NAVAL WAR COLLEGE
Newport, R.I.

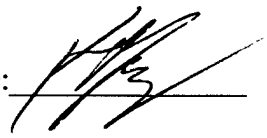
THE OPERATIONAL COUNTER DECEPTION CELL: IS IT THE ANSWER?

by

K. A. Young
Major, United States Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Maritime 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: 

5 February 1999

Faculty Advisor: Captain J. R. Fitzsimonds, USN

UNCLASSIFIED
Security Classification This Page

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): THE OPERATIONAL COUNTER DECEPTION CELL:IS IT THE ANSWER? (U)	
9. Personal Authors: MAJOR K. A. YOUNG, USA	
10.Type of Report: FINAL	**11. Date of Report:** 5 FEB 99
12.Page Count: 27	
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:

INTELLIGENCE	INFORMATION	OPERATIONAL	PRECONCEPTION
DECEPTION	AUTOMATION	FAILURE	
ANALYSIS	COUNTER-DECEPTION	BIAS	

15.Abstract: Operational deception can be utilized by both the strong and weak adversaries with, as history shows, a high chance for success. As the U.S. finds itself engaged in dealing with new and more varied threats, the operational commander and his analysts must be aware of the importance of counter deception operations. While the concept of a dedicated counter deception cell sounds like an effective way to avoid being deceived, a separate, independent cell within the Joint Task Force Intelligence Staff (JTF J2) or Joint Intelligence Center (JIC) has little likelihood of being properly staffed and resourced under current fiscal constraints. Nor does a counter deception cell address the root causes of effective deception operations, namely, the misperceptions, preconceptions, and biases of commanders and analysts exploited by deception. The key is to ensure that intelligence analysts are properly educated in the techniques of counter deception operations and detailed operational level analysis. Analysts must be properly educated, managed, and assigned in order to become experts in the theater to which they will be assigned as valued members of the JTF J2/JIC.

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	

Security Classification of This Page Unclassified

ABSTRACT

Operational deception can be utilized by both strong and weak adversaries with, as history shows, a high chance for success. As the U.S. finds itself engaged in dealing with new and more varied threats, the operational commander and his analysts must be aware of the importance of counter deception operations. While the concept of a dedicated counter deception cell sounds like an effective way to avoid being deceived, a separate, independent cell within the Joint Task Force Intelligence Staff (JTF J2) or Joint Intelligence Center (JIC) has little likelihood of being properly staffed and resourced under current fiscal manpower constraints. Nor does a counter deception cell address the root causes of effective deception operations, namely, the misperceptions, preconceptions, and biases of commanders and analysts exploited by deception. The key is to ensure that intelligence analysts are properly educated in the techniques of counter deception operations and detailed operational level analysis. Analysts must be properly educated, managed, and assigned in order to become experts in the theater to which they will be assigned as valued members of the JTF J2/JIC.

TABLE OF CONTENTS

I. INTRODUCTION

Counter-deception is defined in the U.S. Air Force Doctrine Document 2-5, Information Operations, as "...the effort to negate, neutralize, diminish the efforts of, or gain advantage from, a foreign deception operation." Detecting and exploiting the enemy's deception effort allows the commander to retain or seize the initiative by conducting operations in a manner which the enemy did not anticipate. The document goes on to say that a fully integrated intelligence, surveillance and reconnaissance system can "...identify an adversary's attempts to deceive friendly forces," and recommends that a non-traditional analytical approach be taken to conduct counter-deception operations.[1] As part of the search for a method of counter-deception analysis, the Institute for National Strategic Studies (INSS) has embarked on a study of counter-deception issues. They have proposed the creation of a specific counter-deception analysis cell which would serve the operational commander on a Joint Task Force intelligence staff (JTF J2) or at the Joint Intelligence Center (JIC)[2]. This paper will examine the pros and cons of such a cell and propose an alternative method of addressing the issue. A counter-deception cell is, in the end, an attempt to cure a human analytical problem with institutional reorganization without fully addressing the *human* issue. The solution to the counter-deception dilemma is to focus on improving the intelligence analysts.[3]

II. OPERATIONAL DECEPTION: DEFINITION AND PURPOSE

In U.S. Joint Doctrine, deception is defined as, "those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a

manner prejudicial to his interests."[4] Simple deception operations can be used to reinforce uncertainty and ambiguity and so merely delay an opponent's actions or reactions, but the classic deception operation seeks to target and manipulate the commander's decision process. The opponent's perceived preconceptions are played to, painting a picture that is plausible and all the more important if it is what the opponent wants to believe.[5]

