Naval War College
Newport, R.I.

OPERATIONAL DECEPTION AND MODERN WARFARE: THE USE OF DECEPTION IN THE INFORMATION AGE

By

Francis X. Sheehan

LCDR,USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy

Signature: F. X. Sheehan

08 February 2000

Faculty Research Advisors:
Dr Michael Handel
CDR Mike Michaels, USN

(A)

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):

Operational Deception and Modern Warfare: The Use of Deception in the Information Age (Unclassified)

9. Personal Authors: LCDR Francis X. Sheehan, USN

10.Type of Report: FINAL

11. Date of Report: 8 February 2000

12.Page Count: 24

12A Paper Advisor (if any): Dr Michael Handel, CDR Michaels, USN

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Deception, Intelligence, collection, dissemination, surprise, information superiority, operational deception

15.Abstract:
This paper asserts that the use of operational deception, despite the increased capabilities of sophisticated high-tech collection and dissemination systems, will continue to be feasible and desirable. The nature of deception, its importance to the commander and cognitive factors that facilitate its success are addressed. Those factors, along with technology's ability to assist deception, are examined to demonstrate deception's continued relevance in a high-tech world. Potential deception challenges to U.S. military's efforts to fight future wars based on information superiority are also analyzed. Finally, recommendations and conclusions for the operational commander are provided for the use and avoidance of deception in the information age.

16.Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461

20.Office Symbol: C

Abstract

This paper asserts that the use of *operational deception*, despite the increased capabilities of sophisticated high-tech collection and dissemination systems, *will continue to be feasible and desirable*. The nature of deception, its importance to the commander and cognitive factors that facilitate its success are addressed. Those factors, along with technology's ability to assist deception, are examined to demonstrate deception's continued relevance in a high-tech world. Potential deception challenges to U.S. military's efforts to fight future wars based on "information superiority" are also analyzed. Finally, recommendations and conclusions for the operational commander are provided for the use and avoidance of deception in the information age.

Table of Contents

"All warfare is based on deception."[1]

--- Sun Tzu

Introduction

Throughout history, military commanders have used deception to hide their true intentions and capabilities. Deception's ability to confuse and mislead the enemy has provided commanders with a "competitive advantage." This competitive advantage has often played a crucial part in the outcome of battles, campaigns and wars. Deception, in the past, has shown itself to be a valuable and inexpensive tool for the military commander.

Nevertheless, new technologies seem to threaten the role of deception. Tomorrow's battlefield promises an array of information collection and dissemination systems designed to increase a commander's knowledge and awareness of the enemy. The U.S. future vision of warfare strives for "information superiority" to "mitigate the impact of the fog and friction of war" and promises a nearly transparent battlespace.[2] If this vision becomes a widespread reality, what are the implications for operational deception? Will deception become more or less relevant?

Thesis

This paper asserts that the use of *operational deception*, despite the increased capabilities of sophisticated high-tech collection and dissemination systems, *will continue to be feasible and desirable*.[3] The nature of deception, its importance to the commander and cognitive factors that facilitate its success are addressed. Those factors, along with technology's ability to assist deception, are examined to demonstrate deception's continued relevance in a high-tech world. Potential deception challenges to the U.S. military's efforts to fight future wars based on "information superiority" are also analyzed. Finally, recommendations and conclusions for the

operational commander are provided for the use and avoidance of deception in the information age.

What is deception?

JCS Joint Doctrine defines deception as: "Those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions that will contribute to the accomplishment of the mission."[4] Michael Handel, a noted academic authority on military deception, defines deception as "the process of influencing the enemy to make decisions disadvantageous to himself by supplying or denying information."[5]

Yet, deception is only a means to an end --- the end being surprise. Handel noted that "deception per se has no value; it assumes significance only when used as a means of achieving surprise."[6] The main goals of deception are to manipulate the target's beliefs; to influence the target's actions; and ultimately, to benefit from the target's actions.[7] Deception can target the enemy commander through two basic ways.

