Chapter Three

DECEPTION

All warfare is based upon deception.

—Sun Tzu, *The Art of War*

WHAT IS DECEPTION? WHAT IS MILITARY DECEPTION?

Deception, the employment of trickery or guile, is equal parts art and science. It is typically defined as "causing another to believe what is not true; to mislead or ensnare" (Webster's, 1999). Deception aims to *deliberately induce misperception in another*. Deception is a deliberate enterprise; it is not the result of chance, nor the by-product of another endeavor (McCleskey, 1991). Whaley (1982, p. 188) has defined deception as "information designed to manipulate the behavior of others by inducing them to accept a false or distorted presentation of their environment—physical, social, or political." It is ubiquitous and enduring in human affairs, and equally prevalent in the predator-prey relationships of the plant and animal kingdoms. Note that while we define *human* deception as requiring *deliberation*, this is not the case in the animal or plant kingdoms. Rather than ascribe intentions to other species, we shall simply aver that deception in animals and plants is any act or instrument whereby an individual organism induces a misperception in another. Deceptions may therefore include the lure of the angler fish; the brood mimicry of the cuckoo's egg; the diverting eyespots of the moth's wing; the camouflage of the trapdoor spider's ambush; and the feigned injury of the parent duck.

A closer look at animal biology and behavior reveals important principles of deception, tabulated below (drawn from Wickler, 1968; Dawkins and Krebs, 1978, 1979; Slatkin and Maynard Smith, 1979; Erichsen, Krebs, and Houston, 1980; and Owen, 1980).

- **Species of all types use deception.** Deception (as defined previously) is present in virtually every branch of the evolutionary tree (vertebrates and invertebrates alike). Fish, reptiles, birds, mammals: every category of animal life (and a great many plants) employs deception.
- **Many types of deception are employed in nature (camouflage, concealment, diversion, conditioning/exploit, mimicry).** Not only are many types of deception used, but within a single type of deception—camouflage, for example—deception is polymorphic. That is to say, camouflage (known in biology as “crypsis”) can be as simple as green skin coloration for a background of foliage, or as complex as a nest whose shape, emissions, and entryways are all disguised by local materials (dirt, twigs, stones, etc.).
- **Every environment supports deception in at least one inhabitant of its ecosystem, and usually by many.** Deception is present in every environment supporting life (whether terrestrial, aquatic, or airborne): from desolate Arctic wastes to richly populated equatorial jungles.
- **Deception is used by both predators (offensively) and prey (defensively).** Deception in nature is used both to acquire dinner and to avoid becoming dinner—it is among the best methods for both successfully preying and escaping predation (as opposed to speed or armor, for example). The extremely venomous boomslang snake hunts the well-camouflaged chameleon not by evolving better sensors, but by employing its own excellent camouflage techniques. The chameleon’s crypsis is far less effective while it moves, and if it doesn’t see the boomslang, it moves.
- **A single species can use deception in both ways.** The same methods a given species uses to facilitate predation are often applied with equal effectiveness by that species to escape predation. Many species of small insects and spiders bear a striking resemblance to ants, which allows both protection from preda-

tors uninterested in ants as well as unhindered access to ant colonies where they may scavenge. Interestingly, this type of mimicry is also performed using chemical signature molecules as a "passcode-scent" quite apart from physical appearance.

- **Even minor applications of deception can confer selective advantage.** Experimental data show that even lesser deceptive techniques provide measurable benefits. For example, insects with even slight amounts of crypsis are less likely to be preyed upon by blue jays.
- **Deception is more effective in some environments than others.** Experimental data show that deceptive techniques vary in their effectiveness by environment. Where animal density is high, crypsis offers greater protection from predation (suggesting reasonably that we will see disguise to be more effective among city crowds than in desert wastes).

These latter two principles suggest critical experiments that should be performed in gauging military applications of deception, and we shall return to this topic later on.

Humans, like animals, must make decisions in order to survive. Decisionmakers rely upon their assessment of other actors' interests, intentions, and capabilities, as well as an assessment of the environment or context within which the action takes place. These assessments—or *perceptions*—engender policy preferences and galvanize action. It is incumbent upon decisionmakers to form *accurate* perceptions if they are to successfully navigate the shoals of circumstance; history is famously littered with the ruin of those who failed to do so. For example, the name of Neville Chamberlain, the British Prime Minister who "appeased" Hitler at Munich, is nearly synonymous with catastrophic misperception (though not *necessarily* as a result of German deception). Forming accurate perceptions is a challenge even under favorable circumstances. These latter circumstances might include situations with clear and unambiguous communication between parties, or extensive preparation and rehearsal for a particular turn of events. Unfavorable circumstances might include occasions when events are unfolding at a very fast pace, or when the background "noise" of contradictory opinions interferes with the accurate gauging of an actor's intentions. Within these "unfavorable" circumstances is a subset in which one or more parties attempts to *deceive* the other(s). Such deception might be explicit or implied, may involve concealing what is true or displaying what is false, or a combination of both. As noted above, the aim of deception is to produce an inaccurate assessment, or *misperception*, in the mind of the target that the deceiver can then exploit.

