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): FOREIGN DENIAL AND DECEPTION: MINIMIZING THE IMPACT TO OPERATIONAL INTELLIGENCE (UNCLASSIFIED)

9. Personal Authors: Major Brian P. Cyr, USMC

10.Type of Report: FINAL

11. Date of Report: 4 February 2002

12.Page Count: 26 **12A Paper Advisor (if any):** Professor Richard Martin

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:

Denial, Deception, Network-Centric Warfare, Operational Intelligence, North Korea, Kosovo, Iraq, Analyst, Counterdeception, Sensor

15.Abstract: Foreign Denial and Deception (D&D) is as old as warfare itself and is still practiced across the globe today. Both countries and non-state actors use D&D as a means to gain comparative advantage over their opponents. Indeed, the weaker one is in relation to their adversary, the greater the appeal to use D&D. Since foreign practitioners have frequently employed denial and deception against the United States, it is incumbent upon both joint force commanders (JFCs) and their intelligence staffs (J-2) to increase their knowledge of this asymmetric challenge.

Countering the foreign D&D threat will not be easy. Since we will never be able to completely eliminate D&D, one must take steps to lessen its impact upon operational art. By defining D&D, examining denial and deception means & techniques, and looking at various foreign models, JFCs and their J-2s begin an important step in understanding the adversary. Perhaps the best methodology to "knowledge advantage" over an enemy remains centered on the human dimension. Increasing D&D awareness, emphasizing a multi-collection/analytical approach, and incorporating D&D concepts into our joint doctrine, will allow both the operational commander and his J-2 to not just mitigate foreign D&D, but also to exploit an opponent's biases and perceptions.

Currently, Network-Centric Warfare (NCW) has the potential to leave us vulnerable to foreign denial and deception. While most of the news on this Information Technology Revolution in Military Affairs (IT RMA) centers around technological development, the importance of NCW's organizational, doctrinal, and

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
04-02-2002	Thesis	xx-xx-2002 to xx-xx-2002

4. TITLE AND SUBTITLE
Foreign Denial and Deception: Minimizing the Impact to Operational Intelligence
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Cyr, Brian P. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Joint Military Operations Department
Naval War College
686 Cushing Road
Newport , RI02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Foreign Denial and Deception (D&D) is as old as warfare itself and is still practiced across the globe today. Both countries and non-state actors use D&D as a means to gain comparative advantage over their opponents. Indeed, the weaker one is in relation to their adversary, the greater the appeal to use D&D. Since foreign practitioners have frequently employed denial and deception against the United States, it is incumbent upon both joint force commanders (JFCs) and their intelligence staffs (J-2) to increase their knowledge of this asymmetric challenge. Countering the foreign D&D threat will not be easy. Since we will never be able to completely eliminate D&D, one must take steps to lessen its impact upon operational art. By defining D&D, examining denial and deception means & techniques, and looking at various foreign models, JFCs and their J-2s begin an important step in understanding the adversary. Perhaps the best methodology to ?knowledge advantage? over an enemy remains centered on the human dimension. Increasing D&D awareness, emphasizing a multi-collection/analytical approach, and incorporating D&D concepts into our joint doctrine, will allow both the operational commander and his J-2 to not just mitigate foreign D&D, but also to exploit an opponent?s biases and perceptions. Currently, Network-Centric Warfare (NCW) has the potential to leave us vulnerable to foreign denial and deception. While most of the news on this Information Technology Revolution in Military Affairs (IT RMA) centers around technological development, the importance of NCW's organizational, doctrinal, and operational concepts should not be lost. Focusing on the human factor side of NCW promises to offer significant rewards. In the end, it is the education and training of our JFCs and their J-2s that holds the key to minimizing the impact of foreign D&D to operational intelligence.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	28	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

operational concepts should not be lost. Focusing on the human factor side of NCW promises to offer significant rewards. In the end, it is the education and training of our JFCs and their J-2s that holds the key to minimizing the impact of foreign D&D to operational intelligence.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** **C**	

NAVAL WAR COLLEGE

Newport, R.I.

FOREIGN DENIAL AND DECEPTION: MINIMIZING THE IMPACT TO OPERATIONAL INTELLIGENCE

by

Brian P. Cyr

Major, USMC

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:_____

4 February 2002

Prof. Richard Martin
Faculty Advisor

Abstract

Foreign Denial and Deception (D&D) is as old as warfare itself and is still practiced across the globe today. Both countries and non-state actors use D&D as a means to gain comparative advantage over their opponents. Indeed, the weaker one is in relation to their adversary, the greater the appeal to use D&D. Since foreign practitioners have frequently employed denial and deception against the United States, it is incumbent upon both joint force commanders (JFCs) and their intelligence staffs (J-2) to increase their knowledge of this asymmetric challenge.

Countering the foreign D&D threat will not be easy. Since we will never be able to completely eliminate D&D, one must take steps to lessen its impact upon operational art. By defining D&D, examining denial and deception means & techniques, and looking at various foreign models, JFCs and their J-2s begin an important step towards understanding the adversary. Perhaps the best methodology to achieve "knowledge advantage" over an enemy remains centered on the human dimension. Increasing D&D awareness, emphasizing a multi-collection/analytical approach, and incorporating D&D concepts into our joint doctrine, will allow both the operational commander and his J-2 to not just mitigate foreign D&D, but also to exploit an opponent's biases and perceptions.

