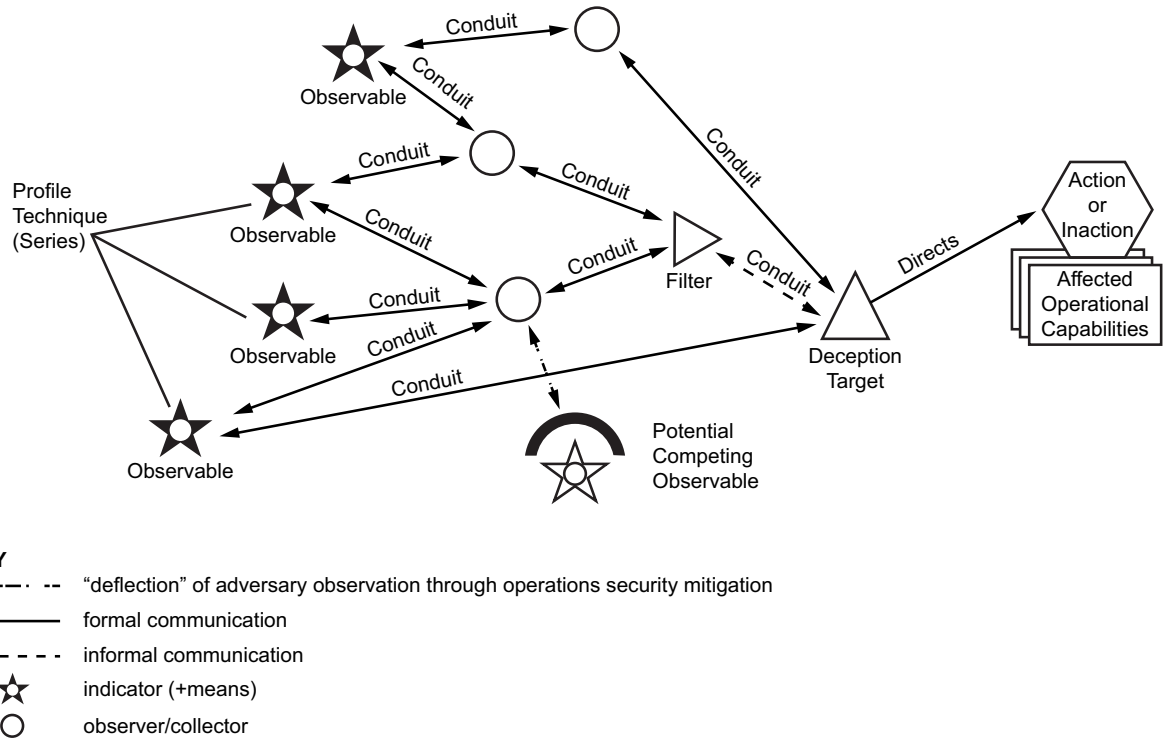


Figure 3-4. Sample Deception Course of Action Sketch.

The final component that must be addressed as a basic part of the TAC-D concept or COA development is risk. Deception planners must conduct a risk analysis on each deception event, series, LOO, and deception concept to inform the commander's evaluation and subsequent approval. Risk management begins in the planning process and continues through preparation, execution, and assessment. The four general categories of risk associated with deception include deception failure, exposure of means or feedback channels (compromise), risk to third parties, and risks associated with deception success. Each risk category is described as follows:

- Deception Failure. TAC-Ds fail for many reasons. It is possible the target will not receive or believe the story, be unable to act, be indecisive even if the story is believed, act in unforeseen ways, or discover the deception operation. The failure or exposure of the deception operation can significantly affect friendly operations by reducing or eliminating the operational advantage that the deception operation was to provide. For this reason, a commander must understand the risks associated with basing the success of any operation on the assumed success of a deception. There are two broad categories of deception failures: deception planners either fail to plan or implement the TAC-D operation carefully enough, or the intended target detects the deception.
- Exposure of Means or Feedback Channels (Compromise). Even if a TAC-D is successful, it is possible for the adversary to compromise the deception means or feedback channels. The risk of compromising sensitive deception means and feedback channels must be carefully weighed against the perceived benefits of a TAC-D operation.
- Risk to Third Parties. Third parties (e.g., neutral or friendly forces not aware of the deception) might receive and act on deception information intended for the deception target. Deception

planners must ensure they are knowledgeable about friendly operation planning at the joint and multinational force level and at the component level to minimize the risk to third parties.

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

Step 3: Tactical Deception Concept Approval

Step 3 in the TAC-D planning process is performed in parallel with the second half of the MCPP step 4, COA comparison and decision. The TAC-D concepts or COAs are typically presented in an access-controlled briefing attended by a subset of the staff, the command group, and other personnel with a demonstrated need-to-know requirement. Prior to the briefing, the DAWG analyzes the strengths and weaknesses of proposed TAC-D COAs using the same or similar criteria developed by the G-5 or G-3 for primary COA comparison in the OPT. Some major considerations are feasibility, effects on actual operations, and security. Planners must also consider how the deception COAs support the overall concept for information. Planners preparing logistics, personnel, and intelligence estimates must determine whether the concepts can support the proposed deception COAs and the potential effect of each deception COA on its ability to support the operational mission. Typically, the MDO identifies which TAC-D concept or COA best achieves the commander's objectives while still aligning with the OPT-recommended COA.

The TAC-D concepts and proposed COAs are briefed prior to the OPT briefing, which facilitates a COA decision. When the commander finalizes the base COA selection, the DPC is informed which deception concept or COA is to be developed into a completed plan and provided with any additional commander's guidance or changes to previous guidance necessary to align the TAC-D effort with the approved base COA.

Step 4: Tactical Deception Plan Development

Step 4 in the TAC-D planning process is performed in parallel with the MCPP step 5 (orders development). Following COA selection, the MAGTF staff applies their previous work and any revised commander's guidance issued in the COA selection step to refine and complete their portion of the plan. The G-2 continues to develop intelligence based on RFIs, while the OPT refines the design approach. The MAGTF and MSC plans result in MSC tasks, which are captured in the operation plan (OPLAN) or operation order (OPORD), and in tools and formats that support future execution, such as the synchronization matrix. This results in a series of nested joint and functional component plans and orders. Deception planners perform these same tasks relative to developing and finalizing the TAC-D plan. Figure 3-5 illustrates the key injects, DAWG activities and key results of this step.

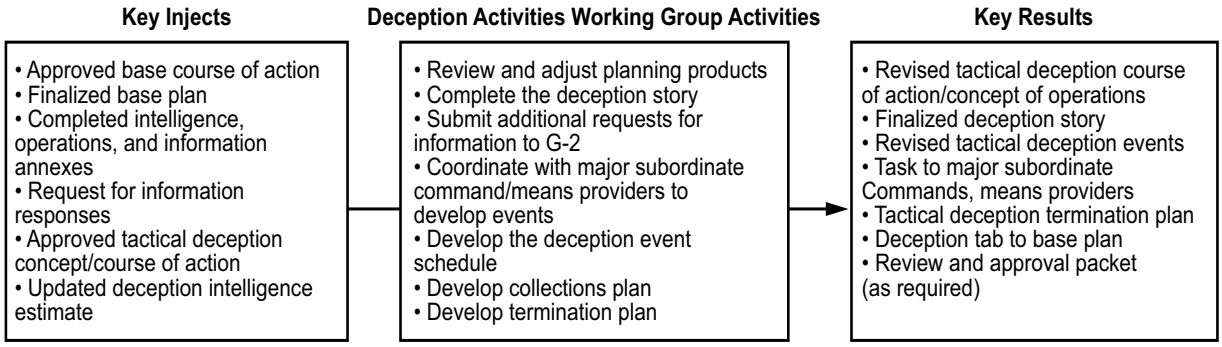


Figure 3-5. Tactical Deception Plan Development.

Using the approved TAC-D COA or concept as a base, the deception planner integrates revised commander's guidance, updated intelligence analysis, and revisions to the primary COA to refine and complete the TAC-D plan. The initial step in this process is to review all previous planning products and adjust them as required. Considerations include the following:

- Are the TAC-D goals and objectives still appropriate to the commander's objectives and end states?
- Are the phasing, LOOs, selected deception targets, deception story, and key indicators still valid and complete?
- Are the selected deception means still appropriate to the conduits identified?
- Have any previous planning assumptions been invalidated?

Following adjustment of the original concept, the DAWG finalizes the deception story to complete the TAC-D plan. Using the same flow of activity used to build the TAC-D COA, the DAWG refines and increases the level of detail as required to fully execute the plan. This involves significant coordination with MSCs and providers of deception means to build planned deception events and series. Planners must continue coordinating with the G-2 to identify remaining intelligence gaps and plan the appropriate intelligence collection assets to support MOP and MOE collection necessary to assess and adjust the TAC-D plan (see Chapter 6).

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

The following factors are considered during deception event scheduling:

- The timing of actual friendly activities.
- The time required for friendly forces to conduct the deception activity.
- Where a particular activity fits in the sequence of events for the operation being portrayed.
- The time required for the adversary intelligence collection assets to collect, analyze, and report on the activity.

- The time required for the deception target to make the desired decision and order the desired action.
- The time required to execute the desired action/inaction.

Each planned deception event is given a unique number to facilitate coordination and execution tracking. The DES is published as an exhibit to the deception tab of the OPLAN or OPORD. Table 3-2 provides an example DES.

Table 3-2. Sample Deception Event Schedule.

