AD-A252 756

DTIC
ELECTE
JUL 1 5 1992
S D
C

(2)

THE UNITED STATES NAVAL WAR COLLEGE
Newport, R.I.

THE OPERATIONAL USE OF INTELLIGENCE: WHAT TO AVOID

by

Michael R. Oakes
Major, USAF

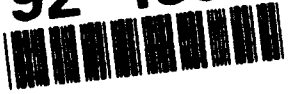
The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College, Department of the Navy or the Department of the Air Force.

Signature: Michael R. Oakes

14 April 1992

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

92-18337



92 7 13 060

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

5343 COPIER

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT DISTRIBUTION STATEMENT A: Approved for Public Release; distribution is unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION OPERATIONS DEPARTMENT 6b OFFICE SYMBOL (If applicable) C	7a NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) NAVAL WAR COLLEGE NEWPORT, RHODE ISLAND, 02841	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
The Operational Use of Intelligence: What to Avoid (U)

12. PERSONAL AUTHOR(S)
Michael R. Oakes, Major, USAF

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Final	FROM _____ TO _____	92 Apr 18	51

16. SUPPLEMENTARY NOTATION A paper submitted to the Faculty of the Naval War College in partial satisfaction of graduation requirements and to compete for essay awards. The contents of this paper reflect my own views.

17 COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Acquisition; Platforms; Analysis; Deception; Surprise

19. ABSTRACT (Continue on reverse if necessary and identify by block number) Military experience throughout history has had numerous examples of effective deception and surprise. Results of the surprise usually means destruction of military forces caught unaware. The reasons for the unawareness lies in a failure to heed intelligence information or incomplete analysis in the intelligence process. This paper looks at four areas of the intelligence process from an operator's perspective. Acquisition, Analysis, Dissemination, and Acceptance of Intelligence is examined while linking these areas to historical accounts from World War II and post World War II events/battles. These comparisons shed some light on areas where the intelligence process goes wrong. The goal of the paper is to examine the limitations of intelligence and make both operators and intelligence personnel wary of the problem areas. The intent is to make operators as well as intelligence personnel aware of areas that lead to traps and how either asking for, or providing the correct information will help military operations. It is not only important to understand what intelligence can do, but what it cannot do as well.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL CHAIRMAN, OPERATIONS DEPARTMENT	22b TELEPHONE (Include Area Code) (401) 841-3414 22c. OFFICE SYMBOL C

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

U.S. Government Printing Office 1988—520-812

343
COPIER

Abstract of

THE OPERATIONAL USE OF INTELLIGENCE: WHAT TO AVOID

Military experience throughout history has had numerous examples of effective deception and surprise. Results of the surprise usually means detruction of the military forces caught unaware. The reasons for the unawareness lies in a failure to heed intelligence information of incomplete analysis in the intelligence process. This paper looks at four areas of the intelligence process from an operator's perspective. Acquisition, Analysis, Dissemination and Acceptance of Intelligence is examined while linking these areas to historical accounts of World War II and post World War II battles. The comparisons shed some light on where the intelligence process goes wrong. The goal of the paper is to examine the limitations of intelligence and make both operators and intelligence personnel wary of the problem areas. Not only is it important to understand what intelligence can do, but what it cannot do as well.

DTIC
COPY
INSPECTED
4

Accession For
NTIS GRA&I ☑
DTIC TAB ☐
Unannounced ☐
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A-1

5343 COPIES

TABLE OF CONTENTS

343
COPIER

Chapter 1

INTRODUCTION

The operational use of intelligence is encumbered with numerous misconceptions. Experience shows a great many commanders know enough about intelligence to ask questions on enemy order of battle, but little about the process undertaken to evaluate his questions and prepare the responses. The answers are obviously needed to continue a campaign or initiate planning for contingencies. When a commander loses confidence in his own intelligence staff, he will use other means to get his answers and decide on courses of action. Loss of confidence is caused through incorrect or ambiguous intelligence information. A commander may search for different information regardless of the efficiency of his intelligence staff if he does not understand its presentation, the information is controversial, or if the commander is reluctant to accept new methods and continues to work with outdated practices.

If you ask a person what he can do, he will tell you his capabilities, not his limitations. This fact is just as true in the intelligence process. To examine the intelligence process and how it can be misinterpreted in the world of operations is a tall order. In this paper, for every paragraph, there could be a chapter. For every chapter, there could be a book. Thankfully, this did not become a book. However, the discussion method here uses historical cases to examine the intelligence process. This examination is a beginning to learn some of the pitfalls associated with intelligence as it is used (or not used) by warfighters. The intent is to have not only a better understanding of what intelligence can do (capabilities), but what it cannot do (limitations).

Background

Interwoven within each level of war is the support system which keeps the machine operating. Intelligence is one of the staff support functions, which iterative in nature, derives and

5343
COPIER

disseminates information, from and to all the levels of war. What is discussed in the following chapters are examples of intelligence used by warfighters at the operational level of war. The operational level of warfare is an area where military leaders have placed a renewed interest. There is nothing new to the operational level, other than rebuilding lessons or practices which have been somewhat dormant since the Korean War. The operational level remains the link from the grand strategy of the nation to the tactical execution in the field.

"Operational art is the employment of military forces to attain strategic goals in a theater of war or theater of operation. ... Operational art thus involves fundamental decisions about when and where to fight and whether to accept or decline battle."[1] If the intelligence staff supports the operational commander, then operational intelligence must satisfy his needs for information and analysis on the enemy. The operational level of war dictates the methods and means necessary to accomplish the ends of attaining strategic goals. These strategic goals can range from the defeat of an armed force and the industrial complex to stabilization and free elections to eliminating religious or human rights restrictions. Strategic goals overlap the operational goals when the use of military force is needed for the ultimate victory, war termination and subsequent peace. It takes information to achieve these goals and the who, where, what, when, and how much questions concerning enemy capabilities and possible courses of action are answered by intelligence.

In his famed book <u>On War</u>, Carl von Clausewitz eloquently stated:

> By intelligence we mean every sort of information about the enemy and his country-the basis, in short, of our own plans and operations. If we consider the actual basis of this information, how unreliable and transient it is, we soon realize that war is a flimsy structure that can easily collapse and bury us in ruins. The textbooks agree, of course, that we should only believe reliable intelligence, and should never cease to be suspicious, but what is the use of such

343 COPIER

> feeble maxims? They belong to that wisdom which for want of anything better scribblers of systems and compendia resort to when they run out of ideas.
>
> Many intelligence reports in war are contradictory; even more are false, and most are uncertain.[2]

There have probably been a few commanders who felt the same way about intelligence as Clausewitz. But his interpretation of intelligence is focused more on the tactical level of war, where maneuver of forces makes the information more perishable. Clausewitz was probably correct about the uncertainty of information at any level of war. His assumptions were undoubtedly founded on the information and sources available to commanders of his age. However, today's battlefield or theater of operations consists of numerous intelligence platforms able to collect a wide variety of information about the enemy. How intelligence information is processed and used determines whether Clausewitz would still be correct today.

The methods for compiling information for tactical employment to attaining strategic goals is very well defined. Intelligence covers the entire spectrum of a warfighter. The degree of information needed at each level of war varies with each customer. Each service or particular unit has different missions and views of its impact in the operational level of war. The difference with each organization is the time variable associated with their applications of force. Time as it relates to speed and distance pose different problems and each commander must evaluate intelligence as it applies to the area his forces must cover (i.e. an infantry battalion 20 miles per day, CVBG 25 Knots per hour, and a fighter formation travelling 500 miles in an hour). Generally, operational intelligence covers a wide, long term view of the theater and the campaign. However, intelligence used in all levels may be the same information applied to different missions and individual capabilities; the Commander needs certain data for planning and reaction(s) to the enemy; the line pilot or soldier only cares who is shooting at him. Intelligence must be responsive and reactive in order to

5343
COPIER

be effective.

Intelligence plays a vital role in all levels of war, but it is more than just knowledge, it is an understanding of the forces in conflict, how they operate, and how reactions from each effect the outcome. Ideally, intelligence should be tailored in the Sun Tzu image where he advises:

> Know the enemy and know yourself; in a hundred battles you will never be in peril.
> When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal.
> If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.[3]

Intelligence needs to be tuned to the commander's intent as well as the campaign operations underway. An intelligence staff, aware of friendly forces and plans, assist a commander to determine how the enemy will react (or is reacting) to applications of force.

This paper uses examples where intelligence data was erroneous, neglected or disregarded during leadership decisions concerning wartime operations. The case studies selected for this paper are from WW II and later to accentuate problems faced today. However, a look into antiquity may show us that lessons then still apply today. If so, what did Aristotle teach Alexander the Great? If one takes a close look at Alexander's campaigns, we see that he was arguably one of the best soldiers and commanders in recorded history. Where then has all the foreknowledge between operations and intelligence gone?

The following chapters provide the underpinnings to show how intelligence information is derived and how its use or misuse determines the net effect over the course of battle.

343 COPIER

Chapter 2

ACQUISITION

Intelligence is most likely viewed as an alphabet soup of "INTs". It is these different disciplines in the intelligence community where information is collected. The beginnings of the intelligence process start with IMINT, SIGINT, HUMINT and a host of others necessary to meet the needs of the warfighter. Management of the different disciplines within intelligence is accomplished through prioritization needed at each level of war. At the operational level, collection of information begins with Essential Elements of Information (EEIs). EEIs can help the commander shape his theater by defining the enemy centers of gravity. Whether or not an EEI can be satisfied will often determine when a particular course of action can be pursued. These EEIs assist the intelligence community to focus collection sources on warfighter priorities in preparation of, or conduct in, an operation.

