DECEPTION 101—PRIMER ON DECEPTION

Joseph W. Caddell

December 2004

*****

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This report is cleared for public release; distribution is unlimited.

*****

This monograph was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *http://www.carlisle.army.mil/ssi/*, at the Publishing button.

*****

This monograph is based on a presentation made at the *Conference on Strategic Deception in Modern Democracies: Ethical, Legal, and Policy Challenges*, sponsored by the U.S. Army War College, the U.S. Naval Academy, and the Triangle Institute of Security Studies on October 31, 2003, at the William C. Friday Conference Center, Chapel Hill, North Carolina.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave, Carlisle, PA 17013-5244. Copies of this report may be obtained from the Publications Office by calling (717) 245-4133, FAX (717) 245-3820, or by e-mail at *SSI_Publishing@carlisle.army.mil*

*****

All Strategic Studies Institute (SSI) monographs are available on the SSI Homepage for electronic dissemination. SSI's Homepage address is: *http://www.carlisle.army.mil/ssi/*

*****

The Strategic Studies Institute publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please let us know by e-mail at *SSI_Newsletter@carlisle.army.mil* or by calling (717) 245-3133.

ISBN 1-58487-180-6

FOREWORD

This monograph reviews the basic concepts related to "deception." The author, Dr. Joseph Caddell, defines terms, provides historical examples, and discusses problems associated with deception. His monograph provides a general overview, a "primer," and is not directed at those who already possess a working knowledge of deception operations. Nevertheless, given the complex and ever changing nature of deception in the political-military environment, it may serve as a useful reminder of the basic assumptions and methods concerning the subject.

The Strategic Studies Institute is pleased to publish this work as part of our External Research Associates Program.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

ABOUT THE AUTHOR

Dr. Joseph Caddell is a Lecturer on Military History at North Carolina State University in Raleigh.

DECEPTION 101—PRIMER ON DECEPTION

Introduction.

Deception is a traditional component of political and military conflict. Indeed, many argue that it is intrinsic to all human interaction. It is sometimes mistakenly confused with unintentional confusion or misinformation. Disinformation, intentional deception, should not be confused with misinformation. Deception depends on two criteria: first, it is intentional; and, second, it is designed to gain an advantage for the practitioner.[1]

Deception in the forms of concealment and activity designed to mislead is common in nature. Protective coloration serves to protect some flora and fauna—either by making them difficult to see or by causing them to resemble something of little interest to predators. Some animals will feign injury to lure predators away from nests or offspring. Students of deception note these examples as evidence of the utility and effectiveness of disinformation even beyond the human experience.[2]

Fabrication and Manipulation.

In the economic and political arenas, deception may appear in a wide variety of forms. Indeed, cynical observers might argue that a synonym for economic disinformation is "advertising." In any case, examining the use of deception in marketing helps illustrate the difference between "fabrication and manipulation." If false information is created and presented as true, this is *fabrication*. It is fabricated for the purpose of disinformation and is simply not true.

Manipulation, on the other hand, is the use of information which is technically true, but is being presented out of context in order to create a false implication. This deception may be achieved by leaving out information or by associating valid information in such a way as to create false correlations. In the advertising world, companies usually avoid making false claims based on "fabricated" information. The laws against false advertising make such behavior problematical. Presenting "true" information "manipulated" to create

a false impression, however, is difficult to prosecute. An example of such activity occurred in the gasoline shortages of the 1970s when some automobile manufacturers advertised cars with inefficient fuel consumption by noting how the *range* of their vehicles compared to smaller, more fuel efficient automobiles. They simply neglected to point out that their gas tanks were considerably larger than those in the smaller vehicles.

The distinction between fabrication and manipulation is relevant to military deception operations. Both forms have proven useful in the history of warfare. Dummy weapons and false orders "leaked" to the enemy are examples of fabrication. But when it is impossible to disguise the presence of large forces or an interest in a given area, partial truths—manipulation—may prove more advantageous.[3]

Political Deception.

Similar considerations relating to fabrication vs. manipulation exist in the political realm. And, while disinformation in the business world is only tangentially of interest to a military audience, political deception may have a close relationship to and impact on military operations. This is not to say that political deception is limited to issues relating to defense or national security, but a quick review of American political history reveals that defense issues have certainly been subject to disinformation—often in the form of manipulation. Here are some examples.

On April 14, 1846, an American military patrol engaged a Mexican force south of the Nueces River in the newly annexed state of Texas. There were 16 American casualties. On May 11, President James K. Polk announced that "Mexico has passed the boundary of the United States, has invaded our territory, and shed American blood upon the American soil." In fact, the presence of U.S. troops in the disputed area south of the Nueces was a questionable action. The area between the Nueces and Rio Grande rivers was disputed territory, and negotiations were underway to resolve the issue. Neither nation was supposed to have troops there. Somehow this fact was left out of Polk's impassioned call to arms. A young congressman from Illinois raised awkward questions about "the sacred spot." Indeed, concern by young Mr. Lincoln and others in the Congress that information

was being "manipulated" led to the famous "Spot Resolution." This registered suspicion concerning Polk's rhetoric and signified a growing regional division, but it did not prevent the Mexican-American War.[4]