At the operational level of war, deception may be used to achieve operational surprise and to mask or inflate capabilities. The intent is to "...influence the enemy major commands and commanders..." and is differentiated from tactical deception by its scope and resource requirements. Operational deception takes longer to develop, coordinate, and orchestrate and must be aimed directly at the opponent's operational and strategic intelligence collection and analysis systems.[6] Deception, however, is a tool founded in imagination and a potential adversary does not have to possess great numerical or technological power to employ deception effectively. Historically, deception has been a favored tool of the weaker side in a conflict since it offers the possibility of "leveling the playing field" due to its role as an important force multiplier.[7] Through deception one retains the initiative, forcing the enemy commander to act in accordance with one's own wishes without having to expend vast resources or personnel. Deception is most effective when the "story" being portrayed is logical and fits into the target's perceptions of his opponent. Deception must also be aimed at the target's intelligence collection systems and must be properly managed and reinforced to have any influence on the targeted commander's decision making process. Barton Whaley in his study of military deception notes not only that most deceptions have been successful, but that deception operations have succeeded even when the target was in possession of all of the data necessary to identify the ruse.[8]

This observation sounds an ominous note in the present era of information dominance. The U.S. expended an enormous effort in recent years obtaining technology to allow it to gather, manage, and exploit every scrap of information possible. The "data deluge" which has hit the intelligence community in recent years is unprecedented and yet we are reminded that perfect data coverage does not automatically mean perfect intelligence. While our automated systems are highly capable at collection and management of data, they still require humans to analyze the data, to derive intelligence, and to make decisions based on that intelligence. Many writers have recently argued that deception can be identified if the analysts were provided with sufficient information from which they could derive an accurate picture. But as Whaley has argued, the one weak link in the decision cycle that proponents of deception have always targeted remains the analysts, and reams of data have been no safeguard against analytical failures resulting in surprise.

In the autumn of 1944, Germany was defending on two fronts against the Allied advance from France and the Soviet advance in the east. Hitler was advised that the more serious threat came from the Soviets and that the main German effort should be the defense in the east, allowing the Allies in the west to advance further on into Germany if necessary. Hitler refused to accept this view and devised a plan calling for a counter offensive which he intended would split the Allied forces, disrupt their advance on Germany, and perhaps unhinge the Anglo-American Alliance. With luck, this would stall the Allies long enough to bolster German warfighting capabilities with the so called "wonder weapons" just becoming available. Perhaps they might even sue for a separate peace so that Hitler could turn his full attentions towards the Soviets.[9] Mindful of the Allies' intelligence collection capabilities, Hitler insisted on tight security. Only the most trustworthy of his senior officers were

informed of the plan which called for an attack through the lightly defended Ardennes Forest and thence on to the strategic port of Antwerp. Orders to units were sent by courier, not radio, since the Germans knew of Allied signals intelligence efforts.[10] The deception plan was designed to fool the Allies into thinking that the Germans were reinforcing their western defensive lines. Troop movements conducted in daylight hours enhanced the deception of a defense in the west, while the most significant troop movements into attack positions in the Ardennes were conducted mostly under cover of darkness.[11]

Despite Hitler's attempts at complete security, Allied intelligence did obtain information that indicated an imminent attack through the Ardennes. German prisoners of war indicated that troop re-organizations and movements were geared towards an impending offensive.[12] Aerial reconnaissance detected large German armored forces staging near the Ardennes with a massive logistical effort exceeding the German divisions' requirements for the defense. While the Germans had been careful at limiting the use of radio traffic to disperse orders, enough radio traffic was intercepted by the Allies to confirm the interrogation reports and the aerial reconnaissance missions. Signals intelligence also indicated a large buildup of German air power poised in the Ardennes region,[13] which also indicated that an offensive was in the works. All of this information was in Allied hands by early December 1944 and indications of an imminent attack continued to roll in up until the 16th, the day the Germans launched 20 divisions through the Ardennes.

With all of these indicators in hand, the German attack still came as a complete surprise. Allied intelligence had correctly estimated that Germany could not sustain a renewed offensive and determined therefore that Hitler would remain on the defensive. In other words, they had mirrored-imaged Hitler, placing their own standards and biases as to the conduct of

war into their analysis of the German buildup, labeling it a strategic reserve and not a counter attack force. Since it was illogical, in their minds, to launch an unsustainable offensive, the Germans would never pursue such a radical option. What they failed to do was to take into consideration Hitler's personality and the precedents of his over-ruling his generals and ordering actions that defied standing military logic. Allied intelligence was adept at the technical end of the intelligence process, the gathering of information through reconnaissance and signals intercept, but had failed at the analytical end of the intelligence process.