Identification Number	Objective	Deception Target	Date/ Time to Initiate	Action	Means	Unit	Date/ Time to Terminate	Remarks
29	Simulate preparation for movement south	Enemy 6th Corps Commander	131500	1. Establish traffic control points 2. Install radio nets 3. Pass scripted message traffic per scenario	Friendly force movement and organic systems	Headquarters 2d Division	131800	Initiate counter surveillance measures to prevent adversary visual photo reconnaissance of notional route

The completed DES forms the basis for tasking and integrating JFC components and providers of deception means in the OPORD.

There are various circumstances that create a requirement to terminate the TAC-D in whole or in part. Developing contingencies for this is referred to as termination planning.

Termination planning ensures the controlled, orderly cessation of planned TAC-D events; protects means and resources; and sets the parameters for any release of information relating to the deception. Planning the termination of a deception operation requires the same care and attention to detail that goes into planning the deception's execution. Termination planning includes contingencies for unforeseen events, such as the deception's premature compromise. In the event of compromise, termination planning for TAC-D includes a notification to rapidly inform those who might be affected.

There are numerous potential termination scenarios. They are typically similar in concept to scenarios used to identify risk in the previous step. Termination scenarios include the following:

- Successful TAC-D 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 changes and the circumstances that prompted the TAC-D no longer pertain.
- Recalculated Risks and Probability of Success. Some elements of the deception estimate have changed in a way that increases the risk and costs to the friendly forces and the commander elects to end the TAC-D component of the COA.

- Poor Timing. When the TAC-D is proceeding and may succeed; however, it is not along a timeline that is synchronous with other information-related capabilities (IRCs), aspects of the operation or campaign, or it becomes evident that the window of opportunity for exploiting certain conduits or the target itself has closed. In this case, the TAC-D ceases to be relevant to the overall operation.
- New Opportunity. At some point in the execution of the TAC-D, it becomes apparent that if some elements of the TAC-D (e.g., choice of conduits, objectives, targets) are modified, the probability of success increases, risks are reduced, or the impact of the deception is greater. In this case, the commander may want to terminate some TAC-D events and activities, while reorienting other elements of the TAC-D.
- TAC-D Compromise. The commander has cause to believe that all or some elements of the TAC-D have become known to the adversary.

The termination concept provides the initial planning considerations to implement and includes the following:

- Brief descriptions of each termination scenario circumstance included in the plan.
- Initial steps for initiating termination operations in each scenario circumstance included in the plan.
- Identity of the commander with termination authority.

The DPC anticipates that as the plan proceeds in execution, the circumstances of termination will probably change. A termination concept entirely suited to the initial set of conditions might be far different from what is required as the TAC-D matures.

The termination concept identifies what information about the TAC-D is released and when. It can include "background details" should questions arise about the role of TAC-D in a particular operation. The termination concept should also include classification and dissemination instructions for deception-related information.

After completing the DES and termination plan, the TAC-D planner has everything required to complete the deception tab in the OPLAN or OPORD. Planners can use exhibits, worksheets, and templates when developing the TAC-D plan to add clarity and detail to an off-the-shelf plan. These products can assist personnel not involved in the original planning process to rapidly understand the TAC-D concept (for review or contingency activation). If higher-level approvals are required, this tab and selected exhibits also form the basis of the deception plan review and approval package.

Step 5: Tactical Deception Plan Review and Approval

Marine Corps Order S3490.01, *(U) Marine Corps Deception Activities*, stipulates review and approval requirements and processes. However, the need-to-know criteria remains in effect and only a limited number of personnel participate in the deception plan review and approval process.

TACTICAL DECEPTION PLANNING DURING THE RAPID RESPONSE PLANNING PROCESS

The R2P2 is typically associated with the MEU; however, other elements can also conduct this process. The R2P2 is designed so Marines spend less time planning, thereby maximizing the time executing forces have to prepare for the mission. When circumstances impose severe time constraints on the executing command, the commander and the staff must allocate enough time to develop a feasible COA, coordinate critical details, and prepare for execution. The R2P2 is dependent on having capabilities in four areas: integrated planning cells, planning and operations SOPs, intelligence, and information management.

Given the compressed timelines associated with R2P2, elaborate deception plans are not suitable. Goals and objectives for deception plans, if applicable at all, are typically narrowly scoped and limited in nature. However, simple employment of deceptive tactics can support the achievement of tactical missions. For example, suppressing or amplifying radio traffic can obfuscate the timing of a tactical recovery of aircraft and personnel mission launch, or a feint by the supporting effort might draw adversary attention away from the main effort's amphibious landing.

Proactively developing potential deception COAs and target and conduit analyses for anticipated missions helps mitigate compressed timelines. These preparatory efforts are closely coordinated with the MEU S-2 and amphibious readiness group N-2, as well as the information warfare commander, if designated, to enable rapid, effective planning as required.

If TAC-D is planned during R2P2, the sequence of planning steps mirrors steps outlined in the above sections. Refer to Appendix H of MCWP 5-10 for additional details on R2P2.

Deceptive Tactics

Marines use deceptive tactics (feints, demonstrations, rues, displays) to gain a momentary advantage during operations. Additionally, deceptive tactics include camouflage, concealment, and decoys as a force protection measure (see Table 3-3).

Planners maintain categories of deception that do not meet the threshold of TAC-D. For example, employing a false battalion command post with extra tents and camouflage netting for the purpose of enhancing the survivability of the real command post is not considered TAC-D.

Deceptive tactics are best conducted at echelons below an MSC, where SJA or appointed MDO review is unlikely. Military deception officers should ensure small-unit leaders understand the applicability and limitation of deception tactics, the criteria for when to use deception tactics, and when using such tactics must be reported to higher headquarters. Additionally, deceptive tactics requires close coordination with higher and adjacent units to ensure effectiveness and prevent friendly fire incidents.

At the small-unit level, leaders should implement deceptive tactics to increase survivability or force protection during combat operations—provided these tactics are in accordance with the law of war and US policy. (For more information see MCTP 11-10C, *The Commander's Handbook on the Law of Land Warfare*).

Table 3-3. Deception Considerations.

	Joint MILDEC	TAC-D	Deceptive Tactics
Employment	Targets an operational level adversary commander for the purpose of taking an action or inaction that supports CCMD or joint task force objectives.	Targets a tactical level adversary commander for the purpose of taking an action or inaction that supports a friendly tactical commander's objectives.	Employment of camouflage, concealment, and decoys, and the use of the four tactics of deception for the purpose of survivability and force protection.
Planning	Planned by a DAWG at the CCMD and Service component level.	Planned by a DAWG at the MSC level and above.	Planned and executed by all Marines from the regimental/group to the fire-team level.
Advantage	Provides an advantage to an operation or campaign.	Provides an advantage to a major battle or engagement.	Provides an advantage to individual Marines and small units.
Authority	See SECRET annex.	Requires approval from any general officer in chain of command.	Subject to unit SOPs.

For further information on employing camouflage and concealment, refer to Marine Corps Tactical Publication (MCTP) 3-34C, *Survivability Operations*.

CHAPTER 4.
TACTICAL DECEPTION EXECUTION

The TAC-D plan is executed as a component of the MAGTF OPLAN or OPORD. When a MAGTF receives an execute order for a given plan, the associated TAC-D plan may also be activated within the given authorities and approval processes as outlined in MCO S3490.1 and CJCSI 3211.01, *(U) Joint Policy for Military Deception*. The DPC, assisted by the DAWG, primarily handles the transition from the TAC-D plan to TAC-D execution. MCWP 5-10 identifies numerous staff actions to transition a plan from future plans or operations to current operations. This same process is applied to transitioning the TAC-D plan, although the same core deception team carries the plan through execution rather than transferring it to different personnel.

DECEPTION EXECUTION COORDINATION

Once a TAC-D plan is activated, it is critical for planners to constantly coordinate at the strategic, operational, and tactical levels as there is potential for a tactical-level deception operation to have strategic implications. To ensure this continual coordination, planners use the deception execution cycle (see Figure 4-1).

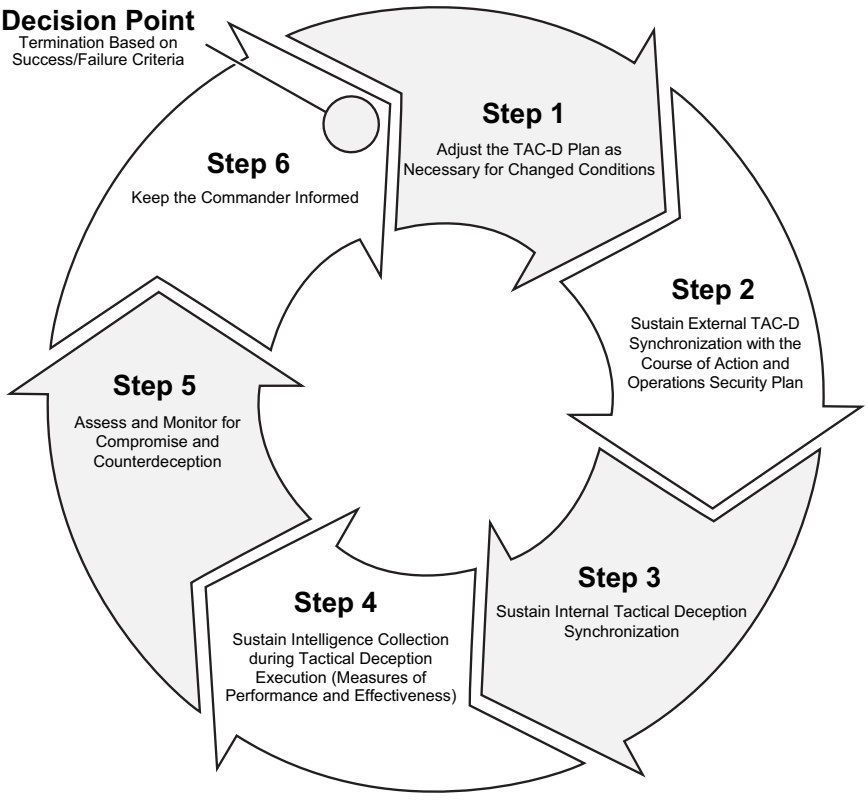


Figure 4-1. Deception Execution Cycle.