In 1898 the destruction of the U.S.S. *Maine* in Havana Harbor created a situation where manipulation of information, primarily by the media rather than by the government, played a critical role in precipitating the war with Spain. The explosion, which destroyed the *Maine* on the night of February 15, 1898, has been examined by investigators for the past 106 years. The conclusions are varied and often contradictory. The initial board of inquiry (March 1898) was unable to arrive at a definite conclusion.[5]

American newspapers, however, were not so ambivalent. Nor were they restrained. Speculation as to the Spanish motives for destroying the *Maine* ran rampant. The strained relations between Madrid and Washington deteriorated even further. The "yellow press" did not cause the subsequent Spanish-American War by itself, but its role was seminal.[6]

This event provides an interesting case study where political, military, and economic interests intertwined to the point that one is hard pressed to segregate them. To what extent is the government responsible for correcting false impressions which appear in a free press? What if a government takes advantage of fabricated or manipulated data to serve its own policy ends?

Examples of specifically governmental disinformation can be found in the period prior to the U.S. entry into World War II. On a number of occasions, President Franklin Delano Roosevelt (FDR) played fast and loose with the truth. Everything from the Destroyer Deal of 1940 to the Lend-Lease Act of 1941 involved a certain amount of information manipulation. In the latter example, the President compared the Lend-Lease aid to Great Britain to the loan of a fire hose to a neighbor to put out a house fire. The analogy, made in a "Fireside Chat" radio address, was effective and generated empathy. Critics, however, pointed out that it was hopelessly inaccurate. Unlike the water hose mentioned in the analogy, the weapons, food, and fuel shipped to Great Britain could not be reeled up and returned "after the fire is out."

An even better example of Roosevelt shading the truth involved a purported German plan to invade the western hemisphere. The plan centered on a map which apparently showed German designs on nations in South and Central America. In his Navy Day speech on October 27, 1941, Roosevelt said he had "a secret map, made in Germany by Hitler's government by the planners of the new world order." The President continued by claiming, "That map, my friends, makes clear the Nazi design not only against South America, but against the United States as well."[7]

The problem here is the simple fact that the map was part of a British disinformation operation, and that it is likely that FDR knew it. William Stephenson, a British intelligence operative (M.I.6 code name "Intrepid"), fabricated the map sometime in 1941 to create alarm in the United States. By September 1941, the State Department was onto Stephenson's ruses. The probability that Roosevelt knew that the map was false when he cited it on Navy Day is quite high. The President was concerned about the threat posed by Nazi Germany and was willing to be deceptive if it was necessary to rouse the American public. As he confided to Secretary of the Treasury Morgenthau in 1942, after the United States had entered the war, "I may have one policy for Europe and one diametrically opposite for North and South America. I may be entirely inconsistent, and furthermore, I am perfectly willing to mislead and tell untruths if it will help us win the war."[8]

Roosevelt is not usually castigated too severely by critics, because most sympathize with his desire to resist Axis aggression in World War II. Similarly, many sympathize with President Dwight D. Eisenhower's later attempt to "cover" the U-2 reconnaissance sorties over the Soviet Union by describing them as National Aeronautics and Space Administration (NASA) weather research flights. In the U-2 case, however, the problems associated with deception being "found out" were exploited by the Soviets in their show trial of the U-2 pilot, Francis Gary Powers, after his shoot-down on May Day 1960.[9]

The use of deception concerning national security issues could also be found in the domestic political arena during the Cold War. Senator Joseph McCarthy's infamous accusations concerning

communist infiltration of the government ultimately demonstrated the cost of being caught practicing deception. But they also showed how effective someone could be in making accusations with virtually no concrete evidence if the limited evidence was couched in the right context.

The "missile gap" of the 1960 presidential campaign was an effective issue used by the Kennedy campaign to challenge Vice President Richard Nixon's supposed strength in foreign and national security policy experience. The fact that the "missile gap" did not exist may or may not have been known by Senator John F. Kennedy and his staff. If he did not know, this was an example of simple misinformation. If he did know, and many believe he did, it was equally simple *dis*information.[10]

The recitation of political deception involving defense issues could go on to cover Nixon's claim in the 1968 presidential campaign that he had a plan to end the Vietnam War, to the Iran-Contra Scandal, and the stories of babies being ejected from incubators by Iraqi soldiers in Kuwait in 1990. In these cases, and others like them, national security issues were clouded by various forms of deception. The point here is that such behavior should not be unexpected. While it has proven effective on occasion, there is a price to be paid if a specific deception fails.

Furthermore, an overarching cost, regardless of success or failure, has been the damage it has done to government credibility. Because governments have practiced deception involving issues as important as national security, it is difficult for many in the media, and the public at large, to discount totally the possibility that government announcements could be disinformation. Recent debates concerning the nature of the 2003 Iraq War have only added to preexisting skepticism.

The debate over whether a democratic republic should engage in deceptions which may deceive their own citizens rests outside the scope of this monograph. Nevertheless, anyone engaged in deception operations, offensively or defensively, should be aware of the credibility issues inherent to this subject. Often there is more at stake than a temporary political or military advantage.

Military Deception.