Just as in war itself, intelligence is both an art and a science. Analysis relies as heavily on experience and imagination as it does on data. Hitler's deception efforts worked well because they targeted Allied preconceptions of what constituted prudent military operations. Standing on the defensive was logical in the sense of the scientific quantification of military operations, whereas the deception and counter offensive dwelt more in the realm of military art, something Allied intelligence did not have the imagination to see. Herein lies the crux of the problem in detecting a well orchestrated deception plan. Analytical bias and cognitive failures have been responsible for successful deception operations in the past and will continue to lead us to be surprised in the future. What then are the major analytical failures inherent in our intelligence system, and are there any ways to combat them?

III. CAUSES OF INTELLIGENCE FAILURES

Douglas Dearth refers to two major categories for intelligence failures. First there are the failures which result from the lack of or mismanagement of information. The resulting incomplete intelligence picture belongs to the "better collection school of thought." The

argument here is that intelligence failures are largely due to a lack of information. Thus, in the example from World War II, if the Allies had only had the *right* information, or had more efficient collection and production management of the information at hand, they would have drawn the proper conclusion. "Intensified collection efforts will yield less ambiguousness, uncertainty, and misperception."[14] Both the civilian and military intelligence communities have spent the last several decades improving the information collection process with new technologies and doctrine, attempting to move intelligence production towards a more automated process. The amount of data now available to modern analysts and commanders is daunting. Technological advancements at the tactical level lend themselves well to short time span missions, such as targeting and precision engagement. Technology benefits the operational and strategic levels by providing automated data bases which facilitate in-depth analysis. However, while it is irrefutable that the quantity of material has dramatically increased over the last decade, the quality of the analysis has not risen in equal proportion. The human element of the intelligence process has not evolved as far or as fast as the technological element. While the increase in data may in some instances have reduced uncertainty, it is by no means self evident that it has reduced misperception.

Perception is resident in the human mind, not a computer chip, and it is the source of the second school of intelligence failure, the "orthodox school."[15] Deception operations seek to influence the analysts', and the commanders' perceptions, preconceptions, inherent biases and so their decision-making processes. In the example of the Battle of the Bulge, the analysts' preconceptions about what was and was not logical in operational art blinded them to seeing that the Germans would launch a counter offensive. In such mirror imaging, the analysts simply decide the enemy will act a certain way because the analysts themselves would

take those actions. Such analysis does not necessarily take into account the opponent's past actions and is often a superficial judgment process indicative of a lack of experience in intelligence operations. Institutional or cultural bias can reinforce mirror imaging, as analysts place their own values into the actions of the opponent's and expects them to act accordingly.[16] A commander's bias can also have a negative impact on the intelligence analysis process since he can unduly influence the analysts' decision making process, steering them to a decision that fits the commanders' own interests. History provides us with many examples where a commander's influence molded the intelligence assessment into a course of action that fit his favorite operational plan.[17] Analysts themselves are not immune to disregarding alternative interpretations of data, and so arrive at an enemy course of action that fits their own "favorite scenario," one that they are comfortable with.

Preconceptions, unfortunately, are difficult to overcome and analysts can easily fall victim to them. Exacerbated by the military's high turnover of personnel, it is rare for analysts to become expert in any job they are doing until just about the time they are reassigned. This is especially so in the intelligence community. During the Cold War, military intelligence focused mainly on the threat from the Soviet Union. Even with the high turnover rate, analysts could still concentrate and "specialize" on a fairly steady threat model since the intelligence community as a whole was focused on it. Despite this dedication of effort, however, intelligence failures still occurred, the worst example of which was the geo-strategic failure to predict the downfall of the Soviet Union.

Even more uncertainty now confronts the military intelligence community with the end of the Cold War. U.S. national interests now force us to move from a dedicated focus on a single, Soviet threat to a broad view across an uncertain world where multiple threats are

less well known, or even undefined. High military turnover rates increase the uncertainty in analysis as intelligence personnel are moved from one theater to the next, each theater with a very different focus, each with a different threat or threats. The analyst therefore arrives with a set of preconceptions built up over the years and because of the operational tempo, is forced to start the analytical process with these preconceptions intact. If not given time to "learn the new target," to become familiar with the new threat environment, the chances for an analytical mistake increase.

IV. A SEPARATE COUNTER-DECEPTION CELL?

The intelligence community has made great strides in overcoming technological inadequacies by acquiring new information management tools and intelligence gathering systems. Information dominance of the battle space will go a long way toward assuring that ambiguities and uncertainties are significantly reduced. Analysts may have not only more data to work with, but higher quality data as well. The "better collection school of thought" has somewhat been addressed, but what about the "orthodox school of thought," the one that addresses itself to failures of thought, not collection management?

