Chapter Four

A FRAMEWORK FOR DECEPTION ANALYSIS

> The United States Armed Forces must establish integrated CCD [camouflage, concealment, and deception] training procedures for defenders, attackers, and intelligence personnel.
>
> (Recommendation from Joint CCD Program FY95 Annual Report)

Consider the battle for Grozny in January 1995. Earlier work by the authors described the broad range of deception measures employed by the Chechen fighters against better-armed, numerically superior Russian forces in Grozny (Gerwehr and Glenn, 2000; examples drawn from Thomas, 1997; Lieven, 1998; Gall and De Waal, 1998; among others). For example,

- Chechens and Muslim volunteers disguised themselves and vehicles as Russian.
- Chechens and Ukrainians disguised themselves and vehicles as Red Cross.
- Chechen fighters purposefully commingled with noncombatants to close with or escape from Russian forces.
- Chechens camouflaged firing points, staging areas, command posts, and observation posts.
- Chechen decoys drew fire.
- Chechen dummies and disinformation confounded Russian intelligence analysts.
- Chechen disinformation misled Russian order of battle and COA estimates (e.g., about man-portable air defense systems).

- Chechens used feints and demonstrations to draw out hidden Russian forces.
- Chechens used false radio transmissions to give Russian units orders or create uncertainties.
- Chechens used fire and rapid maneuver (shoot-and-scoot) to disorient Russian units.

The Chechen-Russian conflict illustrates some important issues regarding deception, both what is known and what remains unknown about deception effects.

First of all, deception was effectively used for all kinds of objectives: force multiplication, force protection, and intelligence collection. Further, the breadth and depth of techniques used indicate that the Chechens were placing a great deal of emphasis on deception and doing so with both forethought and adaptability.

Second, deception was used to achieve a variety of *effects* (masking, misleading, confusing) with a variety of *means* (disguise, decoys, camouflage, feints, etc.), suggesting that Russian intelligence assets were having to wage a continuous and difficult effort to visualize the battlefield accurately, with penalties incurred for any and every intelligence shortfall (whether in acquisition, identification, or uncertainty resolution). Moreover, supporting such a broad array of methods and effects requires resources—radios, uniforms, fuel, camouflaging materials, training, planning, active management, etc.—which again highlights the proposition that the Chechens felt deception to be a critical effort. Importantly, it underlines the failure of Russian interdiction.

Third, there is very little existing capability to model or perform cost-benefit analysis of the deceptions employed. All parties would agree that deception use was instrumental in Chechen successes, but no one has determined which techniques contributed the most, how their conduct was amplified or impeded by environmental or target variables, how much was gained versus how much was invested, etc.

This chapter begins to address the third point: a more nuanced and finely resolved view of deception is the first step toward an analytic taxonomy.

TOWARD A BETTER UNDERSTANDING OF DECEPTION

Deception is an integral part of conflict and always has been. This is nowhere more true than in urban settings, where the complexity of the terrain and the density of available resources allow for a well-stocked bag of tricks. But despite its widespread use, how much is actually known about deception? Surprisingly, there is far less research and guidance than is merited. Consider the following scene:

> The commander of a tank platoon wishes to protect his unit, which is deployed to seize and hold an area of key urban terrain. Many hasty defensive measures are possible, but let us suppose time, mission, and resources permit only a few steps to be taken before the likely counterattack. Some possibilities include clear-cutting what vegetation might exist in the built-up area, emplacing obstacles, and preparing firing positions with sandbags. Among the possibilities for deceptive measures are two staples: decoys and camouflage. With regard to the likely risks and dividends of employing such deceptive measures, there are numerous important questions facing the commander, a sampling of which are shown in Table 1.

To the authors' surprise, there are not well-developed answers to these questions in doctrinal publications on military deception, and there are too many such unanswered questions. This assertion applies not only to adversary use of deception, but friendly applications of deception as well. This is *not* to say that there is any lack of appreciation for the importance of deception in the military community! From the rifleman whose life depends upon the quality of his camouflage to the general whose battle plan hinges upon the success of a feint, combatants readily agree that deception is important if not *essential* to military success. Further, we recognize that there is no lack of wily and creative tacticians in the U.S. armed forces, at all levels. But how can deception be quantified, measured, analyzed, and, ultimately, writ in doctrine with the specificity of a scientific discipline? What guidance can be provided to the soldier or marine—to combatant and commander alike—that will give them more options, better options, and improved estimates of outcome when using deception? The authors believe that well-developed deception theory is necessary; it would provide soldiers and marines useful guidance and prescriptions for deception and counterdeception to *supplement* their own ingenuity and cunning.