Many problems are associated with the study of military deception. Military deception is, by its very nature, covert or clandestine. It comes in a wide variety of forms, and there are disagreements regarding definitions. The Department of Defense (DoD) defines *deception* as: "those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests."[11]

Deception in warfare is probably as old as armed conflict itself. The logic of confusing an adversary is obvious, and the rewards can be realized very quickly. Our first recorded history of war involves the Mycenaean Greek siege of Troy in the 12th century BC and also provides us with our first recorded example of deception in warfare, the famous Trojan Horse. The narrative of military history over the succeeding 3,200 years provides a wealth of examples.[12]

A fundamental dichotomy to be found in this confusing world is the division of deception into "active" and "passive" categories. Put simply, passive deception is designed to hide *real* intentions and capabilities from an adversary. You are hiding something which really exists. Active deception, on the other hand, is the process of providing an adversary with evidence of intentions and capabilities which you do *not*, in fact, possess. Here you are showing your enemy something which is not real. This dichotomy is most often associated with camouflage, but is not limited to this field.

Another distinction is made in regard to the degree of "specificity of deception." In their 1982 work, *Strategic Military Deception*, Donald Daniel and Katherine Herbig note the existence of what they term "A-type" and "M-type" deception.[13] A-type, or "ambiguity increasing," deception is designed to create general confusion and to distract an adversary by making "noise." An example of this was the presence of Japanese Ambassadors Nomura and Kurusu in Washington, DC, prior to the attack on Pearl Harbor in 1941. By continuing diplomatic negotiations, the Japanese made it more difficult for the United States to ascertain Tokyo's intentions. The Americans had to consider a variety of possible Japanese intentions and objectives. This made it more difficult to narrow the analysis and to conclude that military action was the only Japanese option.[14]

M-type, or "misleading variety," deception is more ambitious in that it is designed to mislead an enemy into believing a specific deception plan. Here you engage in an array of deception operations which should supplement and complement one another, all designed to cause your opponent to believe an "alternative" to what you are actually doing. This "alternative" is, of course, not true. This type of deception is more complicated and more ambitious than simple "ambiguity." It requires more preparation, more resources, and usually more time. A modern historical example often cited is Operation BODYGUARD, the deception plan designed to protect Operation OVERLORD, the allied landings in Normandy on June 6, 1944.

BODYGUARD was actually an umbrella project that included a variety of deception plans of the "M-type." The two most famous of these were Operations FORTITUDE NORTH and FORTITUDE SOUTH. These plans were designed to lead the Germans to believe that the main allied offensive in the West would land, respectively, in Norway or the Pas de Calais (Straits of Dover). Over time, FORTITUDE SOUTH became the most plausible, and the bulk of the deception resources were expended on convincing the Germans that the real invasion would cross the English Channel in the Straits of Dover, almost 100 miles from the Normandy beaches. Its success can be seen in that many German commanders believed that, when the actual invasion took place in Normandy, it was merely a diversion from the "real" invasion which would be occurring later at Calais.[15]

The Operation FORTITUDE deceptions included a number of military deception methodologies. The most common of these was camouflage. Camouflage, like deception, comes in both active and passive variants. When the word "camouflage" is used, most people think of *passive camouflage*—the disguise or cloaking of forces and/or facilities to prevent their detection by an enemy. This can include hiding Greek infantry inside a large ceremonial horse, wearing clothing designed to blend into the surrounding terrain, placing cut branches from trees over important equipment, and an almost infinite variety of other techniques. It can even include disguising a bombed, but repaired, airfield runway to look like it is still cratered. Anytime you try to hide something that possesses real capabilities, you are practicing passive camouflage.[16]

Active camouflage entails the artificial creation of the image or impression that you have a force or capability that does not actually exist. In the American Civil War, the Confederate Army charred large tree trunks to resemble artillery barrels and marched infantry units in circles to convince Union officers that they had more weapons and more troops than they actually did. In Operation FORTITUDE SOUTH, the allies used dummy tanks, trucks, aircraft, and landing vessels to give the impression they possessed weapons they did not have. To complement this, they used false radio messages to create the illusion of military units which did not exist. In recent operations in the Balkans and the Persian Gulf, American forces have encountered similar deceptions. Any attempt to create the illusion of a real capability where there is none is active camouflage.[17]

Camouflage may simply be tactical deception designed to make it harder for an enemy to see where to attack your resources. It may be part of a larger deception plan. Active camouflage must always be used carefully. If one is too eager to reveal active camouflage, the enemy may become suspicious of obvious targets. Here the methodology becomes more complicated. If one is going to use active camouflage, say a dummy tank, it is a good idea to use passive camouflage to appear to be hiding the "tank." Otherwise, the deception may not be convincing. Passive camouflage should be used on active camouflage in order to make the false image more credible—only it must not be so good as to actually hide the dummy tank. It must be good enough to be credible, but not so good as to be effective. By the same token, it may be possible to place poorly done active camouflage over a *real* resource to mislead an enemy away from that resource. The complexities should never be underestimated.[18]

Camouflage is often tied to the design of *diversions*. A diversion is the intentional distraction of an enemy's attention away from the area of interest or attack. There are two basic types, feints and demonstrations. A *feint* is an attack by friendly forces to distract enemy attention from the main area of interest or attack. Closely related to this is the concept of the demonstration. A *demonstration* involves the deployment of forces to distract an enemy, but such a deployment does not usually include actual contact or combat. The purpose of a diversion is simple—to mislead an enemy away from your real operations and objectives.[19]

Two other specialized terms utilized in military deception are conditioning and cover. *Conditioning* is the repetition of what could be preparations for a hostile action which you do not commit—thereby lulling the victim into a false sense of security. It is a variation of the "familiarity breeds contempt" theme. This is a concept which is often associated with the outbreak of warfare and relates to peacetime activities which might or might not be preparations for war. It could also, however, refer to repetitive behavior in the conduct of ongoing military operations which is used to desensitize an enemy to a threat.

