# Naval Doctrine Publication 2

# *Naval Intelligence*

DTIC
ELECTE
MAR 0 8 1995
B

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

19950303 101

# *Naval Intelligence*

*"(I)nstitute rigorous, continuous examination of enemy capabilities and potentialities, thereby getting the utmost value of information of the enemy and enabling our forces to be used with the greatest effectiveness. It is particularly important to comprehend the enemy point of view in all aspects."*

– Fleet Admiral Ernest J. King, U.S. Navy (Ret.), 1952


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

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000
AND
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, DC 20380-0001

30 September 1994

# FOREWORD

As in the past, naval intelligence is on watch today, supporting U.S. Navy and Marine Corps forces deployed around the world. Naval intelligence provides vital threat information on the location, disposition, capabilities, and intentions of our adversaries—actual and potential. It supports directly the naval commander's requirements for planning and executing combat operations. When applied effectively, naval intelligence focuses the commander's effort for decisive action against the enemy. It reduces risk to friendly forces and supports all levels of naval, joint or multinational operations, in peace and war.

Naval Doctrine Publication (NDP) 2, Naval Intelligence, is the second in a series of six capstone documents that articulate naval doctrine and provide the foundation for the development of tactics, techniques and procedures. NDP 2 outlines broad guidance for Navy and Marine Corps intelligence. All who serve in—or are served by—naval intelligence must understand its contents.

C. E. MUNDY, JR.
General, U. S. Marine Corps
Commandant of the Marine Corps

J. M. BOORDA
Admiral, U. S. Navy
Chief of Naval Operations

DRO QUALITY INSPECTED 3

# INTRODUCTION

Our nation faces an array of geopolitical, social, and technological changes that are fundamentally altering the course of world events. In response to these challenges, we have articulated a new naval strategy that changes the way U.S. naval forces operate. The focus of naval warfighting has shifted to operations in littoral regions of the world, where outcomes can be controlled or influenced from the sea. This new focus makes the nature of potential threats more difficult to predict. Because of this increased uncertainty, the need for naval intelligence has never been greater.

Naval intelligence provides insights into this uncertain world, both in peace and in war. Properly employed, intelligence can give us an accurate estimate of the situation, forecast likely adversary courses of action, and allow us to apply selective but decisive combat power throughout the battlespace. The fog of war precludes us from having a complete picture of the battlespace, but naval intelligence can lessen the unknowns and reduce risk for friendly forces.

More than any other service, naval forces deploy forward in harm's way. Around the world, naval forces promote regional stability and stand ready to respond to crisis. Every day we train and operate within range of potential adversaries whose military capabilities pose an immediate threat. These circumstances create a unique operational environment for naval intelligence. Embedded in units, staffs, theater and national agencies, it provides around-the-clock support to widely dispersed forces. Its hallmark is tailored, fused, all-source intelligence, provided directly to supported operating forces.

Naval intelligence provides indications and warning, cuing for surveillance efforts, and discrimination between friendly, neutral, and potentially hostile forces. It gives the commander, his staff, and subordinate commands the information they need to plan and execute combat action, and to evaluate the results. A commander, for his part, must understand fully the capabilities and limitations of the overall process to employ intelligence resources effectively throughout his battlespace.

Naval operations demand both general military and naval-specific intelligence, provided by Navy and Marine Corps intelligence professionals, and specialized technical expertise provided by a cadre of career cryptologists.

This publication defines naval intelligence and outlines its enduring principles. It describes the ways naval intelligence supports military planning for routine peacetime operations, operations other than war, and combat. Finally, it identifies specific challenges for naval intelligence in the future.

# Table of Contents

**CHAPTER ONE**
**The Nature of Naval Intelligence ..... 3**
Definition ..... 4
Scope ..... 6
Purposes ..... 7
Support to Operating Forces ..... 10

**CHAPTER TWO**
**Fundamentals of Naval Intelligence ..... 13**
Principles ..... 14
Key Attributes ..... 18
Sources ..... 22
The Intelligence Cycle ..... 24

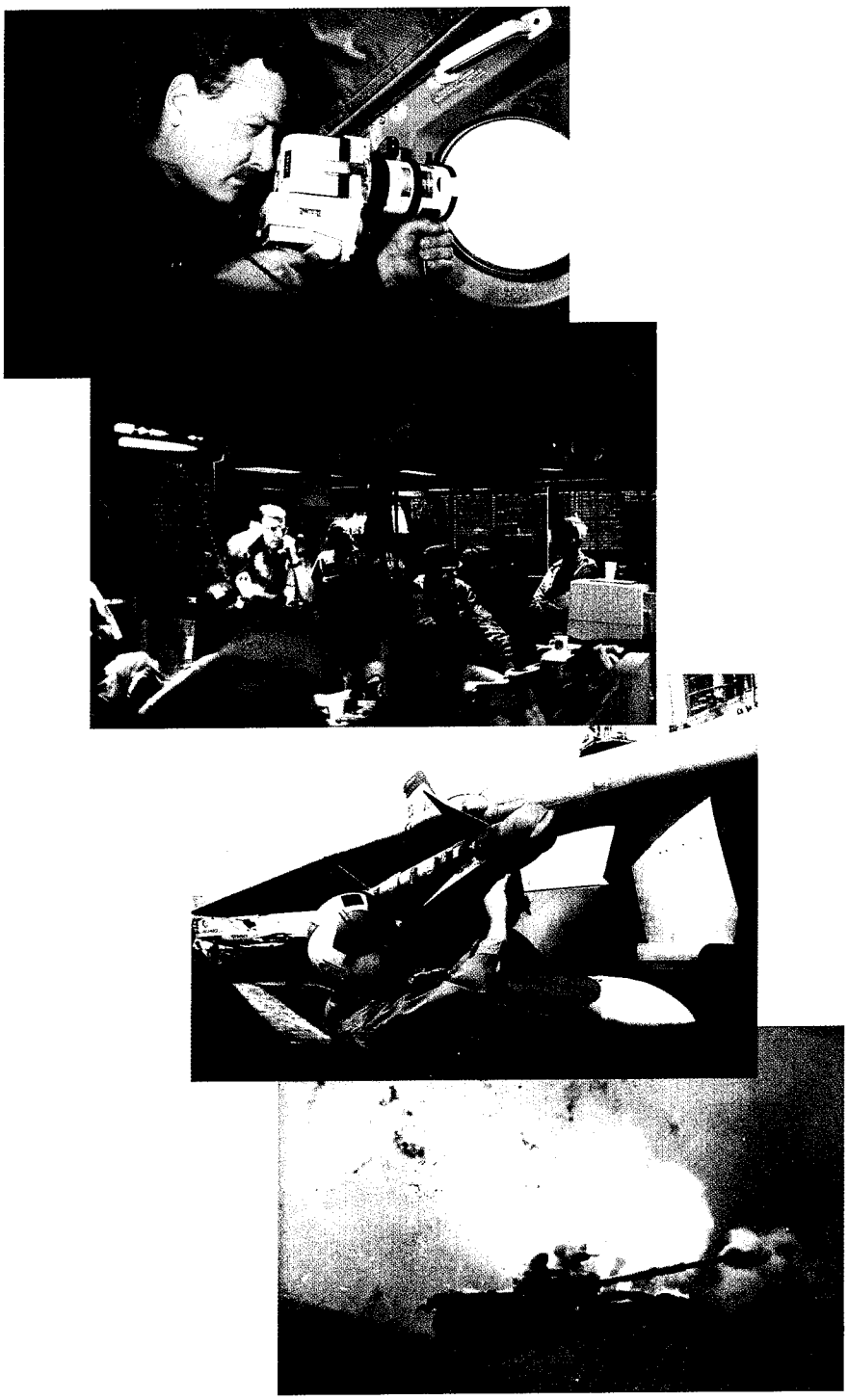
**CHAPTER THREE**
**Naval Intelligence Operations ..... 29**
Functions ..... 30
Structure ..... 38
Support to Planning ..... 39
Support to Operations ..... 43

**CHAPTER FOUR**
**New Direction - Future Challenges ..... 47**
Support for Expeditionary Forces ..... 48
Training and Readiness ..... 50
Coordination and Cooperation ..... 51
Intelligence and the Information Revolution ..... 53
Support to Information Warfare/Command and Control Warfare ..... 54
Intelligence Emphasis ..... 56

**CONCLUSION ..... 58**

**APPENDIX A ..... 59**

**GLOSSARY ..... 62**



## CHAPTER ONE

# The Nature of Naval Intelligence

*"Nimitz's concept of intelligence was dynamic: Facts were high grade ore to be sifted carefully, the pure metal of knowledge extracted and forged into a weapon to defeat the enemy."*

— Gordon W. Prange, Miracle at Midway

The United States is a maritime nation that relies on naval forces to support its national interests. The readiness, mobility, and forward deployments of these forces make the U.S. Navy and Marine Corps ideally suited to serve as primary instruments of national resolve during peace, crisis, and war. Depending on the mission, naval forces can form the nucleus of a Joint Task Force, operate as an enabling force for joint operations afloat and ashore, or act independently. To perform such operations successfully, naval intelligence is required. It provides a fused, all-source picture of the battlespace to support operations at sea, from the sea, and ashore.

The focus on operations in littoral regions has created new and dynamic challenges for naval intelligence. Despite a reduced threat of global confrontation, political instability persists around the world, creating increasingly complex and unpredictable regional threats to national interests. Meanwhile, rapid advances in technology have changed the nature of modern warfare and increased the demands on intelligence. In response, the Navy and Marine Corps employ a highly

capable organization of intelligence and cryptologic personnel–afloat and ashore–closely linked to and integrated with other service, joint and national intelligence operations.[1]

## Definitions

> *"By 'intelligence' we mean every sort of information about the enemy and his country— the basis, in short, of our plans and operations."*
>
> — Karl von Clausewitz: On War, 1832

At the outset, it is important to understand the distinction between information and intelligence. *Information* is an assimilation of data that has been gathered, but not fully correlated, analyzed, or interpreted. While not fully analyzed or correlated, information still has significant value to the tactical commander and plays a key role in threat warning and target acquisition. For example, *combat information* is "unevaluated data, gathered by or provided to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements" (Joint Publication 1-02). Organic, theater and national level cryptologic sensors provide a significant portion of combat information.

*Intelligence*, on the other hand, is "the product resulting from the collection, exploitation, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas." Integration and analysis, combined with a thorough understanding of mission requirements, convert *information* into usable *intelligence.* Thus, intelligence is the product we derive from analyzing all available and relevant information.

[1] The Navy and Marine Corps have different intelligence and cryptologic career paths. Regardless of the service distinctions, both disciplines are essential to successful intelligence support.

To the commander, intelligence is an essential element in planning and executing both combat and non-combat operations. It provides an assessment of an adversary's capabilities, vulnerabilities, and intentions, enabling the commander to employ combat power more effectively in attaining specific military objectives. Intelligence helps a commander identify an adversary's *center of gravity* and *critical vulnerabilities*, so he can bring maximum force to bear on key adversary weaknesses.[2] It also helps the commander assess the effects of military operations. Intelligence strives to reduce the uncertainty facing the commander, thus reducing risk to friendly forces. The commander's information requirements always must be the principal driver of the intelligence effort. By clearly articulating his intent, the commander sets the tone for successful integration of intelligence within the command.

Naval intelligence is a system of personnel, procedures, equipment, and facilities, both afloat and ashore. It supports both naval and joint operations. It is embedded in all major echelons of command and is deployed continuously with naval forces. It encompasses not only dedicated intelligence elements such as a Marine Radio Battalion, but those having other primary functions as well, an example being a destroyer at sea sending a surface contact report. In fact, naval forces are unique in that intelligence collection capabilities are resident in many of our weapons platforms; at the tactical and operational levels of warfare, intelligence collection is just one more capability of ships, submarines, and aircraft. Naval intelligence includes centers ashore for maritime, scientific and technical intelligence, training, administration of intelligence programs, and systems acquisition. Naval intelligence is a part of the joint intelligence architecture in current theaters of operations, connecting naval forces to theater joint intelligence centers, national intelligence agencies, service intelligence centers, and cooperative foreign governments.