Table 1

Sample Questions on Employing Deception

Which deception is best?	Which is better protection for a tank: camouflage or decoys? Is the value of employing both equivalent to (camouflage plus decoys) or (camouflage multiplied by decoys) or something else?
Against whom?	Is this equally true applied against both airborne and ground enemies? Who among the enemy should be targeted? Who among the noncombatant population?
With what parameters?	Does this hold true for more than one tank? Is there an upper numeric limit on the force to be protected? How many decoys provide the right ratio of fake to real? How much is lost by missing the optimization point?
Under what conditions?	Does this answer vary by terrain type within the urban area? By lighting level? By season?
How much deliberation is required?	How carefully should decoys be emplaced? How exposed should they be to adversary reconnaissance? How much is gained (or lost) as increasing time and effort is spent on emplacement?
What is the timeframe?	How long can the camouflage be considered viable? What about camouflage for the decoys?
When is the deception unmasked?	Are camouflage or decoys rendered moot if noncombatants pass close to the site (providing a source of HUMINT to the adversary)?
What value is lost when the deception is unmasked?	Do both camouflage and decoys decrease in value by the same amount when an adversary becomes aware of their use on the battlefield? Can value be regained if the camouflage or decoys are redeployed at another location? How much value? Is there value in replacing the decoys with actual systems at some point in time (e.g., after they are determined to be fakes by the adversary)?

Among the first benefits in developing a deception theory is the generation of *measures of effectiveness*. Existing measures of effectiveness are poorly developed with regard to deception—as opposed to those for vehicle armor or protective vests, for example. Armor provides readily accessible measures of effectiveness: the ability to turn a blow, encumbrance, cost, and so on. But deception is a more difficult nut to crack: if deception persuades a little, is that worse than if

it persuades a lot? Or does it depend on the duration of the misperception it creates? Or on the degree of erroneous action it engenders? A significant fraction of this research was devoted to mining the literature of biology in order to address these questions. We sought to develop a framework for typing, comparing, and assessing deceptions in the hopes of applying such metrics to the military domain.

One of the first steps toward a deeper understanding of deception is to take a more nuanced approach to the phenomenon. It is not enough to simply note that an adversary is employing camouflage, concealment, and deception (CCD) measures. Such an observation is lacking in specificity and therefore equally lacking in prescriptive value. Why? Because deception is a broad category that encompasses starkly different activities. For example, camouflage and decoys seek to produce very different effects upon the target's decisionmaking process and present the target with different problems to solve. Moreover, even two techniques with the same name may be significantly different in their level of sophistication and thus present very different problems for the target to solve.

THREE PERSPECTIVES ON DECEPTION

Level of Sophistication

Let us consider camouflage as a representative category of deceptions. To state that an adversary's vehicles or personnel are camouflaged is only to scratch the surface of the deception. What is the nature of the camouflage? How much consideration of defense versus offense is included in the camouflage's design? Is the camouflage unchanging, without sensitivity to changes in the environment (light, smoke, temperature, etc.)? Is the camouflage crafted in light of the deceiver's experience in employing it? Is it tailored to the target's perceptual structures and tactics for maximum effectiveness? Is it designed to foil a broad array of observers, or just one opponent? Is it applied to the visual spectrum alone, or does it include other portions of the electromagnetic spectrum? Is it aimed at ground observers, airborne observers, or both? These are obviously just a few of the questions that might be asked to uncover the details of a particular deception. The most important answer: camouflage (or any

other category of deception) is one in a spectrum of deceptive measures lumped together under one heading, and they may vary widely in their effectiveness. Why? Because the details matter greatly. Studies of deception in other fields—particularly animal biology—suggest that environmental effects, OPTEMPO, recent history, preconceptions, warning, and a host of other factors weigh heavily in the net effect of any deception.

Consider a simple illustration of this point: two sniper firing positions, both of which may be considered *camouflaged* but which differ remarkably in their details (and probably their effectiveness).

- One occupies a rubbled building and has nearby debris piled up around it to prevent visual acquisition by enemy infantry (the primary target of the sniper).
- The other camouflage scheme is selected with specific attention to the context, the sensor capabilities, and the search strategy of the adversary. It also occupies a rubbled building, and similarly makes use of handy debris. The position and angle of firing is chosen to best suit the opponent's avenue of approach, while the exact color and shading of the netting/debris suit the lighting level of the area. Moreover, the position is draped in a netting that mimics the near-infrared (NIR) spectral reflectance of urban materials and a thermal blanket to dampen heat signature. This netting is employed in response to intelligence that places infrared imaging and radar in the hands of the opponent, and this camouflage might be aimed at ground troops *and* airborne reconnaissance, accounting for the presence of helicopters or UAVs in the arsenals of the foe. Perhaps the area around the firing position is also prepared to dampen muzzle-flash and backblast from weapons the sniper is likely to employ.