In the domain of conflict and war, deception is widely perceived to be both applicable and valuable, from the construction of decoys that draw enemy fire to the use of a feint to deflect enemy attention away from a major attack. Military deception aims to *deliberately induce misperception in another for tactical, operational, or strategic advantage*. Deception, like other components of information operations (IO), has "as its ultimate target the human decision making process" (Joint Pub 3-13, *Joint Doctrine for Information Operations*). Recent U.S. military doctrine (Army Field Manual 101-5-1, *Operational Terms and Graphics;* Joint Pub 3-58, *Joint Doctrine for Military Deception;* and Army Field Manual 90-2, *Battlefield Deception*) defines military deception as

> measures taken to deliberately mislead adversary decision-makers about friendly capabilities, intentions or operations in ways which may be exploited by friendly forces.

In this monograph we shall broaden this definition slightly, replacing the word "adversary" with the word "relevant," operating from the premise that deceptions targeted against noncombatants may also play an important role in military operations. This is consonant with the current doctrine relating to information operations, into which deception is bundled, and which are defined by U.S. Army Field Manual 100-6 (*Information Operations*) as

> continuous military operations within the Military Information Environment (MIE) that enable, enhance, and protect the friendly force's ability to collect, process, and act upon information to achieve an advantage across the full range of military operations; IO include interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision capabilities.

The presence of large numbers of noncombatants is one of the key features distinguishing the urban from other environments, as noted in the previous chapter. Effects upon the GIE—which are defined to be persons, information, and information systems *outside* the control of the National Command Authorities (NCA)—may be as militarily significant as effects upon the MIE, defined to be persons, information, and information systems *within* the purview of the NCA. The GIE includes governmental and nongovernmental actors, social and cultural elements, and innumerable local, regional, and transnational infrastructures. Historical accounts amply document the useful employment of deception in all environments, supported by a broad range of technologies and aimed at both noncombatants (journalists, clerics, civilian leadership, etc.) as well as principals in enemy command structures (generals, intelligence analysts, pilots, etc.). As defined above, deception (as part of information operations) can be valuable in both the offensive and defensive roles; it is clear that an adversary may utilize deception similarly.

A note on terminology: throughout the foreign policy, intelligence, and defense communities—and over time—various definitions and formulations of deception have been proposed. They include "denial and deception," "concealment, camouflage, and deception," "perceptions management," and so on. Here we group them all under a single aegis with the definition outlined above. If an operation, a technique, or measure has as its goal the deliberate purveyance of falsehood to another in order to aid friendly interests, we call it deception. As noted above, this may take the form of hiding things, revealing things, or a combination of the two; for the purposes of this monograph, it is all deception. Thus camouflage (which aims to conceal) is related to decoys (which aim to reveal). Deception is an integral component of information operations, themselves a vital component of overall operational art; it follows that the framework developed for employing information operations governs using deception as well.

WHAT WOULD DECEPTION BE USED FOR?

> I make the enemy see my strengths as weaknesses and my weaknesses as strengths while I cause his strengths to become weaknesses and discover where he is not strong.
>
> —Sun Tzu, *The Art of War*

As a component of both offensive and defensive IO, deception is used to adversely affect an opponent's decisionmaking processes, most often to influence or degrade enemy command and control (C2). For example, deception may promote friendly intelligence, surveillance, and reconnaissance (ISR) activities; may thwart ISR in an adversary; may degrade enemy cohesion and C2; may enhance force protection and survivability; and may create opportunities to engage and even surprise the enemy. These effects could also be gained against an individual enemy soldier in a low-intensity urban insurgency, as described by IRA operative Eamon Collins (1997, p. 124):

> [T]he other [bomb] had been built into the dashboard of a brown Mark 4 Cortina, which would be used as the getaway car. It would be abandoned with the aim of attracting a nosy bomb-disposal squad officer or policeman. If the glove compartment was opened, an electrical circuit would be completed which would detonate ten pounds of high explosives. Another [Active Service Unit] had used a similar trick some time earlier. A bomb-disposal officer had cut out the windscreen of the suspicious car in order to avoid opening the doors; then he had leaned in and opened the glove compartment . . .