---

[2] *Centers of gravity* are "those characteristics, capabilities or localities from which a military force derives its freedom of action, physical strength, or will to fight (Joint Pub 1-02)." *Critical vulnerabilities* are those elements of a military force that are vulnerable to attack and whose degradation or destruction will lead to defeating the center of gravity and, ultimately, his ability to resist. (See NDP 1, Naval Warfare, for further discussion of *critical vulnerabilities.*)

## Scope

Naval forces are prepared to operate at the strategic, operational, and tactical levels of warfare. Naval intelligence provides evaluated intelligence on an adversary's capabilities and intentions to support planning and operations at all levels of warfare.

— ***Strategic Intelligence*** is required for the formation of policy and military plans at national and international levels. At the strategic level, intelligence is oriented toward national objectives and supports the formulation of policies and determination of priorities. Strategic intelligence focuses first on discerning the capabilities and intentions of potential adversaries as well as considering the strategic intentions of allies and other potential multinational partners. Strategic intelligence plays a central role in identifying an adversary's center of gravity.

— ***Operational Intelligence*** is required for planning operations within regional theaters or areas of operations. It concentrates on intelligence collection, identification, location, and analysis to support the operational level of warfare, which includes identifying an adversary's operational critical vulnerabilities. Further, it assists the commander in deciding how best to employ forces while minimizing risk.

— ***Tactical Intelligence*** is required for planning and conducting tactical operations at the component or unit level. It focuses on a potential adversary's capabilities, his immediate intentions, and the environment. It is oriented more toward combat than long-range planning. Far more than at any other level, tactical intelligence support is the primary focus of naval intelligence.[3]

The three levels of intelligence were evident during Operations Desert Shield and Desert Storm. *Strategic intelligence* led to the identification of Iraq as a potential enemy—with its leadership and command and control as centers of gravity; *operational intelligence*

[3] "OPINTEL" is the term previously used in the Navy to refer to tailored, all-source intelligence provided directly to naval operating forces. "OPINTEL" equates to tactical intelligence; it should not be confused with intelligence support at the operational level of warfare.

identified the Iraqi air defense system as a critical vulnerability that, if destroyed, would neutralize the Iraqi military's capability to counter coalition air power; *tactical intelligence* supported plans for destroying or neutralizing critical command and control vulnerabilities, such as the Iraqi radar sites destroyed with high-speed anti-radiation missiles by Navy tactical aircraft at the outset of the air war.

## Purposes

> *"You are supposed to tell us what the Japanese are going to do, and I will then decide whether it is good or bad and act accordingly."*
>
> — Admiral Chester W. Nimitz, U.S. Navy
> CinCPacFlt, 1942

Naval intelligence, which supports all aspects of naval operations, has the following primary purposes:

— ***Supporting the Commander.*** Commanders require intelligence as a tool to evaluate the feasibility of, or determine risk factors associated with, objectives, plan and direct operations, and evaluate the effects of their actions. As the commander's primary advisor for intelligence matters, the intelligence officer must support the commander, his staff, and lateral and subordinate commands—not only with tailored intelligence, but by accurately conveying the capabilities and limitations of the intelligence system as well. The commander and his forces must have a clear understanding of what intelligence can and cannot provide, and how it will support the operation.

To be effective, intelligence support must have credibility which is attained by gaining the trust of the commander. This trust is usually gained over time, after a track record of accurate intelligence assessments has been established. Intelligence allows the commander to fight smarter by supporting his selection of the best courses of action. This includes advising the commander when an objective or planned course of action is probably *not* obtainable, *even if this advice goes against the conventional wisdom.* Each intelligence estimate should

reflect clear analysis and sound judgment. *The ultimate goal is to provide the commander and his forces the intelligence support needed to prevail in combat.*

— ***Identifying Centers of Gravity and Critical Vulnerabilities.*** Naval intelligence strives to provide an accurate picture of the battlespace from which we can identify clear and attainable objectives. For instance, at the operational level, the force commander may decide that to accomplish his objective, a particular target set—such as enemy command and control facilities—must be destroyed. At the tactical level, intelligence support is needed to plan an effective strike against a specific element of that target set, such as a radio-relay site. This tactical intelligence may consist of detailed, analyzed target photographs from tactical reconnaissance or national collection systems, pinpointing essential aim points for the strike leader.

— ***Supporting Planning and Execution of Operations.*** Naval intelligence provides staff support in both deliberate and crisis action planning.[4] During planning, collection resources are identified and tasked to meet intelligence requirements in support of the operation. Gaining knowledge of an adversary's capabilities and intentions may alter operational plans significantly. Similarly, changing operational tasking may in turn modify intelligence requirements. *A close partnership between the intelligence and operations officers will keep operations efforts focused on the mission and ensure that intelligence requirements are met.* Throughout all phases of planning and execution, intelligence and operations are critically interdependent.

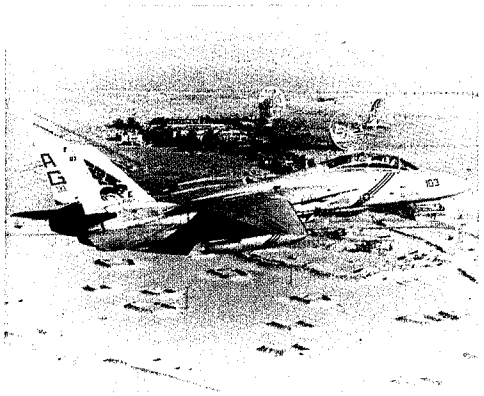
— ***Protecting the Force.*** Naval intelligence provides early warning of impending hostile action and reduces risk by detecting adversary actions that have an impact on friendly planning assumptions. Effective force protection enables us to limit the adverse effects of deception and surprise. Force protection efforts, supported by vigorous counterintelligence operations, can limit or distort the

[4] Deliberate planning is conducted primarily in peacetime to develop operations plans for contingencies identified in joint strategic planning documents. Crisis action planning is the process of formulating and implementing plans and orders in response to time-sensitive crises. (Adapted from Joint Pub 5-03.1)

## NAVAL INTELLIGENCE IN DESERT STORM

In response to Iraq's August 1990 invasion of Kuwait, U.S. forces, under General H. Norman Schwarzkopf, Commander-in-Chief, U.S. Central Command, began deployment to the Gulf. The Office of Naval Intelligence's Strike Projection Evaluation and Anti-Air Warfare Research (SPEAR) group was tasked to provide critical node analysis to support combat preparations.

After a thorough review, SPEAR concluded that Saddam Hussein, aware of the coalition's vastly superior air forces, would likely not send his entire 950-plane armada against the attackers. Rather, he would use them sparingly, relying on hit-and-run tactics, and dispersal to hardened shelters around the country, to enhance their survival.



SPEAR assessed the primary threats to coalition aircraft to be numerous anti-air artillery weapons, man-portable air defense missiles, and radar-guided surface-to-air missiles, supported by a formidable air defense command and control network. Knowledge of Iraq's lethal low-to-medium altitude threat resulted in coalition aircrews modifying their tactics in order to operate at higher altitudes. Iraq's reliance on its air defense network made the system a critical vulnerability. Therefore, neutralizing this enemy capability became an objective of the allied air operation.

Armed with this vital intelligence, the commander, his air staff, and the operating forces were able to plan and conduct operations that not only helped to protect the force better, but reoriented it toward more punishing strike missions as well. A post-war study commissioned by the U.S. Air Force concluded that SPEAR's analysis was "perhaps the best assessment of the Iraqi air force and air defense system" in Desert Shield and Desert Storm.

adversary's assessment of friendly capabilities and intentions. Further, naval intelligence provides the information needed to conduct successful deception measures against the adversary. These measures require detailed knowledge of the adversary's perceptions, vulnerabilities, intelligence-gathering capabilities and limitations, tactics, techniques and procedures, and the physical characteristics of the battlespace. Moreover, intelligence can reduce the likelihood of fratricide by helping to clear the fog of war.

– ***Supporting Combat Assessment.*** Naval intelligence is essential in developing combat assessments that can help the commander decide whether to redirect friendly forces or end operations. Combat assessment is the procedure by which the commander weighs the effectiveness of military operations by considering battle damage assessment, munitions effectiveness, and reattack recommendations. Analysis of the enemy's reaction to friendly operations gives us insights into his morale, materiel status, and ability to continue hostilities.

## Support to Operating Forces

Support to operating forces is the cornerstone of naval intelligence. Because of their mobility and forward deployment, as well as the unique nature of surface, subsurface, air, special and landing force operations, naval forces have special requirements for tailored intelligence on potential threats in both the maritime and littoral environments. Naval intelligence is designed to support operations at sea, from the sea, and ashore—through an organization closely linked with joint and national intelligence centers.

Naval forces engaged in operations are supported by theater Joint Intelligence Centers (JICs). The theater JIC serves as a focal point to ensure that operating forces receive intelligence support from national and service intelligence centers such as DIA, CIA, NSA and the National Maritime Intelligence Center. Naval forces also maintain such organic intelligence capabilities as photographic interpreta-

tion, communications intelligence analysis, and finished intelligence production, which support not only the commander and embarked forces, but theater and national decisionmakers as well.

Communications are key to ensuring that intelligence is available to the commander and his forces at every level throughout the battlespace. Relevant intelligence must be *pushed* to the commander on the basis of preplanned essential elements of information; similarly, because naval forces must be able to respond quickly to any crisis, the commander must be able to *pull* timely and relevant intelligence at any time, from any location as well. Rapid, concurrent dissemination of intelligence ensures that an accurate, complete, and common picture of the battlespace is available to all tactical users. The commander can improve the effectiveness of his forces by exercising his intelligence and cryptologic capabilities realistically, and by ensuring that reliable communications deliver the product to the user.

Naval intelligence personnel and systems are co-located with decisionmakers at nearly every echelon of command. Similarly, cryptologic personnel and systems are woven into the fabric of operating forces–from specially configured surface ships, submarines, and naval aircraft to Marine Air-Ground Task Forces (MAGTF). Embedding intelligence and cryptologic personnel, equipment, and communications at the unit, afloat staff, theater and national levels contributes to effective intelligence support under virtually all circumstances. That said, effective intelligence support can be assured only when the commander and the members of his intelligence organization have a clear understanding of the fundamentals of intelligence.

— § — § — § —



# CHAPTER TWO

# Fundamentals of Naval Intelligence

*"To lack intelligence is to be in the ring blindfolded."*

— General David M. Shoup, U.S. Marine Corps
Commandant of the Marine Corps, 1960

The fundamentals of naval intelligence, distilled from years of operational experience, guide both the commander and the intelligence officer. The commander who understands these fundamentals can employ intelligence to his best advantage; the intelligence officer who understands these fundamentals can support the commander's requirements better. The fundamentals of naval intelligence include principles, key attributes, intelligence sources and the process of the intelligence cycle. They apply across the spectrum of military operations–from peacetime, to operations other than war, to combat.

## Principles

The principles of naval intelligence provide enduring guidelines for effective intelligence operations. Understanding and applying these principles will give decisive advantages to naval commanders.

> *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. When you are ignorant of the enemy, but know yourself, your chances of winning and losing are equal. If ignorant of both your enemy and of yourself, you are certain in every battle to be in peril."*
>
> — Sun Tzu, The Art of War, ca. 500 B.C.

— ***Know the Adversary.*** Since the time of Sun Tzu, *knowing the adversary* has been the paramount principle. *Identifying the adversary* is the first step in gaining this knowledge. Knowing how the adversary thinks (especially how the adversary perceives success and failure) is essential in forecasting his likely courses of action. We know our adversary better by understanding his goals, objectives, strategy, intentions, capabilities, methods of operation, vulnerabilities, and values. We gain this understanding by studying his character, culture, social mores, customs and traditions, language, and history. Only then will the intelligence officer be able to provide the commander a full assessment.

Because naval forces often will be first on the scene in a crisis, naval intelligence *must* identify potential adversaries in peacetime and prepare intelligence for anticipated crises. We will not always have the luxury of planning against a single adversary. Naval forces may be called into action in a variety of contingencies—against a conventional armed force, a terrorist group, or in response to civil or natural disasters. Under these conditions, we must seek to know all potential adversaries, while focusing our intelligence efforts against the most likely one.

*"The commander must appreciate and shoulder his intelligence responsibilities or fail in the discharge of his operational functions."*

— BGEN James M. Masters, U.S. Marine Corps
A C/S-Intelligence, HQMC, 1958

— ***The Commander's Needs are Paramount.*** No commanding officer approaches port without knowing the tides and shoals that may endanger ship and crew. Similarly, no fleet, battle group or MAGTF commander approaches combat without first understanding the opponent. Intelligence, the heart of our combat decisionmaking, enables us to fight smarter by reducing our uncertainty about the adversary. Armed with this knowledge, the commander can then determine his best courses of action and articulate his continuing intelligence needs. Thus, intelligence directly influences operations, from the earliest phases of planning through execution.