Cover is the use of an apparently nonthreatening activity to disguise preparation for or initiation of a hostile act. A common example is the use of a training exercise to hide preparations for an attack. If the training exercise was the last in a long series of training exercises which had not led to actual hostile action in the past, this could also be an example of conditioning—hence the tendency to refer to "conditioning and cover." The two concepts are linked by their complementary definitions. In recent years, both the Yom Kippur War of 1973 and the Falklands War of 1982 were launched under the cover of training exercises similar to exercises which had occurred before.

Levels of Military Deception.

The U.S. military community traditionally recognizes three levels of deception—based on the nature of the intent. *Strategic Deception* intends to "disguise basic objectives, intentions, strategies, and capabilities." This contrasts with *operational deception*, which confuses an adversary regarding "a specific operation or action you are preparing to conduct." And, last, but not least, in the American doctrines, there is *tactical deception*. This is intended to mislead "others while they are *actively involved* in competition with you, your interests, or your forces."[20]

What is important to note here is that the categorization of deception into these three levels is not based on the type of deception being practiced. Rather, it depends on the objective of the deception. Phony tanks or dummy aircraft could be examples of tactical deception if the purpose was to distract an attacker and

cause them not to fire on real equipment and personnel. They could be operational deception if they were part of a larger deception plan designed to mislead an adversary about the timing, place, and nature of a specific military operation. Or, if they were part of an even larger deception plan intended to confuse an enemy as to a basic strategy or strategic objectives, they would be part of strategic deception. The taxonomy is based on objectives, not methodologies.

Conditions Affecting Deception.

A quick review of the historical literature reveals scholarly interest in the nature of deception dating back to Sun Tzu, Vegetius, Machiavelli, and the oft-quoted Clausewitz. In more recent years, the evolution of the "Principles of War" in the American and British armies embraced the advantages of "surprise" and "security." Intrinsic to both of these principles is recognition of the importance of fooling your opponent and, in turn, not being fooled yourself.

What may be more problematical is finding consensus as to how deception works and how best to avoid being taken in. In broad terms, it is obvious that flaws in logical analysis and synthesis make being deceived more likely. Ignorance, arrogance, and fear all complicate one's ability to detect false information.

Preconceived ideas or simple prejudice often lead to that phenomenon known as "cognitive dissonance," where one ignores vital information simply because it interferes with preexisting concepts or theories. A similar, if less precise, problem is the so-called "inertia of rest." This refers to a tendency of people to believe certain assumptions remain valid even after they have been undermined by events. In physics, "inertia of rest" refers to the tendency of an object at rest to remain at rest until acted upon by an outside force. Students of intelligence sometimes refer to the inertia of rest as the tendency in the mind of decisionmakers to remain at peace until acted upon by a hostile force. All of these issues can be used by practitioners of deception to their advantage.

The significance here is that effective deception is often based on exploitation of the victim's cognitive assumptions. German philosopher Goethe is remembered for his observation that "We

are never deceived, we deceive ourselves."[21] This is more than a philosophical truism. It is both a recipe for formulating deception and a warning for those who wish to avoid being deceived.

Deception and Intelligence Operations.

Someone practicing deception needs a route through which to send their disinformation—their adversary's intelligence organizations often provide that route. All intelligence organizations vet the credibility and reliability of information they discover. Practitioners of deception know this and prepare their disinformation, at the least, to confuse and, at the most, to mislead the intelligence services of their enemy.

All intelligence collection methodologies are subject to deception. Signals intelligence (SIGINT) is susceptible to false signals, phony messages, bogus codes, and other forms of disinformation. Photographic or imagery intelligence (PHOTINT and IMINT) must deal with active and passive camouflage in a wide array of forms. Similar problems plague communications intelligence (COMINT), electronic intelligence (ELINT), acoustical intelligence (ACOUINT), and seismic intelligence (SEISINT). In any medium where information can be found, disinformation can be planted or devised.

Human intelligence (HUMINT) involves the use of double agents, the passing of false data, and the like. Human sources may serve as knowing or unknowing conduits of false information. Some in the counterintelligence business note that one can detect double agents by identifying sources which persistently provide false information. At the same time, because this is well-known, double agents can be given valid and verifiable information to establish their credibility—a form of conditioning. Some cynics in this line of work, therefore, observe that you only have to be suspicious of those who provide you with good information and those who provide you with bad information. Detecting deception obviously can be trying work.[22]

Intelligence organizations may practice deception in order to protect their own resources and capabilities. Most of this involves some form of passive deception. In addition to the use of double agents, false intelligence operations can be mounted to feign interest in something extraneous to your real interests—a form of diversion.