Deception may just as readily be employed against an entire enemy army in a high-intensity, major theater urban conflict, as in the case of the Chechens' defense of Grozny, observed by Anatol Lieven (1998, p. 109):

> [T]he lack of obvious barricades and tank traps made [us] think that the Chechens would put up only a symbolic fight in the city. But . . . they were much better tacticians than that.

Alternatively, deception could be applied against anyone at all unfriendly to the deceiver. As Monmonier describes (1996, p. 117), one form of deception useful at all levels of war is disinformation directed at mapping/navigating skills:

> Soviet cartographic disinformation affected all [publicly available] maps of urban areas. Detailed street maps of Moscow and other Soviet cities often failed to identify principal thoroughfares and usually omitted a scale, so that distances were difficult to estimate. Although local citizens were well aware of its presence, Soviet street

> maps of Moscow suppressed the imposing KGB building on Dzerzhinski square, as well as other important buildings.

The principles and practice of deception remain the same in all of the preceding examples, as will be described below. Furthermore, deception has comparable effects at all levels of war—the creation of one or more prejudicial misperceptions in the mind of the target—differing mainly in scale and particulars.

How does deception accomplish these ambitious objectives? As noted above, deception creates misperceptions—the sorts of which are virtually infinite. However, a few general categories serve to encompass a broad range of possibilities. Deception may

- Purposefully condition the target to a pattern of friendly behavior;
- Divert the target's attention from friendly assets;
- Draw the target's attention to a particular time and place;
- Hide the presence or absence of activity from the target;
- Advertise strength or weakness as their respective opposites;
- Confuse or overload the target's intelligence apparatus;
- Disguise friendly forces as neutrals or even members of the enemy's force.

Consider the first category: This venerable ploy is colloquially known as a "crying wolf" tactic, and it relies upon the desensitizing effects of repetition to diminish a target's readiness or alertness. Specifically, the misperceptions created in the target's mind are, first, *that friendly activities follow a consistent, uniform course;* second, *that departure from the pattern (i.e., surprise) is unlikely;* and third, *that jeopardy is reduced overall by the predictability of these activities.* Two historical examples will serve to illustrate this brand of ruse (and simultaneously demonstrate the enduring nature of deception):

- In 1973 AD, Egyptian forces assaulting the Bar-Lev line in Suez City surprised Israeli forces and scored great offensive gains in the opening hours of the Yom Kippur War. Egyptian forces had staged a number of deceptive operations to hoodwink Israeli intelligence, and among these were back-and-forth movements of men and materiel to potential crossing points. Troops were moved to the canal, tank ramps were constructed, and openings were made in the canal ramparts, yet each time there was a flurry of activity there was also a subsequent "standing down" of Egyptian forces. These repetitive events (what Richard Betts calls "alert fatigue") lulled Israeli observers into a less-vigilant state which, coupled with poor Israeli analysis and self-deception, led to near catastrophe. (Drawn from Betts, 1983, and Dunnigan and Nofi, 1995.)

- In 212 BC, Hannibal gained entrance to and seized the city of Tarentum from the Romans in a deception-produced surprise attack. Hannibal exploited the presence of a dissident Greek resident, Cononeus, to create a nightly ritual: Cononeus departed the city in a large hunting party, ostensibly to gather supplies, and returned in the wee hours, his men laden with game. The Tarentine guards became used to the sight (and grateful for the provender), and greatly relaxed their vigilance. When Hannibal introduced some of his best soldiers into the party, disguised as hunters, the guards barely took notice. Hannibal's men overcame the guards and opened the gates for the body of Hannibal's host, which promptly captured the city with few casualties. (Drawn from Asprey, 1994, and Dunnigan and Nofi, 1995.)

An important point to make here (one visible in the preceding examples) is that deception is rarely an end unto itself. For example, deception is most often used *in coordination with other methods* to create windows of opportunity that expose the enemy (i.e., make him or her vulnerable). Moreover, deception is frequently employed to effect *surprise*, among the most precious commodities in conflict.

WHO WOULD USE DECEPTION?

It is a fundamental contention of this report that deception may be usefully employed by both enemy and friendly forces in the urban environment. Ample historical precedent supports this claim. Deception may target both combatants and noncombatants, and it may do so at all operational levels. This means that deception is a powerful tool in the arsenal of the individual infantryman and the CINC alike.

At the strategic and higher operational levels of war, deception is the purview of the joint force commander's (JFC) cell overseeing, developing, deconflicting, and coordinating all information operations (IO) for the joint force. Deception planning occurs, along with other IO activities, concomitantly with all intelligence and operational activities undertaken by the JFC. Moreover, the tight secrecy and coordination necessary to successfully conduct strategic and operational deception is best obtained by the IO cell fully supported by intelligence activities and "incorporated into the JFC's overall operations planning" (JP 3-13).