The commander involves his intelligence staff early in the planning phase to ensure that intelligence will support his effort. In turn, the intelligence staff must keep the commander advised of any changes in adversary activity and any gaps in knowledge that may develop.

— ***Ensure Unity of Intelligence Effort.*** In any theater of operations, unity of effort ensures that intelligence supports the commander's objectives. Clearly stating and prioritizing information requirements are important steps in ensuring unity of effort. This becomes a particular challenge in multinational operations, where naval forces may encounter major differences in language and culture, limitations imposed by bilateral agreements, and differing strategic objectives. In building unity, we should recognize national differences, promote complementary intelligence operations and—most importantly—enable the exchange of intelligence. We can achieve all of this through the coordinated efforts of a joint or multinational intelligence center and the exchange of intelligence liaison personnel and systems.

– *Plan for Combat.* Forward deployed naval forces can be thrust into combat with little warning; thus, naval intelligence resources must be able to function continuously in diverse operational environments. Realistic and continuous intelligence planning and training must support the full range of naval operations. Naval and national intelligence systems must be reliable and give commanders timely access to the intelligence they need. At the same time, the commander must understand the essential nature of this support and prioritize resources to satisfy his needs. For example, automated data processing interoperability should be a key goal, so that own-service systems can talk to other-service, other-theater or national systems via common protocols and formats. Intelligence personnel must ensure that all databases and communications are in place (or readily surged) to support combat operations, afloat and ashore.

– *Use an All-Source Approach.* Developing an intelligence assessment is comparable to completing a jigsaw puzzle without all the pieces. To develop the full picture, the intelligence analyst should seek as many pieces as possible. This is known as the principle of "all-source" analysis.

Rarely will a single source or sensor provide the entire picture of the battlespace. Historical examples exist in which a single source provided the key intelligence, such as the communications intercept that led to the shootdown of Japanese Admiral Isoroku Yamamoto's aircraft during World War II. However, even that key intercept was fused with other known data–location of enemy airfields, likely course and speed of the aircraft, and other current intelligence–to plan the shootdown. The most useful and complete intelligence assessments usually emerge after a fusion of data from multiple sources. To preclude being deceived by our own analytical errors or by adversary deception, we use an all-source technique that permits the development of corroborating data. Further, all-source analysis can disclose conflicting data, which demand additional analysis to discern a more accurate picture. Most often, however, the all-source approach develops complementary data, where information from one source confirms information provided by another.

## ALL-SOURCE INTELLIGENCE AND THE NAVAL EMBARGO OF IRAQ

The operations of the maritime interception force during Desert Shield and Desert Storm clearly demonstrate the importance of all-source intelligence analysis. The embargo of Iraq's overseas trade, mandated by a U.N. resolution, directly involved the U.S. Navy and Coast Guard and eleven other coalition navies. Coalition naval forces patrolled the Arabian Gulf, northern Arabian Sea, and the Red Sea in search of merchantmen carrying munitions, petroleum, and other contraband. Thousands of suspect ships were located, intercepted, and inspected. This complex task required timely and accurate intelligence on the nationalities and characteristics of the merchant vessels, the origins and destinations of their cargoes, and the orders under which their masters operated.



U.S. maritime intelligence activities provided a wealth of intelligence derived from international shipping registers, vessel sightings, electronic intelligence, cryptologic reporting, open sources, satellite imagery, human intelligence, and aerial reconnaissance photographs. This information was collated, analyzed, and fused into intelligence products that were provided to naval operating forces. Complementing this intelligence with information from organic radar, cryptologic sensors, and other surveillance assets, the maritime interdiction patrol force intercepted more than 10,000 ships by the spring of 1991. This enabled the Gulf War coalition to maintain, in the words of General H. Norman Schwarzkopf, a "steel wall around the waters leading to Iraq" that helped hasten the defeat of the Iraqis on the battlefield.

## Key Attributes

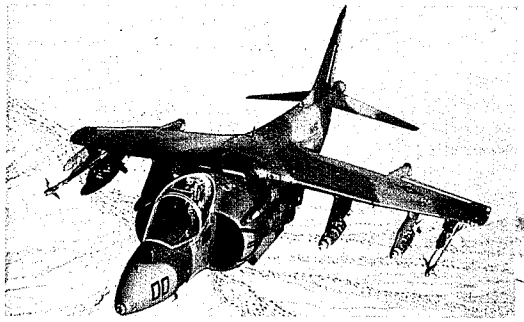
Effective intelligence has several mutually supportive attributes or qualities. In certain cases these qualities can appear as competing goals. For example, although both *thoroughness* and *timeliness* are attributes of any intelligence product, a goal of thoroughness for any one product could actually hinder timeliness. To be effective, naval intelligence must strike a proper balance among the following–sometimes conflicting–attributes:

– ***Timeliness.*** Intelligence should be timely enough to support policymaking or decisionmaking, to enhance the prospect of mission accomplishment. Timeliness is most essential during the formulation of the commander's estimate and when handling highly perishable data normally called Indications and Warning intelligence. To ensure that timeliness requirements are met, the commander must prioritize his information needs.

– ***Objectivity.*** From the facts on hand, the intelligence analyst must be free to assess and report the situation without the influence of bias, distortion, or political constraint. Intelligence analysts should be meticulous in their efforts to discount preconceived notions and not allow these to influence, much less drive, the intelligence effort.

> *"Tell me what you know. . .tell me what you don't know. . .tell me what you think. . .always distinguish which is which."*
>
> — General Colin L. Powell, U.S. Army
> Chairman, Joint Chiefs of Staff, 1990

– ***Usability.*** A commander needs intelligence that is easy to understand and apply to operational decisions. Usability demands timeliness, relevance, and proper format or form. The speed and complexity both of modern threats and our own telecommunications systems place a premium on rapid intelligence dissemination. Commanders need this intelligence in time to react to threats and make better decisions.





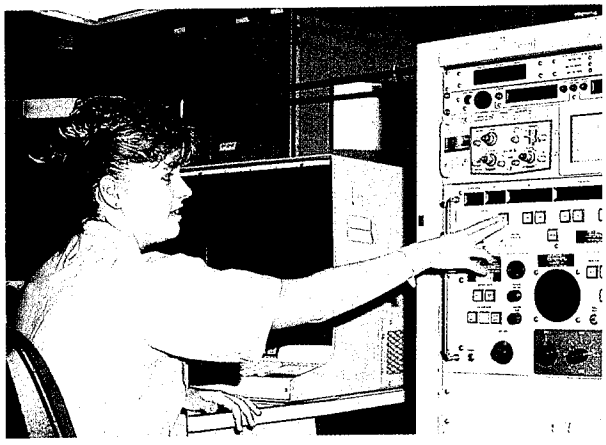
– ***Availability.*** To support the commander's planning and operations, intelligence should be available when and where needed. Availability requires foresight, an ability to predict, a clear understanding of objectives, and thorough intelligence training. In order to respond to rapidly emerging intelligence requirements, the intelligence officer should anticipate, collect, evaluate, produce, and store information. In naval operations, we depend on reliable, interoperable, up-to-date, on-line intelligence databases. We must be able to receive current, meaningful, appropriately classified intelligence to support changing operational requirements rapidly. *Recognizing the need to protect sensitive intelligence sources and methods, we must guard against excessively restrictive classification of intelligence, which would deny it to the commander or operator who truly needs it.* Many intelligence items can be "sanitized" by removing references to the highly-classified source of the data, and released at a lower classification.

– ***Thoroughness.*** Thorough intelligence contributes directly to successful combat planning and execution. Proper identification and prioritization of the commander's essential elements of information help to clarify the scope and detail of the intelligence

required.[5] The intelligence effort should give us the information we need—nothing more, nothing less. Since the intelligence picture never will be complete, the commander should be aware of gaps in available information. By recognizing both the *known* and the *unknown*, a commander can apply appropriate judgment to reduce risk.

—*Accuracy.* Intelligence should be factually correct and convey sound estimates of the adversary's intentions and capabilities. Accurate intelligence reduces uncertainty, thus increasing the commander's confidence in his understanding of the battlespace. Comparison of information received from multiple sources improves the ability to verify information and reduces susceptibility to deception. The dissemination process must not reduce accuracy.

—*Relevance.* Intelligence should pertain directly to the operations at hand and to the level of command for which it is intended. For example, the commanding officer of a destroyer conducting maritime interdiction operations would find it important to learn that a merchant ship with a history of arms smuggling is entering his area of responsibility. The National Command Authorities might find the same intelligence somewhat less relevant. If intelligence does not support the needs of the intended user, it has little value.



[5] Essential elements of information (EEI) are the critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision (Joint Pub 1-02).

## BATTLE OF MIDWAY - THE ATTRIBUTES OF NAVAL INTELLIGENCE

Before the Battle of Midway, Admiral Chester Nimitz asked his intelligence officer, Commander Edwin Layton, to forecast as closely as possible the time and method of the anticipated Japanese attack on Midway. With the objective thus defined, Layton set to work. A decoded message from the Japanese aircraft carrier command contained the phrase, "we plan to make attacks from a general northwest direction," but did not specify the target. Layton thus assumed that the Japanese force would approach Midway from the northwest on an approximate bearing of 315 degrees. He estimated that they would approach under cover of darkness, just as they had at Pearl Harbor six months earlier, and launch their bombers at first light. He knew, too, that the U.S. forces on Midway would launch their search planes at first light.



Using ***available*** intelligence, Layton's analysts discerned that the attack would occur on June 4th. Knowing the time of sunrise on June 4th and the approximate course and speed of the American search planes, Layton was able to forecast with ***accuracy*** and ***timeliness*** when and where they would detect the Japanese carriers. Layton provided Admiral Nimitz ***usable*** intelligence by estimating that the Japanese would approach Midway on bearing 315 degrees and that they would be sighted 175 miles from Midway at about 0600. Nimitz was reportedly surprised by the ***thoroughness*** of Layton's forecast, but immediately grasped the ***relevance*** of the estimate. He ordered his staff to plan a course of action that would take this intelligence into account.

Shortly after 0600 on 4 June 1942, Admiral Nimitz received an urgent message from Midway, "Plane reports two carriers and main body ships bearing 320, course 135, speed 25, distance 180." The battle that followed broke the Japanese initiative in the Pacific and changed the course of the war. As Admiral Nimitz later remarked to Layton, "Well, you were only five miles, five degrees, and five minutes off."

## Sources of Intelligence

Intelligence sources vary greatly in capability, method, sophistication, and utility, ranging from a local informant to a billion-dollar reconnaissance satellite system. All sensors possess capabilities that make them unique. All have limitations as well. For instance, reconnaissance satellites may provide broad area coverage not available from any other sensor, yet collection over the desired area may be affected by adverse weather or orbital geometry. As a rule, however, the utility of the source is not a function of its sophistication; the best intelligence often can come through the simplest collection means. To be effective, intelligence must use all available sources; it cannot simply concentrate on the most familiar. Further, naval intelligence must be ready to function in an environment where some sensor data may be missing.

INTELLIGENCE SOURCES

| | |
|---|---|
| Counterintelligence | CI |
| Imagery Intelligence | IMINT |
| Photographic Intelligence | PHOTINT |
| Human Intelligence | HUMINT |
| Measurement and Signature Intelligence | MASINT |
| Acoustic Intelligence | ACINT |
| Electro-optical Intelligence | ELECTRO-OPTINT |
| Infrared Intelligence | IRINT |
| Laser Intelligence | LASINT |
| Nuclear Intelligence | NUCINT |
| Unintentional Radiation Intelligence | RINT |
| Open Source Intelligence | OSINT |
| Radar Intelligence | RADINT |
| Signals Intelligence | SIGINT |
| Communications Intelligence | COMINT |
| Electronic Intelligence | ELINT |
| Foreign Instrumentation Signals Intelligence | FISINT |
| Scientific and Technical Intelligence | S&TI |
| Medical Intelligence | MEDINT |

Intelligence collection is naturally constrained by resource allocation, the nature of the threat, technology, and the environment. Collection resources are normally managed so that they remain focused on areas perceived as enduring threats. Refocusing the intelligence system on emerging threats may take time. Intelligence assets are necessarily finite and competition for them can be extremely keen, thus, they should be managed carefully.