When we discuss the degree to which any particular deception attends to the adversary's sensors and preconceptions, environmental and contextual effects, and the myriad other factors that influence deception success or failure, we call this the *level of sophistication* of that particular deception. Note that this phrase is intended as a diagnostic, not a value judgment. An "unsophisticated" knife can kill just as readily as a "sophisticated" precision-guided munition (PGM); the utility of the diagnostic lies in its ability to more finely resolve the

Getty Images

Figure 1—The Clouded Leopard's Camouflage Is Well Suited to Its Environment

Frank & Joyce Burek/Getty Images

Figure 2—The Western Diamondback Rattlesnake Conceals Itself Amid Leaves and Undergrowth

Getty Images

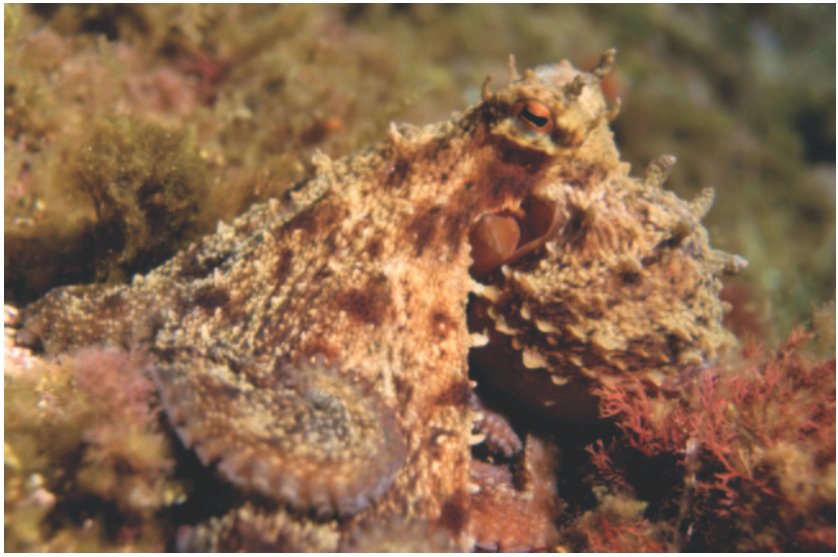
Figure 3—The Okapi Has Camouflaged Coloration and Disruptive Hindquarters Markings

Mike Jones; Frank Lane Picture Agency/Corbis

Figure 4—The Cuckoo Egg Matches the Host Eggs Enough to Pass the Critical Tests

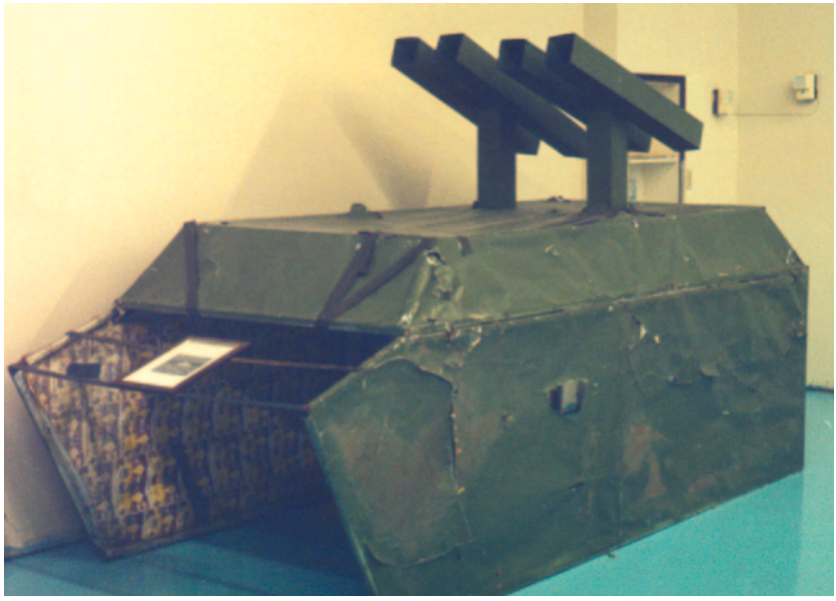
Photo courtesy of BRUCE COLEMAN INC., Photographer Tony Deane

Figure 5—The Blacksmith Plover Has Coloration That Disrupts Its Outline



Sami Sarkis/Getty Images

Figure 6—An Octopus Uses One from Its Array of Possible Colors and Textures to Blend in with Its Background



Photographer COL Andrew O'Donnell, USMC

Figure 7—The Serbs Used This Decoy Against NATO Forces in Kosovo, 1999

James Gritz/Getty Images

Figure 8—The Flatfish Masks Its Presence

Illustration by Barbara Caslon

Figure 9—Amphipod Hyperiella Dilatata Misleads Audiences with a Living Disguise

Photo courtesy of Photo Researchers, Inc., Photographer Dade Thornton

Figure 10—The Deadly Boomslang Appears To Be a Tree Branch to the Unwary

deception phenomenon and therefore lead to more precise use and countermeasures.

The level of sophistication that might characterize any given deception is a spectrum ranging from static and context-insensitive to tailored and premeditated. We can place milestones along this spectrum for the purposes of producing a more nuanced view of deception so long as these markers do not eclipse the fact that this is indeed a spectrum. The authors assert that level of sophistication progresses as Static → Dynamic → Adaptive → Premeditative, as described below.

Static *deceptions are in place regardless of state, activity, or the histories of either the deceiver or target.*

The standard-issue woodland BDU falls into this category; while employed in woods or jungle, it has also been worn in the desert, city, or at sea, and there is no doctrinal instruction that allows soldiers, marines, or other service members to tailor the BDU in beneficial ways.