Currently, Network-Centric Warfare (NCW) has the potential to leave us vulnerable to denial and deception. While most of the news on this Information Technology Revolution in Military Affairs (IT RMA) centers around technological development, the importance of NCW's organizational, doctrinal, and operational concepts should not be lost. Focusing on the human factor side of NCW promises to offer significant rewards. In the end, it is the education and training of our JFCs and their J-2s that holds the key to minimizing the impact of foreign D&D to operational intelligence.

Table of Contents

Introduction

To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds.
Mao Tse-Tung, Selected Military Writings of Mao Tse-Tung

In a recent commentary, Patrick M. Hughes, a retired U.S. Army Lieutenant General and former Director of the Defense Intelligence Agency (DIA), stressed that adversaries did not want to face the U.S. military head-on. Instead, he pointed out, our opponents would rely on "extraordinary denial and deception activities to gain surprise and to take advantage of our values and cultural traits."[1] Indeed, foreign denial and deception (D&D) allows a weaker country or non-state actor to "level the playing field" by concealing or misleading United States intelligence in areas such as military deployments, political intentions, and weapons of mass destruction (WMD).

U.S. military operations in Kosovo, the Gulf War, and Afghanistan have highlighted the use of adversarial D&D at both the strategic and operational levels. In fact, the Department of Defense was so concerned about the Taliban's use of denial and deception, that they provided a first-ever background briefing to the press on the subject.[2] Since future battlefields will continue to witness the use of foreign D&D, it is incumbent upon joint force commanders (JFCs) and their intelligence (J-2) staffs to increase their understanding of this asymmetric challenge.

This paper will examine some ways to counter foreign D&D by emphasizing the *human factor*: increasing our awareness through education and training, stressing both a multi-discipline collection & intelligence analysis process, and a greater incorporation of D&D awareness into our joint doctrine. Network-Centric Warfare (NCW) will also be reviewed, because it too, ultimately relies on the human factor to counter the use of denial and deception. In the end, this author contends that the human dimension is the key to

minimizing D&D's impact on operational intelligence. In order to place this conclusion in the proper context, however, one must first define operational D&D, describe how it succeeds, cover potential means & techniques, and examine a few foreign models.

Defining Operational D&D

All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away, that you are near. Sun Tzu, The Art of War

The earliest recorded example of D&D in warfare was approximately 1450 BC, when the Egyptian general Thot captured Jaffa.[3] General Thot feigned defeat against his opponents and concealed soldiers in baskets as gifts to the city. Once the gifts were brought into Jaffa, he was able to seize power with his "hidden" soldiers. From this example, one can conclude that denial, refers "to the attempt to block information which could be used by an opponent to learn some truth."[4] Deception, on the other hand, refers to misleading an opponent to believing something that is false. Although denial and deception can occur separately, they are often used together to lead an opponent to believe what the deceiver wants him to believe. More importantly, however, the deceiver wants his opponent to not just believe, but "to take (or not take) specific *actions* [emphasis mine]."[5]

The key difference between strategic and operational D&D is the target audience. Strategic D&D is typically aimed at the national level of government or senior military leadership.[6] Operational D&D, in contrast, is more likely centered at combatant and subordinate joint force commanders, along with their component commanders. Although intelligence personnel such as the J-2 may not specifically be the target of denial and deception, they should be considered "the primary conduit used by deceivers to get selected information to the decision maker."[7] This statement highlights the importance that the J-2 must place on understanding D&D and its impact on friendly intelligence collection,

analysis, and dissemination capabilities. In summary, the purpose of operational D&D is to cause commanders to form inaccurate impressions about an opponent's capabilities and intentions, misappropriate intelligence collection assets or fail to advantageously employ their forces. Therefore, to mitigate the results of operational denial and deception to our operations, it is imperative that we understand how it is planned.

Successful Operational D&D Planning

You must know what he believes, what he wishes to believe, and what he is prepared to believe. Major John LeHockey USMC, FMFRP 15-6 Strategic and Military Deception

Based on historical lessons learned, an operational D&D campaign should take into account several factors to increase its chances of success.[8] First, the D&D campaign must be centrally controlled and support strategic/operational objectives, as well as the Desired End State (DES).[9] D&D guidance also needs to be tied to these aims and the DES. Moreover, denial and deception planners should possess a clear understanding of their commander's D&D intent, objectives, targets, and desired perception.

Second, planners must gather and analyze information related to their opponent. The identification of key decision makers, their backgrounds, and psychological profiles are all critical components. In addition, knowledge of an opponent's intelligence collection system (or information channels), decision-making process, and their analysis capabilities must be understood. Finally, the identification of any preconceptions that the opponent's leadership may have about the deceiver force's intentions and capabilities needs to be taken into account.

Next, the operational D&D campaign must develop courses of action (COAs) that are capable of accomplishing the commander's D&D objectives and the DES. A D&D COA will not only restate the denial and deception objective, but will also identify the proposed target and the desired perception.[10] More importantly, the COA provides the D&D cover

story used to create the desired perception. This cover story must be believable, verifiable, consistent, and executable.[11] Cover stories should also reinforce an opponent's preconceptions and biases. These preconceptions and biases can be cultural, political, or doctrinal in nature. Once the cover story is developed, D&D planners identify the means and techniques that will be used to convey or deny information to the target audience. Finally, an event schedule is developed, along with the identification of feedback channels (both operational and analytical). Operational feedback pertains to D&D information reaching the target, while analytical feedback addresses the actions the target is taking because of that information.[12] Feedback channels are difficult to develop, but at the same time, key to the success of the D&D plan. Feedback allows D&D practitioners to determine whether their plan is believed, and more importantly, being acted upon. Having a view of how denial and deception is working (through the opponent's eyes) allows planners to modify or cancel their operation or campaign. While perhaps not as vital as feedback, it is clear that the *mechanism* used to convey or deny information is important in the D&D process. Accordingly, a variety of D&D means and techniques will be examined in the next section.