Sensor selection and employment, processing, and timeliness depend on the nature and characteristics of the target. For example, electronic intelligence (ELINT) may provide us little information when directed against an adversary with unsophisticated weapons; on the other hand, human intelligence (HUMINT) might bring some results in the same case. A proper mix of sensors and sources is the key. Another important factor is the rapid processing of sensor data. The intelligence effort must have enough trained personnel to interpret data within the context of ongoing operations. Finally, we must carefully and continually assess the timeliness of sensor data.

Sensor data can be corrupted and erroneous; therefore, we should not be mesmerized by a display of data on a screen. Such data requires careful analysis and ambiguity must be resolved. Some sensors produce data enabling weapons or tactics to be employed directly, such as ELINT data used to guide an anti-surface missile attacking an enemy ship. In such cases procedures should be in place to disseminate data immediately and ensure that forces acting upon that information will understand what it is, how it will arrive, and what it will look like. Other intelligence sources, however, often produce information that requires careful consideration and analysis before forces can be committed on the strength of it.

## The Intelligence Cycle

Intelligence products result from a series of interrelated activities termed the *intelligence cycle.* Figure 1 illustrates the process through which the commander levies intelligence requirements, information is collected and converted into intelligence, and intelligence is disseminated to users. This cycle normally consists of five steps: planning and directing, collection, processing, production and dissemination. This cycle greatly simplifies a dynamic and complex process, but it is useful to illustrate how the intelligence process works. Naturally, intelligence efforts do not always flow sequentially through the cycle. For example, a request for imagery generates planning and direction, but may not involve new collection if the request can be satisfied from archival imagery.

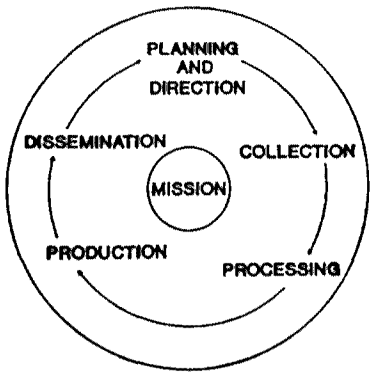



Figure 1

—*Planning and Direction.* During this phase of the cycle, the commander must identify and prioritize his information requirements. This phase is instrumental to the cycle's success. Because a great number of intelligence requirements may have to be satisfied, planning and directing determines the effort required to meet our needs. After the commander identifies his requirements, the intelligence officer formulates a collection plan, taking into account

the collection assets available and the commander's essential elements of information. One of the key elements in the planning phase is assessing current intelligence to ensure that it meets our requirements. Early discovery of any requirements that cannot be satisfied through organic, theater or national intelligence collection resources will highlight potential intelligence gaps. Planning further includes the identification of personnel, transportation and communications requirements.

— ***Collection.*** Collection involves tasking organic, attached, and supporting collection resources to gather information.[6] The collection process determines what will be—and *what will not be*—available to support decisionmaking. Since few collection requirements can be met fully by organic assets alone, collection resources available at the theater and national level will normally be tasked as well. To do this effectively, the intelligence staff must know the capabilities *and* limitations of available collection resources, must understand the requirements validation process to obtain desired collection approval, and must identify the collection resources that can contribute to fulfilling mission requirements.

— ***Processing.*** Processing is the conversion of collected information into a form suitable for producing usable intelligence, such as translating foreign languages, developing film from tactical reconnaissance aircraft, generating hard- or soft-copy images provided by electro-optical or infrared sensors, and converting raw electronic intelligence data into a standard message format suitable for automated handling. Timeliness and accuracy are especially relevant during processing.

[6] *Organic* intelligence resources are intelligence assets or capabilities permanently assigned to a particular command. *Attached* resources are separate assets attached to the joint force to support a particular operation or phase of the operation. *Supporting* intelligence resources are those from another AOR, theater, combatant command, or national organization providing support to the commander from outside his AOR (Joint Pub 2-0).

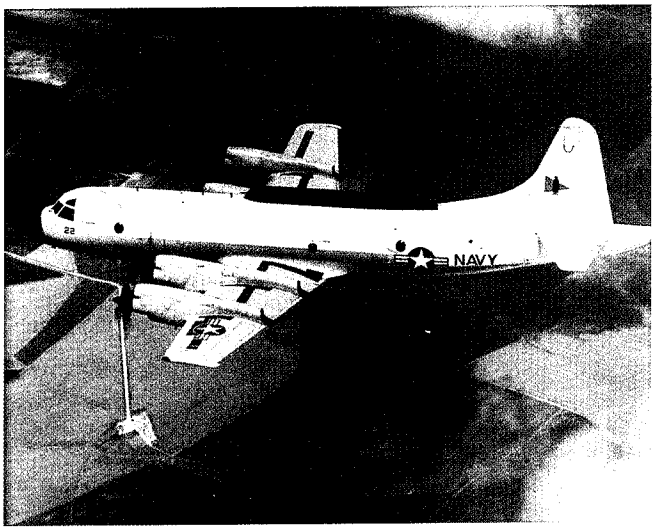
— *Production.* Intelligence production is the integration, analysis, evaluation, and interpretation of information from all available sources into tailored, usable intelligence. A key principle in production is the *fusion* of information from various sources to form a complete and accurate product. Fusion is essential for an effective intelligence production process that accurately reflects and supports the commander's prioritized essential elements of information (EEI). Because of the uncertain nature of combat, the commander, operations officer and intelligence officer should review EEIs periodically to ensure that intelligence assets are supporting mission needs.

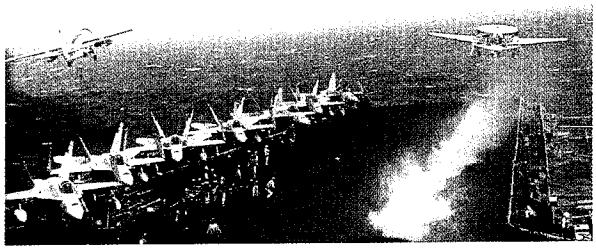
— *Dissemination.* The goal of the dissemination process is to provide the right amount of appropriately classified intelligence when, where, and how it is needed. Getting the product to the user is the last step in the intelligence cycle; but, because the cycle is dynamic, the process does not end with dissemination. *First, intelligence personnel must ensure that the product is actually used.* This is a particular obligation of intelligence personnel who are members of operational staffs. They are in the best position to demonstrate the value of intelligence products to commanders and other staff members. *Second, intelligence personnel must see to it that dissemination is refined by gathering feedback from the commander or other users to ensure that intelligence requirements have been satisfied and the finished intelligence products are usable.* If not, the intelligence staff must take corrective measures to meet the needs of the commander. The dissemination process should not overwhelm the tactical user with massive amounts of data. Instead, intelligence dissemination should follow established procedures designed to push time-sensitive, threat-warning data to the commander, while allowing him to pull less time-sensitive intelligence required for his mission.

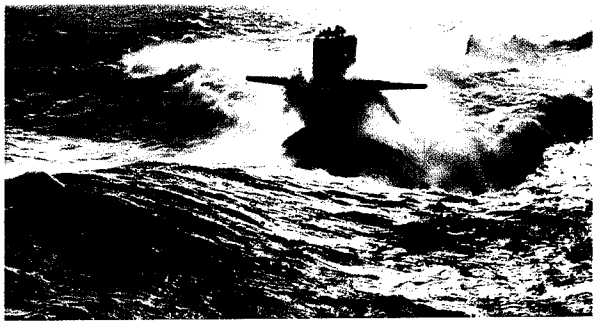
An accurate display of intelligence data is essential to achieving effective employment of intelligence products. Increasingly, tactical commanders prefer to view crucial data in the context of the larger scenario in progress. Effective display of intelligence information is essential in order to translate usable products into modern command and control, and weapons targeting systems. This process should include, as necessary, sanitization of classified data and reformatting into specific compatible data fields.

Intelligence lays the groundwork for naval operations in peace and war. By understanding the fundamentals of naval intelligence, the commander is best able to ensure that intelligence is fully integrated into operations. This integration enables intelligence to support both planning and execution effectively.

— § — § — § —


NAVY





# CHAPTER THREE

# Naval Intelligence Operations

*"The great military victory we achieved in Desert Storm and the minimal losses sustained by U.S. and Coalition forces can be directly attributed to the excellent intelligence picture we had on the Iraqis."*

— General H. Norman Schwarzkopf III, U.S. Army
Commander-in-Chief, U.S. Central Command, 1991

As an integral part of naval forces, naval intelligence resources are forward deployed around the world. Because of this forward deployment, naval intelligence must always be at a high state of readiness, with unparalleled situational awareness of the operating theater. To maintain that awareness, naval intelligence operations in peacetime closely parallel those in war and in operations other than war. More than any other service, naval intelligence supports peacetime operational decisionmaking on a daily basis.

Since its formal establishment in 1882, the Office of Naval Intelligence has been a major player in many successful operations that have meant the difference between ultimate victory and defeat. During World War II, an intensive cryptanalytic effort by the Navy's Communications Security Group—forerunner of today's Naval Security Group—led to the breaking of the Japanese Navy's code and played a pivotal role in attaining final victory in the Pacific. The naval cryptanalytic efforts of World War II foreshadow similar cryptologic tasks that will be required for operations against future adversaries including signals search methodology, language skills, and signal access.

In the Cold War era, the Navy established the Ocean Surveillance Information System (OSIS). OSIS focused naval intelligence efforts on the Soviet Navy threat and provided intelligence support to fleet and headquarters units. OSIS was a synergistic blend of intelligence and cryptologic personnel that provided tailored, fused, all-source intelligence to operating units. More recently, the naval intelligence system has served as a model for the establishment of Joint Intelligence Centers (JICs). These joint organizations matured during Operations Desert Shield and Desert Storm and today help meet the intelligence requirements of naval commanders in multiple theaters and in multiple roles. Regardless of the theater or mission, however, certain basic functions of naval intelligence remain constant.

## Functions of Naval Intelligence

Naval intelligence reduces risk by identifying adversary capabilities, vulnerabilities, and intentions. It attempts to impart thorough knowledge of the situation through the application of certain basic intelligence functions. These intelligence functions form the foundation of required analytical support to the commander. Mission, threat, time, and resources available will determine the priority and level of effort applied to specific intelligence functions in any given situation. The effective incorporation of the following functions into the intelligence process will produce the highest quality support throughout planning and execution.

— ***Intelligence Preparation of the Battlespace.*** Intelligence Preparation of the Battlespace (IPB) is the systematic and continuous analysis of the adversary, terrain, and weather in the assigned or potential battlespace. It is a significant element in the Commander's Preparation of the Battlespace and a key part of our decisionmaking process.[7] Its goals include understanding the adversary's forces, doctrine, tactics, and probable courses of action, together with the physical and environmental characteristics of the target area. IPB identifies gaps in knowledge that require intelligence collection efforts. It consists of five elements:

- *Define the Battlespace Environment:* Defines the area of operations and focuses intelligence assets on the battlespace.
- *Describe the Battlespace's Effects:* Evaluates physical characteristics of the battlespace and their effects on friendly and adversary capabilities to maneuver, attack, employ sensors, and communicate.
- *Evaluate the threat:* Encompasses a detailed study of the threat, identifying adversary capabilities and vulnerabilities.
- *Determine Threat Courses of Action:* Ties the previous steps together providing a predictive analysis of probable adersary courses of action - and friendly force survivability in each case.

IPB is of great importance to all aspects of combat planning. It is not limited to supporting planning, but is a long-term, continuous effort directed against potential adversaries as well. We use IPB to plan action and manage the risk to friendly forces. Risk will always be inherent in military operations, but IPB seeks to reduce that risk. We assess risk by weighing adversary capabilities and intentions against friendly forces and assigned missions. This risk is then analyzed to determine whether additional information or intelligence could alleviate it. Our management of risk thus depends on a clear understanding of both what *is* known and what *is not* known.

[7]Commander's Preparation of the Battlespace is used to mean analysis of the physical characteristics of an area and its affects on our ability to establish superiority in every dimension of the battlespace, as well as a detailed study of adversary capabilities, vulnerabilities, and probable courses of action.