Technical Acquisition

Misconceptions in intelligence usually start forming when the discussion drifts towards assets available for intelligence collection. These misconceptions not only deal with capabilities but availability. Both areas should concern planners since much of the intelligence needed to determine courses of action are based on the collection assets. The United States has devoted much of its intelligence collection effort with technical means manipulated from the country's lead in technology. But even technology has limits, though seldom fully advertised.

Weaknesses in certain technology dependent systems may not be based on the degree of accuracy but on the field of regard for that system. For example, many of the U.S. satellites used for reconnaissance are lauded to have the capability to see a pack of cigarettes. However, what is not really discussed is the degree of difficulty looking for the pack of cigarettes through

5343 COPIER

a soda straw (small field of regard) at a distance of over 200 miles. "A common myth is that a satellite can be 'parked' over any desired location on the globe to provide continuous coverage or that they can be moved with relative ease."[1] Without getting into orbital mechanics and quantum physics, we will just agree that it is a myth and to move a satellite flight path requires an expenditure of energy, which in turn effects a satellite's lifetime in space.

Other airbreathing (ground and air) collection platforms assist the intelligence community with collection in the photographic, electronic, radar, or infrared spectrums. These platforms help determine enemy capabilities and intentions through recorded movements and location of forces.

The Army's method for Intelligence Preparation of the Battlefield (IPB) considers different elements of Mission, Enemy, Terrain, Troops available, and Time (METT-T) provides a beginning framework for ongoing data collection and analysis done at the tactical and operational level. IPB is easily carried into the Commander's estimate of the situation with the similar considerations. The intelligence staff must understand commander's intent and how he intends to defeat the enemy based on resources at hand. Once intent is resolved, then intelligence proceeds to tailor the intelligence product to fit the commander's needs.

HUMINT

This section should really discuss the lack of HUMINT versus the use of it. HUMINT is a vital area that has been severely neglected in the overall American intelligence community. The military continues to support HUMINT with Special Forces personnel to help meet the operational needs. The United States as well as other western countries tend to replace HUMINT with technical means of intelligence collection.

HUMINT is not just what is seen on James Bond movies. HUMINT comes in the form of refugee and Prisoner of War (PW) interrogations, collected documents (both open and closed source), special operations unit reports/surveys to determine

6343 COPIES

terrain, beach conditions or other invasion plan factors, or even Military Attaches and their contacts.

> The present policy in U.S. intelligence circles is to downgrade the value of HUMINT relative to other means of obtaining technical and scientific intelligence. This attitude must change for two reasons. First, the aggregate of other means of obtaining information is decreasing. That does not mean that other means are not more important than HUMINT at this time, but there is a trend away from those means, and we cannot foresee the end of it. Second, opportunities for obtaining HUMINT are increasing with the opening of Eastern Bloc societies and the collapse of the Soviet Union.[2]

A classic example of the value of HUMINT and the apparent lack of interest in American intelligence circles is the comparison between the Falklands War and the Invasion of Grenada. In both cases, Great Britain and the United States had extremely limited information on the facilities or terrain where they intended to operate. The British interviewed numerous people who had lived on or just returned from the Falkland Islands, while the United States failed to contemplate this source of information and attempted to obtain non-existent Defense Mapping Agency (DMA) charts.

Another example of HUMINT use occurred during the initial phase of Desert Shield. There was a lack of information regarding the numerous "gray" weapons and weapons platforms the Iraqis possessed. Attempts to obtain this information through official channels fell far short of anticipations. In one case, the Mirage F-1 EQ variant, the intelligence community (upon the insistence of service operators) consulted with some American pilots just returning from France where they completed test pilot school in the Mirage F-1 EQ. Where a lack of data is present, there is an innate tendency to go it alone and use SIGINT when direct access or HUMINT may work. Had the United States not pursued HUMINT for this case, many of the wartime modes on the Mirage would have not been known prior to the initiation of hostilities.

Former Deputy DCI, Admiral Bobby Inmann stated in an interview in July 1982: "There was a period of time when

5343 COPIER

decision makers believed that satellite photography was going to answer all our needs." No analyst should be left dependent on a single means of acquiring intelligence. Human collection runs the risk of relying on someone who wants to mislead you (e.g. Ultra and the Double Cross [XX] System). Using only technical collection means may leave you without access to certain bits of information needed to corroborate or confirm enemy capabilities and intentions. "It is quite clear that all systems of collection, ranging from newspapers, radio, and television, academic reports and studies, business and embassy reporting, and extending to technical and human source reporting on the clandestine side are important and potentially useful."[3]

Intelligence Fusion

Critical items of intelligence are collected using EEIs to establish priority. Once collected, the information is normally fed into an intelligence center for analysis. However, at times, due to the volume of incoming information, many intelligence centers are overwhelmed with data (drinking from a fire hose) and have little time to sift out pertinent raw details before specifics must be forwarded for distillation and reporting. Depending on the time line involved, much information goes unused or even worse added to the increasing backlog of other existing information. Piling up data without attempting analysis confuses issues with ambiguities.

A good example of excessive data pile-up occurred during Desert Storm. In this case, ELINT cuts for surface-to-air-missile (SAMs) sites were not removed by the CENTCOM intelligence staffs until positive verification was received on their destruction. Although, many pilots reported the SAMs as being destroyed, intelligence maintained their own files for mission planning and waited for SIGINT or IMINT to verify the SAM destruction. A review of the compiled intelligence summaries and threat update from CENTAF and CENTCOM intelligence staffs from 30 Dec 90 through 28 Feb 91 highlighted these discrepancies. The result of the information overload was the Iraqis had 25% more SAMs after three weeks of the Air Campaign.

5343
COPIER

The results of the ambiguous data reported by intelligence was that both naval and land based pilots ignored those order of battle summaries. Instead, the tactical units started with the original CENTCOM threat baseline and used their own unit daily mission reports and debriefs to create a more timely update with accurate data.

Not having enough data can be as bad as an enormous overload of information. An example of insufficient information occurred in the Yom Kippur War. Israel was poor in its intelligence collection capability against the Egyptians once the war began. They lacked an effective ELINT and SIGINT capability and relied on the collection and analysis from conflicting views of their ground commanders.

> . . . (they) lacked the sophisticated intelligence sensors, processing, and analysis capability to analyze a dynamic threat. . .The system only really worked against fixed defenses and SAM sites, and even here the Israeli Defense Force (IDF) lacked an effective fusion capability to blend ELINT and PHOINT. In several cases, SAM defenses were assumed to be absent because photos failed to show SA-6 deployments, although these had been detected by ELINT.[4]

Wartime intelligence collection needs to be responsive to changing battlefield conditions to meet the needs of the commander. Things happen much more quickly in combat and there is no luxury to take time out and conduct a one or two-year study to determine where the enemy will hit you next. Information needs a reasonable refresh rate to be updated, if not, then it needs to be discarded. "Some things remain hidden not because they cannot be detected but because they cannot be detected soon enough. These considerations should temper the confidence of some observers that 'new technologies'. . . will help the United States overcome Soviet efforts to deceive Western spy satellites."[5] Quite often, the question of when something might be knowable is as important as whether it is knowable. A late answer maybe useless!

Knowledge of friendly capabilities has always been a weak

5343 COPIER

point for the intelligence community since their effort is logically aimed at the threat. However, Desert Shield/Desert Storm showed us that the "gray" and even "blue" systems are a threat to our own forces through either weapons sales or capture. The ability to compare and contrast enemy weapons capabilities to that of our own is necessary in order to help friendly forces assimilate the data better. Most intelligence officers are used to reporting and testing specific areas of enemy weapons/weapons platforms versus U.S. capabilities. They are not in the habit of collecting a lot of data on friendly systems.

Finally, EEIs need a definite priority development and maintenance. It is the commanders responsibility to develop the EEIs and ensure they are updated as the battlefield situation or air picture changes. If collection is useful, it has to be based on the process and plans/assessments of the threat we are facing. The intelligence community needs a close organization and a planned approach to investigate all information disciplines then fuse and corroborate the intelligence information.

Vulnerabilities of Collection Platforms

As there has never been a weapons platform or weapon which could not be defeated, there also has never been a system in the intelligence field that could not be deceived. The degree of deception depends upon the either the technical capability of the system or exploiting the people using the system. Deception as well as countermeasures can be developed for any SIGINT or IMINT platform. What one country develops and uses against an adversary can potentially be used against itself. Take for example the use of chaff during WW II. In order to counter the German early warning radars, the British developed strips of metal reflectors to be dropped and mask the air attack by making false radar returns. While chaff ("window" is the British term) was determined to be effective, its use was opposed since it may tip the Germans and allow their development and subsequent use against British radars. According to R.V. Jones, chaff use

343
COPIER

turned into a debate with a "bridge on the River Kwai attitude towards radar, and it hurt ... to think of radar being neutralized, even German radar."[4] Other Electronic Counter Measures (ECM) can be developed once a specific signature of the collection platform has been determined (e.g. radar, infrared, etc.). For other SIGINT collectors, false signal generators or weapons platform emulators provide the enemy with numerous ways to deceive and mislead friendly forces in their intelligence collection attempts.

Collection platforms (including satellites) are also susceptible to attack. Elimination of a platform can greatly inhibit collecting intelligence since there may be no replacements in the near or long term. The lack of a U.S. satellite surge launch capability is a prime example where loss of overhead satellites could not be replaced in the near term due to a lack of launch vehicles and certain satellites. A good long term example would be the potential loss of a J-STARS aircraft during Desert Storm. Since there were only two in existence and both in the development stage, Iraqi destruction of either of the aircraft would have severely hampered if not cancelled the program. Backup systems/platforms must be available in order to keep up with the information requirements of the warfighters. Training for wartime operations should include capabilities to fight a war where conventional platforms may be hurt, damaged, destroyed or eliminated.