Operational D&D Means and Techniques

The importance of deception in warfare is often overlooked, often by the soldiers whose lives depend on it. James F. Dunnigan and Albert A. Nofi, Victory and Deceit

D&D means are defined as methods and resources that can be used to convey or deny information to the deception target. Joint Publication 3-58, *Joint Doctrine for Military Deception*, categorizes deception means as physical, technical, and administrative.[13] One can also use these same categories, as described below, to characterize denial and deception means since both definitions include the words *convey or deny*.

1) **Physical means**: Activities and resources used to convey or deny selected information to a foreign power.
2) **Technical means**: Military material resources and their associated operating

techniques used to convey or deny selected information to a foreign power through the deliberate radiation, re-radiation, alteration, absorption, or reflection of energy; the emission of suppression of chemical or biological odors; and the emission or suppression of nuclear particles.

3) **Administrative means**: Resources and methods to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power.[14]

In addition to means, D&D operations require mastery of various techniques to supply an opponent's intelligence system with erroneous information. These techniques are designed to dissimulate (hide the real) or simulate (show the false).[15] *Dissimulation* conceals or protects something from an adversary's observation. *Dissimulation* includes masking, repackaging, and dazzling. These are further explained below.

1) **Masking:** Using natural or artificial material to evade detection. Examples include: camouflage paint schemes, use of cover and terrain, or maintaining "normal" activities prior to an attack or withdrawal.
2) **Repackaging:** Altering the appearance of an object to make it look like something else. Examples include: disguising an arms factory as a residence, disguising a weapon system as destroyed, and renaming units to hide their actual strength.
3) **Dazzling:** Confusing the sensory processing abilities of the target with stimuli. Examples include: signaling false intentions through activity designed to reflect something else, the use of notional forces, and radar reflectors.[16]

Simulation involves the use of decoys or dummy equipment to represent something that does not exist. *Simulation* encompasses mimicking, inventing, and decoying.

1) **Mimicking:** Creates a replica of reality using one or more distinctive characteristics of the object being mimicked. Examples include: displays, decoys, and heat signature simulation.
2) **Inventing:** Displays the false by fashioning an alternative reality. Examples include: false documents, painted damage (such as craters) on runways, and dummy equipment.
3) **Decoying:** Offers a distracting or misleading option with the intent of diverting an opponent's attention away from the real focal point. Examples include: false target generation, decoy radar emitters, and misinformation.[17]

The coordinated use of D&D means, combined with techniques, helps to create the necessary atmosphere of disinformation that is integral to D&D operations.

Foreign Operational D&D Models

As in Kosovo, enemy ground forces also sought to evade U.S. airpower by dispersing and concealing equipment and troops. Bryan Bender, Kim Burger, and Andrew Koch, "Afghanistan: First Lessons"

Although a variety of countries and non-state actors practice D&D today, many share similar mindsets and methodology. Historical examples make an excellent tool for both the operational commander and his J-2 to gather insight into the mind of the adversary. The commonality among D&D practitioners also provides a point of departure for examining how an adversary may use denial and deception in the future.

The Iraqis have been fast learners in D&D means and techniques, applying their skills most vividly during and after the Gulf War. First, Iraqi Scud missile operations employed a combination of cover, dispersal, and decoys to undermine U.S. intelligence collection capabilities. By not using Scud-associated meteorological radars and communications that were a standard part of Soviet doctrine, the Iraqis denied the United States detectable indications and warning of launch. This, combined with the ability of the Scud Transporter-Erector-Launchers (TELs) to "shoot and scoot," made it virtually impossible for the United States to locate the TELs with the timeliness and accuracy necessary to effectively respond.[18] Second, it was not until the on-the-ground United Nations Special Commission (UNSCOM) inspections after the Gulf War that it became known the extent the Iraqis had achieved in the nuclear, biological, and chemical weapons arena. A striking example is Iraq's nuclear program which relied on an assortment of D&D measures including: the construction of buildings within buildings; purposely making buildings designed for the same purpose look different; hiding power lines and water feeds to disguise a facility's purpose; suppressing emissions; moving key pieces of equipment at night; and placing facilities underground.[19] Because the Iraqis have prevented subsequent UNSCOM inspections, their D&D measures

continue to provide an important means in preventing anyone from gaining deep insight into Saddam Hussein's WMD program.

The war in Kosovo highlighted a Serbian military that was also well versed in D&D means and techniques. First, the Serbs built decoy bridges out of plastic tarp and logs, and placed them nearby camouflaged real bridges.[20] They also painted bridges with infrared patterns to break up their distinguishing shape in order to mislead U.S. intelligence sensors. Second, Serbian forces employed numerous decoy tanks throughout Kosovo; sometimes simply using wood and plastic to fool Allied pilots flying at high altitudes. To add more realism to their deception, they created heat sources--such as burning trash, tires, and cooking oil near the decoy tanks to give off a false infrared signature.[21] Third, Serbian forces disguised the results of Allied bombing in order to deny U.S. intelligence an accurate battle damage assessment. Besides removing and hiding military wreckage, they created fake bomb craters on roads and runways to portray greater damage than what really existed. Finally, to lessen the risk of being bombed, Serbian forces placed equipment in civilian areas or attempted to blend in their own forces with noncombatants.[22]