In recent years, intelligence agencies have even found themselves in the business of conducting training sessions for the media on how to spot deception. Given the importance of public opinion in international affairs, it is not enough that intelligence agencies be able to detect deception by their adversaries. It is essential that the deceptions be revealed to the world. And because no one is sure whom to believe in the deception game, it is sometimes important to have a nongovernment voice reveal the deceptions of others. Following the September 11, 2001, attacks, as preparation for military operations in Afghanistan and Iraq, the Defense Intelligence Agency (DIA) held briefings for the media to point out some basic methods for testing claims other nations might make concerning American atrocities. Based largely on the experience of Iraqi and Serb attempts to make false claims about U.S. bomb damage, DoD offered basic "how to detect deception" training sessions for members of the Fourth Estate.[23] From this, it is clear that the Pentagon appreciates that deception is about more than immediate military utility.

Deception and Terrorism.

Despite the fact that most of the historical examples of military deception discussed to this point allude to conventional military operations, it is important to note that terrorists can use all of the techniques discussed in this monograph. Terrorists rely upon both active and passive deception to operate and to survive. Passive deception includes the use of aliases, secure methods of communication, and bases in areas both difficult to reach and to observe. Active deception may include diversions, conditioning, and cover—often in combination.

If terrorists provide indications that they have hostile intentions against a specific set of targets but then fail to strike those targets, they may gain several advantages. They generate fear, force security forces to expend time and treasure, and create general aggravation and inconvenience (e.g., airlines flight cancellations over holidays). They may cause one to doubt your methodologies and to be less sensitive to such information in the future. Or, tangentially, they could use such information to distract one away from the target they actually mean to strike. Given that terrorism uses fear as a method

to an ends, any activity that generates some degree of fear and uncertainty provides a partial success for the terrorists.

An oft-quoted sound byte which has come out of the "War on Terrorism" is the advice to "think outside of the box." Politicians, media experts, academics, and others have repeated this cliché. Unfortunately, it is virtually useless. "Outside the box" defines all of *infinity*—minus your "box." Because terrorists use a wide array of deception techniques makes this problem all the more obvious.[24]

The Ethics of Deception.

No discussion of the fundamentals of deception would be complete without a brief mention of the legal and ethical aspects of the subject. As one might expect, there has been considerable disagreement in this area for some time. Still, a few basic observations are in order.

Surprising to many, the specific legal restraints on the use of deception are relatively clear and precise. Domestic law imposes few restrictions regarding military deception. Unless one tells a falsehood while under oath in a court of law or makes a false statement in some other setting where they are legally bound to be truthful, domestic law does not apply to military deception. As one legal scholar puts it, "there is no constitutional principle that says that the President of the United States or the Executive Branch must tell the truth."[25]

International law provides more limitations. Generally speaking, the United States recognizes the restrictions established in the Hague and Geneva Conventions over the past 140 years. In combination, these form the "Laws of Warfare," recognized by the U.S. military and codified by official manuals. In the U.S. Army, this information is contained in Field Manual 27-10, *The Laws of Land Warfare*.[26]

The restrictions placed on "stratagems" or "ruses of war" include the prohibition of "treachery or perfidy." Examples include the false use of flags of truce, wearing enemy uniforms or flying enemy colors while in combat, masquerading as international aid personnel, or using hospitals or other protected sites for military purposes. The prohibitions are explicit and specific.[27]

When one enters the realm of ethical considerations, one encounters the complexities inherent to the justification of deception. Unfortunately (or fortunately), lawyers, philosophers, and ethicists

do not always agree as to how one sets out to judge the ethical and moral dimensions of the subject. Broadly speaking, two general approaches, to such measurement exist. These include the idealist and the realist schools. Not everyone agrees how to define these approaches and each contains a number of subsets or permutations. Nevertheless, a basic distinction is generally accepted by all.

The idealists make moral and ethical distinctions based on an absolute set of standards. If disinformation and falsehoods are wrong, all examples of such behavior are wrong. The ends do not justify the means. This is absolute. There are no exceptions.[28]

The so-called realists, or pragmatists, argue that the question ultimately boils down to a cost-benefit analysis. Does the harm done by being deceptive outweigh the good the deception will accomplish? The nature of analysis required to answer that question and the values assigned to the various costs and benefits are subjective. In the eyes of the realists, the ethics of deception are both situational dependent and relative to the value structure of the observer.[29]

This is closely related to the operational cost-benefit analysis that must always accompany a decision to implement deception operations. Clearly no one wishes to conduct deception operations which cost more than they contribute to success. The realist perspective on the ethical implications follows a similar path—and may, on occasion, overlap the operational considerations.[30]

One reason nations agree to international restrictions on "treachery," as noted above, is the realist concern that engaging in those acts could create problems out of proportion to the limited advantages such deception might provide. For example, the limitation on using hospitals or international aid symbols for military cover assumes that nations find the safety of such vital organizations more important than the limited advantages their abuse might afford.