At the tactical and lower operational levels of war, deception is conducted in support of the JFC's overall IO objectives and coordinated by the appropriate commander at all levels, including the individual soldier, pilot, etc. The use of deception must be reported to and overseen by every level in the chain of command up to the JFC and the joint command IO cell. This puts the overall IO cell completely "in the know" and ensures that the JFC's objectives are being met and that other deceptions are not compromised or adversely affected by the actions of the unit. The reverse is not true, however, as top-down deception planning preserves secrecy and follows strict "need-to-know" practices.

Consider the following notional examples as a means of sampling the space of possibilities within which deception might be used by a range of actors:

- **An individual sniper moves about the urban battlefield, using camouflage to conceal firing positions.** As with animals, her use of camouflage serves both offensive and defensive purposes. First, she wishes to conceal her presence and position from potential targets such that they are less wary and more exposed to her fire. Second, she wishes to conceal her presence and position from enemy combatants who are seeking to detect and fire upon her. The sniper wishes to create a similar misperception in both targets' minds: namely, that there is no one present in the rubble-strewn street (or whatever background) they're observing.

- **A tank platoon commander orders multispectral close-combat decoys (MCCD) deployed on and around his prepared urban position (at the mouths of alleys, peeking from garages, etc.) in expectation of an enemy encroachment.** The use of such decoys has been demonstrated to significantly enhance the survivability of armored forces; in this case, the use of deception is primarily defensive in nature. His aim is to create in the minds of enemy attackers (whether infantry or armor) fleeting misperceptions (i.e., a tank exists where there is no actual tank). While the longevity of such deception may be measured in seconds or minutes, the value added by its success may prove decisive on the battlefield.

- **A commander with responsibility for the integrated air defenses (IAD) of a major metropolis, faced with an enemy who has greater air power and a doctrine calling for its exploitation, chooses to employ a variety of deceptions to protect and promote his IAD assets.** Deception has both offensive and defensive applications in this case. To protect his forces, the IAD commander may opt to use decoys to absorb air strikes, simulations of damage where none exists, camouflage and concealment of IAD sites, and the like. To make enemy aircraft more vulnerable, he may attempt to condition the enemy pilots to particular patterns of defensive fire, use disinformation to misadvertise the strengths and weaknesses of his IAD, and so forth. The aim of any of these deceptions is to create misperceptions that assist the IAD mission on either offense or defense.

- **An insurgent leader waging an urban campaign of terror opts to employ disinformation and diversions to both degrade enemy command and control and to create a blanket of distracting "noise" to cloak the activities of her operatives.** Deception has both an offensive and a defensive application in this scenario. First, hoaxes and "false-flagging" are used to create numerous misperceptions in the minds of enemy intelligence analysts, rendering their attentions divided and their preparedness degraded. Second, a distracted intelligence service is less likely to find and fix insurgents, increasing their survivability. This brand of ruse may, as one example, take the form of employing local printing presses to generate disinformative pamphlets and posters. A "hoax" pamphlet might advertise a bombing that never occurs, while a “false-flagging” poster may pin the responsibility for an actual bombing on a rival group or an altogether nonexistent entity. Such “noise” worsens enemy preparedness, and thus may better the chance of success in direct action missions, as well as contribute to the surprise when action is undertaken.

- **A Joint Task Force Commander (CJTF), charged with conducting a noncombatant evacuation operation (NEO) in a semi-permissive urban environment, arranges for false operational plans to be leaked to/intercepted by potential adversaries.** These plans, if believed by an opponent determined to thwart the NEO, will have the opponent fortifying the wrong buildings, preparing the wrong avenues, and the like, all at the wrong time and in the wrong way. The goal of this JTF commander is to create a set of misperceptions in the mind of any potential adversary that will serve both defensive and, if necessary, offensive purposes.
- **A Joint Force Commander (JFC), commanding U.S. forces in support of a United Nations peacekeeping and nation-building mission, is plagued by guerrilla and terror attacks in built-up areas within his area of responsibility. He employs disinformation, demonstrations, and decoys to root out the infiltrators and insurgents.** By creating false targets of opportunity (for example, designating incorrect UN barracks locations in a radio broadcast), phony indicators of vulnerability (e.g., deliberately allowing vehicles too close to false headquarters), and other imaginative falsehoods, the JFC seeks to seize the initiative from the guerrillas/terrorists, divert their attacks to worthless targets, and pierce the veil of anonymity that cloaks their activities. This latter goal is particularly important for an urban setting, with its massive noncombatant population. Deception is used here to create misperceptions about the time, place, units, defensive posture, and other characteristics of potential targets. Deception is thus applied defensively in support of force protection and counterintelligence activities on a large scale within the urban environment. Note that in this case, deception is of necessity targeted at noncombatants deemed to be channels of intelligence for the adversary; this could be the political, social, or cultural leadership.