Finally, hostile satellite tracking is normally accomplished day-to-day, peacetime or wartime whether within a CVBG or in any other tactical unit. This tracking capability needs to remain in intelligence collection process and used in operational planning. Our ability to easily predict adversary satellite overflight (orbital mechanics), enables us to move or hide troop concentrations, aircraft, ships, and equipment. Accurate hostile satellite overflight predictions coupled with emissions control (EMCON) procedures or some form or camouflage cover and decoy (CCD) help enhance security to friendly forces and guard their capabilities and intentions.

343
COPIER

Technical means of intelligence should be used for collection of technical requirements such as: order of battle, technical capabilities, and force depositions. The HUMINT system must be improved and targeted primarily at "soft" information such as intentions. This does not preclude the 007 type of espionage to acquire technical documents, war plans or even the use of HUMINT collectors (special operations) to determine order of battle. Each part of the intelligence collection system should be used within its known limitations and correlated to other sensors. A good example is using national intelligence means for cueing and theater or tactical assets to focus. The bottom line is no single system of intelligence collection is adequate. All complement one another and are subject to certain time variables. If the information collected exceeds the time where it could direct actions against the enemy, then that intelligence becomes useless. The goal for an economy of effort is to collect and disseminate the information before it becomes perishable.

5343 COPIER

Chapter 3

ANALYSIS

Intelligence Analysis may be a misnomer since it should not necessarily be a dissection of information as Webster defines it, but a fusion of pertinent data from which to draw conclusions. The main functions of the intelligence community is to collect, analyze, and disseminate information on potential threats. Presumably, the purpose of this effort is to inform and enlighten leaders in order to make decisions. The intelligence analysis is the starting point to make those decisions by predicting possible enemy courses of action. However, there are as many pitfalls in the analysis process as any where else. In a perfect world, analysis would be conducted without any outside interference or distractions so as to achieve a dispassionate view of a problem or situation. This is not a perfect world and intelligence analysis is effected by a myriad of factors as cultural backgrounds, education and experience in problem solving, organizational makeup, etc. This chapter will discuss many of the major areas which effect intelligence analysis and show examples where the process was led astray.

Capabilities Versus Intentions

The first area to discuss is the argument on what type of data to present: Capabilities or intentions. Normally, a commander will want to know what the enemy is doing and how he is reacting and the effect friendly actions have on that foe. Basically the difference is summed up by:

Capabilities	What can the enemy do?
Intentions	What will the enemy do?

Capabilities are somewhat scientific and tend to remain stable. For the planner, capabilities provide the easiest platform or starting point for planning.

Intentions show the determination a nation has to use the

343
COPIER

force it assembles. A nation's intentions are determined by its cultural background, principles, national policy objectives and even the personality of the national leadership. Individual leadership may direct military action long before the nation is willing for such combat. Intentions are generally left alone since they may require "inside" intelligence information (HUMINT). Areas where intentions can be defined are through examination of what the enemy is doing and not what he is saying. Sometimes what a nation says is not really what it intends. Is the nation talking of peace and detente while mobilizing forces?

Intelligence for the operational and tactical level of war deals more with the tangible and quantifiable information on capabilities. However, it is not limited to just a need for "concrete" evidence on order of battle (troops, missiles, planes, etc.). Both troop numbers and placement, and any logistics information identifying enemy lines of communication are carried in the capabilities category. Intentions of the enemy can vary as to the willingness of the enemy to attack and with what type of weapons. But somewhere in the definition of capabilities, there must be some sort of analysis on the training level of the enemy, readiness, morale, and even who is leading their organization to give a more complete picture.

The goal of intelligence is to estimate the threat as accurately as possible. However, many times in the absence of accurate information, the analyst (and the commander) estimates the threat higher in order to ensure sufficient friendly forces and material are available to undertake operations. Typically, an error is made on the high side in order to increase the safety margin.

Whether or not intelligence agencies can predict intentions, depends on the type of information being collated into the analysis process. For example, if COMINT or HUMINT produced a message or plan directing an attack, then that would be a hard fact outlining an intention to attack. Using this information and corroborating it with some other source of intelligence

343 COPIER

showing troop movement(s), a logical conclusion could be drawn that an attack was eminent.

The U.S. military typically bases its enemy estimates on the capability end of the spectrum. The rationale may be due to our experiences in war and as a result of the times when we were surprised by analyzing intentions. A classic example in American history where estimating enemy intentions resulted in surprise is Pearl Harbor.

> There was no doubt before the attack that the Japanese were capable of launching aircraft from carriers against Pearl Harbor.. This capability was ignored in the firm belief that the Japanese would strike first with saboteurs and submarines. The result was faulty deployment of U.S. forces - a deployment against an estimate of what the Japanese intended to do and not against what they were capable of doing.[1]

To be conservative, a commander executing his plan based on capabilities tends to protect himself against surprise. If estimates and planning are based on unsubstantiated intentions, then it requires the enemy to stick to "your" plan and not make any mistakes to be successful. If we believe our good friend Carl von Clausewitz, then war is full of uncertainty and chance; therefore our planning should be based on enemy capabilities and not intentions. Using the chicken and the egg argument, we would argue that the chicken came first since it represents actuality (capabilities) and the egg represents potentiality (intentions). Logically, actuality always takes precedence over potentiality. Finally, a commander (with the help of intelligence) may tend to overestimate enemy strengths to justify larger amount of friendly troops. Troops and equipment held in reserve not only assist in a breakthrough, they provide the commander a hedge against surprise. The fine line is to determine the right amount of hedging without sacrificing economy of force and efforts in other areas.

Failure to analyze enemy intentions whenever possible is equally damaging to operational planning and execution. Intelligence analysis needs not only to consider the order of

5343 COPIER

battle and capabilities information, it needs to know and pass on how the enemy will use forces, methods of attack, and the conducts of daily operations to determine what vulnerabilities to exploit.

A vulnerability is the determination of a breaking point or points where the enemy has key areas that define his Center of Gravity (COG). Attacking the COG should reduce the enemy's will to fight and force him to terminate hostilities. This is not always true as it goes back to the discussion of intentions. War termination is not as clear cut as we would like to think. When national survival is at stake, conflicting cultures, or unreasonable leadership is involved, then attacking the COG may not effect an end to hostilities. Sometimes determination of a COG is based on impressions of our own needs for operation and what would force us to stop a conflict. Examples of incorrect COGs are the strategic bombing campaigns against Germany in WW II and Vietnam.

It is important to digress a moment and consider how much analysis or problem solving training is accomplished through formal education (civilian or military). The intelligence community accomplishes its analysis by sifting through reams and reams of paper to get facts and insuring proper documentation. The conclusions drawn from this documentation is usually a summary of regurgitated facts and not analysis. Regurgitation is highlighted in many intelligence centers' measure of effectiveness for reporting based not on the quality of information, but quantity. The ability to look at both sides of an argument needs to be ingrained in all forms of military education. Without this type of analysis, how are we expected to evaluate the future and develop comprehensive conclusions?

Ambiguity

There is a tendency in the analysis process to over caveat with uncertainties. The uncertainties yielded serve no purpose other than an evironmental impact on the number of trees killed in the world to produce worthless paper. The weatherman's approach to intelligence, tends to make predictions without

343
COPIER

conveying an accurate forecast. Covering all possibilities by watering down analysis so as to not be wrong regardless of the outcome is a great disservice and provides little assistance to a commander. Whenever possible, uncertainties must be bounded by trends. These bounds provide the warfighter the necessary tools to evaluate risks and decide on course(s) of action.

Ambiguity is used to legitimize different interpretations of data. Intelligence agencies must be able to quantify their analysis with raw data. Leadership demands much from the intelligence community and needs to remain open-minded, whether receiving good or bad news. Intelligence analysts must be allowed to present reports without the threat or penalty of "careericide." If an analyst hedges his report to meet the desires of his superiors, then he is self-defeating and false to his profession.

Mirror Imaging

There is a tendency in any analysis to base conclusions on what the investigator (intelligence officer) knows best; his own background. Different habit patterns, values, and education of an enemy or a potential adversary are sometimes overlooked in an intelligence analysis. Basing the intentions of an adversary on your own views is best called mirror imaging.

History shows mirror imaging as one of the easiest traps that drives poor analysis and results in destructive final outcomes. Surprise attack and destruction of military forces is the payment for analysis with incorrect mirror imaging. Mirror imaging goes beyond comparing our rifles to theirs or our marksmen to the enemy sharpshooters. Mirror imaging gives the euphoric effect you understand what the enemy is thinking because of what you would do if presented with the same situation.

Mirror imaging is more damaging when it only considers actions based on rational behavior (or what you interpret as rational). Rational thought process is good only if you deal with rational leaders. Cultural differences combined with a tyrannical and despotic leader exacerbates the problem

343
COPIER

immensely. Arguably, the largest difference between cultures is when East meets West. The quality and value placed on life can be very diverse. These factors play greatly on the determination on what the enemy might do. Some examples of mirror imaging are the battle for Okinawa in WW II, and the Chinese Intervention in the Korean War. Each of these wars provide a case where mirror imaging analysis led to a military failure and waste of resources.