Step 1: Adjust the TAC-D Plan as Necessary for Changed Conditions

The deception execution cycle begins with the DPC and DAWG reviewing the TAC-D plan. In this step, the DPC and DAWG analyze the current situation and compare it with the operational environment, anticipated conditions, and planning assumptions. Existing RFIs are reemphasized, and new RFIs are developed to address shortfalls in necessary intelligence. Sample DPC and DAWG activities in this step include—

- Reviewing and identifying changes to the adversary's situation. Examples include but are not limited to the following:
  - Changes to adversary decision-making process or key military decision makers.
  - Changes in adversary force structure, disposition, and intelligence collection (conduits or information pathways) to best facilitate the effective delivery of the deception story.
  - Changes in third-party intelligence support.
  - Potential new sources of open-source intelligence based in rapidly evolving social media or other networks.
- Reviewing and identifying changes to the friendly plan. Examples include the following—
  - Revised strategic or commander's guidance.
  - Changes to allocated forces or their flow into theater.
  - Additions, subtractions, or changes to relationships with multinational partners.
  - Changes to basing or overflight permissions.
  - Changes to available TAC-D authorities, resources, or tools.
  - Adjustments to operational phasing or timing. The DPC coordinates with the J-3 on initial deception and operations execution timing to ensure a synchronous, supporting relationship exists that aids the TAC-D, operation, or both.

Once the DP and DAWG update their knowledge of the adversary and friendly situations, all key elements of the plan, from the deception goal and objectives through the final DES, are validated or adjusted as required.

Although this is the first step in the deception execution cycle, it is also a continuous process as conditions evolve and change over the course of mission execution.

Step 2: Sustain External TAC-D Synchronization with the COA and OPSEC Plan

Among the TAC-D planner's most critical execution tasks is ensuring the TAC-D is proceeding in synchronization with the commander's overall operational concept and is in line with the command's employment of other information capabilities.

The DPC and DAWG coordinate vertically and horizontally with commanders and staffs to ensure up-to-date integration between ongoing operations and deception operations. This helps units synchronize the deception story and ensures the portrayal is credible, believable, and realistic. Changes to any operational aspect, such as presence, capability, strength, intent, readiness, future location, timing, or method of planned friendly operations, must be accounted for in the scheduled execution of TAC-D activities. This requires discrete TAC-D participation in the MAGTF's organizational elements that conduct functions such as situational awareness, targeting, assessment, and providing routine updates and operational analysis to the commander.

Because OPSEC measures and countermeasures often support deception activities, deception and OPSEC personnel must coordinate to ensure TAC-D and OPSEC are continuously synchronized to holistically portray friendly activities. This includes cooperation in targeting or exploiting enemy conduits, so they are either neutralized or available, as required, to create the desired OPSEC and TAC-D effects.

Step 3: Sustain Internal Tactical Deception Synchronization

Tactical deception executions, although planned in detail, are dynamic activities on an access-controlled DES or operational-level synchronization matrix. The DPC and DAWG maintain constant communication with components, capability owners, and other resource providers tasked to execute or support each event, so the portrayal of the deception story proceeds as planned. This includes operational-level tasks, such as synchronizing different TAC-D LOOs, and balancing or shifting lines of effort, as appropriate, to sustain the desired deception story progression. Based on feedback, planners might have to adjust, repeat, postpone, or cancel, as appropriate, some planned executions or event series.

Step 4: Sustain Intelligence Collection during TAC-D Execution

The DPC and DAWG work with the G-2 collection manager to help ensure collection assets are able to collect MOPs, monitor MOE and indicators, and inform the commander on the status and current levels of success or revised risk. During combat operations, the DPC and DAWG actively compete with larger components for limited intelligence collection resources.

Step 5: Assess and Monitor for Compromise and Counterdeception

The DPC and DAWG, using the analytic feedback provided by MOEs collected in conjunction with the assessment process, determine the current progression and success of the TAC-D plan. Specially trained intelligence analysts, supported by deception planners, remain alert for indications that one or more components of a deception story may have been compromised. This includes identifying any possible adversary counter-deception efforts. When analysts detect compromise, it can lead to one or more termination or exploitation scenarios.

Step 6: Keep the Commander Informed

The TAC-D operational status should be part of the commander's routine battlefield update and assessment processes. As the principal authority for executing the deception plan the commander is responsible for any decision to alter or terminate the deception operation or, conversely, order a change to either the TAC-D plan or the primary COA to exploit changing conditions. The TAC-D plan also factors in the overall computation of risk, as increased risk might generate a requirement to adjust the plan in other areas.

Maintain Strict Security and Access Controls

Marines must follow meticulous security practices throughout the deception execution cycle to protect the TAC-D plan. Although many decisions regarding need-to-know access are made in the planning process, situations arise that require legal and policy interpretation and adjudication from the command military deception officer (CMDO) and commander. The CMDO and commander must consider balancing the mission with risk, thereby reducing the chance of exposing the deception. In complex military operations, it becomes even more critical for all involved personnel to continuously apply appropriate classification, handling, and access controls. Any OPSEC or other security violations of the TAC-D plan at any echelon should immediately be

reported and evaluated for their potential effect on the deception operation. Frequently, the command counterintelligence staff will be assigned responsibility to monitor for foreign intelligence detection, reflections, or responses to the TAC-D plan.

When incorporating deception events into operations, it is helpful to characterize the participation of members of the staff or MSCs based on their intended level of knowledge or need to know. Witting participants have full knowledge of the plan. Partially witting participants are aware that there is a deceptive component to their activity, but do not have full knowledge of the plan. Unwitting participants are unaware of the deceptive nature of their activities. For example, a platoon tasked to establish a dummy position using various physical and technical decoys is aware they are employing deceptive means, but for OPSEC reasons they might not be told the purpose behind their display.

RELEVANT TASKING PROCESSES

The DES serves as the authoritative synchronization document for the commander and key staff members executing deception events. However, DES distribution is limited and is not typically available to all staff coordinating MAGTF operations. Thus, it is critical that DAWG members ensure each task is appropriately captured in the various tasking processes, documents, and battle rhythm events used coordinate operations across the MAGTF. Several tasking processes are described in the following sections.

Operations and Maneuver Tasking Processes

The assistant chief of staff (AC/S) G-3 is responsible for planning operations, and for preparing and disseminating warning orders, OPORDs and fragmentary orders. They also exercise staff cognizance for Annex C (Operations), Annex W (Aviation Operations), and Annex X (Execution Checklist). The G-3 should always be a witting participant of any TAC-D operation planned and key tasker to unwitting and partially witting units. Relevant operations products include the following:

- The operations synchronization matrix is developed during the COA development step of the MCPP. It is a working document that shows the activities of the command and subordinate elements over time, and displays how units, warfighting functions, and tasks interrelate throughout all operational phases. Additional details to this matrix can include displacement of the command post, priorities and location of the reserve element, information integration specifics, and sequencing of tasks and movements. During orders development, the completed synchronization matrix enables planners to efficiently assign tasks to subordinates and aids in developing Annex X (Execution Checklist) of the OPLAN or OPORD.
- Annex X (Execution Checklist) provides a listing of key events and tasks that the force must conduct to accomplish the mission. The synchronization matrix is the key MCPP tool used to create the execution checklist. The execution checklist allows subordinate commands and supporting and adjacent forces to coordinate their actions and maintain situational awareness. The execution checklist also serves as an excellent command and control and information management tool for the combat operations center. Critical events and tasks are included in the execution checklist. Events and tasks should be listed in the order of envisioned execution.

For further information on AC/S G-3 responsibilities, operations tasking processes, and relevant products refer to MCWP 5-10; MCWP 3-10, *MAGTF Ground Operations*; MCWP 3-30, *Marine Air-Ground Task Force Command and Control*; and MCTP 3-30A, *Command and Staff Action*.

Air Tasking Cycle

Aviation planners use the air tasking cycle to plan air operations that support the MAGTF's mission and to produce the MAGTF air tasking order (ATO) or air plan. The six-phase MAGTF air tasking cycle is compatible with the six-phase joint air tasking cycle. The six phases of the air tasking cycle are command aviation guidance, target and air support mission development, allocation and allotment, tasking, force execution, and combat assessment.

The key output of the air tasking cycle is the ATO. Planners use the ATO to task subordinate units and command and control agencies, and to disseminate the targets and specific missions of projected sorties, capabilities, and forces. It typically provides both general and specific instructions, including call signs, targets, and controlling agencies (refer to JP 3-52, *Joint Airspace Control*). The ATO can include the airspace control order, or it can be separately issued. The ATO also includes special instructions that provide amplifying notes, important details, and changes.

Aviation operations can be critical to generating observable physical or technical deception events. The MAGTF air officer may need to be a witting participant of the DAWG to ensure that these requirements are appropriately captured in the ATO while maintaining requisite security measures.

Refer to MCWP 3-20, *Aviation Operations,* for further information on the air tasking cycle and the ATO.