One proposal is to have a separate so-called "counter-deception cell" resident within the JTF J2 or the JIC. The cell's mission would be to examine the incoming data with a fresh approach, specifically working to identify possible enemy deception efforts. The counter-deception cell would have access to the same information as the existing analytical structure and would be manned with a sufficient number of personnel. Counter-deception cell analysts would not only be schooled in the organization, characteristics and nature of the threat, but

would also be knowledgeable of the characteristics and vulnerabilities of the collection assets available to the JTF J2/JIC. They would be conversant in deception techniques and would pay special attention to the targeted threat's deception capabilities and past utilization of deception. They would raise their concerns first to the JTF J2/JIC analysts concerned. Collection could be re-tasked to alleviate any ambiguity and/or the intelligence assessment could be modified to reflect an alternate enemy course of action. If the original estimate is published unchanged, the counter-deception cell would then raise their objections to the commander, ensuring a balanced view is provided. Such a cell, the embodiment of the "devils advocate" technique of intelligence production, has been a popular proposal in past intelligence structure reorganization.[18]

Such a scheme institutionalizes the deliberate challenging of every intelligence assessment, forcing the commander to weigh other possible enemy courses of action without the advocate being subjected to some form of punishment for "rocking the boat.[19] Proponents argue this technique would be used with a more narrow focus, detecting deception as opposed to formulating alternative courses of action or just arbitrarily challenging the J2's assessment. The counter-deception cell would not only have the power to task collection in support of confirming or denying a possible deception operation, but would also have the ability, in conjunction with the J3, to initiate some form of action which could confirm or deny a deception operation. If JTF forces made some sort of demonstration, for example, that would indicate to the deceiver that friendly forces had not received the deception message, the enemy might be induced to increase the deception signal thereby confirming the existence of a ruse.[20]

On the face of it, the counter-deception cell appears a viable option for the operational commander to improve the chances of detecting and exploiting enemy deception efforts. There are, however, some basic problems with the proposal which may make it prohibative to field. Resource constraints are the first serious obstacle. A new cell requires additional personnel to staff it since it is not practical to remove personnel from the existing JTF J2/JIC for the purpose. There is a shortage in all services of qualified intelligence personnel, one that is already being felt in all echelons of the intelligence community; strategic, operational and tactical. For example, military intelligence personnel retention in the U.S. Army is not high enough to meet requirements. Divisional tactical military intelligence battalions are currently being staffed at less than 80% of requirements in order to provide qualified personnel for higher priority assignments. I have already discussed how the nature of military intelligence personnel management makes it highly doubtful that a newly assigned analyst would have any experience with the regional threat, and would require "on the job training" to become familiar with an opponent's capabilities and methods. Defense Department budget constraints also make it unlikely that personnel assigned to a counter-deception cell would be afforded the luxury of attending residence schooling in deception techniques and so would have to learn "on the job." At least in the U.S. Army, Intelligence Corps personnel do not receive formalized training in deception techniques nor in any specific threat model, save for the generic threat model designed by the Threat Support Division at the Combined Arms Center, Fort Leavenworth, Kansas, which is primarily concerned with the ground maneuver of heavy and light combat forces.[21] Army intelligence personnel are also trained to utilize a litany of check-lists to facilitate intelligence analysis, all geared towards the tactical level. Only those select personnel who attend the Command and General Staff College (or its sister service

equivalents) or the Post Graduate Intelligence Program (PGIP),[22] receive any instruction in military art beyond the tactical level. Likewise, only at PGIP do intelligence personnel receive instruction on intelligence analysis beyond the tactical level. Fortunately, PGIP addresses the topic of intelligence and analytical failures. Unfortunately, attendance is limited to approximately 140 intelligence personnel per year drawn from all military services and civilian intelligence agencies. However, the graduation rate of PGIP students does not reflect the number of graduates in circulation due to the high attrition rate of intelligence personnel within the military. In short, the number of intelligence personnel who have received any institutionalized instruction on the very concepts that lead to intelligence failures and successful enemy deception efforts is minimal when compared to staffing requirements throughout the civilian and military communities. This has a direct impact on the staffing of J2s and JICs since PGIP is not a prerequisite for assignment to either.