North Korea, like the Iraqis and Serbs, has relied upon total secrecy to ensure regime survival. Taking into account the lessons learned from the Korean War, the philosophy of Juche or "self-reliance," and their own mountainous terrain, North Korea established a national security policy, known as the "Four Military Lines," in 1962.[23] This policy emphasized the fortification of their entire country, and was eventually included in the North Korean constitution. The resultant massive denial and deception effort derived from this national policy has been ongoing for over forty years and must not be underestimated. Heavily influenced by Soviet *maskirovka* (deception), North Korea has employed a variety of D&D means throughout their country. Their methodology includes (but is not limited to):

hardening, camouflage, decoys, and signature suppression. An example of the elaborate extent that has gone into the effort to deny and deceive is the Onch'on-Up airfield on the North Korean west coast. Consisting of three runways (including one that is underground), all of which are interconnected by a series of roads, Onch'on-Up airfield can house an entire MIG-29 air regiment underground.[24] Another example of the North Korean D&D effort is their Hardened Artillery Sites (HARTS). HARTS contain long-range artillery & rockets and are located in successive defensive belts north of the Demilitarized Zone (DMZ). What makes HARTS such a problem for U.S. intelligence, is that the sites typically include a cave, tunnel or bunker that encloses the firing piece. In effect, North Korea is able to play a "shell game," whereby it moves equipment in and out of these enclosures to mislead U.S. collection assets and intelligence analysts.[25]

One of the key items to note in examining different foreign models is that there are few differences in D&D means and techniques between cultures. In Barton Whaley's Stratagem: Deception and Surprise in War, Vol. I, a similar conclusion was reached after examining eight different cultures and 93 case studies.[26] The implications for today's J-2 is that there are common threads among foreign D&D models that can be determined and studied in order to provide the commander a picture of how an adversary might think and act. Armed with this intimate knowledge of foreign D&D models, JFCs and their J-2s are better prepared to come up with solutions to counter the denial and deception threat. It is in this next section, that we will examine what specific actions need to be taken in order to lessen D&D implications to operational intelligence.

Minimizing the Impact of Foreign Operational D&D

Tomorrow, deception and counterdeception could become requirements for all warriors, and many will have trouble thinking in ways such practice demands. Martin C. Libicki, "Defending Cyberspace and Other Metaphors"

In order to minimize the threat that D&D poses, this author proposes focusing on the human dimension of the problem by: 1) Creating greater awareness among personnel; 2) Emphasizing both a multi-discipline intelligence collection and analytical effort; 3) Encouraging a greater incorporation of D&D concepts into our joint doctrine.

First, joint force commanders and the Services should ensure that their staffs and units (with an emphasis on their intelligence/operations personnel) understand foreign D&D. The foundation for this education on D&D should begin in the schoolhouse. All formal schools need to emphasize D&D instruction in their curriculums. Why is this so important? Because, one must remember that a decision maker is the target of foreign D&D and the J-2 (or intelligence system) is the means the enemy uses to get to that target! While most schools address operational deception and deception planning, few touch upon the *denial* aspect of D&D. With a few adjustments, classrooms can enhance their operational D&D instruction through guest lectures, additional seminars, and expansion of students' readings on the subject.[28] In addition to formal schools, D&D briefings, course offerings, and other such activities can be used to heighten awareness among intelligence personnel and operators. For example, since 1998 all new intelligence analysts at Defense Intelligence Agency (DIA) must take at least one introductory D&D course.[29] The growing use of mobile training teams from DIA's Joint Military Intelligence Training Center (JMITC) can also make D&D awareness a reality for both J-2s and their commands. The JMITC provides courses on analysis, collection management, and indications & warning--all of which touch upon D&D.[30]

Armed with D&D knowledge through an educational process, specific D&D training can then take place. This operational level training should emphasize gaming simulation in order to interact with various scenarios without involving the high costs of field maneuvers.

The creation of "red cells" for the war game process is an excellent means to aid decision makers in understanding foreign D&D. Red cells can be as small as just the J-2, or involve a variety of multi-disciplined experts and agencies. One of the major reasons for the establishment of a red cell is to portray a "thinking" adversary to a decision maker. Besides military aspects, red cells need to take into account an opponent's distinct cultural/religious/ political perceptions and biases. Use of international officers or students during war games is an excellent tool in revealing cultural mindsets, insight into foreign decision-making, and unique perspectives on coalition warfare. The advantages that we garner in the education and training process does not just rest on greater adversarial awareness, but also in discovering our own vulnerabilities to D&D. In fact, the identification of these critical vulnerabilities can greatly benefit JFCs in the development of their operational risk assessments.

Second, even with the most sophisticated intelligence capability, there is no list or recipe that will *guarantee* the ability to detect and/or minimize D&D. An emphasis on multi-disciplined intelligence collection and analysis, however, still has merit. Through all-source intelligence collection: open-source intelligence (OSINT), measurement and signature intelligence (MASINT), signals intelligence (SIGINT), human intelligence (HUMINT), and imagery intelligence (IMINT), J-2s are able to receive information through many different channels. It is through a *variety* of channels or collection means, that the J-2 increases his ability to detect incongruities in an opponent's D&D cover story. A major reason for this is that the enemy might not have been consistent in portraying his cover story among all channels of information available to him. A different collection platform may pick up on something that another may have missed, and therefore, provide a valuable clue that uncovers the D&D operation. Or a collection source can detect something in a particular

area and "cross-cue" another sensor to look at the same area. Using a multi-discipline collection approach, however, requires that intelligence personnel understand what collection capabilities are best suited for a foreign D&D problem set.