The blacksmith plover (Figure 5; see following page 32) has disruptive coloration that can interfere with the targeting of would-be predators (note that this application of deception doesn't prevent detection, but rather the subsequent attack). While the plover's markings are generally effective in its habitat, it has no ability to turn on or off the coloring scheme nor to tune it to the particular lighting or weather conditions it finds itself in.

Dynamic *deceptions are those that activate under specific circumstances. The ruse itself and the trigger do not change over time, nor do they vary much by circumstance or adversary.*

The preplanned "swarm drill," whose purpose is to mask the insertion of a sniper team upon entering a building. A group of marines (including the sniper team) will overtly enter a building in relatively large numbers, assuming that they are being observed. Upon exiting and moving on, they leave behind the sniper team, and only a precise entry/egress count by an observant foe would detect the difference. Given that the marines enter and exit through multiple points in the building, an exact head count would be very difficult to accomplish.

Octopi (Figure 6; see following page 32) and squid are widely appreciated for their well-stocked inventory of deceptions. Octopi bodies contain special cells (chromatophores) that can expand and contract to manipulate their pigmentation. The function of these cells allows the octopus to appear any combination of red, orange, green, blue, brown, or even whitish. As the background changes, the octopus selects the right concealing color. To complement this capability, the octopus' mantle can also change texture: matching coral, sand, rock, or seaweed as appropriate. Why does this extraordinary complement of ruses come under the heading of dynamic, and not something higher? Because the ruses themselves do not change over time, and neither do the triggering mechanisms (i.e., changes in nearby terrain). The rules are set ahead of time (the animal equivalent of preplanning) and set in stone, even if the color parameter is continuous. This is "scenario-based" deception planning. We note that *possessing great quantities of a capability does not necessarily mean greater flexibility with regard to that capability.*

***Adaptive** deceptions are triggered like dynamic deceptions, but either the trigger or the ruse itself can be modified with experience. This category covers deception improved through trial and error.*

An illustration of adaptive deception in an urban setting:

> [Chechen] mortars mounted on Kamaz trucks fire one salvo and immediately move to another area. They have skillfully *learned* to disorient fire spotters, often creating a friendly fire situation. Thus on the eve of the taking of the palace, a Russian Grad multiple rocket launcher fired on its own reconnaissance company in the airport region, which is ringed by mountains and forests. (Vinogradov, 1995; emphasis added)

The larvae of the green lacewing (*Chrysopa slossonae*) feed rapaciously on woolly alder aphids (*Paraprociphilus tessellatus*), stalking and killing them despite the presence of vigilant black carpenter ants that protect aphids. The lacewing larvae transfer woolly wax from the aphids' bodies to their own as they prey upon them, quickly developing a disguise that the guardian ants cannot penetrate. The reason why this form of deception is called *adaptive* as opposed to *dynamic* is that the parameters of the disguise are not fully deployed and optimized ahead of time, but are instead determined through

interaction with the adversary and environment. This is more "capabilities-based" deception planning, and the set of possible deceptions produced is—if not infinite—likely to be larger and *more tailored to the precise circumstances* than under "scenario-based" planning.

***Premeditative** deceptions are designed and implemented based on experience, knowledge of friendly capabilities and vulnerabilities, and, moreover, observations about the target's sensors and search strategies.*

The "stealth" coatings on low-observable aircraft are good examples of premeditation in deception: they are very specifically designed to thwart the radars of known (and potential) adversaries, with a specific mission (e.g., suppression of enemy air defenses) in mind and thus specific kinds of vulnerabilities to protect.

Primates, cetaceans (whales and dolphins), and humans hold the monopoly on highly sophisticated deceptions. The decoy pictured in Figure 7 (an unclassified photo taken at the Nellis AFB Threat Training Facility; see following page 32) was used by Serb forces against U.S. pilots in Operation Allied Force in 1999. Though crude—constructed of milk crates, baling wire, and green spray paint—it is a good representative of premeditative deceptions. Moreover, despite its primitive design, it drew at least a dozen strikes from Allied forces over several sorties; each time it was destroyed, Serb forces rewrapped it, repainted it, and set it out again to draw fire on the next sortie.

The authors encountered an example of tailored, precisely targeted deception conducted by an Atlantic bottle-nosed dolphin in a May 2000 visit to the Marine Mammal Systems program in San Diego. A certain dolphin in the pod would venture out with her handler to conduct sector-by-sector mine search training. Each search in the exercise normally took a well-established length of time, after which the dolphin would return to the handler and signal whether she had encountered ordnance (training mine of the moored or buried varieties) or nothing in that sector. The handlers began to notice that this dolphin (who was healthy, but quite advanced in age) was missing training mines in her searches and considered the possibility that she might be losing some echolocation capabilities, or processing

skills, or the like. However, upon investigating, they discovered that the crafty dolphin would receive her instructions and dive off as though on a search, but actually circled round and hovered underneath the handler's boat. She waited for a length of time precisely suited to the volume of water she was supposed to be searching and then resurfaced, signaling "all clear." Her assessment of the handler's expectations, manipulation of the signals, and devising of a ruse that matched the circumstances are all hallmarks of a sophisticated deception.