Targeting and Fires Planning

Targeting is the "process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities" (*DoD Dictionary*). It involves analyzing adversary situations relative to the commander's mission, objectives, and available capabilities. This analysis assists target planners in identifying and nominating specific vulnerabilities that, if exploited, will accomplish the commander's purpose.

There are two targeting processes: the decide, detect, deliver, and assess methodology (also referred to as the D3A methodology), and the joint targeting cycle. The decide, detect, deliver, and assess methodology is the Marine Corps' and Army's doctrinal targeting process. The joint targeting cycle is part of the joint targeting process (see JP-3-60 for more information).

Although the two planning methods differ in terminology and number of steps, both address the same basic functions needed for targeting.

Targeting Board. The targeting board is an extension of the planning effort. It translates conceptual and functional planning into the detailed plans needed for execution by serving as—

- A confirmation brief that reflects the staff's translation of the commander's guidance into functional and detailed plans.
- A decision brief where the commander approves the results of the targeting board, subject to modifications, for implementation during execution.

- A guidance session where the commander provides targeting guidance for subsequent targeting cycles.
- A MAGTF coordination and integration event where MAGTF equities generally participate at each board.

The MAGTF targeting board is a forum for members to present and discuss targeting objectives, desired effects, target priorities by category, recommended air apportionment, and other asset apportionments. The board also develops an integrated, prioritized target list of individual targets and recommended guidance for the commander's approval. It consists of representatives from each of the MSCs within the MAGTF and the staff sections.

Theater- and national-level agencies can send representatives to the targeting board depending upon the nature and scope of operations. Typically, the deputy commander chairs the MAGTF targeting board, acting as the commander's executive agent.

Typical products of a targeting board include the following:

- Apportionment decisions and subsequent allocation of sorties, including any off-the-top sorties made available in support of known JFC-wide requirements.
- MAGTF direct support targets, which are targets inside the existing or planned MAGTF area of operations. They come from the MAGTF integrated prioritized target list and include high-priority targets.
- Target nominations for higher headquarters sourcing either because of organic capability shortfalls or because other components in the joint force possess a more suitable capability.
- External target nominations, which are targets outside the MAGTF area of operations for higher headquarters sourcing in support of the MAGTF's shaping operations.
- Restricted, limited, and protected targets including those the MAGTF commander approves and ones that the tactical information section forwards for higher headquarters approval.
- Recommended fire support coordination measures for approval at the appropriate level.
- Guidance for the next targeting cycle.

During targeting board deliberations, planners consider nonlethal targets and target sets, along with related guidance, apportionment, nonlethal means, as well as lethal targets. However, deception targets and objectives are not necessarily discussed in the open forum of a targeting board. Therefore, the MDO, FECC, and AC/S G-3 coordinate to ensure that targeting options presented during the MAGTF targeting board are consistent with the deception plan, and that key nodes, sensors, and decision makers that comprise necessary conduits are not destroyed or affected in ways detrimental to the success of the deception plan.

Refer to MCWP 3-31, *Marine Air-Ground Task Force Fires and Effects*, for more information on fires and targeting processes.

Information Tasking and Control Cycle

MCWP 8-10 outlines an information tasking and coordination cycle (ITCC), which takes place within the structure of the MCPP. During operations, Marines pursue shaping, decisive, and sustaining objectives. The Marine Corps uses the shaping methodology to identify and align tasks against shaping objectives (refer to MCWP 3-31). The ITCC is a direct implementation of the Marine Corps shaping methodology. Information tasking and coordination cycle tasks are tasks against shaping objectives, while the information tasking and coordination order (ITCO) coordinates and reports tasks related to the conduct of information from the Marine Corps shaping methodology and other tasking cycles within the broader MCPP. The ITCC, which parallels the joint targeting cycle, consists of the following phases:

- Commander's objectives, guidance, and intent.
- Target and relevant actor development and prioritization.
- Capabilities analysis.
- Commander's decision and force assignment.
- Mission planning and force execution.
- Assessment.

The Marine Corps ITCO is developed during the fourth phase of the ITCC and directs units to conduct or coordinate information activities. The primary organizations that produce and publish an ITCO are the MIGs and Marine Corps Information Command (MCIC). The ITCO is based on the commander's guidance as written in the information directive. Information direction and control instructions should be provided in sufficient detail to allow units of action to plan and execute all missions listed in the ITCO. These are usually captured in the coordinating instructions and the special instructions.

As with each of the other processes described, OPSEC considerations usually preclude openly describing deception tasks in documents such as the ITCO. The MDO or DAWG, under the cognizance of the FECC, is responsible for ensuring that tasks to information forces in the ITCO align with the deception plan, and that required support from witting or unwitting participants is appropriately captured throughout.

For further information on ITCC, ITCO and other aspects of information in Marine Corps operations, refer to MCWP 8-10.

Logistics

The AC/S G-4 or unit S-4 is the principal staff assistant for all logistic matters. The AC/S G-4 or unit S-4 plans section coordinates and supervises provision of combat service support in the areas of supply, maintenance, transportation, health services, engineer support, landing support, materials handling, food services, mortuary affairs, and host-nation support. Annex D (Logistics/Combat Service Support) provides direction and guidance to the subordinate commanders and staffs on the provision of logistics and combat service support in support of operations described in the OPORD or OPLAN.

Considerations for deception planners include the significant logistical footprints and OPSEC indicators associated with the logistical support of MAGTF operations. Deception planners can leverage OPSEC indicators to support the creation of desired perception as physical means.

Additionally, deception planners coordinate with the G-4/S-4 to move, maintain, and replenish various decoys. These considerations should be implemented during detailed planning. For further information on Marine Corps logistics, refer to MCWP 3-40, *Marine Corps Logistics*.

Combat engineering operations are traditionally associated with several survivability tasks, which can be critical to deception operations. Survivability is categorized into two principal components: avoiding and withstanding attacks. Avoiding attack principally involves a combination of mobility and passive employment of camouflage and concealment. Signatures of critical systems and formations can be camouflaged and concealed with the following techniques:

- Hide.
- Blend.
- Disguise.
- Disrupt.
- Decoy.

For further information on camouflage and concealment, refer to MCTP 3-34C.

TERMINATING TACTICAL DECEPTION OPERATIONS

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.

The actions involved in termination include—

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

All three termination actions occur whether the operation achieves its objective and whether the deception plan remains concealed. In developing the deception plan, the DAWG determines conditions and provisions for the termination of the operation. The termination plan 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.

Terminating a TAC-D operation also encompasses evaluating and reporting. The DPC or DAWG should conduct after action assessments This provides the commander an objective basis for determining the degree of mission success and for improving future deception operations. For further information on assessments, see Chapter 6. For more information on tactical deception planning, see Chapter 3.

CHAPTER 5.
DECEPTION IN SUPPORT OF OPERATIONS SECURITY

OPERATIONS SECURITY OVERVIEW

Requirements for DISO emerge from functional OPSEC planning. Operational security reduces the US and multinational force's vulnerability to adversary exploitation of critical information. Operations security applies to all activities that prepare, sustain, or employ forces.

The OPSEC process is a systematic method used to identify, control, and protect critical information. Subsequently, it analyzes friendly actions associated with military operations and other activities, with the purpose of preserving a commander's decision cycle and allowing options for military actions founded on sound, risk-based decisions. The OPSEC process consists of the following six steps:

- Identify critical information and OPSEC indicators.
- Identification and analysis of relevant threats.
- Analysis of vulnerabilities.
- Assessment of risks.
- Application of appropriate countermeasures.
- Periodic assessment of effectiveness.

When integrated into operations, activities, plans, exercises, training, and capabilities, OPSEC can maximize operational effectiveness by saving lives and resources.

For more information about OPSEC, the OPSEC process, and countermeasure development, refer to JP 3-13.3 and MCTP 3-32B, *Operations Security*.

DECEPTION IN SUPPORT OF OPERATIONS SECURITY

Deception in support of operations security is an OPSEC countermeasure. Deception in support of operations security conveys or denies selected information or signatures to a FIE and limits the FIE's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets. It differs from joint MILDEC and TAC-D plans because it only targets FIEs and is not focused on generating a specific adversary action or inaction.

Deception in support of operations security presents false, confusing, or misleading information and indicators to FIEs as part of a larger OPSEC plan, which makes it difficult for FIEs to identify or accurately derive critical information and indicators. In nearly all cases and applications, DISOs are ambiguity increasing type deceptions because they increase certainty, which drives adversary decisions.

If joint MILDEC or TAC-D are unsuitable for a particular situation, planners can use DISO to protect the commanders' warfighting profiles or obfuscate critical information and indicators, causing FIEs to misdirect their analysis of friendly operations or subsequent application of intelligence resources.

Operations security planners and program managers have a supporting relationship to deception planners regarding the development, approval, and implementation of DISO activities. Operations security planners are not authorized to conduct deception operations unless participating in a DAWG. Planners must coordinate with the command deception officer to conduct DISO activities.

DECEPTION IN SUPPORT OF OPERATIONS SECURITY PLANNING CONSIDERATIONS

Operations security planning guidance should be provided as part of the commander's planning guidance, and OPSEC considerations should be included in staff estimates and during the development and selection of friendly COAs. Typically integrated with the G-39, the process is fundamentally an operations function, not a security function, and requires the participation of planners throughout the staff. Although OPSEC is a consideration carried throughout the MCPP, most OPSEC functional planning is conducted during the MCPP step 5 and 6, orders development and transition. After planners select a COA, they can begin planning to identify and protect critical information. Planners can then conduct threat vulnerability analysis, threat analysis, and risk assessment to decided which countermeasures to implement.