The Battle for Okinawa

Both Plan Orange and the subsequent Rainbow Plans could not have foreseen the use of Kamikazes in Okinawa. The incredible self-sacrificing of life was not played in any of the hundreds of war games at the Naval War College. The Japanese decision "to adopt organized suicide tactics had been made in a matter of minutes, though the psychological groundwork had been laid during many centuries."[2] The Kamikazes made their debut during operations in the Lingayen Gulf, but the reality of their existence and biggest impact was felt in the Battle for Okinawa. Over 1100 Kamikazes were used against American ships. Over 50 raids of 100 planes or more were flown against naval forces in and around the Kurile Islands. In all, Kamikaze attacks inflicted damage "on at least 300 Allied ships of which about forty were sunk. In achieving this, some 2,000 Japanese pilots and planes were destroyed."[3] The number of Japanese planes lost compared to the damage inflicted to Allied forces is taken into account, the Kamikaze threat was not as severe as the Japanese had thought in material costs. However, the Kamikaze was supposed to also show Americans the unwavering Japanese military fighting spirit and devotion to the Emperor. The serious nature of the threat to naval forces was diminished "because supremacy in the air and in the sea had already been gained by the invading forces."[4] It should be noted, Japanese military leaders also suffered from their own mirror imaging with consensus of the leadership thinking the Kamikazes would give them a psychological edge. "Japan's military leaders convinced

5343 COPIER

themselves that their enemy would be daunted by the spiritual strength of the Kamikaze. As it turned out, they grossly misjudged American reactions and overestimated the effect of the Kamikaze and other suicide weapons."[5] Japanese cultural differences were not widely understood until Ruth Benedict finished her anthropological study and published The Chrysanthemum and the Sword shortly after WW II.

The Korean War and the Chinese Intervention

Many have argued the United States and UN missed many signals from the Chinese stating their intent to intervene in the Korean War. Whether or not this is true, the more important point is to discuss the U.S. perceptions on fighting the Chinese if they entered the war.

There is good evidence to show that U.S. intelligence had an accurate picture of the Chinese massing along the Yalu River. However, what was missing from the analysis were the objectives of the Chinese, the actual characteristics of the People's Liberation Army (PLA) and how they would employ. Many believed that the Chinese were concerned about protecting the hydroelectric plants along the Yalu River. Little did we realize that the Chinese were more concerned about having a united Korea under democratic rule along their borders. Coupled with the fact that the U.S. and South Korean supported the Nationalist Chinese on Formosa, should have changed many opinions throughout the intelligence community. Gen MacArthur took mirror imaging one step further in his analysis on possible courses of action in the event of a Chinese intervention. Gen MacArthur told President Truman at Wake Island on 15 Oct 1950: "Now that we have bases for our Air Force in Korea, if the Chinese tried to get down to Pyongyang there would be the greatest slaughter."[6] True, if Air Power is applied correctly, it can be decisive. However, General MacArthur's faith was based more on what he thought airpower could do to a force like the North Korean People's Army (NKPA) he had just defeated, not the Chinese PLA. The Chinese were not dependent on using roads or heavy vehicles. In fact, their methods of infiltration

5343 COPIER

puzzled U.S. intelligence estimates. Intelligence underestimated the number of Chinese infiltrators and considered the differences between the NKPA and the PLA in material strength. They did not apply those differences to the way Mao had trained his armies to live off the land. Based on lack of materials in the PLA, intelligence assumed them to be like the NKPA, but much more inferior.

Unfortunately, intelligence analysis can sometimes be compared to the old adage where a drunkard drops a coin and searches for it underneath the lamp post and not where he dropped it. Intelligence, only searching for answers under the light (mirror imaging), and not where the coin fell, does not produce the truth nor the coin.

At the operational level of war, mirror imaging can lead to a misunderstanding of the enemy's doctrine of war. By assuming the enemy will use his weapons as we use ours, may lead a commander to misallocate resources. A more recent example of this type of mirror imaging which effects weapons development is:

> In the 1970s, U.S. analysts assumed that Soviet submarines would sally forth to attack U.S. lines of communication (LOC) across the Atlantic as the U.S. did to Japan in WW II. Only gradually did it become clear that the Soviets had a different operational concept for their attack submarines. Instead of attacking American LOCs, the Soviets used their attack submarines to protect bastions in which the Soviet ballistic missile submarine fleet could ride out a prolonged war as a secure strategic reserve force.[7]

Politics.

Unfortunately, politics play a very large role in the intelligence process. In this instance, we are not talking about constitutional rights to vote. On the contrary, politics is interference in the intelligence process by altering or using information to suit desires or needs of an individual or interest group. These desires are anything from the budgetary process to diplomatic negotiations. Most military purists agree in theory that intelligence should be devoid of outside

343
COPIER

interference to remain totally objective. However, when we return from Wonderland, we realize this is not so. Michael Handel describes a very good example of the politization of intelligence.

> In 1967, although data concerning the order of battle of the North Vietnamese and Viet Cong forces in South Vietnam were rather ambiguous, military intelligence consistently underestimated the size of the anti-government forces. In trying to demonstrate the efficiency of the United States armed forces operations, they provided proof of the decline in enemy capabilities, which created an optimistic atmosphere that the President welcomed as a vindication of his Vietnam policy. President Johnson preferred the optimistic estimates of the Joint Chiefs and resented what he saw as carping by the CIA that upset the delicate process of consensus-building. Although the evidence concerning the war in Vietnam had grown more pessimistic by 1967, there were always enough ambiguous reports form Vietnam which the President's "intelligence waiter" - his National Security adviser Walt Rostow - could use to present Johnson with his favorite sugar-coated dish of good news.•

Competitive Analysis

It is important to consider the effects of one point of view versus multiple opinions in the analysis process. Without going into a lengthy dissertation on the problems of group think or other psychological phenomena, problem solving and the intelligence process effect the information that may be given to the commander. The decisions made may or may not be affected by the competitive process; it depends on the individual leader.

A commander's desire to have one voice from the intelligence community is apparent in the frustrations suffered during the first days of Desert Shield. Each intelligence agency, including the service component staffs, presented a variation of the threat (capabilities and intentions) based on their background and information available to each. The net result was each agency had differing views as diverse as the organization they represented. With all of the groups involved, there was no concrete analysis upon which to make any decision other than to go find out more information. Certainly,

343
COPIER

excessive points of view can create a noise level sufficient to hide the answers to the questions. Commanders should demand one clear, concise point of view backed up with raw data. On the other hand, one agency cannot or should not monopolize the analysis of the mountains of information received. One point of view does not eliminate the need for different opinions or analyses available to answer the commander's questions. However, multiple conflicting assessments on order of battle or capabilities is ridiculous.

Two areas in Desert Storm where differing opinions greatly effected planning were between Bomb Damage Assessment (BDA) and the targeteers. Both agencies worked in separate areas and in separate facilities and in some cases in separate countries. BDA personnel evaluated mission success primarily based on target photos. Their previous experience had taught them what to expect when General Purpose (GP) bombs were used. BDA experts were not thoroughly familiar with predicted results from many of the new penetrating Precision Guided Munitions (PGMs). IMINT, whether from strategic or theater assets, showed only "small" holes in the roofs and not the internal damage to the facilities. Not all BDA personnel had the advantage of viewing aircraft mission video tapes to witness primary and or secondary explosions after bomb impact. No aircraft videos, combined with overhead information gathered from inadequate oblique angles and reduced visibility situations, presented the BDA personnel a monumental task. These factors and the lack of expertise with newer PGMs, drove BDA personnel to conclude that many of the targets were not destroyed and recommended additional air strikes.

Targeteers had the necessary experience since they worked closely with or were previous pilots who had used these munitions in test and during training exercises. A prime example of the diversity in experience with the new PGMs was the F-117 and the GBU-27. Both of these (the platform and the weapon) had been recently declassified from the "black world" and integrated into the planning process. Still, had both BDA

5343 COPIER

and the targeteers been in the same mission planning cells, there would have been a greater economy of force exerted against Iraq with numerous missions being directed against targets not previously attacked and damaged.

Deception and Surprise

Deception, and its end result surprise, hangs over military leaders as a constant reminder to the fate of those who fail to heed and ignore caution in their analysis and planning. Caution must be used to thoroughly examine the problem, the information, and the solution(s) before settling on a particular course of action.

Intelligence analysis as well as the collection process, is susceptible to deception whether self induced or inflicted by the enemy. Sun Tzu believed that all warfare is based on deception. But part of the art of deception is to learn to think like the adversary. What may make sense for the deceiving side may not necessarily make sense to the intended victim.[9]

But why does deception work? Barton Whaley, who gave us the deception dictum: "The ultimate goal of strategem is to make the enemy quite certain, very decisive and wrong; studied 68 historical cases of strategic surprise or deception between 1914 and 1968. Of the cases studied by Whaley, deception was successful in 91 percent of the cases in which it was attempted; 79 percent of the cases exploited the target's preconceptions." (emphasis added)[10]

In the analysis process, all types of deception operations can be said to be directed at misleading, misinforming, or confusing an opponent on only two basic types of questions. The first is to deceive him about your own intentions, the second is to deceive him about your own capabilities. For example, the Egyptians, on the eve of the Yom Kippur War, spread rumors that their anti-aircraft missile systems had been short of certain spare parts (capabilities) since the expulsion of the Soviet advisors in June 1972, and that therefore they were not yet ready to initiate war (intentions).[11] Deception in war must be

343 COPIER

considered a rational and necessary type of activity because it acts as a force multiplier.

No counter-deception plan can really be full proof since human nature cannot be eliminated from the intelligence collection and analysis process. During analysis, the intelligence community must guard against deception by evaluating all disciplines in the acquisition process. Comparing and contrasting data will assist in identifying misleading information.

Many authors suggest that alertness to deception will assist the intelligence community enough to help detect and counter it. So, how alert is alert? Handel suggests a that the more alert we are to deception, the more likely we are to be deceived. He goes on to say that "experience and conditioning can work two opposite ways. The first is that once victimized by deception, one finds it difficult to accept any information as reliable. The other is that once a source of information is thought to be trustworthy it is difficult to discredit it."[12] These points will be discussed further in Chapter 5 on Acceptance.

Estimative intelligence used in planning does not always present all the facts. It generally covers the easier descriptions of an enemy's capabilities based in detection ranges, accuracy and range of weapons, and force disposition. More in depth information on how the enemy intends to use his weapons and his methods of operations are equally important to a planner. Enemy intentions remain the most difficult to determine since we have yet to invent a machine able to predict human nature.