"Ambiguity-Increasing" versus "Misleading" Deception

In their introduction to *Strategic Military Deception*, Donald Daniel and Katherine Herbig discuss the two variants of deception: "ambiguity-increasing" and "misleading" deception.[8] "Ambiguity-increasing" deception confuses an opposing commander so that he is unsure as to what to believe. By ensuring the level of ambiguity concerning the deceiver's intentions remains high, the target is forced to spread resources thin "to cover important contingencies," thereby reducing the resistance the deceiver can expect at any given point.[9]

"Misleading" deception, rather than increasing ambiguity concerning the deceiver's intentions or capabilities, is designed to *reduce ambiguity* "by building up the attractiveness of

one wrong alternative."[10] Noted deception expert Barton Whaley captured the essence of "misleading" deception with his statement that "the ultimate goal of stratagem is to make the enemy quite certain, very decisive, *and wrong*."[11]

Deception at the Operational Level

Having defined deception in general, it is necessary to discuss deception at the operational level. Operational deception supports major operations or campaigns and is designed to target the *enemy's high command* as opposed to his forces in the field. The objective of deception at the operational level is to influence the decisions and actions of the enemy commanders *before* the battle occurs. Since operational deception overlaps with strategic as well as tactical deception, close coordination is required between commanders at all levels. Effective deception is always planned from the top down so that efforts are not at cross-purposes.[12] Because operational deception's objectives are often "long term and may involve the full spectrum of operational forces" centralized control is required.[13] This ensures the various elements involved in the deception are portraying the same "story" and are not in conflict with operational objectives.[14]

Operational deception, like tactical deception strives to create ambiguous or misleading impressions about friendly force capabilities and intentions only on a much larger scale. Operational deception may, for example, strive to induce the enemy commander to miscalculate which major operation is the main effort. The broader scope of operational deception requires "different organization for centralized control, a longer timeline to plan and implement, and greater intelligence support for initial planning and feedback."[15]

Why is deception important?

Deception is an important force multiplier for the military commander. Deception's ability to bring about surprise reduces the risk and effort required to achieve the commander's objectives. It prompts the enemy commander to act in a way that serves the deceiver's objectives. Using surprise, the operational commander can achieve his objective at reduced overall cost -- saving lives, resources and time. Whaley's extensive study on deception indicates that, in the past, surprise significantly increased enemy to friendly casualty ratios.[16] Deception operations throughout history have demonstrated its benefits as a force multiplier.

Another "plus" of deception is its high probability of success. Whaley's data suggests the likelihood of deception success (both in terms of its ability to surprise and in the increased likelihood for victory). His analysis of forty-seven historical cases of operational and tactical deception between 1914 and 1968 found that surprise was achieved and victory followed in over ninety percent of the cases.[17] Deception, and the surprise that it can cause, enhances the likelihood that successful deceivers will achieve military victory.

Finally, deception is an important tool to the commander because it is cost effective. In an era of limited resources, "the economics of deception become progressively more attractive."[18] A 1989 Marine Corps study on deception noted "the investment for a deception capability is often a small portion (seldom more than five percent) of the total resources committed to combat."[19] While the benefits of deception operations are often difficult to quantify, it sometimes can be done. Roger Hesketh's review of the deception operations associated with the Normandy invasion conclusively showed how deception saved lives and resources.[20] The overwhelming success of that operation, among others, supports Handel's observation that "deception is the cheapest and most effective force multiplier."[21]

In summary, the use of deception makes sense. American sensitivity to casualties and disdain for long wars, coupled with limited resources, suggests deception should be used whenever possible. From an adversary's point of view, the use of deception against the United States also makes sense. Since most of our adversaries lack the forces to meet U.S. strength directly, they have more incentive to use deception. Deception's ability to serve as a force multiplier, its high probability of success, and its cost effectiveness make it a logical choice for a military commander regardless of the size and strength of his forces.

Successful Deception - - the Human Element and Future Warfare

The use of operational deception makes sense, but is that "high probability of success" still there? By analyzing what has made deception successful in the past, we can hope to determine the likelihood for successful deception in the future.[22] A review of deception literature reveals numerous factors that influence deception's success. Of these factors, two are particularly useful when evaluating the continuing relevance of deception from a human perspective since deception, after all, targets the human mind. These are the ability of deception to succeed based on *Exploitation of Preconceptions* and *Conditioning*.