Deception can be a powerful force multiplier for leaders at all levels of war. As these examples hopefully demonstrate, no side automatically owns a monopoly on the use of deception, and all sides should be prepared to counter it.

HOW IS DECEPTION EMPLOYED?

The Contextual Requirements of Deception

Deception cannot and should not occur in a vacuum. The setting necessary for the conduct of deception can be characterized by the following features. Note that while the phrasing refers to "actors," this is shorthand: it could refer to individual items, such as a tank versus a reconnaissance aircraft, or groups, such as a terrorist cell versus a security agency.

- **Two or more actors are in contention.** This does not necessitate a state of open conflict, only unfriendly rivalry. It is presumed that they are seeking individually advantageous solution(s); this does not necessitate a perfectly zero-sum game, but merely something like it.
- **Information may be acquired, processed, and utilized by all actors: this forms their respective perceptions.** We presume that decisions can be made, and that these decisions are at least shaped in some manner by information about other actors and the environment (i.e., by perceptions). A blind, unthinking actor (or preprogrammed robot) is difficult to deceive.
- **Information may be transmitted between actors.** This may be indirect (i.e., via a third party), but if transmission is impossible then deception is not practicable. This also necessitates the complementarity between the methods of sending and receiving: my false radio transmissions are useless if you are not listening to the radio! Note that any collection of intelligence counts as a transmission of information.
- **The actors operate under conditions of uncertainty (i.e., without complete knowledge).** This is perhaps an epistemological consideration, but important nonetheless. A party that cannot be misled or made unsure cannot be deceived. A party in possession of literally all the pertinent facts, or one thoroughly con-

vinced of the accuracy of its perceptions, is extremely unlikely to be persuaded by contraindicators.

- **The actors possess some flexibility in their courses of action.** While an inflexible target may still be deceived, doing so would be an academic exercise. Deception has utility only if the target takes or refrains from some action that the deceiver can exploit.

It appears that the factors of confusion and high operational tempo, the multiple dimensions of threat and uncertainties, the degradation of intelligence and communications, etc., all of which make urban operations so challenging, create a context (as defined here) eminently suitable to deception. We shall revisit this emerging hypothesis in greater detail in the final chapter of this report.

The Process of Deception

> It is very important to spread rumors among the enemy that you are planning one thing; then go and do something else . . .
>
> —Emperor Maurice, *Strategikon*

Military deceivers have uppermost in mind an *objective:* what it is they want the friendly force to accomplish. This could range from simple survival to gaining strategic surprise. Growing immediately therefrom is a notion of what the deceiver wants the adversary to *do* in order to achieve that objective. This could be as simple as getting the adversary to focus at point A instead of point B at a critical moment, or as complex as inducing the adversary to lower the readiness and preparedness of his nation's defenses over the course of years.

If the deceiver knows what the adversary should do, the next step is to consider *who* can galvanize that action: this person is the *target* of the deception. As noted previously, the target may be a principal in the adversary command structure or an influential noncombatant, for example, a revered religious leader. The deceiver parlays intelligence (HUMINT, SIGINT, etc.) about the target into a profile of that person's preconceptions, beliefs, intentions, and capabilities. A well-constructed deception is built around that intelligence and exploits it. The deceiver answers the question, "What more does the target need to believe in order to incite the actions I desire from him?" This is to say, the deceiver generates a list of misperceptions that must be engendered in the target.

Knowing the beliefs the target must hold to goad him to prejudicial action, the deceiver formulates the *story* that must be told to the target (through a variety of media) to produce those misperceptions. This "story" is told through the means of deception: the classic instruments (such as camouflage or disinformation) that comprise the deceiver's arsenal.

Thus the deception planning process is a "backwards-planning" procedure, which begins with the desired end-state (i.e., the objective) and from that derives the target of the deception, the target's desired response, the requisite misperception, and the "story" that needs to be told. In deception plans, *the ends dictate the means*. This is illustrated in Figure 1.