5343
COPIER

CHAPTER 4

DISSEMINATION

The dissemination of intelligence information to the field can be considered the most critical area in all levels of war. After all, what use is intelligence if it remains locked behind some door? Intelligence not used is wasted. Problems are generated in a number of areas in the dissemination process. Difficulty may arise in the articulation of the information, classification of information, transmission, and reception of the material. Whether or not intelligence is received at the warfighting level depends on the ability of the commander's staff to formulate the correct EEI requests and the promptness of the intelligence community to answer those requests. Promptness is heavily dependent on the necessary communication links among all levels of intelligence and units in the field.

Articulation

First and foremost, the intelligence community needs to have the ability to communicate with its customers. Communication skills are not just speaking the same language, it is speaking the same dialect. If questions arise about the employment doctrine of a naval combatant, then the answer must not be formulated discussing the benefits of Airland Battle doctrine. The answers should be tailored to the audience in order to help comprehension. The intelligence community needs to be not only the toastmaster but the writer as well. Articulation is crucial to getting the message across.

Even being a great communicator does not prevent withholding information. There is a propensity in the intelligence community to delay or refuse comment on a net assessment until they resolve the issue to a 100 percent confidence level. This approach is counterproductive at times since the information may become perishable depending on its nature. Granted there does need to be some verification and corroboration of facts before drawing conclusions, but at times waiting for 100 percent may

343 COPIER

not be as important as having 60 or 75 percent of the information to make assessments and operational decisions. Commander's should ask questions for early estimates when a "best guess" is needed. It comes back to the ability to evaluate risks and priorities. The dilemma for warfighters is to determine a compromise between blind trust and mistrust. It should not be a probability of rain (high or low), but a forecast showing a storm front instead.

Security Classification

Many times information is withheld from the warfighter because he or someone on the staff does not have the necessary security clearance to handle sensitive intelligence information. Security is one of the principles of war where operational art builds its foundation. However, when security begins to drive unnecessary complexity and operational/tactical execution, then warfighters must readdress classification issues.

This secrecy problem is not limited to the intelligence community and its adherence to protect sources. Secrecy is also ingrained in the operations world to protect technology advantages and vulnerabilities as well. The need to get into either the "green door" (sensitive intelligence) or the "black door" (advanced technologies) should be based on a "need to know" requirement and the ability to accomplish planning and integration for warfighting.

An example where secrecy impeded operations and placed military forces at a higher risk than necessary was during the Falklands War. Both sides of the conflict were fighting at the edge of their limits in warfighting and ability to collect intelligence. However, when a need for information exceeds the capacity of the available collection platforms, it is time to begin a search elsewhere or provide other collection means. For the British, lack of secrecy and over classification secrecy at the national level hampered operations during the Falklands campaign.

The secrecy (or lack of it) dilemma for the British began when the BBC prematurely broadcasted that the 2nd Paras were

#343 COPIER

assaulting Goose Green. The BBC "loose lips sink ships" wisdom tipped off the Argentineans and they reinforced Goose Green. However, just prior to that the British had intercepted General Menendez's (Argentine Falklands commander) operational estimate from Port Stanley. "General Menendez's appreciation of his position was circulated amongst Intelligence Officers in London, but security clearance was not given for it to be transmitted to either Brigade Commander with the Task Force."[1] If the British Task Force leadership knew of the Argentine reinforcement, they may have increased the numbers of troops assaulting Goose Green or revised the attack plan so as to not go against the brunt of the force. Had the British tactical superiority and initiative not overcome the Argentinean forces, the failure to transmit the intelligence may have had greater strategic implications and further eroded public opinion at home.

Transmission and Reception

As technology advances continue, the critical Command, Control, Communications, and Intelligence (C3I) nodes stagnate. The ability to digest information from the fire hose remains a perennial problem to dissemination of intelligence. It is probably safe to say that even today we are approaching a point where "the machine, the system will become an end to itself."[2] Real-time intelligence capability is always just over the horizon. The intelligence network that feeds inputs through limited nodes must be familiar with operational capabilities. It must pass information through a constricted system in a priority of warning, operational, and informative.

During the Falklands War, the British relied upon their Sea Harriers and Shipborne Electronic Support Measures (ESM) to provide attack warning. Neither system could provide the same detection capabilities as an Airborne Early Warning (AEW) platform. The consequences of no AEW was numerous ships lost to low-flying attack aircraft. While the British tried to make due with the helicopters and Harriers, they lacked the proper intelligence nodes and "proper fusion of operational planning

343 COPIER

and all-source intelligence."[3]

> "One special C3I problem may have existed because of the need to rely heavily on satellite communications. Britain had confirmed that it had shut down the radars on the H.M.S. Sheffield when it was hit by an Argentine launched Exocet. Some reports indicate these radars were turned off both to minimize the risk of detection and to allow satellite transmissions. Reports also indicate that the Sheffield was relying on ESM that could not operate effectively during satellite transmission."[4]

It is important to consider the same possibilities for U.S. forces when working C3I networks. Many other cases can be cited where intelligence is unable to pass on their analysis because it is overloaded with a glut of information. Information pollution inhibits intelligence work and forces situations where vital information does not get to the people who need it. Intelligence information that does not get to the people fighting the war (making decisions or pulling the trigger) is worthless! Further budget cuts and force drawdown may increase the burdens of information overload on intelligence.

Equipment Compatibility

Having the proper means to transmit vital intelligence is a necessary component for dissemination. Both interservice and defense intelligence agencies have proceeded on separate courses when purchasing C3I equipment. In many cases, information cannot be transmitted and must be passed manually to various units. An examination of equipment compatibility during Desert Storm shows that many work arounds were used. Air Tasking Orders (ATOs) and necessary target imagery could not be passed interservice. Link ups between stateside BDA personnel had at least two separate links to receive and transmit information. Many stateside overhead receiving locations could be considered vulnerable to a determined adversary. In Desert Shield/Storm, couriers were needed to transport the information to appropriate operations centers afloat. In addition there were requirement misunderstandings at CENTAF for the target photos. Much of the

343 COPIES

precision in PGMs is obtained through current target and routing imagery. There were instances where this information was not forwarded to the necessary agencies due to an overload of information or misinformation on weapons and weapons platform capabilities.

Finally, the informal lash-ups previously discussed led to poor organization of intelligence functions and duplication of effort. The informal lash-ups not within the chain of command or within the local operational planning staff can cause additional headaches for the commander with inefficient analysis and reporting from intelligence.. Agencies outside of the theater of operations may not be aware of on-going operations or capabilities on-hand.

The large variation of missions within a joint or combined operation create problems for the commander in that his staff may not be familiar with the capabilities of the units they support. The intelligence staff needs to not only be proficient with the intelligence process, but they need to be aware, understand and anticipate the needs of the warfighters in order to get the information to the field in a timely manner. Warfighters can improve information transfers by including intelligence in the planning (and update) process.

343
COPIER

CHAPTER 5

ACCEPTANCE

Although, accepting information is not an actual part of the intelligence process, it is vital for the conduct of military operations. Without accepting the information, a commander walks into a left hook with a blindfold. Acceptance examines the salesmanship, the believability where analysis leaves off. If human nature affects intelligence analysis, then human nature and acceptance greatly effects outcomes.

"Bad News"

For years, military historians and theorists have wondered why leaders (political and military) failed to believe intelligence information. Perhaps, these leaders assumed their intelligence staffs were complete in their analysis and there was no need to question the results. The opposite approach drove the leaders' choice to not accept intelligence information since it went against the course of action they had determined would garner success. The motivation to accept new information once a course of action has been determined is difficult to say the least. In fact, many times a course of action may have been selected on false assumptions and based on previous successes in similar situations. A commander, fully committed to the course of action he has selected, may not acknowledge new intelligence information since it is contrary to his convictions. This dissonance can drive a commander to ignore the intelligence and remain bound to a concept of operations or ambition to succeed, regardless of rational thought. The antithesis of success is failure; for a soldier, failure is not shooting straight; for a commander, failure is not obtaining victory. Frederick the Great stated: "It is no disgrace for a commander to be defeated, but it is a disgrace for him to be surprised."[1] Acceptance of intelligence or the lack thereof may be the root of all surprise.

Examples where theater commanders proceeded on a course of

343 COPIER

action regardless of the information presented vary. One such example was during Operation Market-Garden in WW II. Here, the commander chose to ignore intelligence information since it was contrary to his preconceived and prescribed course of action. While the operation was deemed a success overall, there were many areas where "bad news" was ignored so as to not postpone action.

> Montgomery - despite every warning, and contrary to his own military good sense, which was acute - refused to turn his troops back in their tracks to clear the Schelde estuary. Instead he determined upon using the First Allied Airborne Army (the British 1st, American 82nd and 101st Airborne Divisions) to leap across the Meuse and the lower Rhine, establish a foothold on the North German Plain and capture the Ruhr, the heartland of Germany's war economy. Market the seizure of the bridges at Eindhoven and Nijmegen by the American Divisions proved a brilliant success. Garden, the descent of the British 1st Airborne Division on the more distant Rhine bridges at Arnhem, did not.[2]

Fairly well known historical accounts of the planning for this operation disregarded intelligence information on the Panzer tanks, armored cars, and half-tracks in the vicinity of Arnhem. The "bad news" reported by intelligence was disregarded as it would have impeded the operation as originally planned.

Warning and Enemy Estimations

Other examples where leaders fail to heed intelligence information stem not from poor judgement, but the difficulty of the intelligence process itself. "Noise" produced by fragmentary data and analysis within the indications and warning arena may tend to drive political/military leaders to ignore intelligence. In fact, the incremental approach to analysis may be more conducive to a "Cry Wolf Syndrome" than complete ignorance of information.