If deception is selected for development as a countermeasure, the process is similar to the 5-step TAC-D process with the following additional considerations:

- Mission Analysis. The goal of a DISO is always to support OPSEC. The objective of DISO, unlike TAC-D or joint MILDEC, reflects the requirement to obfuscate or misdirect FIE attention or resources from discovering the critical information or indicators that lead to a correct assessment of the friendly activity.
- Concept Development. The target of a DISO is always the FIE. A DISO can be either ambiguity-decreasing or ambiguity-increasing; depending on whether the intent is to provide a plausible, yet incorrect explanation for friendly activity, or simply to provide numerous false indicators of activity in addition to the true indicators that may be present in the environment. These can result in desired perceptions and a deception story that reflects either uncertainty regarding friendly activity that extends across the period of vulnerability, or an apparently verifiable explanation for friendly activity that does not result in further scrutiny. Conduits and means development leverage the work done in threat vulnerability and analysis. Unlike TAC-D, conduit analysis is primarily focused on the sensor, with the purpose being a fundamental short-circuiting of the FIE's analytic process whereby the true indicators of friendly activity do not proceed further up the chain.

- Concept Approval. As with any deception activity, DISO concepts must be approved per standing policy requirements (CJCSI 3211.01; SECNAVINST S3490.1, *Deception Activities*; and MCO S3490.01) as well as any additional requirements levied by the supported command or higher headquarters.
- Plan Development. After a concept is approved, planners conduct detailed planning for execution. An ambiguity-decreasing DISO can require a similar level of detail as a TAC-D, requiring a DES and linkage with other aspects of the operational activity. An ambiguity-increasing DISO can simply be a list of actions to be taken when the opportunity presents itself to provide numerous, false indicators of activity during operations.
- Plan Review and Approval. Regardless of the level of required detail, the plan must still be reviewed and approved by the appropriate authority per policy.

Unit commanders employ DISO to create multiple false indicators that confuse adversary or adversary forces operating in the unit's area of operations by targeting the FIE, making unit intentions harder to interpret. A DISO uses controlled information about friendly force capabilities, activities, and intentions to shape perceptions. It targets and counters intelligence, surveillance, and reconnaissance capabilities to distract intelligence collection away from, or provide security and secrecy for, unit operations. A DISO can exhibit the detail of other deliberate deception activities, or it may be a relatively simple countermeasure to use. In either case, it is appropriate for use at the tactical level, provided the correct steps have been taken for approval.

CHAPTER 6.
DECEPTION ASSESSMENT

Assessment is "a continuous process that measures the overall effectiveness of employing capabilities during military operations" (*DoD Dictionary*). It is the basis for adaptation, keyed to the overall purpose, oriented on the future, and focused on emerging opportunities. Successful assessment requires the commander's situational understanding and recognition of the difference between planned goals and the situation as it exists. The difference between what was planned and what happened becomes the catalyst for decision making, either to correct deficiencies or seize opportunities.

Operational assessment focuses on the commander's objectives, end state, and related information requirements, linking and reflecting the status of progress of task accomplishment, effects creation, and objective achievements. Marine Corps Reference Publication 5-10.1, *Multi-Service Tactics, Techniques, and Procedures for Operation Assessment*, outlines a six-step approach to assessments, which includes—

- Developing an assessment approach.
- Developing an assessment plan.
- Collecting information and intelligence.
- Analyzing and synthesizing the feedback.
- Communicating the assessment and recommendations.
- Adapting plans, as required.

A primary responsibility of the MDO (supported by the DAWG) is assessing the effectiveness of the deception operation in achieving the commander's objectives. Deception is assessed in a similar manner as other operations—through developing, collecting, and analyzing indicators referred to as MOPs and MOEs.

As with all other aspects of the deception planning process, assessing the deception activities typically requires elevated security controls; although, the individual indicators collected may not betray the existence of the plan when not associated with deception. The following paragraphs highlight specific deception considerations relevant to the steps of the assessment process to guide the MDO in deception assessment. For further details on each step of the assessment process, refer to Marine Corps Reference Publication 5-10.1.

DEVELOP ASSESSMENT APPROACH AND ASSESSMENT PLAN

Planners develop the assessment approach and assessment plan during the planning process and focus on the linkages with other planners to ensure it is concurrently developed with the operational design. The outputs of these steps include the development of MOPs and MOEs, as well as a collection plan for gathering the information and intelligence needed to assess progress and inform decision making.

The development of deception MOPs and MOEs differs slightly from similar processes for other capabilities. One way to easily conceptualize MOPs and MOEs for deception is to use the "see, think, do" methodology outlined in Chapter 2. An MOP is most closely associated with see: did Marines portray the planned indicator, and did the adversary see our execution and transmit the desired message to the deception target creating an observable? Measures of effectiveness are associated with think and do: what perceptions and conclusions did the adversary draw from a particular observable (alone or in the context of other observations), and are those perceptions leading toward the desired action/inaction captured in a deception objective?

The G-2 and DAWG develop MOEs to provide the commander with the necessary time and space to adjust plans, as needed. For example, if one of a Marine's deception objectives is for the adversary to hold the armored reserve away from the decisive point of ground action, the staff should develop MOEs related to the accomplishment of that objective. Measure of effectiveness examples related to the action or inaction of the reserve might include—

- An increase or decrease in preparation of defensive positions (implying a period of static activity).
- An increase or decrease in adversary intelligence collection in the vicinity of our main axis of advance at the expense of other sectors (is the adversary indicating 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 adversary reserve.

Because a deception operation's success or failure might not be known until the adversary reacts (or does not react), coordination between the G-2 and DAWG and a deliberate focus on development of viable MOPs and MOEs is imperative. Without this coordination and focus, the operation could lose initiative or could result in friendly loss of life.

COLLECT INFORMATION AND INTELLIGENCE

Organizations collect relevant information throughout both planning and execution. They refine and adapt information collection requirements about the operational environment and anticipated and completed actions. Staffs and subordinate commands provide information during execution through applicable battle rhythm events. Intelligence staffs continually provide updates about the operational environment and the impact in support of the collective staff assessment effort.

Measure of performance collection for deception involves two conceptual steps:

- Determining that the tasked friendly unit or capability is employing the desired means to create an indicator at the appropriate time and location.
- Verifying that the intended adversary conduit(s) cued on the friendly signature(s), transmitted the collected data, and delivered the information to the deception target in a discernible context.

During the exaction of a plan, planners use the J-3 operations reporting channels to determine whether scheduled deception executions took place. The element responsible for executing the deception operation, which the DAWG and J-3 determine prior to execution, is also responsible for reporting on the status of the operation.

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

The defining difference of a deception MOP versus a traditional MOP ("did friendly forces perform the directed action") is that part of every successful deception execution involves action by the adversary. The conduit that the deception operation seeks to exploit must function.

The MOE development and collection process for deception operations focuses on the current cognitive state of the deception target. Planners can measure the adversary's cognitive state using the following two methods:

- Evaluating the decision maker's comments or public statements.
- Identifying and monitoring adversary activities that indicate the deception target was effectively influenced toward the desired perception and subsequent action or inaction.

The baseline MOE is whether the adversary capability to be affected was employed in the manner that met the desired effect. Planners might not know whether this activity occurred until the moment they see the desired effect.

Analyze Feedback and Communicate Recommendations

The analyze and synthesize the feedback steps take place during execution. Planners uses analysis to identify positive or negative movement toward creating desired effects, achieving objectives, or attaining end-states. Recommendations generated by these analyses might include updates to critical assumptions; adjustment of operations, priorities, and decision points; or the decision to transition between phases or to execute a branch plan. Relevant considerations for deception

activities include assessing failure modes, emerging planned or unplanned hazards, and the decision to terminate or execute a branch plan. The DAWG continually analyzes, interprets, and makes recommendations during the execution phase of the operation.

Following execution, the DAWG should conduct a final operational assessment. If the deception plan was well designed—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.

ADAPT PLANS OR OPERATIONS

Based on feedback and recommendations, commanders direct changes or provide additional guidance that dictates operational updates or modifications to drive progress to objectives and end states. Modifying the deception plan might align within pre-planned branches or sequels, or it might require developing a new concept or plan that requires appropriate approval.

The decision to execute the termination plan comes with a particular set of assessment requirements. Commanders are concerned with terminating deception operations in a way that protects both short- and long-term interests of the command. During termination planning, planners include specific alternative actions, or outs, if a deception fails (e.g., is not noticed, believed, relevant, misunderstood, or too ambiguous) to create the intended effects. These considerations must be continually updated based on the most recent assessed state of the target. Consequently, the planners must continually review the termination plan throughout the planning and execution of the deception based upon the ongoing results of assessment.

EVALUATING AND REPORTING

Termination of a deception encompasses evaluation and reporting. The DAWG should conduct an after action assessment. 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 might become available over a long time, a series of interim after action reports might be required before making a final assessment. The after-action report provides a comprehensive overview of the deception as it was planned to work compared with how it was conducted.

CHAPTER 7.
ORGANIZATIONS, ROLES, RESPONSIBILITIES, AND ASSOCIATED AUTHORITIES

ROLES

Commanders and their staff have distinct and coordinating roles and responsibilities in deception. All planners must understand the roles and responsibilities of everyone involved with MCDA and then tailor each planning team accordingly.

Commanders

The commander's role is critical in planning deception. Although deception might not be appropriate to every operation, the commander determines the utility of deception's contribution to achieving objectives. Commanders make the decision to use deception after evaluating the analysis and recommendations from the planners. Commanders have the authority to direct the development of a deception plan, and to direct execution of the plan upon review and approval at the appropriate level.