Exploitation of Preconception

> We are of course gratified by evidence which confirms our preconceptions. We all like to be right. We tend therefore to attach undue weight to evidence which supports our point of view and to reject that which does not.[23]

The exploitation of an enemy's preconceptions has long played an important role in deception operations. A well known deception maxim, "Magruder's principle," asserts that it is easier to induce an opponent to maintain a preexisting belief than to convince him to change that belief.[24] Deceptions that "slant the target's mind-set in directions he is predisposed to take" stand a greater chance of convincing him than those that go against his expectations and assumptions.[25]

Again, Whaley's research on deception provides historical evidence that supports "Magruder's principle." In 110 out of 131 cases (84 percent), deception schemes were "more often than not keyed to enemy preconceptions."[26] Of these 110 cases, surprise was achieved in over 95%. Exploiting preconceptions increases the probability of surprise and, therefore, victory.

The selection of the invasion site and cover plan for the Normandy invasion illustrates the application of "Magruder's principle." Through Ultra communication intercepts, the Allies were well aware of Hitler's belief that the Allied invasion of Europe would occur in the Pas de Calais region. The Pas de Calais region was a plausible choice for the Allies since it provided better air cover and the shortest transit time from England. Because the deception plan exploited the strong German expectations, it was difficult for the Germans to react even when conclusive evidence contradicted their beliefs.[27]

This example, along with more recent examples such as the U.S. use of deception during Desert Storm, illustrates the continued validity of deception based on reinforcing enemy preconceptions. As Handel observed, "After all, human nature cannot be expected to change; and since most deception operations are designed to reinforce the existing beliefs and perceptions of the deceived, successful deception will continue to be an important factor in war."[28]

Conditioning

Man's susceptibility to conditioning can also facilitate deception. Conditioning can desensitize the deception target to changes in the operational situation. For example, a CIA study on deception cites the breakout of three German ships from Brest on 12 February 1942. The Germans used jamming, made to appear like atmospherics, to condition British radar operators. Each day the jamming duration was increased slightly. After one month, British

operators became accustomed to the interference and were unable to detect the departure of the German ships.[29]

As Michael Dewar noted in *The Art of Deception in Warfare*, "the tendency is for the mind to be lulled by regularity and routine. It tends to pay less attention to events which occur again and again and is not good at spotting marginal or gradual changes."[30] This helps explain why surprise is often achieved when activity is designed to appear as routine exercises. For example, Egyptian deception, before the October 1973 Arab-Israeli war, lulled the Israelis into a false sense of security. From the autumn of 1972 until October 1973, the Egyptians conducted about forty major exercises involving the crossing of water obstacles. Through constant repetition and conditioning, they convinced the Israelis that these were harmless training exercises.[31]

Deception and Technology

Having observed just some of the reasons why deception is successful from the human perspective, it is useful to look at the ability of technology to facilitate deception and its implications for the future use of operational deception. A common myth which has contributed to the de-emphasis of deception is that "advances in technology are perceived to make successful deception more difficult, if not impossible, to achieve."[32]

Yet, technology has modernized many of the deceptive means used in the past. For example, sophisticated decoys, with innovative technology, emit "signatures" (visible, IR, and radar) that emulate platforms (tanks, mobile/fixed launchers, communications nodes, etc), significantly complicating the intelligence process.[33] Additionally, technological advances, such as visual and thermal camouflage and stealth technology, have also improved the effectiveness of

deception operations. As Handel observed, "In terms of its forms and the means employed, deception will, like war itself, change as new weapons and technologies appear."[34]

The tremendous growth in intelligence collection capabilities has not eliminated the possibility of deceiving high-tech opponents. In many ways it has increased the opportunity to feed him false information.[35] R.V. Jones, a key figure in British scientific intelligence during World War II, noted that a mastery of our adversary's technological means of gathering intelligence is required to be successful in deception.[36] The impact of high-tech sensors on deception and counter deception is that an increased level of expertise and specialized planning is now required to do either.