Yom Kippur War, Oct 1973

Prior to October 1973, Israel had built an excellent reputation for preparedness against the Arabs. Their tenacity had eliminated threats to their small nation not less than three times before. However, just prior to the 1973 war, Israel made

5343 COPIER

some changes in the way they conducted military operations. The Israelis developed a new strategic defensive concept which consisted of massive fortifications on the Sinai along the Suez Canal. Their intelligence network remained very intricate and depended on valuable HUMINT for much of their early warning. In their "Concept", Israel assumed Egypt would not attack without further means of long-range interdiction on Israeli airfields and Syria would only attack with Egypt and not alone. The "Concept" along with their previous one-sided victories against the Arabs, created an atmosphere which "contributed to an unwillingness in the Israeli military and political leadership to believe a situation could exist where the Arab world would seize military initiative and move against Israel."[3] The Israelis caught all of the hints signaling an Arab invasion, but would not believe them. They knew of the exercises going on along the Suez Canal, aerial photography of the movements and equipment, intercepted communications, and they had complete confidence in their HUMINT source to give them at least 48 hours notice of an attack.[4] So what went wrong?

Basically, the Israelis were caught in a strict adherence to their "Concept" and reliance on one source of intelligence to warn them of attack. Instead of 48 hours, they were alerted with less than twelve hours notice (informed at 0400 with the first attacks around 1400 the same day).[5] The Israelis faced a threat who had gone to great lengths to study how they had been defeated in 1967. The Israelis were all too accommodating for both Nasser and Sadat in their recounting of the success in the Six Day War. Sadat was very careful to deceive not only the Israelis, but the Americans and his own troops as well. "In a survey carried out among the 8,000 prisoners in Israeli hands, only one knew on 3 Oct that the preparations were for a real war; 95% learnt only on the morning of 6 Oct that the exercise in which they were engaged was in fact preparation for war and that they were about to go to war."[6] As facts become available, the same circumstances might be said of Iraqi troops prior to

343
COPIER

their invasion of Kuwait.

The Israeli net assessment prior to the outbreak of hostilities had numerous flaws. Since there had been four previous periods of escalation in which the Israelis had noted Egyptian mobilization and preparation for war, they assumed this latest movement was more of the same. The assumption the Egyptians would not attack without air power did not correctly account for the use of surface-to-air missile capabilities to protect their armored movements against the Israeli Air Force (IAF). Finally, the last hint of war might have been when a Soviet satellite was launched on 3 October. It was placed in orbit and the flight path altered to fly over the Sinai, Suez Canal, and the Syrian-Israeli border.[7] There is no evidence, the Israelis were aware or that the U.S. provided this satellite information to the Israelis at the time.

Certainly, depending on the reliability of an intelligence source, one source may carry more weight than another. However, a basic "Rule of Hoyle" would be to never accept or depend on one source alone! The net assessment accomplished by the Israeli Defense Forces (IDF) was not questioned or cross-examined for its validity. However, it was the leadership who failed more than the intelligence network. Both IDF military and political leaders set the stage and were caught in a self-deception trap through the direction(s) given to military intelligence. They believed what they wanted to believe. Intelligence had been right in the past, so there was no need to question their most recent assessment. Acceptance through overconfidence?

Operations vs Intelligence Communities

Human nature hinders acceptance of intelligence as much if not more than any other factor. In fact, human nature is probably the weakest link in the intelligence field. Human nature plays on how we accomplish our tasks, the personalities involved in the process, emotions and the human frailties attached, understanding the facts or whatever else is involved that may alter rational articulation(s) of a problem. This

343

section deals with the conflict between two ways of life: The operator and the information support network (intelligence).

Operators are the line infantry troops, the fighter, attack, and bomber crews, the submariner, the surface action sailor. It is the operator who goes into harms way. And those who go into harm's way deserve accurate intelligence and demand the right to question the information. For this reason, there has always been and will always be some sort of mistrust between operators and the intelligence corps. It is the job of intelligence to build up trust through adequate preparation, analysis and presentation. If a CINC fails in his campaign, he can probably recover. If intelligence fails, it is probably a disaster since we are starting from the point of being surprised. Surprise erodes confidence in any future intelligence estimates.

Two excellent examples where trust and understanding were present between operations and intelligence are Admiral Nimitz and Layton in the Pacific, and General Patton and Col Koch in Europe. Reading each others' memoirs can at times be a trip down memory lane in their praise for each other; but a close look at their campaign successes shows an understanding of the intelligence information available, the analysis involved, and the trust each commander placed into their N-2 or G-2. Through them we remember battles which will remain in the annals of military history as insightful and ingrained as decisive victories - examples like Midway and the Battle of the Bulge.

In the case of Midway, Admiral Nimitz understood the type of information his intelligence chief provided. Using "Magic" information resulted in the Japanese being surprised at Midway. For General Patton's success, Colonel Koch had an excellent understanding of his commander's method of employment and could anticipate courses of action. Colonel Koch followed simple principles attuned to Patton's philosophy: "Know your enemy, the terrain he controls, and the weather."[8] Colonel Koch's methods are what the Army calls the Intelligence Preparation of the Battlefield (IPB).

In order for Patton to accomplish the remarkable feat in the

343 COPIER

Battle of the Bulge, he had to have an awareness of the surrounding movements of troops and anticipate other variables. But how did the Bulge occur and where did the other operational commanders in the area go wrong and allow the Germans the opportunity for an offensive?

Battle of the Bulge

The situation for Allied troops early in December 1944 was one of a broad offensive operation against a withdrawing German Army. The withdrawals were determined to be in preparation for the final defense of the Ruhr and/or a possible spoiling attack against advancing Allied Armies, but not an offensive. The majority of this analysis was accomplished using Ultra information. Once the German codes were broken by the strategic intelligence facility at Bletchley Park, there became a greater and greater reliance on Ultra due to its intrinsic merit in the intelligence arena. Ultra became extremely reliable on determining the Germans intentions strategically. However, over-reliance and excessive applications to the operational and tactical arena should have set off bells and whistles in someone's mind whether from operations or intelligence. What happened prior to the German offensive commencing was a large reduction in Ultra traffic. Although there were numerous intercepted messages outlining German troop movements and air cover requests to the Luftwaffe, Bletchley Park did not report anything out of the ordinary to intelligence agencies on the continent.

What was missing from completing the intelligence equation was the lack of fused data to derive a logical conclusion. Units at the tactical level (patrols, PW interrogations, refugees, etc) were reporting movements of heavy tracked vehicles and the indications of an imminent offensive. "A very interesting report. Build-up of troops has been confirmed by Tac/R [Aerial reconnaissance] and PW statements. However, presence of large numbers of engineers with bridging equipment suggests preparation for offensive rather than defensive action."* These reports were ignored rather than requesting

5343 COPIES

patrols be sent out to investigate.

At G-2, Ultra was the only accepted information in the analysis process. If Ultra did not report the Germans building for an offensive, then they were only moving men and equipment to reinforce the defense. The last bit of information filed at Bletchley Park before the battle began was ". . . all SS units were observing wireless silence."[10] The obsession to collect and accept from only one source of information forced one of the most grievous intelligence mistakes since Pearl. On December 16, 1944, the Germans surprised the Allies with their Ardennes offensive.

A quick look at the German failure in this campaign shows a rigidity to one course of action in their offensive. The Germans felt they could get to the Meuse river, then Antwerp, and cut the strained Allied supplies lines before the Americans could respond with reinforcements. Their intelligence planning was based on the accepted assumption "... that reference would have to be made to the political leaders in Washington and London before any major troop movement to the area could be made. ... This belief coloured their entire strategy and when it was found to be wildly over optimistic they had neither the resources nor the power, given Hitler's control of decision making, to take remedial actions."[11] Reluctance to accept other sources of information slighted the analysis and selection of a course of action.

Desert Storm

If the American military has learned anything over the past fifty years it would be the acquisition and use of intelligence information. Although that is probably a very broad statement, it is true the military has made great leaps in intelligence to help determine when and where an enemy will attack. Our technology used to collect information has made quantum leaps, but we have not changed the acceptance variable. The acceptance dilemma is not just a function of the personalities involved. In Desert Shield/Storm acceptance was also driven from an organizational standpoint. The initial intelligence network set

3343
COPIES

up in Saudi Arabia accommodated for a lack of available CENTCOM intelligence personnel. The quest for knowledge and desire by many to be a part of the great event (too many fingers in the same rice bowl) caused an inordinate amount of informal intelligence chains to become institutionalized. The different information nodes (at various command levels) all reporting their own analysis created "noise" with no one clear voice out in the crowd. The results of this "noise" was a lack of confidence with the Joint Intelligence Center and a continuing need for intelligence analysis which was succinct, believable and acceptable to the CINC.

It should not have been a surprise to Gen. Schwarzkopf that his J-2 staff was inadequate. The CENTCOM J-2 deployed with inadequate personnel and equipment. While we spent an inordinate amount of effort to work interservice (joint) exercises, we did not spend the time to work on how to inform each other. "The CENTCOM J-2 was not structured for a deployment or conflict on the scale of Desert Storm. The Military Intelligence Board, assisted in identifying required wartime architecture and functions, and in providing qualified personnel from throughout the armed forces."[12]

Every Achilles has his heel and accepting intelligence is a heel for the political/military team. If human nature is the weakest link, then the tensile strength must be increased through a better understanding and assimilation of the intelligence process. Intelligence analysis and reports are an integral part of the planning sequence for any operation. To err, alter, or ignore intelligence information will doom an operation to failure and subject military forces to undue risks.