## INTELLIGENCE PREPARATION OF THE BATTLESPACE

**Desert Shield/Desert Storm**

During Operation Desert Shield and throughout air operations of Desert Storm, U.S. Navy and Army special operations personnel and force reconnaissance Marines established a series of observation sites along the Kuwaiti-Saudi Arabian border. Tasked to conduct surveillance of the border and intelligence collection in support of follow-on operations, these sites were manned by Navy SEALs, Army Special Forces and Marine Corps force reconnaissance teams, augmented with Marine Corps and Army SIGINT personnel. Through nightly patrols and continuous visual and electromagnetic monitoring of Iraqi forces, the surveillance teams were able to conduct all-source collection of Iraqi army activity across the border. Their efforts laid the groundwork for a thorough IPB that was instrumental in planning for the forthcoming ground offensive to liberate Kuwait.

—*Indications and Warning.* The goal of Indications and Warning (I&W) is to provide early warning of potential hostile action. To accomplish this goal, intelligence must convey understanding of the adversary. This understanding is gained through Intelligence Preparation of the Battlespace and allows us to interpret indications, thus allowing adequate warning. I&W prevents surprise and reduces risk by detecting adversary actions that may threaten friendly forces. It can support strategic, operational, or tactical levels of warfare. Strategic I&W is concerned primarily with detecting a potential adversary's preparations for war, policy shifts, advances in military capability, or acquisition of new technology. By focusing on reduction of surprise and threat avoidance, I&W supports operational and tactical commanders.

I&W is essential for naval forces because of their forward presence in areas of potential crisis. Threat response times are greatly decreased in the littoral regions, making I&W crucial for avoiding or countering threats. Early investment in collection, regional threat analysis, target databases, and training help build a coherent picture of the adversary's capabilities and intentions. The commander's re-

quirements must be anticipated and understood in order to identify potential organic collection deficiencies and to focus theater or national intelligence assets on potential adversaries far enough in advance.

– ***Situation Development.*** Analysts use situation development to build on the IPB process. Situation development helps us assess and predict an adversary's actions. For example, current intelligence may reveal that an adversary is removing coastal defense missiles from storage. Intelligence must evaluate intentions: Is the activity merely proficiency training–or is there hostile intent? If it is training, are there opportunities to collect intelligence? If hostile intent is assessed, are any friendly forces at risk?



Predicting an adversary's future actions is difficult. We may lack complete information because of gaps in our collection ability, or due to adversary concealment efforts. Nevertheless, situation development can reduce risks by assessing capabilities and likely courses of action. In the example of coastal missiles, intelligence can give an accurate picture of the threat by calculating where the missiles might go, how quickly the adversary can fire them, and which of our naval

forces are in the threat envelope. The intelligence analysts use IPB as background; they then place the threat in context by assessing location, current operating patterns, training cycle status, and geopolitical situation. Situation development is especially critical in high-tempo operations when time is short and the cost of miscalculation is high. Although they are unable to foresee the future, intelligence personnel can make judgments that help the commander make better decisions.

> *"The credit must be given to Nimitz. Not only did he accept the intelligence picture, but he acted upon it at once."*
>
> — Admiral Raymond Spruance, U.S. Navy (Ret), 1982

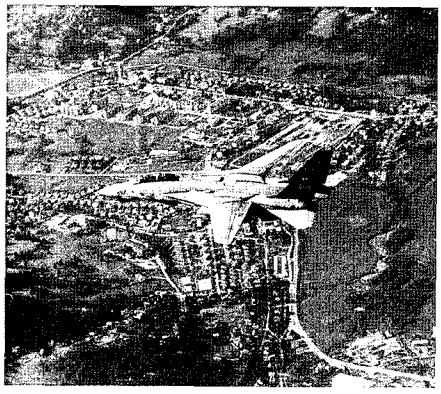
— ***Targeting.*** Targeting is a function of intelligence and operations, by which an adversary's critical vulnerabilities are identified for possible attack or disruption. The primary goal of targeting is to enable us to use resources effectively in defeating the adversary. Targeting is more than a function of planning the physical destruction of enemy facilities. Targeting is an analysis process in which the components of a target, or target system—and their vulnerabilities and relative importance—are assessed to determine what effect their loss or impairment would have on the adversary. Intelligence can indicate where selective employment of force can have a major effect on the adversary.

During the targeting process, we first develop and then select targets in accordance with the commander's guidance, objectives and the results of the Intelligence Preparation of the Battlespace. Targets may be either *physical* targets, such as bridges and command centers, or *functional* targets, such as enemy command and control capability. Operations personnel then match the targeting information to the appropriate instruments of force in a process commonly termed *weaponeering.* Continuous involvement of intelligence personnel in targeting deliberations may identify gaps in available data that a weapon requires for proper operation. Early identification of such shortfalls can activate intelligence collection to fill the gaps. Timely feedback from battle damage assessment is crucial to targeting be-

## INTELLIGENCE SUPPORT TO TARGETING - OPERATION DENY FLIGHT

Beginning in April 1993, the Navy has flown many F-14 Tactical Aerial Reconnaissance Pod (TARPS) sorties over Bosnia-Hercegovina as part of Operation Deny Flight. Operating from aircraft carriers stationed in the Adriatic Sea, the TARPS aircraft photographed hundreds of square miles of disputed territory, using thousands of feet of film. After the aircraft recovered aboard the carrier, Intelligence Specialists quickly and accurately provided the commander and other senior decisionmakers the location and types of belligerent arms, equipment, and forces. The Intelligence Specialists also produced annotated TARPS photos for carrier and shore-based strike team leaders to assist in planning potential contingency operations.





cause it allows us to assess mission effectiveness and permits us to husband resources and eliminate needless risk.

– ***Battle Damage Assessment.*** Battle damage assessment (BDA) is an element of Combat Assessment.[8] BDA evaluates the effectiveness of friendly force operations by exploiting and analyzing intelligence on enemy forces, facilities and functions. BDA in-

[8] Combat Assessment (CA) is the determination of the overall effectiveness of force employment during military operations. CA is composed of three major components, (a) battle damage assessment, (b) munitions effects assessment, and (c) reattack recommendations. The objective of CA is to identify recommendations for the course of military operations. (Joint Pub 1-02).

cludes not only physical damage assessments, but functional damage assessments as well. Physical damage assessments quantify the extent of damage to a material target, such as imagery indicating the center span of a targeted bridge has been destroyed, thus severing an enemy resupply line. Functional damage assessments determine the disruption to operational targets, for example, determining the effectiveness of electronic jamming on enemy command and control capabilities. BDA helps determine the impact of friendly operations on enemy combat effectiveness.

Verification of combat effectiveness is essential, especially for subsequent planning and reporting purposes. BDA may require analyzing large amounts of data, with limited or imprecise information available to fully evaluate results. Therefore, all-source intelligence is essential to the BDA function. The commander must consider BDA throughout all phases of mission planning and execution, for all levels of warfare. At the *tactical* level, BDA supports reattack decisions; at the *operational* level, BDA determines the extent of achievement of operations and campaign objectives; at the *strategic* level, BDA provides key information for senior decisionmakers with regard to campaign progress—and attainment of national security objectives.

*—Intelligence Information Management.* Intelligence must be delivered to the user *on time and in a usable format.* By providing a push-pull information capability to the commander, intelligence information management seeks to ensure timeliness, availability, and usability of intelligence. Intelligence information management monitors the flow of intelligence from collector to customer, identifying chokepoints and single points of failure across all intelligence cycle activities.

Effective dissemination of intelligence requires knowledge of communications systems architecture and equipment. As a management tool, intelligence information management facilitates the dissemination of intelligence to support operations as the battlespace expands. It helps the intelligence officer understand and articulate

intelligence dissemination requirements to the communications and operations officers. Such interaction ensures that the intelligence dissemination needs are met.

—*Force Protection.* Force protection is both offensive and defensive. It is supported by all intelligence functions, but is executed primarily through counterintelligence operations and force security measures. To neutralize or destroy the effectiveness of hostile intelligence collection activities, counterintelligence and security are essential. These protect information against espionage, personnel against subversion and terrorism, and installations and material against sabotage. Adversary forces can be expected to use every available means to thwart or otherwise impede the operations of our naval forces. Counterintelligence and security measures aid in identifying our own vulnerabilities and reducing risks, and are essential in achieving surprise during military operations.

Naval intelligence identifies adversary intelligence collection capabilities, assesses friendly vulnerabilities, identifies risk, and enables the commander to plan for operational security, deception and surprise. Force protection encompasses the measures taken by the commander to protect his forces, posture and information, and to deny such protection to his adversary. The commander must consider force protection in every aspect of planning and tailor it to the intended operations and the adversary's capabilities.

Security addresses both the protection of information and its dissemination. Sensitive intelligence requires protection, but commanders should be denied neither the intelligence they require to fight effectively nor intelligence that might keep friendly forces from being placed at risk. Decisions regarding releasability of intelligence must be made early–balancing operational requirements with the need to protect sensitive sensors or sources. Sanitization may be a viable option which would make the information available while still protecting the source or sensor.

## Structure of Naval Intelligence

Naval intelligence forces have been designed as an integrated system of personnel, procedures, facilities and equipment structured to support naval, joint and multinational operations. To be effective, naval intelligence must be structured to ensure both top-down and bottom-up intelligence support. Top-down intelligence support leverages national or theater intelligence resources to support the tactical commander; bottom-up support ensures that organic intelligence supports operations while contributing to the larger intelligence effort.

To support naval forces engaged in littoral operations, the primary work of naval intelligence is conducted at the tactical level in dedicated intelligence centers afloat, such as a Carrier Intelligence Center, or deployed ashore with the MAGTF command element. These forward deployed intelligence centers are staffed by personnel from embarked flag staffs, ships' company, carrier air wings and MAGTF intelligence organizations. Personnel assigned produce not only current intelligence, but other finished intelligence products that support a variety of contingency operations. Intelligence centers provide assessments of the adversary's capabilities and build and maintain threat intelligence files and databases. Depending on mission requirements, these centers may be augmented with liaison personnel from other services or national intelligence agencies.

Naval intelligence centers serve as fusion centers where information from various sources (cryptologic sensors, tactical airborne reconnaissance, units in contact with the enemy, etc.) is validated, correlated, analyzed, and disseminated to support operations. These centers also use links to theater and component sensors and to the joint intelligence centers, to complement organic capabilities and to facilitate national, theater, and tactical intelligence support to a wide range of operations. A fundamental operating principle of the intelligence center is that all-source intelligence must be integrated with operations and contribute to our common tactical picture. These operations are facilitated by reliance on a wide variety of automated data processing systems.

Because naval forces will normally operate as a component of joint forces, both afloat and ashore intelligence centers are integral parts of an intelligence architecture that connects the commander to joint and service intelligence centers, national intelligence agencies, and the intelligence centers of other nations.[9] Interoperability, cooperation in resource management, and intelligence sharing throughout this architecture is essential to support the commander's decisionmaking.



## Support to Planning

Intelligence is the cornerstone of planning. During all phases of planning, intelligence on capabilities, vulnerabilities, and intentions of potential adversaries is essential. Intelligence reduces the unknowns that planners must face and forms the basis for both deliberate and crisis action planning. Early involvement of the intelligence staff in planning (including exercise planning) is essential to ensure that intelligence continuously supports the entire operation.

[9] For a description of some of the joint and naval intelligence organizations that support naval operations, see Appendix A.

In *deliberate planning,* the commander's emphasis is on developing a carefully crafted plan for military operations. As shown in Figure 2, Intelligence Preparation of the Battlespace (IPB) is the predominant intelligence function during development of the commander's estimate and concept of operations. IPB identifies information requirements and shortfalls and permits refocusing collection and production resources to accomplish the plan. Planning must be sufficiently flexible to accommodate and respond to new information as it becomes available.