Technology's alleged ability to make deception and surprise more difficult has, paradoxically, increased the incentive to use deception. For example, since attack preparations will be accompanied by observable and significant evidence of attack, surprise will be more difficult to achieve. Consequently, the use of *deception* to achieve surprise will become even more necessary. As Dewar observed, the need to overcome "transparency has therefore raised the value of deception to the extent that a successful surprise attack now depends entirely on successful deception."[37]

Deception in the Information Age

Joint Vision 2010 (JV 2010), the JCS template for future U.S. military operations identifies "information superiority" as the linchpin of the emerging operational concepts of U.S. fighting. [38] While acknowledging that the friction and fog of war can never be eliminated, JV 2010's concepts strive to mitigate their impact through technology. Advocates of the new information-based "Revolution in Military Affairs" argue that technology will remove uncertainty, chance and surprise from the battlespace.[39] Yet, as shown certain aspects of

deception and surprise transcend technology's abilities to provide answers. Deception's target remains the same, only the pathways to the target have changed. Deception, despite powerful and seductive "enabling technologies," will still pose a challenge to the humans in the loop through manipulation of perceptions.[40]

In order for our adversaries to confuse or mislead us, they must first gain an understanding of how our sensors work. This is not always difficult to do. For instance, various Internet web sites provide detailed information on the orbital mechanics of U.S. satellites and other intelligence collection capabilities.[41] Additionally, this type of information can be obtained through relatively unsophisticated technical means as well.

Knowledge of U.S. sensor capabilities and limitations can obviously be used against us. For example, according to various newspaper reports, India's understanding of U.S. sensor capabilities was crucial to their unexpected May 1998 nuclear detonation. An Indian government official stated at the time, "It's not a failure of the CIA. It's a matter of their intelligence being good, and our deception being better."[42] While the Indian nuclear detonation case involved various levels of deception including strategic, it nevertheless, demonstrates the capability to exploit our current sensor limitations.[43]

An adversary with an understanding of our sensor's capabilities and limitations can use various means to degrade our attempts at "information superiority." This could be accomplished through either ambiguous or misleading deception. For example, our adversaries may use ambiguous information to overload and confuse our analysts and decision-makers. Low-tech approaches such as concealment, use of tunnels, camouflage, and human intelligence may be used to mislead us concerning adversary capabilities and intentions.

We would be arrogant and naive to think we are not susceptible to deception. Successful deception is still possible today and will continue to be possible in the future. Therefore, what are the likely deception implications for warfare based on "information superiority?" An analysis of deception's possible relationship with a warfare model based on "information superiority" is useful. Network Centric Warfare provides such an example.

Deception and Network Centric Warfare

Like JV 2010, the concept of Network Centric Warfare (NCW) sees information superiority as a key to success in the future battlespace. NCW focuses on "gathering, processing and managing information to take advantage of the growing power resident in networks."[44] Using a networked grid of sensors, it seeks to create and sustain shared battlespace awareness at all levels of command that will allow for speed and self-synchronization.[45] Because of the synergistic effect of networking, the NCW concept envisions fewer, yet more lethal, platforms to conduct missions.

The concepts of NCW offer the military commander tremendous potential. Nevertheless, certain aspects of NCW would appear to be particularly vulnerable to deception. These include problems with *information*, *speed of command* and *self-synchronization.*[46]

NCW Information

NCW's reliance on "information superiority" and gathering of information will significantly increase the amount of raw data available to the commander. The sheer amount of data alone will pose potential ambiguity problems. Additionally, more information does not always equate to a better understanding and does nothing to protect against deception. Increased reliance on automated systems will be required to separate the meaningful signals from the

"noise." Much of this data will enter the network without any human processing, providing a potential vulnerability to deception.

Speed of command

NCW, with its emphasis on speed of command, will require the commander to make decisions rapidly. Therefore, an adversary's deception effort (while standing the possibility of getting lost in the noise) could very rapidly become the basis for action. This in turn will effectively speed the deception procedure.[47] If deceptive information enters the network, NCW's common operating picture and shared awareness will allow deceptive information to reach the military commander as well as commanders at all levels much more rapidly.