In addition to understanding capabilities, knowing how adversaries exploit inherent weaknesses in our own collection platforms is equally important. Preventing the knowledge of these vulnerabilities from falling into the hands of adversaries has become more difficult in an increasingly connected and transparent world. Indeed, the U.S. intelligence community failed to spot or predict key developments in weapons proliferation, such as the Indian nuclear tests in 1998, because countries have taken steps to conceal their activities from overhead surveillance. India was successful because it used means such as: working underground, in bad weather/at night, and knowing the scheduled orbits of U.S. satellites.[31] Due to these unique challenges, there continues to be an effort to rethink the deployment of existing collection systems, the development of new sensors, and operational security (OPSEC) measures to foil future D&D operations.

Along with collecting information, a big challenge for the J-2 in uncovering D&D is during the analysis and production phase of the intelligence cycle.[32] First, it is important that intelligence personnel not become too overconfident from their past analytical successes, or worse, become complacent. Everyone needs to understand that they can be denied or deceived. Clever adversaries have duped even the most seasoned analysts. Perhaps by examining an opponent's effort, we may find a way to detect D&D even among the best practitioners. Every D&D operation leaves clues.[33] No cover story will ever be so flawless that there are not some inconsistencies that can be discovered--if the J-2 looks in the right place. Analysts must determine what the most obvious and reasonable ways an adversary might act based on his capabilities, even if available evidence contradicts such possibilities.

This is where the importance of knowing an enemy and being able to think like him becomes important. In order to do this, analysts need to be open to evidence that does not fit their own preconceptions and biases. This is a very difficult matter for most intelligence personnel to confront. Perhaps, the best approach to this problem may be to have other analysts or operators play the "devil's advocate," and see if the available evidence could add up to a plausible cover story that the enemy may be using.[34] If the J-2 appears to be detecting a D&D cover story, then the following guidelines will aid in exposing any inconsistencies within the denial and deception operation:[35]

- Determine whether the enemy is capable of even conducting the action it is portraying. Is the enemy exaggerating or concealing real capabilities? How have they historically used their capabilities? What does their doctrine state?
- Has information been too forthcoming or flows too neatly into a single pattern?
- Do you only have a very small body of consistent data in which to draw conclusions? Typically, conclusions drawn from very small samples are highly unreliable.
- Was the information gathered from normally expected channels? Can the information be verified by other means? If not, then why not?
- Conversely, what is missing? Is information that is normally gathered from expected channels absent? Are normally available channels inaccessible? Why?

While the above questions are only a start in helping analysts uncover D&D, they do offer a means to focus the J-2 on both the *military capabilities* and *intentions* of an adversary--the essence of operational intelligence.

Finally, increased awareness and collection/analytical emphasis will be difficult to achieve without doctrine to support it. Little has been written on D&D in operational doctrine, especially in regard to countering it. This is important because doctrine establishes a common language for both training and the conduct of operations.

Beginning in 2000, elements of D&D made its debut into joint doctrine, albeit only in cursory fashion. Joint publication 2-0, *Doctrine for Intelligence Support to Joint Operations*,

specifically lists avoiding deception and surprise as a fundamental intelligence purpose. It further, states that "intelligence analysts should remain sensitive to the possibility that they are being deceived."[36] The publication fails, however, to provide the reader any advice on *how* to escape being deceived. It also does not address the subject of *denial.* Moreover, although Joint publication 2-0 considers "anomalies" in an opponent's actions to be especially valuable to analysts, it does not suggest how these irregularities may be used to uncover a foreign D&D operation. Published after Joint publication 2-0, Joint publication 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace* does a much better job in providing tools to counter D&D. It devotes a section on the Joint Intelligence Preparation of the Battlespace (JIPB) process providing several examples of how an adversary may deceive an analyst and achieve surprise. Furthermore, the publication highlights the need for the intelligence analyst to develop multiple hypotheses concerning an adversary's adoption of various COAs. In fact, it may be the "throwaway," or less likely COA, that an opponent uses in his D&D plan to maximize surprise. Finally, Joint publication 2-01.3 also contains an outstanding case study on Egyptian deception and "psychological conditioning" against Israel during the Yom Kippur War in 1973. Psychological conditioning takes place when the analyst gradually accepts a level and type of adversary activity, previously considered abnormal, as normal.[37] In this case, the Egyptian's made the Israelis believe that a military exercise was taking place, when in reality wartime preparations were ongoing. Again, the only problem with this short case study is that it does not specifically state how an analyst was to avoid being a victim of psychological conditioning in order to prevent falling into an enemy's deception effort.

Alas, even joint publications in the operations realm fall short in describing how one is to counter or minimize the impact of D&D. For example, Joint Publication 3-13, *Joint*

Doctrine for Information Operations, defines counterdeception, but delineates that it "does not include the intelligence function of identifying foreign deception operations."[38] Furthermore, Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, calls for intelligence analysts to be trained in military deception methods, but does not state how to accomplish this task.[39] The lack of intelligence and operational focus on the D&D problem is even exemplified in Joint Publication 3-58, *Joint Doctrine for Military Deception*, which contains no attempt to define D&D nor offers any suggestions in countering it.