In application, considering the level of sophistication of particular deceptions can make valuable contributions. For example, if an urban insurgency is disguising its fighters as noncombatants, it would behoove the constabulary force to carefully consider the level of sophistication of such disguises. Hasty, poorly resourced disguises might be uncovered by simple checkpoints, while those with expertly-forged documents and ample preparation time might require chemical sniffers, a gauntlet of interviews, or other more elaborate counterdeception techniques.

Effect Sought

While the sophistication of any deception method is pivotal to its success or failure, another vital component is the type of *effect* the deception seeks to produce. By "effect" we mean the specific type of disadvantageous misperception the deceiver is seeking to produce in the mind of the target. Consider: camouflage and concealment are closely related, yet they have almost nothing in common with decoys or feints. Camouflage and concealment are *masking* techniques that reduce signals (ideally, to the point of undetectability). A warfighter or analyst seeking to overcome masking techniques is seeking to *acquire* a target in the face of opposition. But in the case of the decoy or feint, acquisition is a given; it is *identification* or discrimination that is sought. These are *misdirecting* techniques whose purpose is the clear and unambiguous transmission of a *false* signal (often in the hopes of diverting attention, resources, or attacks away from real assets or activities). The warfighter or analyst faced with misdirecting techniques must refine his or her capabilities for discerning true from false—an enterprise entirely separate from improving acquisition. A third category of methods—which the authors will term *con-*

fusing techniques—represents still another set of problems to the warfighter and analyst. These methods seek to degrade or paralyze the target's perceptual capabilities through voluminous background noise, oversaturation, unpredictability, and the need for haste. Confusing methods often interfere with *both* acquisition and identification; combating them requires a set of potential solutions to be explored quite apart from those previously mentioned. Table 2 illustrates how common CCD and other deceptive techniques map into these three major categories.

What is the defeat to be inflicted upon the target? Is the deceiver attempting to *mask* his/her signature? Is the deceiver attempting to present a signature with some element of falsity in order to *misdirect* the target to inappropriate belief? Is the deceiver seeking to *confuse* the target with paralyzing uncertainty? These are the three general types of effects sought by deception; they broadly group the type of misperception being induced by the deceiver. This is enormously

Table 2

Major Types of Deceptive Effect Sought

Deceptive Effect	Definition	Common Examples
Masking	Concealing signal	Camouflage Concealment Commingling with noncombatants Signature reduction
Misdirecting	Transmitting clear and unambiguous *false* signal	Feint/demonstration Decoy/dummy Disguise Disinformation (e.g., forged documents)
Confusing	Raising the "noise" level to create uncertainty, paralysis	Generating additional commo traffic, movement, etc. Shoot-and-scoot to disorient foes Purposeful departure from established pattern (also called conditioning/exploit) Randomization

important when we consider the information processing and decisionmaking of the target. The mental process of acquiring is quite different from the mental process of identifying, and both are different from the process of resolving uncertainty.

Consider the individual infantryman engaged in peacekeeping (patrolling) duties. If a curfew is in effect, merely *spotting* anyone moving about comprises a violation. The exact identity of that person is of minimal relevance. On the other hand, if the peacekeeper is seeking to apprehend wanted criminals, then spotting is subsidiary to *recognizing* the individual. Lastly, if our peacekeeper runs across groups of persons who appear furtive or up to no good, then, although spotting and recognizing play a role, the peacekeeper must *choose* or resolve between several different plausible explanations (and thus courses of action). Figures 8 and 9 (see following page 32) show examples of masking, misleading, and confusing techniques in the animal kingdom.

An example of a living disguise in military affairs can be seen in the accounts of U.S. Marines in Beirut, described by Hammel (1985, p. 154):

> Women were sent into the streets to reconnoiter the Marine and LAF [Lebanese armed forces] positions. The most blatant of the scouts was a heavyset middle-aged woman—or a large man dressed in a woman's clothing—who made trip after trip across the end of the alley. One of the Marine riflemen reached the end of his tether late in the afternoon and dropped her in her tracks with one M16 round. An Amal gunman who was duck-walking in the woman's ample hidden side scuttled for a nearby building when his cover fell to the street.

In application, explicit consideration of effect sought is of immediate value in planning friendly deceptions as well as countering adversary deceptions.

- Let us consider first a simple illustration on the friendly side. If U.S. or allied troops are to be deployed in a constabulary role into an urban area with great numbers of neutral or hostile noncombatants, deceptions that seek to *mask* the friendly presence are likely to be of limited utility (due to human intelligence (HUMINT), etc.). This suggests that resources like camouflaged

BDUs and netting are probably of limited value and should be deemphasized. But deceptions that seek to *mislead* should be greatly effective in the noisy, chaotic, densely populated setting of the urban landscape, and thus resources like smoke, decoys, and false radio transmission capability should be pushed up the requirement ladder.