Self-synchronization

NCW's self-synchronization and decentralized control allows units to act independently. A commander, rapidly reacting to deceptive information, may employ his forces in the wrong place or time or against the wrong target. While this has happened in the past (i.e. Halsey at Leyte Gulf), NCW's emphasis on fewer platforms means forces "lost" to deception compound the commander's task more significantly than in the past because of the synergistic effect that NCW strives to obtain. As it defeats "synergism," the loss of a NCW "part" is of greater impact than it would have been in a non-NCW setting.

While the above deception challenges to NCW clearly show a potential threat to warfare based on "information superiority," a counter-argument can be made that NCW's improved sensors will provide the intelligence insights needed to overcome deception. Yet, no matter how improved a sensor may be, an enemy who knows he is being observed can manipulate the information that the sensor reports. Well-planned and smoothly executed deception is hard to

detect. Good intelligence may be able to detect deception. Nevertheless, even *good* intelligence can be deceived.

Recommendations for the Commander

This paper serves as a warning to the commander that, despite sophisticated technologies and attempts to obtain "information superiority," deception will still be feasible. Therefore, the U.S. military needs to reexamine its attitude and approach to deception and counter-deception.

Despite some historical successes, the U.S. military has failed to embrace the use of deception. This can be attributed to several factors including U.S. reliance on material superiority, as well as ethical and cultural reasons. While deception is never a substitute for the other factors required for military success, its ability to save lives, *in and of itself,* argues strongly for its expanded use. *Increased deception training, organizational changes, improved doctrine and planning* are just some of the ways to provide the commander with better deception and counter-deception capability.

Our training needs to emphasize the importance of deception. Dewar observed "The importance attached to a particular skill in any army can usually be judged by the training time, manpower, and resources dedicated to it."[48] Like any art, deception needs to be practiced to be perfected. Rather than giving lip service to deception, it should be integrated into all our training, exercises, and operations in peacetime so that we will have a strong capability during wartime.

Training to avoid deception is equally important and even more difficult. Expert analysis is the key to counter deception. Operational commanders must ensure qualified analysts, educated in counter deception techniques, are assigned to their Joint Intelligence Centers.[49] An understanding of our own information processing capabilities and limitations are crucial for

counter deception. An awareness of what the enemy knows about our sensors, collection capabilities, and methodologies will have to be an area of greater emphasis for our intelligence professionals.

Our doctrine and organization should also reflect deception's importance. Like training, our current doctrine does not provide the depth required to perform operational deception adequately. The often "ad hoc" nature of a Joint Task Force leads to "ad hoc" deception planning. The Joint Information Operations Center (JIOC) in San Antonio, Texas would be a logical choice to provide the theater and JTF commanders with the necessary personnel to conduct deception at the operational level. Operational deception support could be added to the C2W support which the JOIC is already tasked to provide to the CINCs. The theater Joint Intelligence Centers would continue to provide the commander with the intelligence expertise to support deception planning.

Because technology has the potential to shorten wars, deception planning must be done well in advance. Deception concepts and schemes should be incorporated into OPLANS. Additionally, money should be spent on technology that can support deception (e.g. sophisticated decoys) so that various technical deception means are available when needed.[50] Handel observed, "During the shorter wars of the future, deceivers may not have the time to implement intricate deception operations; instead cover plans will have to be prepared before the outbreak of the war in order to be used in its initial stages and may be much more difficult to apply at later stages."[51] The longer timelines required for operational deception mean last minute deception is hard, if not impossible, to accomplish.

The commander must never forget that he is the target of the enemy's deception efforts. Military commanders must avoid perceiving what they expect to see. While difficult to do, they

must also avoid having made up their minds on what the enemy is going to do or not do, and what the enemy forces are capable of or not capable of doing.

Conclusions

> No major operations should be undertaken without planning and executing appropriate deception measures. As time goes on ...there is danger that these two means (cover and deception) may in the future not be considered adequately in our planning.[52]
>
> ---General Dwight D. Eisenhower

General Eisenhower's warning to ensure adequate planning and execution of deception still applies today. His warning, however, would have been complete if he had also mentioned the need for counter deception efforts as well. The nature of deception and the nature of man indicate deception will continue to be a viable factor in future wars. Deception's ability to reduce cost and casualties make it an effective tool that commanders should incorporate into planning.