Another obstacle to fielding a counter-deception cell is the very concept of a devil's advocate. The cell leader must guard against his analysts taking the "routine" approach towards counter-deception analysis. It is easy to fall into the trap of routinely challenging the JTF J2/JIC assessments, thereby creating animosity between the two analytical cells. If the J2 feels its every assessment is going to be challenged by an untouchable counter-deception cell, then a subconscious effort may arise to discredit the cell's efforts, thus allowing misperceptions to go unchallenged, resulting in a successful enemy deception effort. The concept of "routine" can also dilute the quality of the effort, especially if the counter-deception cell is focused on a threat that has not or is not in the habit of utilizing deception. The cell can become complacent, falling victim to a deception they were supposed to detect. There is also the threat of the "cry wolf" syndrome. If the deception cell routinely surfaces

doubt about the J2's estimate, or continually identifies possible enemy deceptions that do not materialize they will find their credibility on the wane, and no one will listen when the real deception hits. Conversely, the commander's perception of the validity of the intelligence could suffer should the counter-deception cell concur with the J2's estimate. This could lead to the commander incorrectly assuming that "...uncertainties have been resolved,"[23] thereby strengthening the J2's assessment, bringing it closer to the commander's perception of "ground truth."

Finally, the formation of a counter-deception cell does not necessarily remove the biases described earlier because the personnel assigned would come from the same background and institutions as the rest of the JTF J2/JIC staff, resulting in one biased cell double checking the assessments of another biased cell. The danger here is that an amplification of bias could result, increasing their susceptibility of the enemy's deception efforts.

V. COUNTER PROPOSAL

One can see that there are several reasons why a separate counter-deception cell within the JTF J2/JIC would not improve the chances of detecting enemy deception operations. The analytical pitfalls of running a sponsored "devil's advocate" section invite confusion and timidity on the part of the J2 and could jeopardize the fragile trust between "operators" and intelligence personnel. The problematic ability of the operational commander to staff such a cell given the shortages of intelligence personnel within the military and the ever increasing demand for operators of new C4I systems makes it unlikely that a separate

counter-deception cell could be resourced. How then, are we to address the issue of counter-deception? We can assume, not unreasonably, that it is inevitable that future adversaries will use deception operations to increase their combat power against U.S. forces given Whaley's results in his study of past deception operations where the advantage lies with the deceiver who, historically, has enjoyed a high rate of success. So what is to be done?

The JTF J2s and JICs already employ intelligence analysts who have the responsibility to provide reliable, timely intelligence products that must assess the likelihood of enemy deception. In other words, there already is a counter-deception cell at the operational level - it is the JTF J2/JIC! Intelligence analysts routinely question reports, scrutinize data, and re-task collection to confirm or deny suspicions. The JTF J2/JIC is already tasked with providing the operational commander with their best assessment of the enemy situation, deception plans included. The reasons for past failures to identify deception operations have already been addressed so the focus must be on how to improve the existing structure to conduct more effective counter-deception operations.

Fortunately, the first steps toward reducing uncertainty in the intelligence process have been taken as the intelligence community fields new technologies to collect and manage information. One can never eliminate uncertainty, but one can, through the use of improved collection, reduce uncertainty by providing a "clearer picture" of enemy activity. Non-human collectors have always provided the means to quantify enemy capabilities, but a quantitative analysis falls short in providing clues to an enemy's *intent.*[24] Improved collection and data management provide additional information to narrow the possibilities of "intent," allowing the analyst to make a more educated assessment thereby reducing the chance of being deceived. The U.S. has been engaged in a technological revolution over the last several years,

bringing to the intelligence and operational fields new systems of data collection and management which go a long way to removing ambiguity and uncertainty in the assessment process. Information dominance of the battlespace is clearly the answer to the "informational end" of the problem. Systems which eliminate intelligence stovepipes so that analysts, and commanders, can obtain the full range of available information to make independent assessments are becoming available for widest possible dissemination. Some of these systems will also interface with friendly operational systems, allowing intelligence analysts to better understand the friendly situation, helping to improve assessments concerning enemy intentions. A previous lack of J-G-N-S2/3 crosstalk has always been an obstacle to quality intelligence production, and with the inception of network-centric warfare,[25] we are finally reaching an era where cooperation will become the norm as opposed to the exception.

The danger lies in depending too much on technology to prevent intelligence failures. Already we have seen that these new automated systems are most efficient in obtaining and moving information within the intelligence community, so much so that the common complaint is that analysts are now overwhelmed by too much data.[26] The shear amount of data available today at the operational level only increases the noise level that an analyst must work through. Information overload increases the chances of being deceived.[27] Technology, if incorrectly managed or over relied upon, can become a facilitator of deception if the analysts are unable to identify the "wheat from the chaff" and fail to detect the enemy deception. Technology is vital, but is not the "silver bullet." We must also consider improving the analysts as well as the tools we give them.