In summary, even with D&D concepts starting to make inroads into joint doctrine, more work in this regard remains to be done. Additional guidance on countering D&D, or at least minimizing its impact, is critical in formulating both operational and intelligence judgments. In order for the JFC and their J-2's to mutually understand D&D, it first must be prevalent in the lexicon of joint doctrine.

Network-Centric Warfare (NCW) and D&D

Many countries and disaffected groups will develop techniques of denial and deception in an attempt to thwart U.S. intelligence efforts--despite U.S. technological superiority.
Senators Gary Hart and Warren B. Rudman, "New World Coming: American Security in the 21st Century"

NCW is a hot buzzword in the military, offering a way to fight where forces use a common network to share and act on information faster than their adversary. With a major emphasis on transformation in the military, many in the intelligence community are looking for a solution to the D&D problem through NCW. Relying heavily upon technology as an enabler, NCW stresses *the co-evolution* of operational concepts, doctrine, and organization.[40] NCW's framework encompasses sensor, engagement, and information grids.

The sensor grid is the most important of the three grids and has had the greatest investment placed on it so far. Gaining sensor advantage over an adversary entails not just

providing more friendly sensors to the battlespace, but also denying the enemy his own sensor access. Of course, having more sensors does not lesson our susceptibility to foreign D&D operations. On the contrary, it can open up more channels for an opponent to apply denial and deception. An enemy may be able to use the same cost effective D&D effort as they are capable of today and reap higher rewards *because we have increased our sensor grid*.[41] The key for the U.S. intelligence community as discussed before, is not just using more sensors (quantitative), but a *variety* (qualitative) that can better separate "signals from noise" in the battlespace.[42] Advanced collection platforms, such as those involving multi-spectral or hyper-spectral sensors, can help in detecting specific forms of D&D. A drawback, however, is that commercial industries that specialize in camouflage, concealment, and deception (CCD) merchandise have done a remarkable job in keeping pace with our latest technology. Indeed, commercially available countermeasures are readily accessible to any nation or group that has the money to spend on them.[43]

The information grid is also potentially vulnerable within the NCW framework. As we gather information from our sensors, and then move it through a network that rapidly forms our common operational picture of the battlespace, we create avenues for D&D exploitation. If an adversary is successful in denying or deceiving our sensor grid, it is likely that our common operating picture (COP) will also be affected.[44] Foreign D&D impacts the COP by creating ambiguity for all users, most importantly in the decision maker and his J-2. By presenting a false picture of the battlespace, an operational commander's own preconceptions may be reinforced, leading him to misdirect assets or reach an unforeseen culmination point in a campaign or major operation.

Because NCW inherently produces vulnerabilities that our adversaries could capitalize on--namely, the *denial* of our ability to collect information and/or providing misleading

information (via *deception*), we leave ourselves open to exploitation. NCW, however, is not just a tech-focused concept, but relies on "human-to-human connections."[45] To minimize the battlespace effects of friction, uncertainty, and disorder that D&D creates, NCW requires savvy JFCs and J-2s. These individuals must possess an intuitive sense and ability to function in an increasingly fast Observe, Orient, Decide, and Act (OODA) loop. They will also have to rapidly combine their knowledge of the adversary (culture, values, modes of operation) with the real-time picture they receive from sensors in order to "convert information advantage to operational advantage."[46] Finally, JFCs and J-2s must absorb a multi-dimensional picture without mentally creating information overload for themselves. All of these human factors reinforce the fact that NCW will only become operationally viable in countering D&D *after* training, organizational competency, and doctrine are in place.

Conclusion

> *High quality intelligence can be developed only when there is a curiosity about and respect for the enemy.* Professor Michael I. Handel, Strategic and Operational Deception in the Second World War

Foreign D&D is nothing new and will continue to be a way our adversaries will asymmetrically threaten our operational intelligence community. From Saddam Hussein to Kim Jong-Il, there will always be opponents who devise clever and not-so-clever means to thwart our sophisticated intelligence system. Regardless of technological prowess, the human dimension of countering D&D will remain of greatest importance. Truly understanding an adversary, to include his perceptions and biases, will be paramount for the J-2 and the operational commander. Because the J-2 will be the means that adversaries use to get to the decision maker, it is also important that they are familiar with a variety of D&D means and techniques employed throughout the world.

In understanding the challenges that NCW creates, JFCs and J-2s will be better prepared to operate within its framework. Already early lessons learned from Afghanistan point to the importance of intelligence, surveillance and reconnaissance (ISR) and networking capabilities in creating a clearer picture of the battlespace for military prosecution.[47] As we develop tactics that go along with sharing information between sensors and shooters, our emphasis on D&D awareness, intelligence collection/analytical processes, and doctrine will collectively minimize the foreign D&D threat to operational intelligence. In the end, the importance of the human contribution in achieving success in this endeavor must not be lost on JFCs and their J-2s.

Notes

[1] Patrick M. Hughes, "A Case for Greater Support for the U.S. Intelligence Community," 20 January 2001, <http://www.homelanddefense.org/journal/Commentary/Hughes_Commentary.htm/> [14 December 2001].

[2] "Background Briefing on Enemy Denial and Deception," 24 October 2001, <http://www.defenselink.mil/cgi-bin/dlprint.cgi/> [14 December 2001].

[3] Major John LeHockey, FMFRP 15-6 Strategic and Operational Military Deception: U.S. Marines and the Next Twenty Years (Washington, DC: HQMC 1989), 16-17.

[4] Roy Godson and James J. Wirtz, "Strategic Denial and Deception," International Journal of Intelligence and Counterintelligence, 13, no. 4 (2000): 425.