Deception's means and methods will continue to change, but its basic principles will remain unchanged.[53] High-tech sensors are the new conduits by which our adversaries intend to target us. Technology will continue to raise the level of sophistication required to successfully conduct deception. Additionally, U.S. attempts to gain "information superiority" will increase our adversaries' incentive to use deception.

Success in the deception/counterdeception battle will go to the military commander who best understands human nature - - first in general, but also more specifically, an understanding of his adversary's perceptions and expectations. There can be no "information superiority" without a superior understanding of human nature and good intelligence. Finally, the commander who best understands how to use information channels to influence enemy forces and prevent their use against his own decision-making process will ultimately prove successful in the art of military deception.

Appendix A

Principles of Military Deception[54]

Focus. The deception must **target the adversary decision-maker** capable of taking the desired action(s). The **adversary's intelligence system is normally not the target.** It is only the primary conduit used by deceivers to get selected information to the decision-maker.

Objective. The objective of the deception must be **to cause an adversary to take (or not to take) specific actions,** not just to believe certain things.

Centralized Control. A deception operation must be **directed and controlled by a single element.** This approach is required in order to avoid confusion and to ensure that the various elements involved in the deception are portraying the same story and are not in conflict with other operational objectives. **Execution of the deception may,** however, **be decentralized** so long as all participating organizations are adhering to a single plan.

Security. Knowledge of a force's intent to deceive and the execution of that intent must be denied to adversaries. Successful deception operations require **strict security. Need-to-know criteria must be applied to each deception operation and to each aspect of that operation.** Along with an active operations security (OPSEC) effort to deny critical information about both actual and deception activities, **knowledge** of deception plans and orders **must be carefully protected.**

Timeliness. A deception operation **requires careful timing.** Sufficient **time must be provided for** its portrayal; for the adversary's intelligence system to collect, analyze, and report; for the adversary decision maker to react; and for the friendly intelligence system to detect the action resulting from the adversary decision maker's decision.

Integration. Each **deception must be fully integrated** with the basic operation that it is supporting. The development of the deception concept must occur as part of the development of the commander's concept of operations. **Deception planning** should occur **simultaneously with operation planning.**

Notes

[1] Sun Tzu. The Art of War. Translated by Samuel B. Griffith (New York: Oxford University Press, 1982) 66.

[2] John M. Shalikashvili, Joint Vision 2010. (1996): 16.

[3] Douglas Smith and Eileen MacKrell examine deception's continued feasibility and future relevance in Douglas V. Smith. Military Deception and Operational Art. (Research Report, U.S. Naval War College, Newport, RI: 1993) and Eileen F. MacKrell, "Contemplating the Counterfactual: Military Deception in an Age of Perfect Knowledge." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

[4] Joint Chiefs of Staff, Joint Doctrine for Military Deception (Joint Pub 3-58) (Washington, D.C. May 1996), V.

[5] Michael I. Handel, ed., Strategic and Operational Deception in the Second World War (London: Frank Cass, 1987), 1.

[6] Handel. Strategic and Operational Deception, 1. Handel also observed deception, despite having long been recognized as one of the most important elements inherent in warfare "has never been accepted as a principle of war." Nevertheless, deception serves as a tool to assist the commander in carrying out other principles of war. Deception's contribution to the principle of surprise is the most obvious. Yet, deception also assists the commander in attaining security, mass and economy of force.

[7] Donald C. Daniels, ed., Strategic Military Deception (New York: Pergamon Press, 1982), 5

[8] Ibid., 6.

[9] Ibid. For example, during the Second World War, the Allies' Plan Bodyguard main goal was to prevent the Germans from shifting their forces to reinforce the Channel Coast, specifically Normandy. The Allies posed deceptive threats throughout Europe to prevent the Germans from focusing exclusively on an assault across the English Channel. By creating "uncertainty", the Allies brought about a situation advantageous to their cause.

[10] Ibid. Perhaps the best known case of misleading deception is Fortitude South, the deception plan associated with the Normandy landings. Fortitude South sought to portray the Normandy landings as a feint to a main invasion at Pas de Calais. By providing deceptive information to the Germans mainly through double agents, the Allies mislead the Germans with regard to the Allies' true intentions. Allied deception efforts were instrumental in the German decision to postpone reinforcing the Normandy front for six weeks after D-Day.