Automated systems cannot "...evaluate information, develop intelligence requirements, task...assets, or produce intelligence. These remain the responsibilities of the *commander and*

his intelligence personnel (emphasis added)."[28] We have shown that the human connection, despite the dangers of cognitive failures and bias, is the key link in the intelligence process. Currently, the service intelligence training centers focus on producing tactical intelligence analysts. This is sufficient for initial assignments where junior officers and enlisted personnel must concern themselves with tactical level threats that operate in limited spheres of time and space where in-depth analysis is not required or practical. The service intelligence schools work on a system of checklists more geared toward the tactical environment. While students may receive instruction on strategic intelligence collection systems and agency missions, students are not educated in the finer shades of analysis nor are they required to think beyond the tactical fight.

The problem arises when these analysts are then assigned to operational or strategic billets after six years or more experience but without having been trained, or better yet, "educated," to "think" at the operational or strategic level. At the operational level the stakes are higher, and the need for more in-depth analysis and for "thought" is a magnitude beyond what is experienced at the tactical level. Selected intelligence analysts who attend PGIP, do, as part of a larger curriculum, receive instruction specifically devoted to the subject of intelligence analysis and warning. Cognitive failures are examined, bias is discussed, analytical methods are addressed, and most importantly, historical examples of intelligence failures are analyzed. Intelligence personnel who are assigned to operational and strategic positions should either attend PGIP or some similar joint intelligence program which addresses in-depth analysis and the operational commander's requirements.

In the area of specific counter-deception training, the Central Intelligence Agency, the National Defense University, and the Air Force Information Warfare Center all have courses

that include counter-deception training. Currently, an analyst must find scarce travel funds to attend one of these courses or have the command arrange for a mobile training team.[29] These courses should be examined as a framework for an operational level counter-deception course which can be produced on an interactive CD ROM and/or placed on the Joint Deployable Intelligence Support System (JDISS) so that the JTF J2/JIC personnel in the field can be trained by distance learning. It is imperative that the analytical techniques developed by these agencies be given wide distribution to analysts at the operational level. The material could also be used to form the basis of an elective course in counter-deception and intelligence warning at the staff and senior staff colleges and at PGIP.

Another area requiring improvement is theater familiarity. The lion's share of the analytical work is performed by commissioned officers of the various services. The services tend to manage their intelligence officers as a "one size fits all" commodity and expect them to succeed in any environment. While I am not advocating the view that intelligence officers should be so specialized that they are incapable of working outside of a discreet niche, I do feel that it is a mistake to arbitrarily reassign officers who, for example, have worked in units totally focused on the USCENTCOM mission and then suddenly send them to USSOUTHCOM and then wonder why they do not understand the target. Junior officers should be assigned to tactical intelligence positions within the same theater, gaining experience that they can rely upon later when they report to the JTF J2/JIC within the same theater for their operational level assignment. Junior officers with less than six years experience should not be sent to the JTF J2/JIC as they are often overwhelmed by the mission requirements and are ill equipped to make a useful contribution. Mid-career officers with institutional knowledge of an area or opponent are a key component of a successful

intelligence operation. Officers who mature and learn within a single theater environment will make a positive contribution to the operational intelligence effort as opposed to becoming unproductive or unwittingly producing inaccurate estimates because they are unfamiliar with the target. When there is no choice but to assign an officer "across boundaries," then the officer should receive the requisite schooling, en route, to ensure that the officer can at least hit the ground at a fast walk if not a run. The endless cycle of assigning officers to positions where it takes them a year to learn the mission and the target, a year to work the mission, and six months or so worrying about reassignment must stop. We cannot afford long lead times waiting for officers to become proficient through on the job training.

The responsibility of counter-deception does not, however, lie solely with the intelligence analyst. Ultimately, it is the commander who decides what course of action to take. While we do not need, nor is it practical, to train commanders to be full fledged intelligence analysts, we must equip them with a base understanding of the mechanisms for intelligence failures. The services have come a long way in familiarizing commanders with the capabilities of the intelligence community. Commanders must also be equipped with their own ability to sort through cognitive failures and biases in order to arrive at well thought out decisions. The service staff colleges and senior staff colleges must incorporate into their curriculum instruction that addresses analysis, cognitive failures, and counter-deception. In the Joint Maritime Operations (JMO) block of the College of Naval Command and Staff, there is one short reading on operational deception which only explains definitions and missions.[30] There is no mention of counter-deception, nor is the topic of analytical bias addressed during the Command Estimate Process of JMO. Commanders, just like analysts, come to the planning board with their own set of preconceptions and biases which can have a severe

impact on the conduct of an operation. As Richard Betts puts it, "operators have more influence in decision making but are less capable of unbiased interpretation of evidence because they have a vested interest in the success of their operations..."[31] If this is the case, we have an obligation to equip future commanders with the cognitive tools to not only detect deception, but to engage in a more rational decision making process. The staff colleges and senior staff colleges should include required readings on the pitfalls of cognitive failures and should ensure that instruction on intelligence operations paints a balanced picture of capabilities and limitations.