G-3 Operations and Training and G-5 Plans

The division of planning labor between the G-3 and the G-5 is command specific. According to their specific planning responsibilities (tailored to clearances, access levels, and need to know of specific individuals), the G-3/G-5 supervise the incorporation of deception into the information portion of operations estimates. Based on these estimates, the G-3/G-5 recommend various options for information activities (including deception activities) to the commander. Once the commander has selected a particular COA and received additional approvals as necessary, the G-3/G-5 supervise the completion of planning for the selected deception concept. The G-3 typically supervises deception execution.

G-39

The G-39 and the deception planning element are generally assigned to the G-3 but also participates in G-5 planning. The G-39 is typically responsible to the G-3 for developing the information portion of any planning effort conducted by the staff. These responsibilities include supervising deception planning and integration into the overall information plan. The G-39 monitors the implementation and execution of the TAC-D plan. For DISO, the G-39 ensures OPSEC planners and deception planners work together for integrated, effective execution.

Military Deception Officer

Where designated, the MDO is responsible for coordinating deception planning and execution. Military deception officers are authorized at the Marine Corps component command, MEF, and MSC echelons of command. As stated in Chapter 3, the MDO coordinates DPC activities, which

consist of MAGTF, MSC, and MSE deception planners. Military deception officers additionally provide programmatic oversight, management, and security compliance for deception activities within their command.

> **NOTE:** JP 3-13.4 includes an additional billet of CMDO. Command military deception officers are only appointed at the 4-star level of command and designated as primary participants by Office of the Under Secretary of Defense for Intelligence and Security and the Joint Staff (e.g., at the Military Department, Service, or CCMD level). The only Service-retained CMDO in the Marine Corps is the Headquarters, United States Marine Corps (HQMC) CMDO, who is appointed by Deputy Commandant (DC), Plans, Policies and Operations. Military deception officers work closely with the appropriate CMDO to ensure that deception plans and activities are in accordance with CCMD, DoD, Department of the Navy, and Service guidance and policy, as appropriate.

Military deception officers should horizontally and vertically integrate MCDA (see Figure 7-1). Key throughout the process, regardless of level of command, is coordinating with intelligence support and other staff sections, de-conflicting deception with other information activities, and facilitating integration of supporting deception activities with higher and adjacent headquarters.

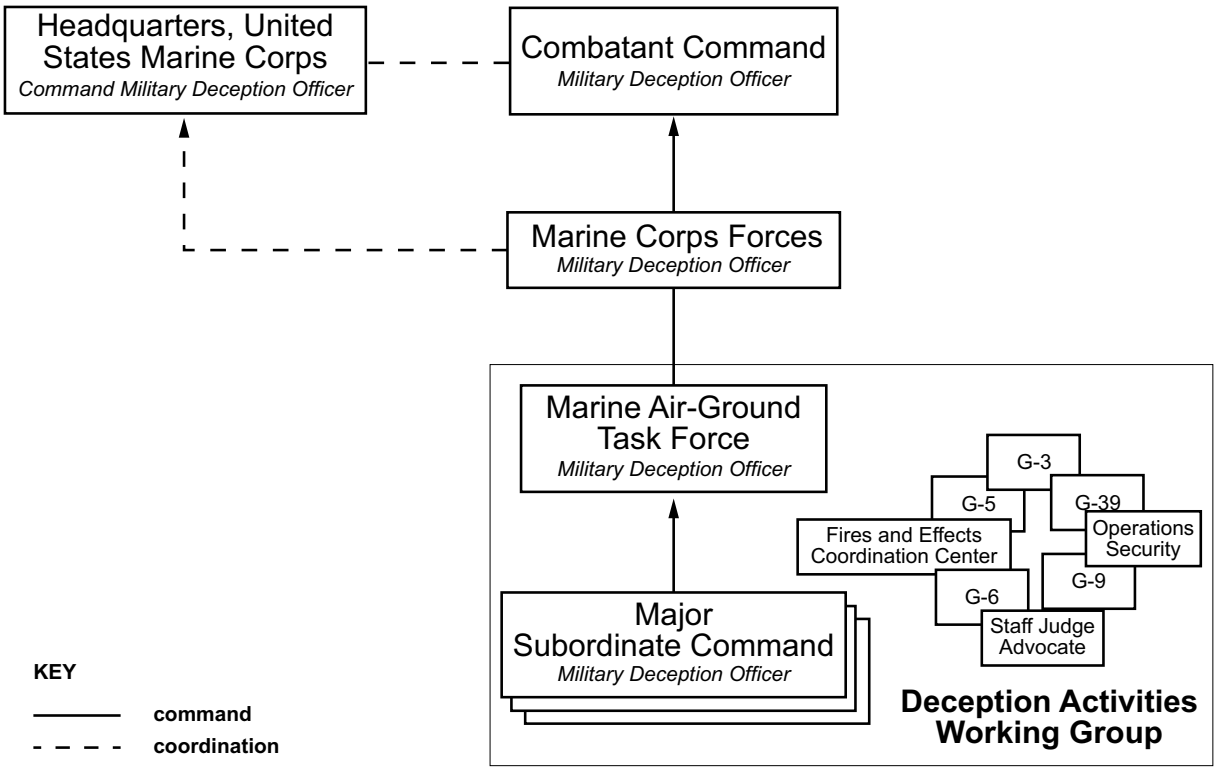


Figure 7-1. Vertical and Horizontal Integration.

At levels below the MSCs, there might not be a fully trained MDO organic to the unit, in which case the commander assigns an officer the duties of MDO. Any officer can serve in this role; however, it is typically a trained planner with the functions and skill sets aligned to the MDO's

duties. Regardless of their background, the deception planner must understand key deception terms, concepts, and theories. Additionally, deception planners contribute to the DPC and coordinate and synchronize with the staff and between echelons of command.

Deception Planner

The deception planner plans and executes deception plans within their organization. In this capacity, planners report to their organization's MDO. Deception planners work with other planners (internal and external to the G-39) as necessary to integrate detailed plans and coordinate execution.

Operations Security Officer

The MDO works with the OPSEC officer to ensure that measures and countermeasures are timed and implemented in a manner that assists the unit in presenting false indicators that confuse threat forces or make unit intentions harder to interpret.

Legal and Staff Judge Advocate

Legal personnel assist in planning the deception operation to achieve the objective while complying with legal requirements. These requirements include compliance with applicable US 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 staff additionally review all deception activities to eliminate, minimize, or mitigate the possibility that MCDA explicitly or implicitly target, mislead, or attempt to influence the US Government, US Congress, US public, or US news media. They also provide training to the staff, on law and policy applicable to deception operations.

RESPONSIBILITIES

Deception responsibilities of the commander and the staff are outlined in the following sections.

Commander

The commander retains explicit and inherent responsibilities for the deception effort. The commander—

- Assesses higher headquarters' plans and orders for stated and implied deception tasks.
- Considers the use of deception in every operation.
- Tasks the staff to evaluate the utility of deception.
- States the tentative deception objective in the initial planning guidance.
- Approves the deception objective, story, and plan.
- Allocates necessary resources to ensure successful execution.
- Seeks appropriate approval to employ certain deception means, as required.
- Determines when to exploit deception or counterdeception.

Assistant Chief of Staff G-2

The G-2 assists the commander and MDO by supporting MCDA and applying appropriate operations, intelligence, and counterintelligence resources. The G-2—

- Supports the DAWG and helps develop relevant plans.
- Facilitates understanding of target adversary assets, units, resources, and capabilities, including developing and refining the DIE in collaboration with the DAWG.
- Analyzes the adversary to include their 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 MDO RFIs concerning analysis data for behavioral influences or human factors for threat military, paramilitary, or violent extremist organizations.
- Helps prevent reporting of unintentionally collected deception information to the commander as valid facts.
- Assists the G-3 in conducting post execution assessments and MOEs.

Assistant Chief of Staff G-3

The G-3 typically establishes a staff deception element to manage deception operations as part of the IO cell. The G-3's overall responsibilities include—

- Recommending the deception objective, story, and plan to the MAGTF commander.
- Planning the deception effort.
- Ensuring the deception effort is coordinated through the IO cell with all other aspects of the plan integrated through the joint targeting process.
- Ensuring, in coordination with the SJA, that the deception effort is planned and conducted in accordance with US law and policy, and US international legal obligations.
- Supervising the deception plan's execution.
- Developing MOEs to assess the deception operation in conjunction with the deception planners.
- Controlling the deception plan's termination.
- Submitting a detailed and clear RFI to G-2 for intelligence information key to deception planning, execution, and assessment.
- Collaborating with the G-2 to produce the DIE.
- Providing feedback to the G-2 on intelligence products to include clarifying or requesting additional RFI, if needed.

In addition to these responsibilities, the G-3, as the fires and effects coordinator facilitates understanding of target adversary assets, units, resources, and capabilities; exploits fires capabilities; and synchronizes deception activities alongside other fires activities.

Assistant Chief of Staff G-4

The G-4 provides the logistic support and guidance needed to conduct deception operations in coordination with deception planners. The G-4—

- Assesses logistic requirements needed to conduct the deception operation.
- Determines logistic capabilities to support the deception operation.
- Provides input to and assessment of the deception plan to ensure logistics feasibility.
- Assesses the ability of logistic assets to support the deception plan without hindering the support necessary for execution of the overall operation.
- Develops logistic plans that support the deception operation.