The actual execution of the deception planning process moves in the reverse direction: informational elements being manipulated are transmitted (or obscured), creating the story, in the mind of the target(s), to achieve the objective. A simple historical example will serve to illustrate the process:

- Facing German submarine warfare prior to World War I, Winston Churchill sought to confuse and entrap German submarines (*the objective*). The entity that controlled German submarines was

RAND *MR1132-1*

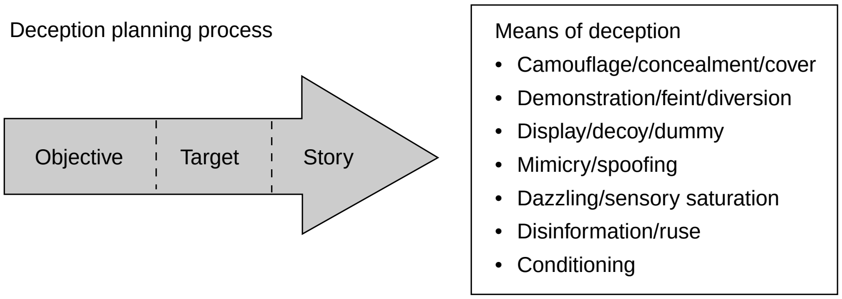
Deception planning process
Objective
Target
Story
Means of deception
• Camouflage/concealment/cover
• Demonstration/feint/diversion
• Display/decoy/dummy
• Mimicry/spoofing
• Dazzling/sensory saturation
• Disinformation/ruse
• Conditioning

Figure 1—The Deception Planning Process

> the German High Seas Fleet (*the target*). Churchill reasoned that the German High Seas Fleet would be baffled and ripe for ambush (*the target response*) if the number and disposition of British vessels were inflated and/or ambiguous (*the misperception*). Churchill therefore urged the construction of numerous decoy, dummy, and notional ships (*the means*) to produce such inflation and/or ambiguity (*the story*).

If we accept the premise previously introduced—that the characteristics of urban operations allow or perhaps facilitate deception—is it any surprise that combatants readying their urban environment for battle will do so to best facilitate the deception process? As noted by Matsulenko (1974, p. 33, emphasis added),

> In October 1942, [Soviet] Engineering Forces prescribed the construction of obstacles, preparation of built-up areas, and delimiting of defensive boundaries *in conjunction* with the development of operational and tactical deception plans.

The Means of Deception

> Let every soldier hew him down a bough, and bear it before him; thereby shall we shadow the numbers of our host, and make discovery err in report of us.
>
> —William Shakespeare, *Macbeth* , Act V, Scene IV

The means of deception are the tools in the deceiver's toolbox. As noted in Joint Pub 3-58: *Joint Doctrine on Military Deception*, they are "[m]ethods, resources, and techniques that can be used to convey information to the deception target."

We note that an imprecision in the definition must be clarified: the term "convey information" can in practice apply to both revealing and concealing data from an adversary. Most deceptions have elements of both, to varying degrees; for example, false radio traffic transmitted along with genuine communications can both cover the genuine signals with obscuring "background noise" and portray a false order of battle to the eavesdropping adversary. In the former, service deception plays a masking role, while in the latter, deception plays a suggestive role.

There are an infinite number of "methods, resources, and techniques" that may be employed in a deception, but they generally group into a finite number of categories. Current joint doctrine generally groups deception into three areas: physical, technical, and administrative (Joint Pub 3-58).

- **Physical means.** Activities and resources used to convey or deny selected information to a foreign power. Examples include military operations (including exercises, reconnaissance, training activities, and movement of forces); the use of dummy equipment and devices; tactics; bases, logistic actions, stockpiles, and repair activity; tests and evaluation activities.
- **Technical means.** Military material resources and their associated operating techniques used to convey or deny selected information to a foreign power through the deliberate radiation, re-radiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles.
- **Administrative means.** Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power.

The above taxonomy focuses upon the form rather than the utility of the means; an alternative would be to focus upon their function:

- **Camouflage/concealment.** The former is the use of natural or artificial material on or about the deceiver to evade detection. The latter is the judicious use of cover and terrain by the deceiver to hide from observation.
- **Demonstration/feint/diversion.** The act of drawing the attention of a target away from an area or activity the deceiver chooses. Demonstrations make no contact with the adversary, while feints do.
- **Display/decoy/dummy.** The placement of a natural or artificial construct away from a deceiver to portray an entity or object of significance to the target.

- **Mimicry/spoofing.** The use of a natural or artificial construct by the deceiver allowing him or her to portray an entity of significance to the target.
- **Dazzling/sensory saturation.** Overloading the sensory processing abilities of the target with an overabundance of stimuli. The principal idea is to raise the "noise" level high enough to drown out the target signal.
- **Disinformation/ruse.** The doctoring of media (printed, electronic, photographic, etc.) passed to the target.
- **Conditioning/exploit.** Either (1) exploiting a target's preexisting bias, belief, or habit, or (2) generating and then exploiting such a bias, belief, or habit. As noted by Collins (1997), "No matter how security-conscious someone is, there is almost always some aspect of his behavior which becomes habitual." Whether the habit is naturally acquired or induced by the would-be deceiver prior to an operation is incidental.