343
COPIER

Chapter 6

CONCLUSIONS

Intelligence, and the use of it, has come a long way since the days of consulting the Oracle at Delphi. Predicting the future may require some assistance and divine guidance, but it must also have a firm foundation in facts and analysis. Divine guidance augmented with prescience or with what Clausewitz called "coup d'oeill" - the ability to see the entire picture - assists leaders in the operational art. Commanders must avoid "learning impairments" or the inability to accept new ideas. This does not mean disregard tried and true practices outlined in Principles of War. Openness to new technology applications, ideas, and methods of employment is essential. An open mind towards intelligence and the information they can provide will only improve chances of success on the field of battle. This chapter will hopefully reinforce the ideas and lessons discussed earlier.

Leadership and Organization

Although intelligence works from a supporting role, it does not mean it is unimportant or that it should be relegated to some secondary or tertiary place. Information is literally available instantaneously. The more the operational community can participate in and understand about intelligence, the more successful future campaigns are likely to be.

Intelligence staffs need to shift their focus away from the Soviet threat. This does not mean to completely ignore the Commonwealth of Independent States (CIS). It means devote more attention to emerging regional threats and their infrastructure. Determining "rationality" may be much more difficult without the Soviets around to play Super Power. Many more nations are in the card game now and cards is a game of chance. "War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgement is called

343
COPIES

for; a skilled intelligence to scent out the truth."[1]

The United States, as a technologically superior force, could easily fall into a false security trap where the enemy "is not as capable as ourselves". For years, leaders have believed that American technology, training, and initiative were enough to whip anyone. Commanders must be wary of any arguments that includes these ideas as the only basis for analysis. The intelligence community is not familiar with the training required to maintain proficiency with our high-tech weapons nor are they familiar with force readiness at any given time. Commanders must provide the leadership to their staffs to ensure these unfamiliarities are reduced and eventually eliminated. In war, anyone can kill anyone, regardless of technology or training; Custer forgot that fact at the Little Big Horn!

"Experience is the only way to acquire a proper education in the use of intelligence on the higher levels of command."[2] How does the military leadership overcome a lack of experience with operational commanders placed in command positions due to rapid advancement in rank? An officer placed in command, promoted five years ahead of his peers, has not had the time necessary to develop valuable experience at the lower echelons of leadership and operations. He arrives and is placed at the helm when he may not even know how to steer.

For limited experience, it is necessary to either base command on experience and leadership abilities or provide additional training opportunities for the inexperienced commanders prior to assumption of command. Once in place, inexperienced commanders will have to devote the majority of their time running the organization and not on other ethereal endeavors such as intelligence analysis.

All commanders with or without experience need to involve intelligence more into operations and planning. Intelligence plays a vital role in the allocation and apportionment of resources. Economy of force, providing the right force at the right time and the right place, to defeat potential adversaries depends a great deal on accurate intelligence. The best way to

5343 COPIER

achieve the desired synergism is to co-locate operations and intelligence personnel to the maximum extent possible. Whether it is an Air Force, Navy, Marine, or Army unit this interface would be combining intelligence with operations functions all the way down the line from J-2 and J-3 down to squadron/company level intelligence officers with the weapons and tactics instructors.

Finally, commanders must be clear in their objectives and intents. "The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish by that test the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature."[3] A ruthless and complete dissection of objectives and the course(s) of action is necessary in order to increase the chance for success in a military operation. This dissection demands accurate and unambiguous intelligence.

Analysis

It is difficult to untangle the political from the military as in the Yom Kippur War. Use of force is an extension of policy, while no military action can be taken without political consequences. Although it is hard to do, the intelligence process needs to be disengaged from politics. The litmus test for the separation of intelligence from politics is an unambiguous and objective analysis.

Avoid relying on one source of intelligence (Ultra and the Battle of the Bulge or HUMINT in Yom Kippur). Reliance on a single source is a set up for surprise. All sources require constant cross checking of information to prevent enemy deception. Cross-referencing sources improves not impedes intelligence.

In the past, the U.S. and its military commanders have paid drastically by misunderstanding adversaries with mirror imaging (Pearl Harbor and Korea). As the "new world order" emerges, we must be in the position to examine evidence closely and evaluate the possibilities from both the rational and irrational points

5343 COPIER

of view. It is not certain whether U.S. superior fire power will always overcome in the future as nuclear proliferation continues.

There is only one syllable difference between the words "fusion" and confusion". Multiple information inputs which are reported incrementally without fusion and proper analysis is worthless. As discussed in Chapter 2, Desert Storm highligted how failing to compare and evaluate different sources of intelligence (fusion) results in erroneous reports. These bad intelligence summaries showed the Iraqis with 25 percent more SAMs after three weeks into the Air Campaign. Lack of fusion reduces confidence in intelligence. The need for tailored intelligence information is established in the warfighting command. Each Theater CINC must have his own Joint Intelligence Center (JIC) on location. The JIC must have the correct electronic architecture to collect from all sources and disseminate information to the field. The function of the JIC is to provide the commander the tailored intelligence and analysis as it is needed. The JIC should tie into national sources as necessary, but it must be responsive to the commander and provide him information on both targeting and BDA. Dependence on sources outside of the theater can create bottle necks and possibly create inaccurate information. The Theater J-2 working in concert with the J-3 and J-5 will know the needs of the planners and will be in tune with the on-going operations. This team will assist intelligence to anticipate the type of information needed to complete the campaign(s). Battlefield situations are dynamic and require constant revision of intelligence to support operations in the air, on land or sea. This can only be accomplished in-theater with support from other sources, not the other way around!

Precision Guided Munitions are only of value if the targets can be located. Location requires intelligence. This intelligence must be responsive and in tune with all of the information available around the battlefield to make accurate assessments. The J-2 staff that remains informed of the current

5343

situation can be of great assistance to the commander in the planning process. Up to date order of battle information, targeting and BDA can be assisted with mission reports form the field. An in-theater JIC should be able to fuse this information with other sources for a more complete picture and analysis.

If at the operational level intelligence center(s) there is no information available or conflicting reports are received (e.g. Ardennes-1944, Beirut International), then the Fusion Center(s) needs to look closer at sources that are still available. Troops in contact, Tactical Reconnaissance aircraft, or RPVs can help in the process to determine where the enemy is and where he is heading. Remember, No News is just that - No News.

Hopefully, the cases presented show the importance of accurate and timely intelligence including the understanding of enemy intentions. These intentions are difficult to predict as the enemy may not even know what he will do. However, using all intelligence disciplines, fused properly, with a greater emphasis on HUMINT enemy intentions may be clearer. Increasing HUMINT may require Special Operations Forces use in a campaign.

Intelligence Analysts need to ensure they present their reasoning and any evidence which supports their views with raw data. A careful analysis requires looking at all sides of the problem within a timely manner. Late intelligence work is worthless and better time could be spent reading the newspaper as the events unfold.

Training

Education, basic outlooks and experience all help to determine a commander's reception to intelligence. Training should begin with required academics in professional military education as well as tactical schools. Intuition plays as much a factor as any in accepting risks as they are presented. A classic example of accepting risks based on valuable intelligence is Admiral Nimitz and Midway. If the Japanese were sending out messages in the hopes of deceiving the Americans,

343
COPIER

then the meager U.S. fleet would surely have been in the wrong place and defeated. Training must include exercises that force analysis of enemy forces, not pre-planned canned scenarios. There must be live evaluations to determine actions of the opposing forces. These evaluations are over and above the evaluation of enemy exercises. The objective of evaluating "friendly" exercises or wargames would be to determine intentions and true capabilities of opposing forces. Once the intelligence staffs completed their analysis or the exercise, they would have the opportunity to discuss their results with the "other side" after the exercise is complete. Although the U. S. intelligence community is prohibited from collecting information on its own citizens, it is not prohibited from analyzing unit maneuvers and their actions. Training for commanders must include measures to learn the pitfalls and limitations in the intelligence process.

Intelligence officers must have a good working knowledge of Blue force capabilities in order to help determine how the threat is reacting to friendly forces. Knowledge of Blue capabilities needs to be based on realistic assessments and not on overconfidence as demonstrated by the Israeli intelligence staff. A rational dissection of facts is still the most prudent approach.

Intelligence will never be a substitute for military force. It can assist military leaders in selecting logical courses of action with the appropriate levels of force to counter any threat. Determining intentions will continue to be one of the most difficult tasks the intelligence community will have to face. However, knowing where the pitfalls are in the intelligence process will help prevent being surprised and being studied in the future in a continuing list of military misfortunes, defeats and disasters.

While it may be dangerous to attempt and draw many conclusions or lessons from previous wars, they do provide a basis for study. These cases applied to the theory of war "become a guide to anyone who wants to learn about war from

5343 COPIER

books; it will light his way, ease his progress, train his judgement, and help him to avoid pitfalls."[4] There are numerous cases throughout history, from Cannae and Chancellorsville to Desert Storm, where intelligence has played a direct role in the outcome of the battle.

For operational intelligence, as with most other endeavors in war, the battle is the pay off. Were we correct, did we deceive the enemy, did they deceive us? Intelligence, when it was only associated with espionage has always been a "yucky" business. However, intelligence is more than spying. The misunderstanding about what intelligence can do for a commander multiplies the confusion. The real role of intelligence is to reduce the Clausewitzian dictum that war is a matter of uncertainties.

The final question remains - When is a leader a leader? Is it when he is out front? Or is it when he posseses the perceptions as to what can be achieved and how to accomplish those goals. For the operational commander, or any leader, perception requires the proper use of intelligence and avoidance of its pitfalls. The prudent leader understands his intelligence capabilities and their limitations as well if not better than he understands the capabilities of the men and weapons under his command. Understanding intelligence, allows a commander the insight to know what he must do himself; how to ask questions and what questions to ask!

5343 COPIER

NOTES

Chapter 1

1. FM 100-5. Operations. (Washington D.C., 1986), p. 10.

2. Carl von Clausewitz, On War Michael Howard and Peter Paret, ed., (Princeton: Princeton University Press, 1976), p. 117.