Assistant Chief of Staff G-5

The G-5 generally maintains contingency plans and initiates crisis action planning efforts. The G-5—

- Coordinates with the CMDO to ensure deception planning is included in OPLANs, concept plans, and campaign plans.
- Includes deception elements in OPTs to ensure deception operations are considered from the inception of planning.

Assistant Chief of Staff G-6

The G-6 ensures communications system support and related communications system support activities necessary to support deception activities. The G-6—

- Provides planning guidance on communications system support to deception planners.
- Assesses supporting communications system network capabilities and interoperability required to support deception operations.
- Reviews deception plans and coordinates communications system support requirements.
- Develops and implements technical solutions to reduce the possibility of deception compromise and high-risk information vulnerability.
- Develops communications system support plans to support the deception operation.

Other Supporting Staff Sections

Planners also consult and coordinate with other relevant supporting staff to ensure MCDA's success. The MDOs must consult with the following supporting staff sections:

- Inspector General. Ensures MCDA are included and evaluated, as appropriate, during inspector general inspections.
- Comptroller. Ensures appropriate MCDA resources are identified and appropriately resourced.
- COMMSTRAT. Reduces the inadvertent reveal of MCDA related information. Public affairs officers can support authorized activities by providing communications, visuals, and other messaging products.

- EMSO. Exploits the electromagnetic spectrum to demonstrate friendly intentions and shape perceptions.
- Civil Affairs. Ensures deception plans do not inadvertently undermine the relationships with the civilian population or with host-nation military authorities. Failure to consider CMO could compromise deception plans or have other unintended consequences.

ORGANIZATIONAL ROLES AND RESPONSIBILITIES

The unique roles and responsibilities outlined in Table 7-1 are intended to provide a summary of relevant organizations and units throughout the Marine Corps with roles in DoD deception activities (refer to MCO S3490.1 for a detailed discussion of roles and responsibilities. Gaining authority to conduct DoD deception activities can be complex. Because of DoD deception activities' inherently secret nature, coordination is essential to effectively portray an alternate reality to the adversary. Therefore, MDOs should coordinate with the higher-echelon MDO to ensure they receive the appropriate authority and approval at the requisite level.

Table 7-1. Unique Roles and Responsibilities in Military Deception Context.

Echelon of Command or Organization	Unique Roles and Responsibilities	Relevant DoD Deception Activities for Planning
HQMC	DC for Plans, Policies and Operations: • HQMC office of primary responsibility for deception. Develops and supervises MCDA plans, policies, and strategy, including programs, requirements, and strategy. • Marine Corps operations deputy is required to synchronize availability and readiness of Service-retained forces.	DISO
	DC for Information: • Occupational field sponsor for influence and includes responsibility for personnel management. • Resource sponsor for intelligence support to MCDA.	
	DC for Combat Development and Integration: • Advocates for materiel, nonmateriel, and training resources. • Incorporates deception into formal concepts and experimentation. • Facilitates concept design and development in support of MCDA.	
	DC for Programs and Resources: • Executes Marine Requirements Oversight Council process to secure appropriate resources to support MCDA.	
Marine Corps component commands	• MDO support to CCMD and support joint MILDEC planning if tasked by CCMD. • Effectively integrates Service capabilities into CCMD operations. • Coordinates with naval planning elements/commander, task forces to ensure synchronization and naval integration. • Informs assigned Fleet Marine Forces units of CCMD directives and authorities to conduct deception. Ensure deception plans comply with MILDEC directives and authorities.	Joint MILDEC DISO

Table 7-1. Unique Roles and Responsibilities in Military Deception Context (Continued).

Echelon of Command or Organization	Unique Roles and Responsibilities	Relevant DoD Deception Activities for Planning
Marine expeditionary force, brigade, and unit	Task-organized for specific missions, on order, must be able to deploy to conduct specific missions, which may include TAC-D and DISO.	DISO TAC-D
MIGs	• Provides MCDA expertise in response to MEF tasking. • Provides forces in support of MCDA, as tasked by MEF	N/A
Marine Forces Reserve	Commands, controls, and assigns forces in support of reserve mobilization as required to augment and reinforce the active component with trained personnel able to support ongoing planning and operations, including experimentation and exercises that may include DISO and TAC-D concepts, tactics, techniques, and procedures.	DISO
Marine Corps Information Command	Integrates, synchronizes, and enables information activities to leverage authorities and approvals across key elements of the information environment, given commanding general Marine Corps Information Command role aligned as commanding general Marine Forces Cyber Command, Marine Forces Space Command, joint force headquarters-cyberspace —Marines. In coordination with relevant commands.	DISO
Marine Corps Intelligence Activity	As part of DC for Information/Intelligence Division, is responsible for intelligence support and intelligence activities to support preparing for MCDA. Coordinates with relevant units to support preparation (e.g., DIE) activities.	DISO
Marine Corps Information Operations Center	• Functions as Marine Corps' OPSEC support element. • Provides operational support to Marine components, MAGTFs, and subordinate units. • Provides information environment subject matter expertise to appropriate advocates and proponents for effective integration of information into Marine Corps operations.	DISO
Training and Education Command	• Facilitates training and education in support of DoD deception activities. • Aligns appropriate training and readiness manuals to establish appropriate individual and collective deception tasks. • Incorporate deception into formal school programs of instruction.	N/A

APPENDIX A.
DECEPTION ACTIVITIES WORKING GROUP CONSIDERATIONS

Although the G-3/G-5 is responsible for the deception plan, the MDO typically leads the DAWG. To fulfill the responsibilities for functional and detailed planning, considerations include—

- Maintaining program integrity through adherence to OPSEC and associated security measures.
- Ensuring that staff classify plans in accordance with Department of Defense Manual 5200.01 (Vol 3), *DoD Information Security Program: Protection of Classified Information*, and applicable security classification guides.
- Exercising staff supervision over deception activities.
- Coordinating the deception effort through information activities.
- Providing expertise in deception planning.
- Facilitating DAWGs with stakeholders from across the command staff sections in support of the broader planning OPT.
- Coordinating with unit operations planners to review and analyze plans for deception requirements.
- Determining requirements or opportunities for deception operations with the G-2 using Red Teams from the enemies' perspective for most likely and most dangerous COAs.
- Submitting detailed and clear requests to the G-2 for information and intelligence that is key to deception planning, execution, and assessment.
- Recommending the deception objective, story, and plan to the commander.
- Managing information required to develop deception plans and cultural analysis to determine the effects of ambiguity.
- Coordinating with other staff sections to develop the deception targets, objectives, and story.
- Understanding deception authorities and coordinating with designated officials at higher echelons to gain concept of operations or plan approval.
- Coordinating with legal or SJA assets to ensure that the deception effort is planned and conducted in accordance with the US laws and policies, rules of engagement, and international law and the law of war.
- Developing the deception tab and associated exhibits (e.g., DES).
- Producing, distributing, briefing, and coordinating the deception plan on a need-to-know basis.
- Supervising execution of the deception plan.
- Providing feedback to the G-2 on intelligence products to include clarification or additional RFIs, if needed, throughout execution and assessment.
- Coordinating with the G-39 to ensure themes, messages, and actions conveyed to the adversary decision maker enable the deception plan.
- Assessing the execution and effects of deception plans.

APPENDIX B.
DECEPTION EVALUATION CHECKLIST

The MDO must complete 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 to the overarching plan?
- Did the deception activity address a common list of indicators that required either display or concealment?
- 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 a DES prepared?
  - Did the DES 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 adversary from taking undesirable actions?
  - Was the story flexible enough to allow changes during its execution to take advantage of unexpected adversary actions?
- Was the deception or OPSEC activity compromised?
  - 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 (e.g., dummies, decoys) were constructed, used, and how? How many were used?
- What other resources or services were required? Were they available?
- What other missions could not be accomplished because resources (e.g., operational) were being used for deception operations?
- Do the benefits of deception justify any loss of operational resources?
- Were dedicated, secured communications lines and other means of transmission of the deception 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?

APPENDIX C.
G-2 EVALUATION CHECKLIST

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 G-2 have an established adversary database and an understanding of adversary doctrine?
- Was there awareness of adversary 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 adversary reaction to friendly deceptions?
- What adversary activities were identified as being deception related? Why?
- What was the deception story?
  - At what level of the adversary organization was it focused?
  - Did the deception story cause the adversary 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 adversary collection systems?
- What countersurveillance techniques were used to deny the adversary 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 adversary'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 adversary 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 adversary reaction to the friendly unit's deception?

APPENDIX D.
MILITARY DECEPTION MAXIMS

The following maxims were developed in 1981 by a research team contracted by the Central Intelligence Agency, which analyzed various sources and disciplines including game theory, historical evidence, social science, and decision analysis theory. This study (often called the MathTech study) and its list of maxims have been referenced in successive versions of JP 3-13.4 as well as throughout other deception literature. Interested readers are referred to the study and source documents for further commentary and discussion.

MAXIM 1: MAGRUDER'S PRINCIPLE—THE EXPLOITATION OF PRECONCEPTIONS

It is generally easier to induce an opponent to maintain a pre-existing belief than to present notional evidence to change that belief. Thus, it may be more fruitful to examine how an opponent's existing beliefs can be turned to advantage than to attempt to alter these views.

MAXIM 2: LIMITATIONS TO HUMAN INFORMATION PROCESSING

There are several limitations to human information processing that are exploitable in the design of deception schemes—among these, the law of small numbers and susceptibility to conditioning.