[5] Joint Chiefs of Staff, Joint Doctrine for Military Deception, Joint Pub 3-58 (Washington, DC: 31 May 1996), I-3.

[6] Godson and Wirtz, "Strategic Denial and Deception," 425.

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

[8] Major Donald J. Bacon, Second World War Deception: Lessons for Today's Joint Planner, Wright Flyer Paper, no. 5 (Maxwell Air Force Base, AL: Air Command and Staff College, 1998), 13-21.

[9] Joint Pub 3-58, IV-2 to IV-9. DES is defined in Milan N. Vego's, Operational Warfare, (Newport, RI: Naval War College, 2000), 637.

[10] Ibid., IV.

[11] Ibid., A-2.

[12] Ibid., IV-7, IV-8.

[13] Joint Pub 3-58, GL-2, GL-3.

[14] Ibid., GL-2, GL-3.

[15] LeHockey, 279, 281.

[16] Ibid., 279-280.

[17] Ibid., 281-282.

[18] Michael R. Gordon and General Bernard E. Trainor, The Generals' War: The Inside Story of the Conflict in the Gulf (Boston: Little, Brown and Company 1995), 230.

[19] David Kay, "Denial and Deception: The Lessons of Iraq," Roy Godson, Ernest R. May, and Gary Schmitt, eds., U.S. Intelligence at the Crossroads: Agendas for Reform, (Washington DC: Brassey's, 1995), 120.

[20] Peter Martin, "The Sky's the Limit: A Critical Analysis of the Kosovo Airwar," 1 November 1999, <http://www.infowar.com/iwftp/cloaks/99/CD_1999-214.txt/> [18 December 2001].

[21] Ibid. See also Steven Lee Myers "Damage to Serb Military Less Than Expected," 28 June 1999, <http://www.nytimes.com/library/world/europe/062899kosovo-bomb-damage.html > [18 December 2001] and Tim Ripley "Kosovo: A Bomb Damage Assessment," Jane's Intelligence Review, (September 1999): 10-13.

[22] Ibid.

[23] Joseph S. Bermudez Jr., The Armed Forces of North Korea (London: I.B. Tauris Publishers, 2001), 8-9.

[24] Ibid, 140.

[25] Roy Godson and James J. Wirtz, eds., Strategic Denial and Deception: The Twenty-First Century Challenge (New Brunswick: Transaction Publishers, 2002), 177-178.

[26] Barton Whaley, Stratagem: Deception and Surprise in War, Vol. I (Boston: 1969), 24-85.

[28] This author suggests articles from Michael I. Handel's Strategic and Operational Deception in the Second World, Donald C. Daniel and Katherine L. Herbig's Strategic Military Deception, or Roy Godson and James J. Wirtz's Strategic Denial and Deception.

[29] Jennifer Lasley, "Denial and Deception: A Serious Threat to Information Superiorty?," (Unpublished Research Paper, National Defense University, Washington, DC: 2000), 11.

[30] Based on author's personal experience after completing the following JMITC mobile training team courses: Intelligence Analyst, Indications and Warning, and Collection Management.

[32] The intelligence cycle consists of six phases: planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback.

[33] Barton Whaley, "Toward a General Theory of Deception," John Gooch and Amos Perlmutter eds., Military Deception and Strategic Surprise (London: Frank Cass, 1982), 190.

[34] Richard J. Heuer Jr., Psychology of Intelligence Analysis (Washington DC: CIA 1999), 72-73.

[35] This list (modified by the author) comes from an unpublished handout on deception from the Armed Forces Staff College, dated approximately 1993. See also Handel's Strategic and Operational Deception in the Second World War, pages 36-37.

[36] Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, Joint Pub 2-0 (Washington, DC: 9 March 2000), I-4.

[37] Joint Chiefs of Staff, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace, Joint Pub 2-01.3 (Washington DC: 24 May 2000), II-56.

[38] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13, (Washington DC: 9 October 1998), GL-5.

[39] Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1 (Washington, DC: 7 February 1996), III-6, III-7.

[40] Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare--Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 33.

[41] Bart Whaley and Jeffrey Busby, "Detecting Deception: Practice, Practitioners, and Theory," Roy Godson and James J. Wirtz eds., Strategic Denial and Deception (New Brunswick: Transaction Publishers, 2002), 196-200.

[42] Ephraim Kam, Surprise Attack: The Victim's Perspective (Cambridge, Harvard University Press, 1988), 50-53.

[43] Mark Hewish and Bill Sweetman, "Hide and Seek," Jane's International Defense Review (April 1997): 29.

[44] Kevin N. Kearney, "Denial and Deception--Network-Centric Challenge," (Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1999), 8-9.

[45] Commander Sheila Scarborough, "Network-Centric Warfare Meets the Laws of the Navy," U.S. Naval Institute Proceedings (May 2001): 31.

[46] Naval War College Faculty, "Network Centric Warfare: A Capstone Concept for Naval Operations in the Information Age," (Unpublished Smooth Draft, U.S. Naval War College, Newport, RI: 2000), 7.

[47] Bryan Bender, Kim Burger, and Andrew Koch, "Afghanistan: First Lessons," Jane's Defense Weekly, 19 December 2001,<http://ebird.dtic.mil/Dec2001/s20011217 first.htm>[17 December 2001].

Bibliography

"Background Briefing on Enemy Denial and Deception." 24 October 2001. <http://www.defenselink.mil/cgi-bin/dlprint.cgi/> [14 December 2001].