- Now let us think about the adversary. Consider a foe who is exploiting the presence of noncombatants by deliberately introducing "false positives" into U.S. intelligence-collection efforts: staging sniping or bombing incidents, transmitting phony signals intelligence (SIGINT), passing false HUMINT rumors, etc. The effects sought are *misleading* and *confusing*. In employing them the adversary wishes to lead friendly intelligence capabilities into a labyrinth of false trails, dead ends, and wasted efforts. Recognizing that an adversary is attempting these effects instead of masking should drive numerous friendly adaptations: a greater quantity of similar surveillance probably offers little value added, but a diversification of surveillance methods is likely to offer much. Mounting additional sensors (e.g., cameras) on lamp-posts or low-flying UAVs offers additional *detection* capabilities and thus merely gives the adversary another opportunity to generate a false positive. Mounting different sensors (e.g., explosives sniffers) offers the ability to *discriminate* among detections and thus is the proper countermeasure to misleading-type deceptions.

Means of Deception

We have already discussed a broad definition for deception that allows for consideration of many techniques to be brought to bear against many targets (whether combatant or noncombatant) in support of the friendly mission. Whether the effect sought by a particular technique is masking, misdirecting, or confusing, the *means* by which the deception is conducted can generally be thought of as comprising two parts: the *form* and the *function*. The part that is primarily a matter of substance or form (debris, dyes, temperature, shape, etc.) is called *morphological*. The part that is primarily a matter of implementation or function (timing, location, pattern, etc.) we term *behavioral*. Thus we would say that a tank with a coat of

nonreflective paint matched to its environment (in order to avoid detection) is employing a predominantly morphological deception, but a tank driving at civilian speeds on civilian roads among civilian vehicles (in order to avoid detection) is employing a deception of the behavioral type. Note that the categorization of form and function is not meant to straitjacket: some deception techniques will have elements of both. For the purposes of analyzing examples, however, we will generally assert that any individual deception has a *primary* means of achieving its effect. Thus, while an F-117's ability to remain undetected relies to some extent on pilot skill, it is to a greater extent a function of the aircraft's shape and composition.

Why should we pay attention to the different means of deception? The answer is fairly obvious: if we want to conduct deception effectively, we should have the resources to support the effort, and this includes not just physical resources (for morphologic means), but the proper training and doctrine to conduct behavioral deceptions as well.

Sophistication, Effect, and Means: The Details Matter

In the preceding sections we have attempted to offer a more finely resolved view of deception; the authors believe that dimensions of analysis are necessary to usefully bound the deception "space." Military deception and animal/plant deceptions can be understood within the same theoretic framework, and it is useful to compare one domain with the other to develop both a comprehensive view of deception and a sensitivity to important nuances that affect deception success and effect.

Categorizing deceptive techniques and behaviors is an important step toward a complete taxonomy, but it is only a first step. The ultimate goal of our research will be to fully inform decisionmakers on the topic of deception, particularly in urban operations. To proceed toward a comprehensive and useful analytic framework, we must relate deceptions of quite different sorts applied against different targets in different circumstances. The theory we hope ultimately to establish will enable decisionmakers to:

- Evaluate the costs and expected dividends from a given deception measure employed in a particular context.

- Compare the costs and benefits of any two or more deception measures, including different implementations of the same type (i.e., a range of potential investment levels in the same camouflage technique will produce a corresponding range of potential benefits).
- Make tradeoffs between the investment in deception and the investment in other friendly measures (e.g., speed, lethality, armor, intelligence collection).
- Understand the interaction between deception measures and other friendly measures (e.g., camouflage and armor, or decoys and speed, or disinformation and intelligence collection).
- Understand what type of problem is posed by different types of adversary deception measure; this will prescribe a more precise method of counterdeception.
- Perform cost and benefit analysis on candidate counterdeception measures given the range of deception(s) they face and context they are fielded in.

AGGREGATING DECEPTIONS FOR GREATER EFFECT

We have identified a minimum of four ways in which individual deceptions may be aggregated to achieve operational/strategic-level benefits:

		Application	
		Space	Time
Method	Same		
	Different		

Individual deceptions can vary in their method and, moreover, in where and when they are applied.

- **Employing multiple, similar methods of deception.** Individual ruses can be employed en masse. For example, decoys can obviously be used one at a time or in groups.
- **Employing multiple, different methods of deception.** Ruses may differ in form, may be aimed at different targets, and may

induce different (though complementary) misperceptions. For example, a false map purporting to depict a belt of obstacles and strong points in a city, placed into the hands of an enemy patroller, along with a demonstration by armored vehicles and infantry, both communicate a false impression of defender tactics, techniques, and procedures (TTPs) to enemy reconnaissance. False radio messages could likewise misrepresent the location and vulnerability of critical nodes in the city to enemy SIGINT while, further, members of the indigenous population pretending to be sympathetic to the enemy cause communicate false vulnerabilities. Who falls prey to these deceptions individually/tactically may incur negative operational or strategic consequences.