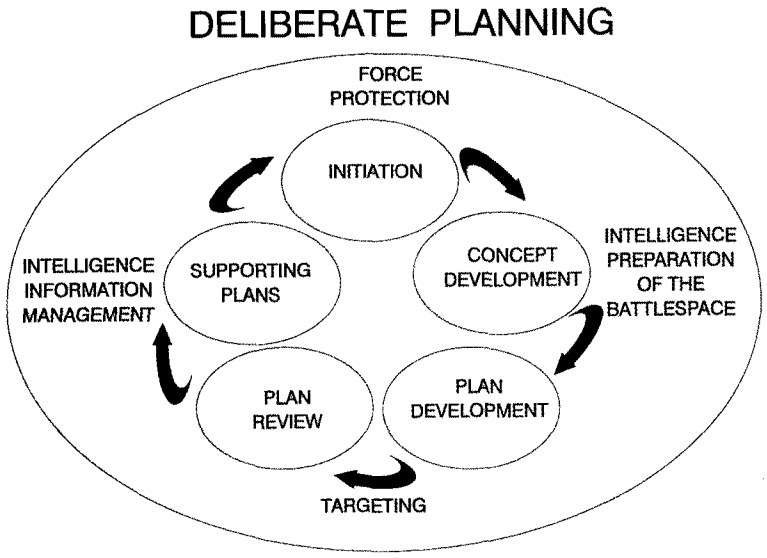



FIGURE 2

Targeting is an essential task in developing an operational plan. Throughout plan development, targeting materials are built and maintained as appropriate. During the entire deliberate planning cycle, intelligence information management (to include communications and dissemination architectures) and force protection (to include information security) are essential to ensure that the intelligence portion of the plan is executable. Indications and Warning generally do not support deliberate planning.

In *crisis action planning,* the commander's emphasis is on developing a course of action to respond to an emergent crisis. As depicted in Figure 3, intelligence is especially vital in crisis action planning since the crisis itself often grows and evolves while planning is underway. Indications and Warning play a key role in detecting events that generate crisis action planning. Situational development guides the modification of plans–both as the crisis unfolds and subsequent to selection of the preferred course of action. Because planning timelines are greatly reduced during crisis action planning, intel-

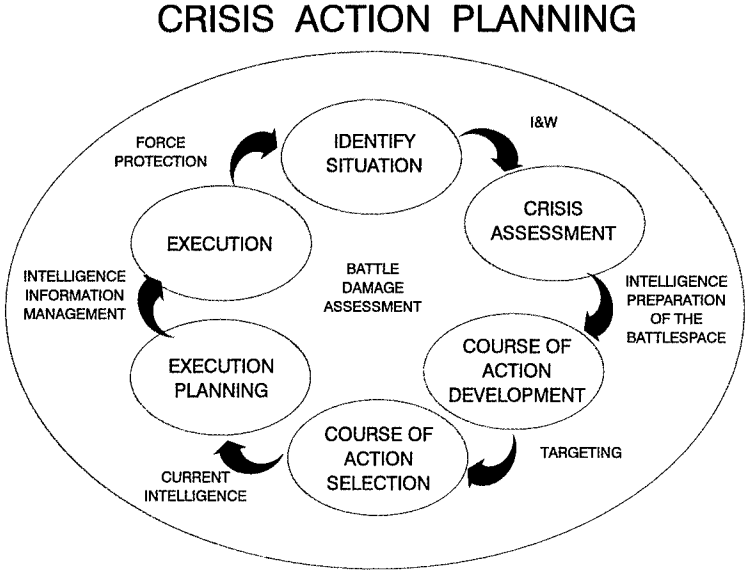



FIGURE 3

ligence preparation of the battlespace and targeting become the key tasks in support of the commander. Battle damage assessment is especially important during the execution planning and execution phases, but must be considered throughout all phases. As with deliberate planning, intelligence information management and force protection are ongoing concerns. Continuous involvement of intelligence, from planning to mission completion, guarantees the full integration of intelligence with operations in support of the commander's effort.

## SUPPORT TO PLANNING - THE INCHON LANDING

In July 1950, only a few weeks after North Korean forces stormed across the 38th parallel and pushed South Korean and U.S. forces into the southeast corner of the Korean peninsula, the supreme allied commander in Korea considered a major counterstroke. After a prototypical Intelligence Preparation of the Battlespace, General Douglas MacArthur decided that naval forces could dramatically alter the course of the war by seizing Inchon, a major port on Korea's Yellow Sea coast. Possession of Inchon would enable the allies to recapture a key air base, and mount a major ground offensive on Seoul which would cut off North Korean forces in the south.

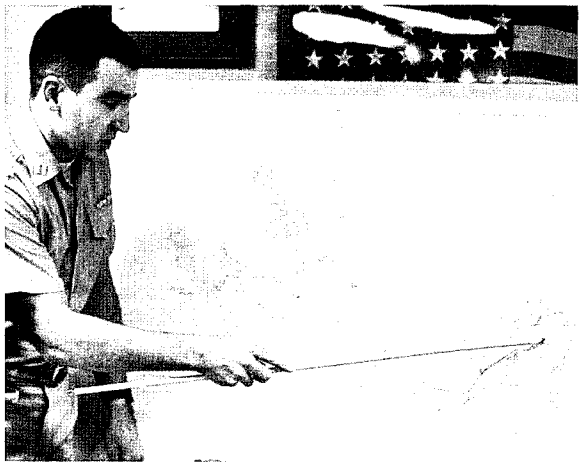
The North Koreans recognized the potential harm a landing at Inchon could do, but they believed the area was entirely unsuitable for a major amphibious operation. Tides rose and fell an average of 32 feet daily; the current ran swiftly in the narrow, winding waterways; and the approaches to the harbor were easy to mine, lined by defensible islands, and marked by extensive mud flats, high seawalls, and dominating hills. Moreover, harbor facilities were rudimentary, with little room in the roadstead to deploy logistic shipping.

In planning for the amphibious operation, the allies capitalized on high quality intelligence to overcome these disadvantages and take the enemy by surprise. Aerial photographs, the testimony of former inhabitants, and first-hand reports of naval special warfare teams that went ashore to conduct reconnaissance of the Inchon area shaped the operational planning of the amphibious task force commander, Rear Admiral James Doyle, and his staff. Naval intelligence helped Admiral Doyle select the best water approach, set the time for the amphibious assaults, and identify the North Korean Army line of communication as a critical vulnerability.

This comprehensive planning bore fruit on 15 September, when the allied amphibious task force launched its initial assault from the sea. By the 19th, the 1st Marine Division seized the air base at Kimpo and began the assault on Seoul. U.S. Army troops pushed out from the Inchon beachhead and on the 27th linked up with their comrades advancing north from the Pusan perimeter. Two days later, the Marines captured Seoul. Thus, by skillfully incorporating intelligence into operational planning, in a little more than two weeks, allied forces were able to oust the invaders from the Republic of Korea.

## Support to Operations

Naval forces have unique, multidimensional intelligence requirements. Countering threats to air, surface, subsurface, and landing forces requires in-depth knowledge of the threat, weather, hydrography, terrain, ports, and airfields. The sophisticated nature of the threat in naval warfare causes naval forces to demand detailed technical intelligence on an adversary's weapon systems. The intelligence picture is formed from all sources in the battlespace, including dedicated force intelligence collection resources, national and theater assets, liaison officers, and units in contact with the enemy. Naval forces also have unique intelligence collection capabilities, especially in their ability to collect intelligence covertly. Such collection can take place at the tactical, operational, or strategic levels.



During peacetime, naval intelligence plays an important role by supporting day-to-day decisionmaking for forward deployed naval forces. It also supports policy formulation and decisionmaking on force structure, systems acquisition, and doctrine and tactics development. Intelligence resources monitor foreign nations and regions to detect and characterize threats to U.S. national interests. Further, peacetime intelligence enhances naval training and exercises by providing realistic threat scenarios to train against.

Military operations other than war take place in a world populated by a growing number of impoverished and unstable nation-states seeking wealth, power, or security. Operations other than war can include combat or non-combat actions in the following areas: arms control, combating terrorism, nation assistance, non-combatant evacuation operations, other civil support operations such as disaster relief or humanitarian assistance, sanctions enforcement, international peace operations, support to insurgency and counterinsurgency, and counterdrug operations. In addition, a deteriorating situation may demand that naval forces quickly make the transition from such operations to sustained combat operations. Great demands can be placed on the intelligence system during operations other than war; these might include requirements for such nontraditional intelligence as determining the projected level of flood water or the local infant mortality rate. To build a picture of the adversary, we must have a broad understanding of the theater of operations and the underlying reasons for conflict. To gain this understanding, naval intelligence personnel must seek nontraditional sources of information with unique access, such as open sources, academia, emigres, and civilian area experts. Reliance on organic intelligence collection assets will increase and may require early deployment of such collection resources as tactical counterintelligence, HUMINT, and cryptologic teams. Littoral operations also may increase requirements for rapidly identifying and deploying specialized linguists and area experts.

Cryptologic operations play a key role in supporting naval expeditionary operations. Naval cryptologic personnel, afloat and ashore, employ tactical sensor systems that provide the commander time-sensitive combat information on an adversary's composition, disposition, location and intent. This information can be disseminated as electronic warfare support data directly to the tactical decisionmaker or processed into SIGINT by afloat or ashore analysis cells. Cryptologic operations can provide unique situational awareness by giving the commander insight into an adversary's decisionmaking cycle. For this reason, cryptology plays an important role in Command and Control Warfare. Cryptologic efforts rely increasingly on a complementary mix of tactical, theater, and national assets.

## INTELLIGENCE SUPPORT TO OPERATIONS OTHER THAN WAR

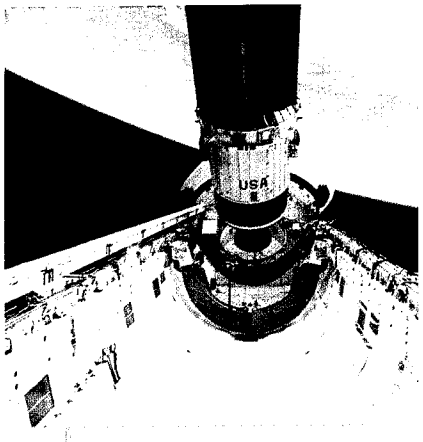
- Since the standup of Joint Task Force Four in 1989, naval cryptologic operations have played a major role in the detection and monitoring of illicit drug trafficking in the Caribbean Sea and Pacific Ocean.

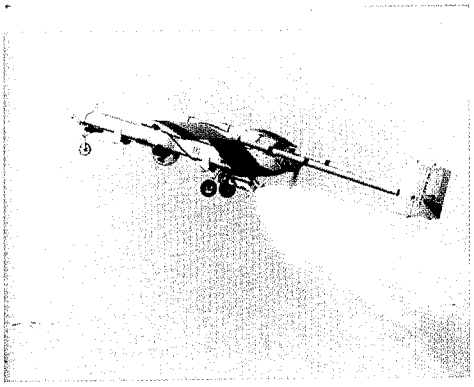
- During Operation Restore Hope in 1993, Marine Corps tactical HUMINT operations proved to be indispensable. By "taking the pulse" of the local populace, HUMINT personnel were able to determine which indigenous forces were friendly, neutral or potentially hostile, where weapons caches were located and where threat situations might develop. Additionally, they provided the Joint Task Force Commander an appreciation of Somali perception of, and reaction to, United Nations' support and relief operations.

- During the Mississippi River flooding in the summer of 1993, naval tactical aircraft flew photographic reconnaissance missions over the Mississippi River Valley, mapping the extent of flood damage and providing that information to the Federal Emergency Management Agency and other civil authorities charged with flood relief efforts.

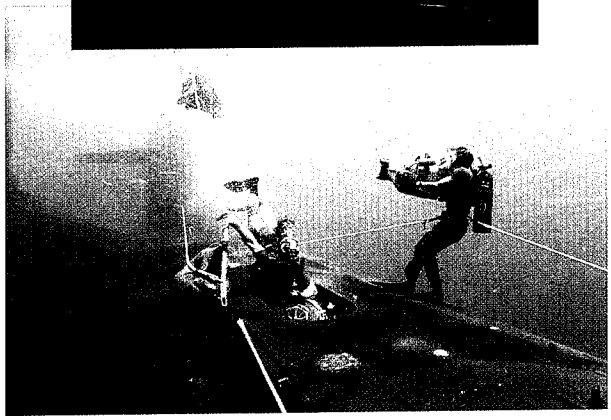
Combat operations place unique demands on naval intelligence personnel for innovation, initiative, and intensity of effort. Employing the same tools and structures used during peacetime and operations other than war, the intelligence staff carries out the primary intelligence functions to support ongoing combat operations. Intelligence during combat must identify enemy capabilities, intentions, and critical vulnerabilities in a timely and accurate manner, providing the commander maximum leverage in applying combat power against the enemy. During combat, the timeliness, tactical relevance, and accuracy of intelligence are especially vital.