The realist school also notes that there are potential ethical costs inherent to any deception operation. A political or military organization which indulges in disinformation loses a corresponding amount of credibility. Indeed, if one is practicing deception in order to affect public or international opinion, the "blow back" from loss of credibility can easily prove quite damaging. This consideration gained international attention when it was revealed in early 2002 that DoD had established an "Office of Strategic Influence." While it

was quickly asserted that this organization would not be deceptive, media sources implied that foreign media might be provided with manipulated information. This set off a flurry of charges and denials and the eventual closing of the office. Even the appearance of deception can be expensive.[31]

This is especially true in nations which are democratic republics with a valued tradition of press freedom. The ability of the public to make informed decisions about all political policies, especially military policies, relies on a well-informed media. When the military serving a democratic republic misleads the public or is involved in an action which misleads the public, it is difficult to imagine that there are many advantages that would justify that cost.

This is not to say that realists would deny military organizations the right to conduct deception operations. What they would advocate is a careful cost-benefit analysis of deception operations and a recommendation to favor those deception operations where it is possible to mislead the enemy without misleading your own people.

Dealing with Deception.

A comprehensive methodology for dealing with deception will never be written. It is a nebulous and ever changing field of virtually infinite proportions. Indeed, to believe that such a methodology is possible would be to misunderstand the nature of deception.

Nevertheless, a few useful observations may be possible. Over the years, many pundits have quoted the Faber College motto from the movie *Animal House*—"Knowledge is good." Trite as it may sound, it is absolutely true regarding deception. The more that you know about your adversaries and about the events which are unfolding, the better prepared you will be to combat deception. Understanding your enemy's intentions and capabilities helps to define the general limits of their objectives and operations. Never rely on a limited number of sources of information or a limited number of collection methodologies. The more sources one has, the more cross references one can make. The more one knows, the harder it is for someone to manipulate information out of context. The more one knows, the more likely one will detect a fabrication.

Knowledge should also include knowledge about oneself. Recognize the biases and assumptions one, one's organization, and one's culture possess. Beware of "mirror imaging"—anytime one assumes that others will behave in a way similar to oneself, one is opening the door to self-deception.

The old intelligence advice to "know your enemy" must encompass advice to study your enemy's methods of deception. During the Cold War, western intelligence services studied Soviet *Dezinformatsia* and *Maskirovka* doctrines. This was quite helpful in detecting and dealing with many deceptions. Nevertheless, this familiarity never prevented the deception campaigns from posing a threat. Such study will never be fool-proof—there will always be new and unexpected techniques and approaches.

Summary.

Deception comes in many forms and "types." It has many objectives and can be accomplished by many methods. It may be active or passive. It operates on many levels. In short, there is much to know about deception.

What is known about deception in the past is of considerable, if general, use in the present. We have developed terms to describe the different methods and levels of disinformation. This is useful. We know the dangers inherent to mirror imaging and cognitive dissonance. This is important. We can appreciate the need for the synthesis of intelligence methodologies. This is vital. But, despite these realizations, we can never be confident we are not being deceived.

These observations may seem self-evident to even a casual student of deception. Therefore, one might wonder why these obvious statements need repeating. The answer is simple. In successful deception operations, the perpetrator hopes that one or several of these self-evident observations will be over looked.

GLOSSARY OF TERMS RELATING TO DECEPTION

Strategic Deception:	Deception which disguises your *basic* objectives, intentions, strategies, and capabilities.
Operational Deception:	Deception which confuses or diverts an adversary in regard to a *specific* operation or action you are preparing to conduct.
Tactical Deception:	Deception which misleads others while they are *actively involved* in competition with you, your interests, or your forces.
"A" Type Deception:	"Ambiguity Deception" geared toward creating general confusion.
"M" Type Deception:	"Misleading Deception" designed to mislead an adversary into a specific and preconceived direction.
Fabrication:	The *creation* of false information or images to mislead an adversary as to your intentions and/or capabilities. This is deception *via* manufactured data (e.g., forgeries).
Manipulation:	The use of true or factual data in such a way as to create a false impression. The information is not false, but through using it out of context, leaving out some of the details, or providing a false balance of emphasis, the impression is skewed (e.g., being quoted out of context).
Active Deception:	Any attempt to create the impression of intentions and capabilities which you do not, in fact, possess.
Passive Deception:	Efforts designed to prevent detection of your actual capabilities and intentions.
Denial:	Methods used to conceal state and military secrets, particularly from foreign intelligence collection.

Deception (as used in the combination "Denial and Deception"):	The manipulation of information and perceptions to induce the target of that deception to take or not take an action, thereby benefiting the deceiver.

Note: "Denial and deception are interrelated. Denial is the basis for a successful deception. One cannot manipulate or blur the truth or lie convincingly unless the truth is first concealed." John Yurechko, Defense Intelligence Agency, "DoD Briefing on Iraqi Denial and Deception," Tuesday, October 8, 2002, 12:58 p.m. EDT.