[11] Barton Whaley, "Stratagem: Deception and Surprise in War, Vol I" (Unpublished Research Paper, Massachusetts Institute of Technology: 1969),135.

[12] Joint Pub 3-58, I-3.

[13] Steven Watters, "Operational Deception: Are We Deceiving Ourselves?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1994), 12.

[14] Joint Pub 3-58, I-3.

[15] Watters., 11. Deception at the operational level requires sufficient time for successful execution. Joint Pub 3-58 notes that time must be provided for the "adversary's intelligence system to collect, analyze, and report, for the adversary decision maker to react, and for the friendly intelligence system to detect the action resulting from the adversary decision maker's decision." Therefore, deception planners at the operational level must remain conscious of the increased time required for operational deception.

[16] Whaley., 193.

[17] Michael Dewar, The Art of Deception in Warfare (Newton Abbot: David and Charles, 1989), 196. Additionally, Whaley discovered that out of sixty-eight instances of strategic deception in the same period surprise was achieved in ninety –two percent and victory followed in eighty-seven percent of cases.

[18] Ibid., 7.

[19] John LeHockey, Strategic and Operational Military Deception: U.S. Marines and the Next Twenty Years. Marine Corps Combat Development Command (Quantico, VA 1989), 117.

[20] Roger Hesketh, "Fortitude: A History of Strategic Deception in North Western Europe, April 1943 to May 1945," published as official debrief of the Fortitude operation in unbound manuscript form. (260 pages).

[21] Michael I. Handel, op. cit., personal presentation note to CDR Marv Butcher as quoted in Douglas V. Smith. Military Deception and Operational Art. (Research Report, U.S. Naval War College, Newport, RI: 1993), 17.

[22] The same methodology was used by Smith in Military Deception and Operational Art and Eileen F. MacKrell, "Contemplating the Counterfactual: Military Deception in an Age of Perfect Knowledge." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

[23] Dewar.,9.

[24] Deception Research Program. Office of Research and Development, Central Intelligence Agency, Deception Maxims: Fact and Folklore (Washington: Central Intelligence Agency, 1980), 5.

[25] Daniels., 21.

[26] Deception Maxims., 5.

[27] Ibid.,5.

[28] Handel., War Strategy and Intelligence. 39.

[29] Deception Maxims., 13.

[30] Dewar, 30.

[31] Ibid.,16.

[32] FM 90-2 Battlefield Deception. Washington, D.C., Department of the Army, 1988,1-0.

[33] Kevin N. Kearny, "Denial and Deception – Network Centric Challenge." Unpublished research Paper, (U.S. Naval War College, Newport, RI: 1999), 6.

[34] Handel. War Strategy and Intelligence. 394.

[35] FM 90-2, 1-1.

[36] R.V. Jones., "Future Conflict and New Technology," The Washington Papers Vol. IX No. 88 (Beverly Hills, CA: Sage Publications, 1981), 77.

[37] Dewar, 20,117, 207.

[38] Deborah Monroe, "Net-Centric Warfare: Are We Ready to be Cyber-Warriors?" Unpublished Research Paper, (U.S. Naval War College, Newport, RI: 1999), 2.

[39] Paul K. Van Riper. "Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare." National Security Studies Quarterly, Summer 1998, Vol. IV, Issue 3, 2 and 16.

[40] Monroe, 2.

[41] For example, the Federation of American Scientists (FAS) maintains a web site with detailed information on U.S. intelligence capabilities.

[42] John Diamond, Internet Associated Press Report "India Able to Evade Satellites," <http://www.fas.org/irp/news/1998/05/05170059 > (29 Jan 2000)

[43]An enemy's use of deception to hide his intentions or capabilities could prevent us from correctly identifying his critical strengths and weaknesses and center of gravity.

[44] Arthur K. Cebrowski, "Network Centric Warfare: An Emerging Military Response to the Information Age." Presentation at the 1999 Command and Control Research and Technology Symposium. 29 June 1999, 1.