VI. CONCLUSION

Operational deception can be a valuable combat multiplier in war, and can be utilized the strong and weak adversaries alike, and historically, deception has a high chance for success. As the U.S. finds itself engaged in dealing with new and more varied threats, the operational commander and his analysts must be aware of the importance of counter-deception operations. While the concept of a dedicated counter-deception cell sounds like an effective remedy, we have seen that the cell has little likelihood of being properly staffed and resourced under current fiscal and manpower constraints. Nor does a counter-deception cell address the root cause of intelligence failure, namely, the lack of quality, educated, analysts. As one U.S. Army publication puts it, " notwithstanding the synergy possible with the power of ...technology, fog and friction will remain; the challenge of sorting out the signals from the noise amidst a mass of expanding data will also remain. Many solutions to the dilemma of uncertainty for the commander are technical. But there can be no *information revolution*

without the human influence and understanding of soldiers and commanders who link and integrate information, technology, and action."[32] Expert analysis is central to this revolution and to effective counter-deception operations. Operational commanders must insist that this standard be addressed by the service intelligence and personnel proponents. Every effort must be taken to properly educate, manage, and assign qualified intelligence officers to the JTF J2s/JICs if effective analysis and counter-deception operations are to become a reality.

NOTES

[1] Department of the Air Force, Information Operations (U.S. Air Force Doctrinal Document 2-5) (Washington D.C.: 1998), 17-18

[2] Major Timothy Smith, USAF, interview by author, 29 January 1999, U.S. Naval War College, Newport, R.I. Major Smith is currently working as part of a U.S. Naval War College team exploring the counter-deception cell proposal on behalf of the INSS.

[3] For the purposes of this paper, intelligence analysts are commissioned, warrant and non-commissioned officers unless otherwise specified.

[4] Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations (Joint Pub 2-0) (Washington, D.C.: May 1995), GL-6.

[5] Douglas H. Dearth, "Failure in Intelligence, Decision-Making and War," in Strategic Intelligence: Theory and Application eds Douglas H. Dearth and R. Thomas Goodden (Washington, D.C.: Defense Intelligence Agency, 1995), 185-6.

[6] Charles E. Burgdorf, An Appreciation for Vulnerability to Deception at the Operational Level. (Fort Leavenworth: School of Advanced Military Studies, U.S. Army Command and General Staff College, 1987), 4-6.

[7] Michael I. Handel, War, Strategy, and Intelligence. (London: Frank Cass and Company, 1989), 311.

[8] Barton Whaley, "Stratagem: Deception and Surprise in War, Vol I" (Unpublished Research Paper, Massachusetts Institute of Technology: 1969), 146.

[9] James L. Stokesbury, A Short History of World War II. (New York: William Morrow and Company, 1980), 352.

[10] Barton Whaley, "Strategem: Deception and Surprise in War, Vol **II**" (Unpublished Research Paper, Massachusetts Institute of Technology, 1969), A-426.

[11] Burgdorf, 10.

[12] Hugh M. Cole, The Ardennes: Battle of the Bulge (Washington DC: U.S. Army Center of Military History, 1993), 59-60.

[13] Charles B. MacDonald, A Time for Trumpets (New York: William Morrow and Company, 1985), 59-63.

[14] Dearth, 199.

[15] Ibid

[16] Michael I. Handle, "Intelligence and the Problem of Strategic Surprise" in Strategic Intelligence: Theory and Application eds Douglas H. Dearth and R. Thomas Goodden (Washington, D.C.: Defense Intelligence Agency, 1995), 232.

[17] Richard K. Betts, " Analysis, War and Decision: Why Intelligence Failures are Inevitable" in Strategic Intelligence: Theory and Application eds Douglas H. Dearth and R. Thomas Goodden (Washington, D.C.: Defense Intelligence Agency, 1995), 298.

[18] Handle, "Intelligence and the Problem of Strategic Surprise," 248.

[19] Ibid

[20] Katherine L. Herbig and Donald C. Daniel, "Strategic Military Deception" " in Strategic Intelligence: Theory and Application eds Douglas H. Dearth and R. Thomas Goodden (Washington, D.C.: Defense Intelligence Agency, 1995), 280.