Bacon, Donald J., Major. Second World War Deception: Lessons Learned for Today's Joint Planner. Maxwell Air Force Base, AL: U.S. Air University. Air Command and Staff College, 1998.

Bender, Bryan, Kim Burger, and Andrew Koch. "Afghanistan: First Lessons." Jane's Defense Weekly. 19 December 2001. <http://ebird.dtic.mil/Dec2001/s20011217first.htm/> [17 December 2001].

Bermudez, Joseph S., Jr. The Armed Forces of North Korea. London: I.B. Tauris Publishers, 2001.

Cebrowski, VADM Arthur K. and John J. Garstka, "Network-Centric Warfare--Its Origin and Future." U.S. Naval Institute Proceedings (January 1998): 28-35.

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

Dunnigan, James E. and Albert A. Nofi. Victory & Deceit: Dirty Tricks at War. New York: Quill William Morrow, 1995.

Godson, Roy and James J. Wirtz. "Strategic Denial and Deception." International Journal of Intelligence and CounterIntelligence,13, no. 4 (2000): 424-437.

_____, eds. Strategic Denial and Deception: A Twenty-First Century Challenge. New Brunswick: Transaction Publishers, 2002.

Gordon, Michael R. and General Bernard E. Trainor. The Generals' War: The Inside Story of the Conflict in the Gulf. Boston: Little, Brown and Company, 1995.

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

Hart, Gary and Warren B. Rudman. "New World Coming: American Security in the 21st Century." 15 September 1999. <http://www.nssg.gov/Reports/ New_World_Coming /New_World7/new_world7.htm/> [14 December 2001].

Heuer, Richards J., Jr. Psychology of Intelligence Analysis. Washington DC: CIA, 1999.

Hewish, Mark and Bill Sweetman. "Hide and Seek." Jane's International Defense Review (April 1997): 26-32.

Hughes, Patrick M. "A Case for Greater Support for the U.S. Intelligence Community." 20 January 2001. <http://www.homelanddefense.org/ journal/Commentary/ Hughes_ Commentary.htm/> [14 December 2001].

Kam, Ephraim. Surprise Attack: The Victim's Perspective. Cambridge: Harvard University Press, 1988.

Kay, Martin. "Denial and Deception: The Lessons of Iraq." Roy Godson, Ernest R. May, and Gary Schmitt, eds. U.S. Intelligence at the Crossroads: Agendas for Reform. Washington DC: Brassey's, 1995. 109-127.

Kearney, Kevin N. "Denial and Deception--Network-Centric Challenge." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1999.

Lasley, Jennifer. "Denial and Deception: A Serious Threat to Information Superiority?" Unpublished Research Paper, National Defense University, Washington, DC: 2000.

LeHockey, John. FMFRP 15-6 Strategic and Operational Military Deception: U.S. Marines and the Next Twenty Years. Washington DC: HQMC, 1989.

Libicki, Martin C.. "Defending Cyberspace and Other Metaphors." February 1997. <http://www.ndu.edu/inss/actpubs/dcom/dcomch04.html/> [17 December 2001].

Martin, Peter. "The Sky's the Limit: A Critical Analysis of the Kosovo Airwar." 1 November 1999. <http://www.infowar.com/iwftp/cloaks/99/CD_1999-214.txt/> [18 December 2001].

Myers, Steven Lee. "Damage to Serb Military Less Than Expected." 28 June 1999. <http://www.nytimes.com/library/world/europe/062899kosovo-bomb-damage.html> [18 December 2001].

Naval War College Faculty. "Network Centric Warfare: A Capstone Concept for Naval Operations in the Information Age." Unpublished Smooth Draft, U.S. Naval War College, Newport, RI: 2000.

Ripley, Tim. "Kosovo: A Bomb Damage Assessment." Jane's Intelligence Review, (September 1999): 10-13.

Scarborough, Sheila. "Network-Centric Warfare Meets the Laws of the Navy." U.S. Naval Institute Proceedings, (May 2001): 31-33.

Tse-tung, Mao. Selected Military Writings of Mao Tse-tung. Peking: Foreign Language Press, 1966.

Tzu, Sun. The Art of War. trans. Samuel B. Griffith. London: Oxford University Press, 1963.

U.S. Central Intelligence Agency. Director of Central Intelligence. "Jeremiah News Conference." 2 June 1998. <http://www.cia.gov/cia/public_affairs/ press_release /archives/1998/jeremiah.html/> [20 December 2001].

U.S. Joint Chiefs of Staff. Doctrine for Intelligence Support to Joint Operations. Joint Pub 2-0. Washington, DC: 9 March 2000.

U.S. Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace. Joint Pub 2-01.3. Washington, DC: 24 May 2000.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, DC: 9 October 1998.

U.S. Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1. Washington, DC: 7 February 1996.

U.S. Joint Chiefs of Staff. Joint Doctrine for Military Deception. Joint Pub 3-58. Washington, DC: 31 May 1996.

Vego, Milan. Operational Warfare. Newport: Naval War College, 2000.

Whaley, Bart and James Busby. "Detecting Deception: Practice, Practitioners, and Theory." Roy Godson and James J. Wirtz, eds. Strategic Denial and Deception. New Brunswick: Transaction Publishers, 2002. 181-221.

Whaley, Barton. "Toward a General Theory of Deception." John Gooch and Amos Perlmutter, eds. Military Deception and Strategic Surprise. London: Frank Cass, 1982. 178-192.

_____. Stratagem: Deception and Surprise in War, Vol. I. Cambridge: Massachusetts Institute of Technology, 1969.