Consider the following example from the January 1995 battle for Grozny:

> [The Chechens] would listen in to Russian units on a captured radio set. When a unit sounded as if they were in trouble and calling for instructions, one of the Chechens would grab the receiver and shout commands in Russian to retreat. (Gall and De Waal, 1998, p. 206.)

Under the current Joint Doctrine definition, this would be considered a *technical* type of deception, conveying erroneous information to adversaries through radiation of false radio signals. Under the second taxonomy scheme, this same deception would be part mimicry and part conditioning/exploit, as functionally the effort is aimed at imitating a trusted source of authority and engendering a preconditioned response.

In practice, deceivers combine material and behavioral elements as needed to craft deceptions based upon operational requirements plus good intelligence of the target. Nearly anything can be drafted into the employ of the deceiver as needed, and the above categories should serve to illustrate the broad range of instruments available. It should also be noted that deception is almost always conducted to further some concurrent activity. Thus, a terrorist might employ a disguise to gain access to a political dignitary's residence. Or a combatant commander might use a diversion to draw enemy forces away from the actual avenue used for an assault. This is not a requirement per se for deception to take place, but deception is seldom seen without it.

HOW USEFUL IS DECEPTION?

It is widely understood that deceptions have aided combatants in both offense and defense for the length of recorded history and the breadth of conflict, from insurgency to invasion. Historical accounts document the employment of deception in a spectrum of environments, supported by a broad range of technologies, both high and low. The following examples, drawn from disparate parts of the spectrum in terms of technology and scale, should serve to suggest that deception is valuable both offensively and defensively, in cities as well as other environments, and in conflicts of varying intensity, regardless of technology and "home turf" advantages.

- In roughly 1200 BC, Joshua captured the city of Ai by means of deception, shortly after the fall of Jericho. After suffering a minor defeat in his first attempt at taking the city, Joshua devised a ruse that has been repeated countless times since: the feigned retreat. Arraying the bulk of his host before the gates of Ai, Joshua offered battle, all the while hiding a goodly portion of his force to the rear of the city, out of sight. When the soldiers of Ai took the field and began battling his men, Joshua ordered a retreat designed to look as if it were a rout. When the exultant men of Ai came after them, Joshua's hidden force emerged and stormed Ai, overwhelming the skeletal force left behind and seizing the city. As the news hit the men of Ai their charge faltered, and Joshua wheeled his force and pinned them between his men and the now-captured city. Their force in disarray, the men of Ai were slaughtered. (Drawn from Handel, 1985, and Dunnigan and Nofi, 1995.)
- In September of 1864, the Confederate guerrilla fighter Nathan Bedford Forrest surrounded a well-defended Union fort at Athens, Alabama. Forrest's force numbered about 4,500, while the dug-in Union force at the fort numbered under 2,000. Forrest suspected the unpleasant outcome of any attack against a

prepared, well-armed enemy in built-up terrain, and further knew that reinforcements were on their way to relieve the beleaguered Union defenders. Forrest arranged a parley with the fort's commander, Colonel Wallace Campbell, and contrived an artful deception to receive him. In a trick that Erwin Rommel would repeat in Tripoli nearly a hundred years later, Forrest arranged for Campbell to be given a tour of the besieging force—all the while having each unit that Campbell left pack up and be placed in his path again. This clever bit of trickery convinced Campbell that he faced a force roughly four times his own and induced him to promptly surrender without a fight. (Drawn from Asprey, 1994, and Dunnigan and Nofi, 1995.)

- The Battle of Kursk, in mid-1943, demonstrated the powerful—indeed decisive—leverage deception offered to combatants on both the offense and defense at the strategic and operational levels. The Germans massed an enormous combined force in their offensive against the Soviet Union at the Kursk "Bulge." A worried Soviet High Command (STAVKA) generated strategic and operational defense plans thoroughly incorporating *maskirovka* [deception and OPSEC] measures. Moreover, *maskirovka* was employed to conceal preparations for Soviet offensives to follow hard upon the heels of the defense. The deception measures included diversionary operations (feints and demonstrations), false troop and logistics concentrations, false and confusing radio traffic, false airfields and aircraft, and the dissemination of false rumors both at the front and in German-held areas. (Drawn from Glantz, 1989.)