[45] Ibid., 3.

[46] For a more detailed discussion along these lines see Kearney's "Denial and Deception: Challenges to Network Centric Warfare."

[47] It should be noted that NCW's rapid speed of command may prove too rapid for enemy deception to be effective at the operational level which often requires more time.

[48] Dewar, 123.

[49] K.A. Young, "The Operational Counter Deception Cell: Is it the Answer?", Unpublished Research Paper, (U.S. Naval War College, Newport, RI 1999), 19.

[50] Diane H. Olsen, "Deception: Past, Present and Future Possibilities." Unpublished Research Paper, (U.S. Naval War College, Newport, RI), 26.

[51] Handel, Strategic and Operational Deception, 27.

[52] Dewar, 121.

[53] Handel, War, Strategy and Intelligence, 393.

[54]Joint Pub 3-58, I-3.

BIBLOGRAPHY

Cebrowski, Arthur K., "Network Centric Warfare: An Emerging Response to the Information Age." Presentation at the 1999. Command and Control and Technology Symposium 29 June, 1999

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

Deception Research Program, Office of Research and Development, Central Intelligence Agency. Deception Maxims! Fact and Folklore. Washington: Central Intelligence Agency, 1980.

Dewar, Michael. The Art of Deception in Warfare, Newton Abbot: David and Charles, 1989.

Diamond, John. "India Able to Evade Satellites", Internet Associated Press Report < http: //www.fas.org/irp/news/ 1998/05/05170059 >

FM 90-2, Battlefield Deception. Washington, D.C.: Department of the Army 1988.

Handel, Michael I., ed Strategic and Operational Deception in the Second World War. London: Frank Cass and Co. Ltd, 1987.

Handel, Michael I. War, Strategy and Intelligence. Totowa, NI: Frank Cass and Co. Ltd, 1989.

Hesketh, Roger F. Fortitude: A History of Strategic Deception in Northern Europe, April 1943 to May 1945, published as official debrief of the Fortitude operation in unbound manuscript form (260 pages).

Jones, R.V. "Future Conflict and New Technology," The Washington Papers Vol IX no 88 Beverly Hills, CA: Sage Publications, 1981.

Kearny, Kevin N. "Denial and Deception – Network Centric Challenge." Unpublished Research Paper, (U.S. Naval War College, Newport, RI: 1999).

LeHockey, John. Strategic and Operational Military Deception: U.S. Marines and the Next Twenty Years. Marine Corps Combat Development Command Quantico, VA: 1989.

MacKrell, CDR Eileen F. " Contemplating the Counterfactual: Military Deception in an Age of Perfect Knowledge." Unpublished Research Paper, U.S. Naval War College, Newport, R.I: 1996.

Monroe, Deborah. "Net-Centric Warfare: Are We Ready to be Cyber-Warriors?" Unpublished Research Paper, U.S. Naval War College, Newport, R.I. 1999.

Olsen, Diane H., "Deception: Past, Present and Future Possibilities," Unpublished Research Paper, U.S. Naval War College. Newport, R.I., March 1994.

Palmby, William G. "The Effect of Technology on Operational Deception." Unpublished Research Paper, U.S. Naval War College, Newport, R.I. 1994.

Shalikashvili, John M. Joint Vision 2010. Washington, D.C.: Chairman of the Joint Chiefs of Staff, 1996.

Smith, CDR Douglas V. Military Deception and Operational Art, Research Report, U. S. Naval War College, Newport, RI: 1993.

Sun Tzu. The Art of War. Translated by Samuel B. Griffith. New York: Oxford University Press, 1982.

U.S. Joint Chiefs of Staff, Joint Doctrine for Military Deception (Joint pub 3-58) Washington, D.C.: May 1996.

Whaley, Barton. "Stratagem: Deception and Surprise in War, Volume I." Unpublished Research Paper, Massachusetts Institute of Technology, 1969.

Watters, Steven. "Operational Deception: Are We Deceiving Ourselves?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1994.

Young, K.A. "The Operational Counter Deception Cell: Is It the Answer?" Unpublished Research Paper, U.S. Naval War College, Newport, R.I. 1999.