- **Applying deception at different points in time.** Individual deceptions may occur in a sequence devised to engender operational or strategic effects. Consider this simple illustration: What occurs in the mind of an infantryman "hunkered down" in the rubble if what starts out as the sounds of distant, sporadic gunfire becomes a torrent of shots (perhaps interspersed with explosions) nearby? An individual ruse (staged sniper fire) can be employed with others (of a kind, or different) *over time* to create desired effects. In this simple case, it may be that headquarters (HQ) begins receiving reports of an impending attack.
- **Applying deception at different points in space.** Deceptions conducted at different places may have a synergistic effect. In a simple illustration of this point, consider the combatant whose reconnaissance elements spot enemy forces (actually dummies) in each of the cardinal directions. Such a combatant may conclude that he or she is surrounded and take appropriate action: shifting from offensive to defensive postures, or even surrendering (in the most extreme case). Although this is a simple example, it nevertheless makes the point that the distribution of ruses in physical space can have an aggregated effect at the operational or strategic levels of war.
- **Level of sophistication.** As the deceiver's intelligence picture improves, the power or scope of deceptions may increase. The incorporation of new information about the target of the deception (their sensors, preconceptions, history, etc.) or the environment (ambient light and noise levels, terrain type, engagement

ranges, etc.) greatly increases the level of sophistication of the deception. Although it has not yet been experimentally demonstrated that level of sophistication correlates with success, it is a reasonable hypothesis. Consider the use of a lure: the angler fish *Lophius piscatorius* has a worm-like bit of webbing on the end of its forward dorsal spine which it bobs about to attract prey. This deception is not terribly specific (the angler preys upon numerous smaller species indiscriminately) but still quite effective. On the other hand, the PIRA often carefully tailored its deception techniques based upon what it knew of British standing operating procedures (SOPs), as Curtis (1998) relates. In one incident, a tractor tire with wires visibly poking out is left outside a betting shop in Brompton Park, Belfast, as a lure. British SOPs demand that the tire be examined by ordnance-disposal personnel and the area secured by troops. Knowing this, and knowing that the soldiery securing the perimeter are likely to be diffusing their attention between outside threats and the disposal operation in their midst, the PIRA forces set a successful ambush, killing one and wounding two. The nature of the lure in this case is based quite specifically upon knowledge of the foe (learned through previous encounters, informers, etc.). Not only are the resulting deceptions more likely to succeed, but the consequences of the deception are made much more deadly. Although this example is tactical, a few such successes that result in significant friendly casualties, well-publicized mission failures, property damage, or third-party misfortunes could have operational- or strategic-level effects.

This principle of accumulating operational or strategic value by combining tactical-level deceptions is eminently visible in a historical review of military deception, which often reveals exactly this sort of aggregation. For example, disparate Egyptian deception measures preparatory to the 1973 surprise attack at the Suez Canal were designed with a specific cumulative effect in mind. *Together* they were meant to create a strategic deception aimed at Israeli intelligence analysts and commanders. The Egyptians demobilized 20,000 troops days before the attack; staged numerous and repeated canal-crossing exercises; used frequent maneuvers and construction activities to cache crossing equipment at hidden depots near the canal; spread a variety of rumors via radio, print, and word of mouth that

made an attack seem unlikely; and continued to build *defensive* lines as though settling in for a long haul at these positions (Betts, 1982; Haykal, 1975). It seems fair to say that the strongest doctrinal embrace of this method would be Soviet (now Russian) doctrine of *maskirovka*, which has long espoused that strategic-level benefits will grow from aggregations of tactical- and operational-level deceptions (Glantz, 1989).

COUNTERDECEPTION

> [His] voice attempted one final deception: "Thy abominable sins forbid thee to look upon my radiance . . ." he began. No one was listening; he was riddled with spears. (J.L. Borges, *A Universal History of Infamy [The Masked Dyer]*)

The other side of the coin in developing deception theory is counterdeception theory. The authors believe that deception and counterdeception capabilities must not be isolated from one another, but analyzed and developed in a complementary fashion with a significant amount of cross-pollination.

That said, how shall we begin our consideration of counterdeception? As noted above, deception seeks to engender errors in the perceptual apparatus of the target with the goal of causing bad decisions to be made. What comprises the perceptual apparatus of an entity?

- The intended target of any deception possesses sensory devices (radars, forward-looking infrared radars (FLIR), eyeballs, ears, etc.) . . .
- which he or she employs in a given method (inch-by-inch scrutiny, quick scans, random walks, spiral searches, etc.) . . .
- and the resulting data is processed in a certain way (compared en masse to a template, examined completely from scratch, ranked by vividness, etc.).

These three elements of perception comprise a trajectory from sensation to cognition, and each represents a milestone where efforts to shield the entity from deception can be focused.