Dezinformatsia:	The dissemination of false or misleading information intended to confuse, discredit or embarrass the enemy. (Marshals of the Soviet Union A. A. Grechko and N. V. Ogarkov [successive Chairmen of the Main Editorial Commission], *The Soviet Military Encyclopedia*; *English Language Edition*, Vol. 1, William C. Green and W. Robert Reeves, ed. and trans., Boulder, CO: Westview Press, 1993, pp. 345-346.
Maskirovka:	"A means of securing the combat operations and daily activity of forces; a complex of measures designed to mislead the enemy as to the presence and disposition of forces and various military objects, their condition, combat readiness and operations and also the plans of the commander . . . *Maskirovka* contributes to the achievement of surprise for the actions of forces, the preservation of combat readiness and the increased survivability of objects" (Grechko and Ogarkov, pp. 277-280).
Passive Camouflage:	The disguise or cloaking of forces and/or facilities to prevent their detection by an enemy.
Active Camouflage:	The artificial creation of the image or impression that you have a force or capability that does not actually exist.
Diversion:	The intentional distraction of an enemy's attention away from the area of interest or attack. Two basic types: feint and demonstration.
Feint:	An attack by friendly forces to distract enemy attention from your main area of interest or attack.

Demonstration:	The deployment of forces to distract an enemy, but such a deployment does not usually include actual contact or combat. The purpose of a diversion is simple—to mislead an enemy away from your real operations and objectives.
Conditioning:	The repetition of what could be preparations for a hostile action without conducting hostilities—thereby lulling the victim into a false sense of security. This is a variation of the "familiarity breeds contempt" theme.
Cover:	The use of an apparently nonthreatening activity to disguise preparation for or initiation of a hostile act. A common example is the use of a training exercise to hide preparations for an attack.

Note: Conditioning and cover may occur in combination with one another—they can be mutually supportive. A common example is a military training exercise.

ENDNOTES

1. For a general review of concepts of deception, see Colonel Michael Dewar, *The Art of Deception in Warfare*, Newton Abbot, Devon, UK: David & Charles Publishers, 1989, pp. 9-22; Jon Latimer, *Deception in War: The Art of the Bluff, the Value of Deceit, and the Most Thrilling Episodes of Cunning in Military History, from the Trojan Horse to the Gulf War*, Woodstock, NY: The Overlook Press, 2001, pp. 1-5; and James F. Dunnigan and Albert A. Nofi, *Victory and Deceit: Deception and Trickery at War*, San Jose, CA: Writers Club Press, 2001, pp. 1-31.

2. An excellent overview of camouflage in nature is provided in Marco Ferrari, *Colors for Survival: Mimicry and Camouflage in Nature*, Charlottesville, VA: Thomasson Grant & Howell, 1993. How examples in nature have affected military deception is discussed in Guy Hartcup, *Camouflage: A History of Concealment and Deception in War*, New York: Charles Scribner's Sons, 1980, pp. 9-11; and in J. Bowyer Bell and Barton Whaley, *Cheating and Deception*, New Brunswick, NJ: Transaction Publishers, 1991, pp. 48-52.

3. The process of choosing methods of deception is examined in Latimer, pp. 71-100; while Bell and Whaley, pp. 45-74, discuss characteristics of types of deception.

4. An introduction to this crisis is available at Digital History under "Western Expansion, The Mexican War," at *http://www.digitalhistory.uh.edu/database/article_display.cfm?HHID=316, accessed* July 20, 2004. For a variety of opinions as to the motives of the Polk administration, see Archie P. McDonald, ed., *The Mexican War: Crisis for American Democracy*, Lexington, MA: D. C. Heath, 1969; and Ramón Eduardo Ruiz, *The Mexican War: Was it Manifest Destiny?* New York: Holt, Rinehart and Winston, 1963.

5. See President McKinley's "Report on the Findings of the Sampson Board's Inquiry into the *Maine's* Loss," March 28, 1898, accessed at *http://www.spanamwar.com/McKinleymaine.htm*, July 15, 2004.

6. Philip Knightley and John Pilger, *The First Casualty: The War Correspondent As Hero and Myth-Maker from the Crimea to Kosovo*, Baltimore: Johns Hopkins University Press, 2002, provide a general survey of the role of the media in reporting events leading up to war and the wars themselves.

7. John F. Bratzel and Leslie B. Rout, Jr., "FDR and the 'Secret Map'," *The Wilson Quarterly*, Vol. 9, New Year's 1985, pp. 167-173.

8. This is discussed in "Ex-British Agent Says FDR's Nazi Map Faked," *Foreign Intelligence Literary Scene*, Frederick, MD: University Publications of America, December 1984, pp. 1-3; "President Roosevelt's Navy Day Address on World Affairs," *The New York Times*, October 28, 1941; and Mark Weber, "Roosevelt's 'Secret Map' Speech," *The Journal for Historical Review*, Vol. 6, No. 2, Spring 1986, p. 125.

9. See Michael Beschloss, *Mayday: The U-2 Affair: The Untold Story of the Greatest US-USSR Spy Scandal,* New York, Harper Collins, 1987.

10. Robert McNamara's explanation of the "missile gap" can be accessed in his 1996 interview for the CNN series "The Cold War," at *http://www.cnn.com/SPECIALS/cold.war/episodes/12/interviews/mcnamara/*.

11. *The Department of Defense Dictionary of Military and Associated Terms*, amended as of June 9, 2004, is available at *http://www.dtic.mil/doctrine/jel/doddict/*.