— § — § — § —


USA







# CHAPTER FOUR

# New Direction - Future Challenges

*"Our world without the Cold War confrontation is a safer world, but it is no Garden of Eden. . . Intelligence remains our basic national instrument for anticipating danger: military, political, and economic."*

— President George Bush, 1991

U.S. national security planning focuses on the uncertain environment of regional conflict. Many factors promote regional instability: the breakup of multiethnic nations, state-sponsored terrorism, drug trafficking, proliferation of advanced weapons technology (including weapons of mass destruction), and militant religious fundamentalism. U.S. military strategy necessarily emphasizes operations in littoral regions of the world to support national and international security interests.

We face a world characterized by political disorder and confrontation, intense economic competition among nations, and a growing technological threat. Potential adversaries now can buy sophisticated surveillance, communications, and weapon systems on the world market at affordable prices. New centers of power and influence are emerging, sometimes threatening U.S. interests. Naval intelligence professionals must anticipate and understand these changes. Multiple threats worldwide present other new challenges, and naval intelligence must employ new methods and procedures so that naval forces can meet them.

At present, naval intelligence organizations are reorienting their efforts to meet future needs. These include facing significant challenges with respect to supporting expeditionary forces, keeping training and readiness at a high level, coordinating and cooperating with other services and nations, exploiting the opportunities of the information revolution, and preparing for future operations. These challenges are interrelated and require skilled, mission-oriented intelligence professionals who can manage multiple intelligence disciplines to provide the commander a tailored, all-source assessment of the battlespace.

## Support for Expeditionary Forces

Forward deployed naval forces will continue to be the National Command Authorities' force of choice to remain engaged overseas. Unrestricted by host nation access, naval forces continue to provide a strong and flexible overseas presence to deter potential aggression or respond to crises. Naval forces may be called upon for forcible entry into areas defended by integrated air, sea, and ground weapon systems. Some defenses will consist of forces in fixed positions; others will include mobile combined-arms units backed by naval forces and aircraft. A future adversary may employ the newest missiles, mines, and military technology against our aircraft, ships, submarines, and landing forces. The proliferation of these modern weapons and the spread of emerging technologies have made these threats more lethal, placing U.S. and multinational forces at greater risk. As the lessons of military history show, we cannot afford to discount the Third World threat.

Intelligence requirements in littoral regions are significantly different from those of open-ocean operations. Our proximity to littoral threats will mean less warning and reaction time for friendly forces. Any potential adversary's acquisition of advanced technology is a significant concern as well. Consequently, naval intelligence must maintain detailed databases on potential threats and develop methods to exploit each adversary's weaknesses.

Identifying those areas where military operations may be conducted is vital. Detailed information on the environment and local infrastructure (bathymetry, weather, topography, ports, air facilities, etc.) will be required to support the full range of expeditionary operations. Nontraditional intelligence sources, collection means, and dissemination methods must be explored and employed. Open-source intelligence may be especially important. In addition, forces deploying to areas known for infectious diseases must have advance information about local medical conditions. Forward deployed expeditionary forces must incorporate medical intelligence as a force protection measure.

The naval command and control architecture must ensure connectivity between naval forces afloat and ashore (including theater and national support agencies)—and must be useable by the warfighter. Intelligence databases and communications must be interoperable with other services, non-DOD government agencies, and joint intelligence centers to ensure the uninterrupted flow of intelligence to the commander. Naval intelligence must be prepared to support amphibious operations during sustained operations ashore, while simultaneously supporting requirements of the ships, submarines, and aircraft that maintain battlespace dominance in the littoral area of operations. To be most effective in expeditionary operations, naval intelligence personnel should be integrated into national, theater, and service intelligence organizations to articulate naval capabilities and operational philosophies, influence decisions, and optimize intelligence support to naval forces. This support requires extensively trained naval intelligence professionals.

## Training and Readiness

To remain ahead of the challenges associated with geopolitical upheavals, socioeconomic crises, and rapid technological innovation, naval intelligence personnel must receive comprehensive and specialized training. Intelligence training should be updated continuously, reflecting tomorrow's challenges. Basic, intermediate, and advanced training, both ashore and afloat, should include non-institutional methods—such as on-the-job training—and should develop well-rounded, career-oriented professionals who will have credibility within the intelligence and cryptologic communities, the naval Service, and external agencies and organizations.

Training underpins broad professional experience. Personnel rotation policies and deployment cycles must enable intelligence personnel to maintain career paths that provide them experience in naval, joint, and multinational operations. Of particular concern is adequate foreign-area and language expertise. Operations in littoral regions of the world create unprecedented specialized language requirements, thus adequate language training should be made available. Foreign language proficiency, especially in languages not commonly studied, must be emphasized continually in training programs.

As naval professionals, we must train the way we fight. To be effective during real-world operations, naval intelligence must be integrated into all aspects of operational training. Such training increases exposure to operations and provides the intelligence professional a deeper understanding of capabilities and limitations—essential in advising the commander on ways to counter adversary capabilities.

Another cost-effective way to train is to capitalize on modeling and simulation to test concepts, doctrine, and connectivity—without having to deploy actual forces. Intelligence must be used in exercises and simulations—especially free-play sessions—to maintain the skills necessary to support all forms of naval, joint, and multinational operations. Intelligence training is the prerequisite for real-time intelligence support to operations.

Other intelligence assets that enhance training and readiness are reserve intelligence and cryptologic personnel. These personnel are trained and readily available, and can be integrated quickly into the active component. They include academics, business executives, and country-area experts whose civilian jobs may place them in close contact with influential foreign leaders or littoral regions of particular interest. Identifying and establishing databases of unique reserve skills and expertise will enhance intelligence support to naval expeditionary operations. In concert with these actions, the active component should ensure that unique reserve skills and expertise, able to support combat operations and contingencies, are identified early in the planning process. The reserves represent a large pool of talent that can significantly augment the commander's intelligence effort.



## Coordination and Cooperation

In the future, closer coordination and cooperation with other services and other nations will assume even great importance than they have today. Future joint and multinational operations will require compatible intelligence systems that complement those employed by other services, multinational forces, and national agencies, including non-DOD government agencies.

Experience in operational theaters around the world demonstrates that early planning for intelligence sharing improves intelligence support and shortens delays in dissemination. Simple procedures should exist—and be exercised often—to handle sharing of classified material. Sometimes multinational partners may have more current data or better access to specific information about an adversary or the environment than our own forces. Exchanging personnel and systems can improve the flow of information, minimize misunderstandings, and improve the efficacy of operations as well as aid in area stability. Liaison officers act as bridges between cultures, languages, doctrines and methodologies. Coordination and cooperation among intelligence personnel facilitate planning and execution. Naval intelligence personnel should strive to provide intelligence support under simulated wartime or crisis conditions to ensure they can do so under the strain and confusion of combat.



## Intelligence and the Information Revolution

Naval commanders today must orchestrate combined arms operations across the dimensions of air, land, surface, subsurface, space, and time. To fight and win in this multidimensional battlespace, the naval commander must harness sophisticated information technology.

Emerging communications, computer and reconnaissance technology is revolutionizing the commander's ability to maintain situational awareness and control his forces effectively. Since naval forces are forward deployed, the naval intelligence system should be flexible and responsive to the commander's needs. The communications architecture for intelligence dissemination must provide the naval commander a global, instantaneous, secure, and survivable capability that includes:

- Responsive surveillance of selected geographic areas
- Real-time information transfer to commanders at various echelons
- Responsive, secure communications between decisionmakers and operational commanders
- Intelligence push/pull with automatic over-the-air database update for forward deployed forces

Driven by technological advances, naval expeditionary forces are now part of an electronic web that ties sensors, decisionmakers and operating forces together in an integrated, global network. To provide the commander timely and accurate information to operate amid the chaos of battle, management and tailoring of information will be crucial to success in future conflicts.

The commander relies on electronic information and communication systems to gain situational awareness, select a course of action, and direct military operations. Naval intelligence systems must provide continuous, comprehensive support to the commander. Potential adversaries possess or seek similar decisionmaking capabilities that can provide them combat advantage over their adversary. Establishing command and control dominance will give the commander a complete and transparent view of the battlespace, while the adversary still struggles to peer through an opaque lens.

Naval intelligence must seize the opportunities offered by the technological revolution. Because of the vast amount of sensor data available today and the high speed at which it is processed and displayed, superior intelligence analysis, fusion and dissemination capabilities are needed to gain best leverage from the information advantage. Quality of intelligence always must take precedence over quantity. To be effective, intelligence must be processed and presented as an integral part of the commander's tactical picture. Only through *accurate* depiction will the commander's needs be satisfied. Accordingly, data displays must be revised and updated continually to ensure the information remains accurate.

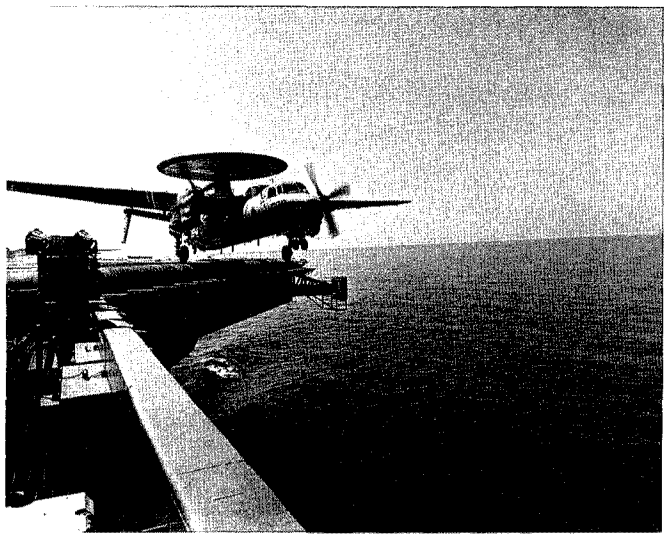
## Support to Information Warfare/Command and Control Warfare

Information Warfare/Command and Control Warfare (IW/C2W) offers the commander an additional means to engage adversarial forces. IW/C2W seeks to deceive, disrupt or destroy the adversary's information infrastructure and command and control process to subdue the opposition rapidly. At the same time, IW/C2W seeks to protect our information infrastructure and command and control process from attack.

To be successful, IW/C2W must be based on sound intelligence. Current and precise knowledge of the adversary's information and command and control systems—especially their critical and vulnerable nodes—is paramount in IW/C2W planning and execution.[10] Intelligence plays a vital role by identifying essential and vulnerable adversary nodes, as well as by recommending those nodes that we should *not* degrade or destroy because of the intelligence gained through their exploitation. Naval intelligence gives the commander the ability to strike an adversary at precise times and places—to blind, cripple, deceive, or destroy him.

[10] In this context, *nodes* are points within the command and control system where personnel, equipment and procedures converge to perform command and control functions. Nodes can include command centers, radar and surveillance sites, intelligence facilities, communications stations, as well as the supporting infrastructure. Nodes are linked together by communications or data networks. *Critical nodes* are the essential elements of a command and control system whose disruption or destruction immediately degrades the ability of a force to command, control or effectively conduct combat operations.

IW/C2W relies on fused, all-source intelligence to plan and execute operations. It requires complete all-source databases, sound analysis, and rapid and reliable communications. Further, without accurate knowledge of the adversary's weaknesses, strengths, disposition, and intentions, the commander may find that his efforts are ineffective. Standard intelligence functions must be applied innovatively and meticulously to support all aspects of IW/C2W: deception, operations security, psychological operations, electronic warfare, and destruction.



Naval cryptology, in particular, is essential in IW/C2W efforts to disrupt the adversary's decisionmaking process and sever the links between the adversary commander and his forces. Dominance of the electromagnetic battlespace lies at the heart of IW/C2W. Cryptologic operations characterize and map this battlespace. By detecting, locating, exploiting, and attacking threat emitters, cryptology supports immediate decisionmaking for employment of electronic attack, threat warning and avoidance, and targeting.

## Intelligence Emphasis

*"It is my desire to conserve, to the maximum practible extent, the DNI [Director of Naval Intelligence] organization and strength and if possible to get them more help. The greater the contractions of the Navy— the more important our DNI and Communications Intelligence become."*

— Fleet Admiral Chester Nimitz, U. S. Navy
Chief of Naval Operations, 1947

The unpredictable nature of future threats demands that naval intelligence invest wisely in areas that will enhance the capabilities of naval expeditionary warfare. An area that continues to show promise is an active and dedicated involvement in the use of national sensors for operational and tactical intelligence support. We must ensure that sensors and collection methods, afloat and ashore fusion centers, and dissemination systems are highly capable and responsive to support operations. These capabilities are required to provide the commander and his forces the broad area coverage they need, along with timely Indications and Warning.