MAXIM 3: THE MULTIPLE FORMS OF SURPRISE

Surprise can be achieved in many forms. In military engagements, these forms include location, strength, intention, style (capability), and timing. Should it not prove attractive or feasible to achieve surprise in all dimensions, it may still be possible to achieve surprise in at least one of these. Thus, for example, if intentions cannot be concealed, it may still be possible to conceal timing (cry-wolf syndrome), place, strength, or style.

MAXIM 4: JONES' LEMMA

Deception becomes more difficult as the number of channels of information available to the target increases. However, within limits, the greater the number of controlled channels the greater the likelihood of the deception being believed.

MAXIM 5: A CHOICE AMONG TYPES OF DECEPTION

Where possible, the objective of the deception planner should be to reduce the ambiguity in the mind of the target, forcing the target to seize upon a notional world view as being correct—not making him less certain of the truth, but more certain of a particular falsehood. However, increasing the range of alternatives or the evidence to support any of many incorrect alternatives—in the jargon "increasing the noise"—may have particular use when the target already has several elements of truth in their possession.

MAXIM 6: AXELROD'S CONTRIBUTION: THE HUSBANDING OF ASSETS

There are circumstances where deception assets should be husbanded despite the costs of maintenance and risk of waste, awaiting a more fruitful use. Such decisions are often susceptible to rational analysis.

MAXIM 7: A SEQUENCING RULE

Deception activities should be sequenced to maximize the persistence of the incorrect hypothesis(es) for as long as possible. In other words, "red-handed" activities should be deferred to the last possible instant.

MAXIM 8: THE IMPORTANCE OF FEEDBACK

A scheme to ensure accurate feedback increases the chance of success in deception.

MAXIM 9: THE MONKEY'S PAW

Deception efforts may produce subtle and unwanted side effects. Planners should be sensitive to such possibilities and, where prudent, take steps to minimize counterproductive aspects.

MAXIM 10: CARE IN THE DESIGN OF PLANNED PLACEMENT OF DECEPTIVE MATERIAL

Great care must be exercised in the design of schemes to leak notional plans. Apparent "windfalls" are subject to scrutiny and often disbelieved. Genuine leaks often occur under circumstances thought improbable.

MAXIM 11: INTEGRATED PLANNING

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

APPENDIX E.
COMMON MISTAKES AND RISK CONSIDERATIONS

EVALUATING FAILURE

Most deceptions neither completely fail, nor completely succeed. Where a deception activity may fall on the spectrum of results is often a result of unaddressed risk and insufficient mitigation. This appendix deliberately includes risk as a key consideration. Risk must be continuously assessed through all aspects of deception, from the understanding of theory, application of tactics and techniques, planning, execution, and assessment. While not exhaustive, this appendix provides deception planners with a consolidated list of risk considerations.

Deception can fail to achieve the desired objective for one or more of the following reasons:

- Incomplete understanding or misunderstanding of the target's intelligence apparatus.
- Incomplete or incorrect modeling of the deception process.
- Inadequate or improper channels or means to convey the deception story.
- Incomplete or inadequate control over the important variables of the deception process.
- Incorrect assessment of the target’s reaction.
- Deception story falls outside the deception window—too sophisticated to be received, or too simplistic to be believed.
- Unreasonable expectations.
- Target’s inability to react in the intended manner even if deception is considered credible.
- Inadequate time for the deception process to run its course.
- Plain bad luck can cause detection, inadequacy, or both.

In operations, a deception fails because it is—

- Not noticed.
- Not believed.
- Not thought relevant—too ambiguous.
- Misunderstood.

Planners should use the "theory of outs" when planning a deception operation. This includes planning—

- An escape route.
- Alternative objectives—including branches.
- Termination criteria.

Deceptions can fail because of poor OPSEC, including the following:

- Failure to maintain good OPSEC can lead to identification of the operation as a deception effort with the resulting second- and third-order effects such as the refocusing of adversary intelligence collection and combat power against actual friendly force dispositions and intent.
- The deception plan should be properly classified and not exposed to unprotected computer networks or sent via unsecured e-mail. Any exposure can lead to plan failure.

DECEPTION FAILURE

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

APPENDIX F.
(U) SUPPLEMENTAL GUIDANCE ON MARINE CORPS DECEPTION ACTIVITIES

Appendix F is classified and available at HTTPS://intelshare.intelink.sgov.gov/sites/ALSA/MCdoctrine.

GLOSSARY

Section I: Abbreviations and Acronyms

AC/S	assistant chief of staff
ATO	air tasking order
CCMD	combatant command
CMDO	command military deception officer
CMO	civil-military operations
COA	course of action
COMMSTRAT	communication strategy and operations
DAWG	deception activities working group
DC	deputy commandant
DIE	deception intelligence estimate
DISO	deception in support of operations security
DoD	Department of Defense
DPC	deception planning cell
EMSO	electromagnetic spectrum operations
EW	electromagnetic warfare
FECC	fires and effects coordination center
FIE	foreign intelligence entity
G-2	intelligence staff section
G-3	operations and training staff section
G-4	logistics staff section
G-5	plans staff section
G-6	communications system staff section
G-9	civil affairs staff section
G-39	Information Operations Branch
HQMC	Headquarters, United States Marine Corps
ITCC	information tasking and coordination cycle
ITCO	information tasking and coordination order

J-3	operations directorate of a joint staff
JFC	joint force command
JP	joint publication
LOO	line of operation
MAGTF	Marine air-ground task force
MCDA	Marine Corps deception activities
MCPP	Marine Corps Planning Process
MCTP	Marine Corps tactical publication
MCWP	Marine Corps warfighting publication
MDO	military deception officer
MEF	Marine expeditionary force
MEU	Marine expeditionary unit
MILDEC	military deception
MISO	military information support operations
MOE	measure of effectiveness
MOP	measure of performance
MSE	major subordinate element
OIE	operations in the information environment
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OPT	operational planning team
R2P2	rapid response planning process
RFI	request for information
TAC-D	tactical deception

Section II. Terms and Definitions

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

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

deception event
A deception means executed at a specific time and location in support of a deception operation. (DoD Dictionary).

deception goal
Commander's statement of the purpose of military deception as it contributes to the successful accomplishment of the assigned mission (DoD Dictionary).

deception objective
The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location (DoD Dictionary).

deception story
A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception (DoD Dictionary).

deception target
The adversary decision maker with the authority to make the decision that will achieve the deception objective (DoD Dictionary).

desired perception
In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective (DoD Dictionary).

electromagnetic warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. (DoD Dictionary)

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 (DoD Dictionary).

information environment
The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information. Also called **IE**. (DoD Dictionary)

link
A behavioral, physical, or functional relationship between nodes (DoD Dictionary).

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

node
An element of a network that represents a person, place, or physical object (DoD Dictionary).

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. (DoD Dictionary).

operational planning team
A group built around the future operations section that integrates the staff representatives and resources. The operational planning team may have representatives or augmentation from each of the standard staff sections, the seven warfighting functions, staff liaisons, and/or subject matter experts. Also called **OPT**. (USMC Dictionary)

REFERENCES AND RELATED PUBLICATIONS

Department of Defense Issuances

Department of Defense Directive

2311.01	DoD Law of War Program

Department of Defense Instruction

DoDI S-3604.01	DoD Military Deception

Department of Defense Manual

5200.01 (Vol 3)	DoD Information Security Program: Protection of Classified Information

Miscellaneous

DoD Law of War Manual (as amended)

Department of Defense Dictionary of Military and Associated Terms

Joint Chiefs of Staff Issuances

Chairman of the Joint Chiefs of Staff Instruction

3211.01F	Joint Policy for Military Deception

Chairman of the Joint Chiefs of Staff Manual

3130.03A	Planning and Execution Formats and Guidance

Joint Issuances

Joint Publications

3-0	Joint Campaigns and Operations
3-04	Information in Joint Operations
3-12	Joint Cyberspace Operations
3-13.3	Operations Security
3-13.4	Military Deception
3-52	Joint Airspace Control
3-60	Joint Targeting
3-85	Joint Electromagnetic Spectrum Operations

Allied Publications

Allied Joint Publication

3.10-2	Allied Joint Doctrine for Operations Security and Deception

Miscellaneous

Geneva Convention

UK Military Deception 4th Edition

Navy

Secretary of the Navy Instruction

S3490.1	Deception Activities

Marine Corps

Marine Corps Doctrinal Publications (MDCPs)

1	Warfighting
1-3	Tactics
1-4	Competing
8	Information

Marine Corps Warfighting Publications (MCWPs)

3-10	MAGTF Ground Operations
3-20	Aviation Operations
3-30	Marine Air-Ground Task Force Command and Control
3-31	Marine Air-Ground Task Force Fires and Effects
3-40	Marine Corps Logistics
5-10	Marine Corps Planning Process
8-10	Information in Marine Corps Operations

Marine Corps Tactical Publications (MCTPs)

3-30A	Command and Staff Action
3-32B	Operations Security
3-34C	Survivability Operations
11-10C	The Commander’s Handbook on the Law of Land Warfare

Marine Corps Reference Publication (MCRP)

5-10.1 Multi-Service Tactics, Techniques, and Procedures for Operation Assessment

Marine Corps Order (MCO)

S3490.1 (U) Marine Corps Deception Activities

Marine Corps Bulletin

5400 Establishment of Information as the Seventh Marine Corps Warfighting Function

Miscellaneous

Marine Corps Civil-Military Operations School Circular on Marine Civil Affairs Operations

Army Issuances

Field Manual

3-13.4 Army Support to Military Deception

Army Techniques Publication

3-13.1 The Conduct of Information Operations

Miscellaneous

Army Combined Arms Center references/POI