3. Sun Tzu, Translated and introduction by Samuel B. Griffith, The Art of War (London: Oxford University Press, 1975), p. 84.

Chapter 2

1. Rocky Roland, "Space Capabilities and Limitations." (Newport: Naval War College, 1991), p. 4.

2. Roy Godson, Intelligence Requirements for the 1980's: Elements of Intelligence. (London: National Strategy Information Center, Inc., 1983), p. 56.

3. Ibid., p. 33.

4. Anthony H. Cordesman and Abraham R. Wagner. The Lessons of Modern War. Volume I: The Arab-Israeli Conflicts, 1973-1989. (San Francisco: Mansell Pulishing Ltd., 1990), pp 47-48.

5. Godson, pp 34-35.

6. R.V. Jones, The Wizard War. (New York: Coward, McCann, & Geoghegan, Inc., 1978), p. 290.

Chapter 3

1. O.G. Haywood Jr., "Military Decision and Game Theory." Journal of the Operations Research Society of America. Vol 2, No. 4, Nov 1954, p. 377.

2. Ivan Morris, The Nobility of Failure. (New York: Holt, Rinehart and Winston, 1975), p. 283.

3. Stephen Howarth, To Shining Sea: A History of the United States Navy, 1775-1991. (New York: Random House, 1991), p. 462.

4. Masahide Ota, The Battle of Okinawa: The Typhoon of Steel and Bombs. (Tokyo: Kume Publishing Co., 1984), p. 6.

5. Morris, p. 285.

5343

6. Godson, p. 85.

7. Ibid., p. 80.

8. Michael I. Handell, War, Strategy and Intelligence. (London: Frank Cass and Company Limited, 1989), p. 198.

9. John Gooch and Amos Perlmutter, Military Deception and Strategic Surprise. (London: Frank Cass and Company Ltd., 1982), p. 135.

10. Donald C. Daniel and Katherine L. Herbig, Strategic Military Deception. (New York: Pergamon Press, 1982), p. 60.

11. Gooch, p. 126.

12. Ibid., p. 144.

Chapter 4

1. Lawrence Freedman, "Intelligence in the Falklands." Intelligence and National Security, Vol 1, No 3. Sep 1986, p. 327.

2. Michael McKnight, (London: Penguin Books, 1987), p. 41.

3. Anthony H. Cordesman and Abraham R. Wagner, The Lessons of Modern War. Volume III: The Afghan and Falklands Conflicts. (San Francisco: Mansell Pulishing Ltd., 1990), p. 325.

4. Ibid., p. 275.

Chapter 5

1. T.N. Dupuy, Understanding Defeat. (New York: Paragon House, 1990), p. 72.

2. John Keegan, The Second World War. (New York: Peguin Books Ltd., 1989), p. 437.

3. Chaim Herzog, The War of Atonement: October, 1973. (Boston: Little, Brown and Company, 1975), p. 10.

4. Eliot A. Cohen and John Gooch, Military Misfortunes: The Anatomy of Failure in War. (New York: The Free Press, 1990), p. 127.

5. Herzog, p. 52.

6. Ibid., p. 39.

7. Ibid., p. 48.

6343

8. Oscar W. Koch, G-2: Intelligence for Patton. (Philadelphia: Whitmore Publishing Company, 1971), p. 43.

9. Charles B. MacDonald, A Time for Trumpets. (New York: Bantam Books, 1985), p. 77.

10. Ibid., p. 78.

11. Correlli Barnett et al, Old Battles and New Defences: Can We Learn from Military History? (London: Brassey's Defence Publishers, 1986), p. 109.

12. Interim Report of the CSIS Study Group on Lessons Learned form the Gulf War. "The Gulf War: Military Lessons Learned." Washington, D.C., July 1991, p. 14-1.

Chapter 6

1. Clausewitz, p. 101.

2. Michael I. Handel, Intelligence and Military Operations. (London: Frank Cass and Company Limited, 1990), p. 25.

3. Clausewitz, p. 88.

4. Ibid., p. 141.

6343 COPIES

BIBLIOGRAPHY

Abrahmamsson, Bengt. Military Professionalization and Political Power. Beverly Hills: Sage Publications, 1972.

Barnett, Correlli et al. Old Battles and New Defences: Can We Learn from Military History? London: Brassey's Defence Publishers, 1986.

Bolger, Daniel P. Americans at War: 1975-1986 An Era of Violent Peace. Novato, California: Presidio Press, 1988.

Carver, Michael. War Since 1945. London: The Ashfield Press, 1990.

Clausewitz, Carl von. On War. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Cohen, Eliot A. and John Gooch. Military Misfortunes: The Anatomy of Failure in War. New York: The Free Press, 1990.

Collins, John M. Grand Strategy: Principles and Practices. Annapolis, Maryland: Naval Institute Press, 1973.

Cordesman, Anthony H. The Arab-Israeli Military Balance and the Art of Operations. London: University Press of America, Ltd., 1987.

Cordesman, Anthony H. and Abraham R. Wagner. The Lessons of Modern War. Volume I: The Arab-Israeli Conflicts, 1973-1989. San Francisco: Mansell Pulishing Ltd., 1990.

Cordesman, Anthony H. and Abraham R. Wagner. The Lessons of Modern War. Volume III: The Afghan and Falklands Conflicts. San Francisco: Mansell Pulishing Ltd., 1990.

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

Dulles, Allen. The Craft of Intelligence. New York: Harper & Row, Publishers, 1963.

Dupuy, T.N. Understanding Defeat. New York: Paragon House, 1990.

FM 100-5. Operations. Washington D.C., 1986.

FMFM 1. Warfighting. Washgington D.C.,1989.

FMFM1-1. Campaigning. Washington D.C., 1990.

5343 COPIER

Freedman, Lawrence. "Intelligence in the Falklands." Intelligence and National Security, Vol 1, No 3. Sep 1986.

Godson, Roy. Intelligence Requirements for the 1980's: Elements of Intelligence. London: National Strategy Information Center, Inc., 1983.

Godson, Roy. Intelligence Requirements for the 1990's. Toronto: Lexington Books, 1989.

Gooch, John and Amos Perlmutter. Military Deception and Strategic Surprise. London: Frank Cass and Company Ltd., 1982.

Handel, Michael I. Clausewitz and Modern Strategy. London: Frank Cass and Company Limited, 1986.

Handel, Michael I. Intelligence and Military Operations. London: Frank Cass and Company Limited, 1990.

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

Hastings, Max and Simon Jenkins. The Battle for the Falklands. New York: W.W. Norton & Company, 1983.

Haywood, O.G., Jr. "Military Decision and Game Theory." Journal of the Operations Research Society of America. Vol 2, No. 4, Nov 1954.

Herzog, Chaim. The War of Atonement: October, 1973. Boston: Little, Brown and Company, 1975.

Hopple, Gerald, W. and Bruce W. Watson. The Military Intelligence Community. London: Westview Press, 1986.

Howarth, Stephen. To Shining Sea: A History of the United States Navy, 1775-1991. New York: Random House, 1991.

Hughes, Wayne P. Jr. Fleet Tactics: Theory and Practice. Annapolis, Maryland: Naval Institute Press, 1987.

Interim Report of the CSIS Study Group on Lessons Learned form the Gulf War. "The Gulf War: Military Lessons Learned." Washington, D.C., July 1991.

JCS Pub 1. Dictionary of Military and Associated Terms. Washington D.C., 1986.

JCS Pub 0-1. Basic National Defense Doctrine. Washington D.C., 1991.

Jones, R.V. Future Conflict and New Technology. London: Sage Publications, 1981.

5343
COPIER

Jones, R.V. The Wizard War. New York: Coward, McCann, & Geoghegan, Inc., 1978.

Keegan, John. The Second World War. New York: Peguin Books Ltd., 1989.

Kennedy, William S. Intelligence Warfare: Penetrating the Secret World of Today's Advanced Technology Conflict. New York: Cresent Books, 1987.

Koch, Oscar W. G-2: Intelligence for Patton. Philadelphia: Whitmore Publishing Company, 1971.

Layton, Edwin T. "And I was There:" Pearl Harbor and Midway- Breaking the Secrets. New York: William Morrow and Company, 1985.

Lowenthal, Mark M. U.S. Intelligence: Evolution and Anatomy. Washington D.C.: Praeger Special Studies, 1984.

MacDonald, Charles B. A Time for Trumpets. New York: Bantam Books, 1985.

Middlebrook, Martin. Task Force: The Falklands War, 1982. London: Penguin Books, 1987.

Morris, Ivan. The Nobility of Failure. New York: Holt, Rinehart and Winston, 1975.

Ota, Masahide. The Battle of Okinawa: The Typhoon of Steel and Bombs. Tokyo: Kume Publishing Co., 1984.

Pforzheimer, Walter. Bibliography of Intelligence Literature. Washington, D.C.: Defense Intelligence College, 1985.

Purcell, Thomas C. "Operational Level Intelligence: Intelligence Preparation of the Battlefield." Alexandria, Virginia: Defense Technical Information Center, 1989.

Putney, Diane T. Ultra and the Army Air Forces in World War II. Washington D.C.: Office of Air Force History, 1987.

Regan, Geoffrey. Great Military Disasters. New York: M. Evans & Company, Inc., 1987.

Roland, Rocky. "Space Capabilities and Limitations." Naval War College.

Seabury, Paul and Angelo Codevilla. War: Ends and Means. New York: Basic Books Inc., Publishers, 1989.

Strauss, Barry S. and Josiah Ober. The Anatomy of Error: Ancient Military Disasters and Their Lessons for Modern Strategists. New York: St Martins Press, 1990.

DEPARTMENT OF THE NAVY 5343 COPIER

Sun Tzu. Translated and introduction by Samuel B. Griffith. The Art of War. London: Oxford University Press, 1975.