12. Good background narratives discussing deception in warfare prior to the 20th century can be found in Latimer, pp. 6-36; Dewar, pp. 23-34; and Dunnigan and Nofi, pp. 32-109.

13. See Donald C. Daniel and Katherine L. Herbig, *Strategic Military Deception*, Oxford, Pergamon, 1982, pp. 5-7.

14. The importance of "noise" in the intelligence failure regarding Pearl Harbor is most clearly explained in Roberta Wohlstetter's elderly, but seminal work, *Pearl Harbor: Warning and Decision*, Stanford, CA, Stanford University Press, 1962.

15. The D-Day deceptions are recounted in many sources, but the best analysis to date is to be found in the British official history, Michael Howard, *British Intelligence in the Second World War*, Vol. 5, *Strategic Deception*, London, HMSO, 1990; Anthony Cave Brown, *Bodyguard of Lies*, New York, Harper & Row, 1975; and in Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War*, New York, Scribner, 2004.

16. For examples of chicanery with runway craters, see Alfred Price, *Targeting the Reich*, London: Greenhill Books, 2003, p. 86; and Seymour Reit, *Masquerade: The Amazing Camouflage Deceptions of World War II,* New York: Hawthorn, 1978, photographs following p. 90.

17. Biblical scholars will remember the accounts of Gideon in the Old Testament, and classical scholars will point to examples which range from the previously mentioned Trojan Horse to the ruses employed by Caesar in Gaul. For an overview of the origins of deception doctrines, see Everett L. Wheeler, *Stratagem and the Vocabulary of Military Trickery*, Leiden: E. J. Brill, 1988.

18. In an unsubstantiated story told to the author by a World War II U.S. Army Air Force pilot, American photo intelligence detected a number of Japanese dummy aircraft on dispersal sites on the island of Rabaul. These dummies fooled no one, and they were ignored by allied bombing raids. However, late in the war, when Rabaul had been by-passed by General MacArthur's island hopping campaign, it was used as a "seasoning" target for newly arrived allied aircrew. On one of these raids, an inexperienced bombardier struck the dummy aircraft by mistake. The result was a series of secondary explosions which went on for hours. The Japanese had placed ammunition and fuel stockpiles under their obvious "active camouflage." This story has not been confirmed by other sources to date, but, even if it is not true or is possibly embellished, the point remains valid—active camouflage *could* be used as passive camouflage.

19. Each of these terms is defined in *The Department of Defense Dictionary of Military and Associated Terms*, amended as of June 9, 2004, and is available at *http://www.dtic.mil/doctrine/jel/doddict/*.

20. Again, each of these terms is defined in *ibid*.

21. See a collection of Johannes von Goethe's quotations in the John Petrie Collection at *http://www.arches.uga.edu/~jpetrie/goethe.html.*

22. An examination of the counterintelligence problems associated with double agents can be found in David C. Martin, *Wilderness of Mirrors*, New York: Harper & Row, 1980.

23. DoD provided these briefings to media audiences in Washington, DC, in 2001 and 2002, and examples are available online at *http://www.defenselink.mil/news/Oct2001/g011024-D-6570C.html* and *http://www.defenselink.mil/news/Oct2002/t10082002_t1008dia.html*.

24. An interesting collection of essays is to be found in John Norton Moore, ed., *Deception and Deterrence in "Wars of National Liberation," State-Sponsored Terrorism and Other Forms of Secret Warfare*, Durham, NC: Carolina Academic Press, 1997.

25. Gene R. Nichol, Jr., "US Domestic Legal Constraints on Deception" at *http://www.duke.edu/web/tiss/archives/conferencerecords/Deception/Nichol.html*.

26. FM 27-10, *The Laws of Land Warfare*, Foreword, at *http://faculty.ed.umuc.edu/~nstanton/FWD.htm*.

27. *Ibid*., Chapter 2, Section V. at *http://faculty.ed.umuc.edu/~nstanton/Ch2.htm#s5*; and Scott L. Silliman "International Legal Constraints" at *http://www.duke.edu/web/tiss/archives/conferencerecords/Deception/Silliman.html*.

28. See the discussion in Elizabeth Kiss, "Strategic Deception in Modern Democracies: The Ethical Dimension" at *http://www.duke.edu/web/tiss/archives/conferencerecords/Deception/Kiss.pdf*; Rushworth M. Kidder, "Ethical Deception?" at *http://www.globalethics.org/newsline/members/issue.tmpl?articleid=11180122325517*; and Major John Mark Mattox, "The Moral Status of Military Deception" at *http://www.usafa.af.mil/jscope/JSCOPE00/Mattox00.html*. An interesting overview of the basic issues can be found in Sissela Bok, *Lying: Moral Choice in Public and Private Life,* New York: Pantheon, 1978.

29. Again, note the discussions to be found in Kiss and Mattox above.

30. See Walter Jajko's overview of the role of ethical considerations in deception planning in his "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning" at *http://www.poliscitaylorandfrancis.com/pdfs/cst/novdec02_jajko.pdf*.

31. See the press coverage of this issue in CNN stories at *http://www.cnn.com/2002/US/02/19/gen.strategic influence* and *http://www.cnn.com/2002/US/02/26/defense.office.*