1. **Type or amount of data collected.** What can be done with the sensor? Can it be tuned to another window of the spectrum (e.g., switching from visible light to infrared)? Can another sensory modality be brought on-line (e.g., switching from visual to auditory searching)?
2. **Method for collecting data.** What can be done to the sensory processing? Can the search *plan* be changed (e.g., from scanning/cueing to inch-by-inch scrutiny)? Can the search *pattern* be changed (e.g., from outward spiraling to sector-by-sector)?
3. **Analysis of data collected.** What can be done with the analysis of sensory inputs? How can thinking help? Can the inputs be corroborated? Can counterscenarios be concocted?

There are other ways in which deception can be combated, as suggested by examples in both military history and the animal kingdom:

4. **Unmasking adversary deceptions with friendly deceptions.** Fighting fire with fire: What deceptive counteractions can be taken? Can bluff or bluster uncover an adversary's deception?
5. **Rendering adversary deceptions moot.** Can the deception or its effects be overwhelmed? That is, can the effects of misperception be mitigated through actions that lessen the importance of accurate perception? For example, if an enemy tank has deployed decoys, this counterstrategy would simply target them all with destructive fires and not bother to tell them apart. Or if an enemy force feints right and comes left, an "overwhelming" response would be to simply respond forcefully at both locations, not bothering to discern which is real. Needless to say, this strategy requires great resources.

How is this typology useful? As with the framework we employ to unpack the deception phenomenon, it is meant to offer a more finely resolved view of a complex issue and thus represent an intermediate step toward creating a comprehensive theory of deception and counterdeception. Table 3 illustrates both military and animal examples of these counterdeception categories.

Table 3

Examples of Counterdeception

Focus	Simple Military Examples	Biological Examples
Type of data collected	Defeat adversary visual camouflage with foliage-penetrating (FOPEN) radar	Insectivorous bats (*chiroptera*) defeat the well-developed visual camouflage of moths by using a different sensory medium: echolocation.
Method for collecting data	Defeat adversary camouflage by modifying current search protocols (e.g., use complementary/ corroboratory emitters) or by increasing deliberation	*Photinus* fireflies defeat the aggressive mimicry of *Photuris* fireflies by slowing their approaches and prolonging the time of communication. The deception is often revealed by not acting hastily.
Analysis of data collected	Defeat adversary camouflage by developing improved imagery intelligence (IMINT) analyst techniques and training	Reed warblers defeat cuckoo brood parasitism (mimicry) by applying rules to their nest contents. If an egg doesn't resemble the others closely enough, if the egg appears in the nest too early, or if an adult cuckoo was spotted nearby during the laying period, then the reed warbler is likely to reject an egg.
Unmasking adversary deceptions with friendly deceptions	Defeat adversary camouflage by employing a feint to encourage concealed targets to maneuver	The Boomslang snake (*Dispholidus typus,* pictured in Figure 10; see following page 32) defeats the camouflage of a chameleon by lying in wait and employing its own excellent camouflage. When unaware of danger, the chameleon moves/forages and thus reveals itself to the snake.
Rendering adversary deceptions moot	Defeat adversary camouflage by saturating areas with fire to destroy concealed targets	A variety of avians that feed on butterflies of the *Satyridae* family, geckos, and other species with disposable, diverting body parts (e.g., eye spots on wing tips) strike repeatedly or take large bites, meaning that the deceptions have no impact even when effective.

As discussed previously, the defense community's knowledge is somewhat impoverished when it comes to the specific costs,

benefits, risks, optimization points, contextual interrelationships, etc. of deception. This is equally true of counterdeception; the reader should consider the list in Table 4 a counterpart to the one in Table 1.

It seems clear that as much needs to be done on this topic as on deception itself. A key finding emerging from this research is that different counterdeception methods can and should be applied toward different deception techniques. The authors believe that as a starting point, experimentation should be done to define these relationships. Are improvements to analysis (e.g., changes to training) more suited to countering *masking* (e.g., camouflage) techniques than *misdirecting* (e.g., feints) techniques? Even more specific questions can and should be asked: for example, will improvements to sensors fare better against *behavioral* means of masking than *morphological* means of masking? How much better? What level of investment is required in improved training to significantly affect outcomes? As noted previously, there are numerous such questions; the answers will be of great value. A body of thoroughly vetted experimentation and analysis is needed that clearly prescribes what sorts

Table 4

Issues in Countering Deception

Matching up	Which counterdeception methods work against particular types of deception? Why?
Most effective	Which are the most effective against particular deception techniques?
Broadest effectiveness	Which are effective against the broadest range of deceptions?
Context	Which are the most affected by the context of their use?
Time	Which require the most time?
Manpower	Which require the most manpower?
Automation	Which can be automated?
Positive interactions	Which complement each other? Which complement other operational capabilities?
Negative interactions	Which hinder each other?
Monkey's paw	Do any of the methods help against one type of deception but actually incur a vulnerability to another type?

of countereffortsto employ to stave off particular types of deception (or the reverse: if the opponent has x, y, and z intelligence capabilities, then use deceptions a, b, and c).

This entire framework is most useful when considered as a set of hypotheses to be experimentally tested and thoroughly analyzed. If borne out, they could pay significant dividends in driving technological, doctrinal, and organizational change in the U.S. armed forces wherever adversaries are resorting to such measures.