[21] Department of the Army, Heavy Opposing Force Handbook (TRADOC PAM 350-16) (Fort Monroe: 1994). This manual is one of a series of generic threat doctrines created by the Threat Support Division, Fort Leavenworth, KS and published by HQ TRADOC.

[22] The Post Graduate Intelligence Program is a nine month graduate level course run by the Joint Military Intelligence College, part of the Defense Intelligence Agency. Students receive 30 semester hours of instruction on intelligence collection, analysis, production, indications and warning, strategy, and are afforded the opportunity to take electives on various regional, national or technical topics. A Masters of Science Degree is awarded upon successful completion of a thesis.

[23] Betts, 305.

[24] Germany with 3000 tanks attacked Russia, despite its 17,000+ tanks, in June 1941, achieving almost complete surprise.

[25] VADM Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare. Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, Volume 124, number 1, 32-33.

[26] Timothy B. Hendrickson and Major Michael G. Knapp, USAR, "Project Pathfinder: Breaking the Barriers to More Effective Intelligence Analysis." Military Intelligence, January-March 1996, 33.

[27] Michael I. Handle, "Intelligence and Deception," The Journal of Strategic Studies, March 1982, 154.

[28] Department of the Army, All-Source Analysis System and the Analysis and Control Element (FM 34-25-3) (Washington D.C.: 1995), 1-11.

[29] Smith, interview.

[30] Commander M.R. Critz, USN. "Operational Deception." (Unpublished Instructional Paper, U.S. Naval War College, Newport, R.I.: 1996.), 1-3.

[31] Betts, 298.

[32] Department of the Army, Information Operations (FM 100-6) (Washington D.C.: 1996), v.

BIBLIOGRAPHY

Betts, Richard K. " Analysis, War and Decision: Why Intelligence Failures are Inevitable" in Strategic Intelligence: Theory and Application. Edited by Douglas H. Dearth and R. Thomas Goodden. Washington, D.C.: Defense Intelligence Agency, 1995.

Burgdorf, Charles E. An Appreciation for Vulnerability to Deception at the Operational Level. Ft Leavenworth: School of Advanced Military Studies, U.S. Army Command and General Staff College, 1987.

Cebrowski, VADM Arthur K. and John J. Garstka, "Network-Centric Warfare. Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, Volume 124, number 1, 29-35.

Cole, Hugh M. The Ardennes: Battle of the Bulge Washington DC: U.S. Army Center of Military History, 1993.

Critz, M.R., Commander, USN. "Operational Deception." Unpublished Instructional Paper, U.S. Naval War College, Newport, R.I.: 1996.

Dearth, Douglas H. "Failure in Intelligence, Decision-Making and War," in Strategic Intelligence: Theory and Application. Edited by Douglas H. Dearth and R. Thomas Goodden. Washington D.C.: Defense Intelligence Agency, 1995.

Department of the Air Force, "Information Operations" (U.S. Air Force Doctrinal Document 2-5) Washington D.C.: 1998.

Department of the Army, All-Source Analysis System and the Analysis and Control Element (FM 34-25-3) Washington DC: 1995.

Department of the Army, Heavy Opposing Force Tactics Handbook (TRADOC PAM 350-16) Ft Monroe: 1994.

Department of the Army, Information Operations, (FM 100-6) Washington D.C.: 1996.

Handle, Michael I. "Intelligence and the Problem of Strategic Surprise" in Strategic Intelligence:Theory and Application. Edited by Douglas H. Dearth and R. Thomas Goodden. Washington, D.C.: Defense Intelligence Agency, 1995.

Handle, Michael I. "Intelligence and Deception," The Journal of Strategic Studies, March 1982, 122-154.

Handel, Michael I. War, Strategy, and Intelligence. London: Frank Cass and Company, 1989.

Hendrickson, Timothy B. and Major Michael G. Knapp, USAR, "Project Pathfinder: Breaking the Barriers to More Effective Intelligence Analysis." Military Intelligence, January-March 1996, 33-35, 50.

Herbig, Katherine L. and Donald C. Daniel, "Strategic Military Deception" " in Strategic Intelligence: Theory and Application Edited by Douglas H. Dearth and R. Thomas Goodden Washington, D.C.: Defense Intelligence Agency, 1995.

MacDonald, Charles B. A Time for Trumpets New York: William Morrow and Company, 1985.

Smith, Timothy, Major USAF. Interview by author, 29 January 1999, U.S. Naval War College, Newport, R.I.

Stokesbury, James L. A Short History of World War II. New York: William Morrow and Company, 1980.

U.S. Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations (Joint Pub (2-0) Washington, D.C.: May 1995.

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