- The successful terrorist/revolutionary 1946–1948 campaign of the Zionists to drive the British from Palestine in the aftermath of World War II and establish a Jewish state has, as its pivotal event, the perpetration of a deception. The Irgun, led by Menachem Begin, used a well-crafted and precisely targeted deception to erode British mettle and energize the Irgun's popular support. British forces, who had annually suppressed Yom Kippur [Day of Atonement] rites at the Western Wall, were fed false (but persuasive) information by the Irgun that the upcoming event would be attended by Irgun members in force, who were prepared to violently resist any British suppression. The methods included English-language pamphlets and rumors circulated through informers. In reality, no Irgun members were to attend (although no one but the Irgun would know this). The British backed away from the supposed confrontation, and this policy change was trumpeted by the Irgun as a major victory for themselves and for all Jews. (Drawn from Begin, 1972.)

- In 1990–1991, “DESERT STORM demonstrated the effectiveness of the integrated use of operational security (OPSEC) and deception to shape the beliefs of the adversary commander and achieve surprise. Deception and OPSEC efforts were combined to convince Saddam Hussein of a Coalition intent to conduct the main offensive using ground and amphibious attacks into central Kuwait, and to dismiss real indicators of the true Coalition intent to swing west of the Iraqi defenses in Kuwait and make the main attack into Iraq itself . . . Deception measures included broadcasting tank noises over loudspeakers and deploying dummy tanks and artillery pieces as well as simulated HQ radio traffic to fake the electronic signatures of old unit locations.” (*Joint Staff Special Technical Operations Division*, quoted in JP 3-13.)

If history is any guide, deception (particularly in coordination with other IO methods) can be a valuable force multiplier at any of the levels of war or peace, in crisis or in conflict.

WHAT ARE THE DANGERS OF EMPLOYING DECEPTION?

> Oh, what a tangled web we weave, when first we practice to deceive!
>
> —Sir Walter Scott, *Marmion*

Deception is admittedly a double-edged sword: lethal when wielded competently, dangerous if mishandled. As noted in JP 3-58, “deception planners must carefully consider the risks versus the possible benefits of the deception.” There are three fundamental challenges to the employment of deception: cost, deconfliction, and discovery.

As noted in current doctrine (JP 3-13), practicing deception successfully may be among the most rewarding of investments but it also requires an expense:

> Military deception operations are a powerful tool in full-dimensional operations, but are not without cost. Forces and resources must be committed to the deception effort to make it believable, possibly to the short-term detriment of some aspects of the campaign or operation.

It is also critical that deception is properly coordinated and overseen so as not to create confusion or fratricide among friendly forces. For example, a camouflaged soldier lying in wait wants to ensure that while he is undetected by the enemy, his location and identification are known to friendly forces, for obvious reasons. At a higher operational level, a combatant commander who employs false radio transmissions to dupe the enemy into thinking his forces will be imminently attacking an enemy-held town in force must be careful to ensure that such a deception does not drive noncombatants living in the town into a panicked and dangerous flight. The processes of carefully screening and targeting deceptive efforts to affect only the desired target are known collectively as deconfliction.

In the dynamic environment of a military operation, it is imperative that deception planners carefully and continually monitor (and reexamine as necessary) all the components of the deception process: objective, target, story, and means. One key reason for this is the need to be able to mitigate damage should the deception be discovered. As noted in joint doctrine concerning deception (JP 3-58), deceivers must be wary of "deception failure, exposure of means or feedback channels, and unintended effects." The danger of deception exposed can be grave, as was the case when the British exposed and turned every German spy in England during World War II. This provided the British with an excellent tool for perpetrating their own schemes against the Germans.

Finally, a consideration of the legality of employing deception is warranted. Deception is in principle coordinated with command and control warfare (C2W), civil affairs, psychological operations, and public affairs to harmoniously advance U.S. military interests. In practice, however, the generation and dissemination of patently false or misleading information is a complex, evolving, and legally murky issue. As noted in Joint Publication 3-58, it is generally accepted that U.S. forces may employ deception (whether administrative, physical, or technical) against hostile forces with impunity (in a legal or ethical sense). Further, it is contrary to U.S. policy to deliberately misinform or mislead the U.S. public or U.S. decisionmakers (leaving room for operational security/secrecy). However, in between these two poles is a great, gray area that may have a significant impact on military outcomes. What about employing deception against neutral or unfriendly forces not directly involved in the operation? Against noncombatants (particularly influential ones) friendly to an adversary? Against NGOs? What if deceptive information targeted against an adversary leaks out to international news media and is then fed back to the American public? The answers to these questions are unclear, which traditionally means that if the stakes are high, then all is permitted that is not expressly forbidden. While a thorough treatment of this topic is beyond the scope of this report, the interested reader may find a useful and up-to-date discussion in Greenberg, Goodman, and Soo Hoo (1999).