Since naval expeditionary forces must be fully integrated with national and theater collection platforms, a dedicated effort should be made to provide timely, accurate, and complete sensor-to-shooter connectivity. To complement these capabilities, naval forces require an organic collection and intelligence-processing capability to locate high-value targets and gaps in adversary defenses quickly and accurately, through an integrated network of organic reconnaissance systems. Competition for national sensors, orbital limitations, or other factors may sometimes preclude adequate support to operating forces; therefore, the commander must have alternate capabilities. This need is particularly compelling when projecting power ashore in littoral regions where adequate charts and maps are lacking.

The spread of highly sophisticated telecommunications systems in littoral regions today presents a major challenge to naval cryptology. Rapidly evolving technology and equipment will increase

the complexity of this threat and its supporting infrastructure. Naval cryptologic systems must be able to exploit the target threat, maintain a high state of readiness, be as survivable and mobile as the forces they support, and have the flexibility to allow tailoring of cryptologic direct support units for specific mission requirements.

Although we live in an age of instantaneous communications, technical collection is not the only way to gather intelligence about an adversary. For instance, counterintelligence operations can neutralize and degrade an adversary's intelligence effort while HUMINT operations can provide unique intelligence, normally not accessible by other means, about adversary activity–to include rare insight into his intentions. Recent operations demonstrate that naval expeditionary forces need to have a strong tactical HUMINT capability.



The HUMINT capability must be expanded to meet the operational requirements of the future without decreasing the counterintelligence force protection role–collection, investigations, operations, multidiscipline analysis, and support to operations security and counter-reconnaissance. Employed as part of an all-source intelligence effort, HUMINT and counterintelligence operations provide the commander unique information.

— § — § — § —

# CONCLUSION

In an increasingly multi-polar world, naval intelligence professionals face many new and profound challenges. Mission success depends on dedicated personnel with intellectual curiosity, initiative, integrity and a detailed understanding of operations. Closely aligned to the need for dedicated personnel is the need for unsurpassed intelligence capabilities that are relevant and operationally responsive.

The strength and lasting character of naval intelligence lie in its integration with naval operating forces. This union will enable the commander to achieve decisive combat results. In order to accomplish this, naval intelligence must be able to survey the battlespace and anticipate the commander's requirements by understanding an adversary's capabilities, assessing his intentions, and identifying his centers of gravity and critical vulnerabilities.

NDP-2, Naval Intelligence, articulates those time-honored and battle-tested principles which have been derived from more than a century of experience. Naval commanders must consider intelligence as an integral part of their combat power—and the potential difference between victory and defeat.

# APPENDIX A: JOINT AND NAVAL INTELLIGENCE ORGANIZATIONS THAT SUPPORT NAVAL OPERATIONS

1. The joint intelligence architecture normally exists at four levels:

National. The National Military Joint Intelligence Center (NMJIC) is the central body for management of national intelligence operations. Closely tied to the Defense Intelligence Agency (DIA), the NMJIC supports the intelligence needs of the Chairman of the Joint Chiefs of Staff and the needs of the unified commanders. The NMJIC focuses mainly on global Indications and Warning, operational intelligence, national targeting support, production and database management. The National Security Agency/Central Security Service (NSA/CSS) also provides signals intelligence, combat information and information security devices and assistance in its role as a Combat Support Agency.

Unified Command. The theater Joint Intelligence Center (JIC) supports the Unified Commander, service components and subordinate Joint Task Forces (JTFs). Its functions are similar to those of the NMJIC, although limited to the Unified Commander's geographic or functional area of responsibility. The theater JIC is the primary source for target area intelligence assessments and databases.

Joint Task Force. At the JTF level, the JIC supports the intelligence needs of the JTF commander and subordinate warfighting

component commands. The JTF JIC is normally established to support and focus on a specific military operation and is typically collocated with the JTF commander and staff. It may be afloat or ashore and is usually composed of intelligence personnel from the JTF staff augmented by personnel from the theater JIC, component services, and national agencies.

Service Component. At the component level, service intelligence centers, such as an amphibious flagship's JIC, support the intelligence needs of the component commander and subordinate units. Although closely linked to the larger joint intelligence architecture, naval intelligence centers, afloat or deployed ashore as part of a MAGTF, focus their efforts on executing naval operations. During joint operations in littoral regions, when a naval commander is commander of the JTF, naval intelligence centers may function as both the service component intelligence center and a JTF JIC simultaneously.

2. The Department of the Navy has established intelligence organizations that provide unique and continuous intelligence support to naval maritime and expeditionary operations.

National Maritime Intelligence Center (NMIC) - The National Maritime Intelligence Center incorporates the Office of Naval Intelligence, the Marine Corps Intelligence Activity, and the Coast Guard Intelligence Coordination Center, and is the national resource for all maritime and expeditionary intelligence-related issues.

Office of Naval Intelligence (ONI) - The Office of Naval Intelligence organizes and trains intelligence personnel, provides highly specialized, maritime-related intelligence analysis, and administers intelligence oversight, security, and intelligence manpower issues. Its day-to-day operations include liaison with both DOD and non-DOD agencies, long-term analysis of foreign military and naval forces and operations, foreign liaison support, scientific and technical analysis, strategic trade analysis, and intelligence systems acquisition.

Commander, Naval Security Group (COMNAVSECGRU) - The Commander, Naval Security Group Command is the Navy's executive agent for cryptology and information warfare/command and control warfare. COMNAVSECGRU is responsible for cryptologic planning and programming, systems acquisition, training, and administration of the naval cryptologic field activities around the world. Marine Corps participation within the Naval Security Group is provided by the Marine Support Battalion that collocates companies at selected naval cryptologic field activities. Marine Support Battalion also provides support to naval expeditionary operations through augmentation of Fleet Marine Force Radio Battalions.

Marine Corps Intelligence Activity (MCIA) - The Marine Corps Intelligence Activity focuses on crises and predeployment support to expeditionary warfare. It complements and coordinates the efforts of theater, other service, and national intelligence organizations providing unique threat, technical, and terrain-analysis products that are tailored to Marine Corps tactical units preparing to deploy to a theater of operations. The activity functions as the service collection and production manager, and as the primary coordination link with ONI for expeditionary intelligence analysis and production. Additionally, MCIA provides threat and technical intelligence assessments supporting the Concept Based Requirements System in areas of service-unique doctrinal development, force structure, force modernization, training and education, and acquisition.

Coast Guard Intelligence Coordination Center (ICC) - The Intelligence Coordination Center, a Coast Guard tenant command at the NMIC, provides strategic intelligence support to Coast Guard law enforcement, military readiness, port security, marine safety, and environmental protection missions. The ICC serves as the Coast Guard's 24-hour I&W watch, maintaining a current picture of all maritime threats. It serves as the Coast Guard's primary interface with the collection, production, and dissemination elements of the national intelligence and law enforcement communities.

# GLOSSARY

**Acoustic Intelligence (ACINT):** Intelligence derived from the collection and processing of acoustic phenomena. (Joint Pub 1-02)

**All-source Intelligence:** Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, HUMINT, IMINT, MASINT, SIGINT, and open source data, in the production of finished intelligence. (Joint Pub 1-02)

**Battlespace:** All aspects of air, surface, and subsurface, land, space, and the electromagnetic spectrum that encompass the area of influence and area of interest. (NWP 1-02)

**Commander's Estimate of the Situation.** A logical process of reasoning by which a commander considers all the circumstances affecting the military situation and arrives at a decision as to a course of action to be taken to accomplish the mission. (Joint Pub 1-02)

**Communications Intelligence (COMINT):** Technical and intelligence information derived from foreign communications by other than the intended recipients. (Joint Pub 1-02)

**Counterintelligence (CI):** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Joint Pub 1-02)

**Critical Vulnerability:** That element of a military force that is vulnerable to attack and whose degradation or destruction will lead to defeating the enemy's center of gravity and, ultimately, his ability to resist. (NWP 1-02)

**Deception:** Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1-02)

**Electronics Intelligence (ELINT):** Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (Joint Pub 1-02)

**Electro-optical Intelligence (ELECTRO-OPTINT):** Intelligence other than signals intelligence derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (O.O1 micrometers) through far infrared (l,OOO micrometers). (Joint Pub 1-02)

**Foreign Instrumentation Signals Intelligence (FISINT):** Technical information and intelligence information derived from the intercept of foreign instrumentation signals by other than the intended recipients. (Joint Pub 1-02)

**Fusion:** In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (Joint Pub 1-02)

**Fusion Center:** In intelligence usage, a physical location to accomplish fusion. It normally has sufficient intelligence automated data processing capability to assist in the process. (Joint Pub 1-02)

**Human Intelligence (HUMINT):** A category of intelligence derived from information collected and provided by human sources. (Joint Pub 1-02)

**Imagery Intelligence (IMINT):** Intelligence derived from the exploitation of collection by visual photography, infrared sensors,

lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. (Joint Pub 1-02)

**Indications and Warning (I&W):** Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United states, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attack; and other similar events. (Joint Pub 1-02)

**Infrared Intelligence (IRINT):** Intelligence derived from information collected by infrared sensors. (NWP 1-02)

**Intelligence:** The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. (Joint Pub 1-02)

**Intelligence Estimate:** The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (Joint Pub 1-02)

**Intelligence Requirement:** Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (Joint Pub 1-02)

**Joint Intelligence Center (JIC):** The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. (Joint Pub 1-02).

**Laser Intelligence (LASINT):** Technical and geolocation intelligence derived from laser systems; a subcategory of electro-optical intelligence. (Joint Pub 1-02)

**Littoral:** 1. Seaward: Area from the shore to open ocean that must be controlled to support operations;

2. Landward: Area inland from shore that can be supported and defended directly from the sea. (NWP 1-02)

**Measurement and Signature Intelligence (MASINT):** Scientific and technical intelligence obtained-by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same. (Joint Pub 1-02)

**Medical Intelligence (MEDINT):** That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information which is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. (Joint Pub 1-02)

**National Intelligence Support Team (NIST):** A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. (Joint Pub 1-02)

**Naval Cryptology:** Action taken to exploit and attack foreign communications and other electromagnetic signals, while protecting our own, for the purposes of command and control warfare, electronic warfare, signals intelligence, and signals security. (NWP 1-02)

**Nuclear Intelligence** (NUCINT): Intelligence derived from the collection and analysis of radiation and other effects resulting from radioactive sources. (Joint Pub 1-02)

**Open Source Intelligence** (OSINT): Information of potential intelligence value that is available to the general public. (Joint Pub 1-02)

**Operational Intelligence**: Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations. (Joint Pub 1-02)

**Photographic Intelligence** (PHOTINT): The collected products of photographic interpretation, classified and evaluated for intelligence use. (Joint Pub 1-02)

**Radar Intelligence** (RADINT): Intelligence derived from data collected by radar. (Joint Pub 1-02)

**Reconnaissance**: A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (Joint Pub 1-02)

**Scientific and Technical Intelligence (S&TI)**: The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture. (Joint Pub 1-02)

**Signals Intelligence (SIGINT):** A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. (Joint Pub 1-02)

**Strategic Intelligence:** Intelligence that is required for the formulation of strategy, policy, and military plans and operations at national and theater levels. (Joint Pub 1-02)

**Surveillance:** The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (Joint Pub 1-02)

**Tactical Intelligence:** Intelligence that is required for planning and conducting tactical operations. (Joint Pub 1-02)

**Targeting:** 1. The process of selecting targets and matching the appropriate response to them taking account of operational requirements and capabilities. 2. The analysis of enemy situations relative to the commander's mission, objectives, and capabilities at the commander's disposal, to identify and nominate specific vulnerabilities that, if exploited, will accomplish the commander's purpose through delaying, disrupting, disabling, or destroying enemy forces or resources critical to the enemy. (Joint Pub 1-02)

**Target Materials:** Graphic, textual, tabular, digital, video, or other presentations of target intelligence, primarily designed to support operations against designated targets by one or more weapons system(s). Target materials are suitable for training, planning, executing, and evaluating military operations. (Joint Pub 1-02)

**Technical Intelligence (TECHINT):** Intelligence derived from exploitation of foreign material, produced for strategic, operational, and tactical level commanders. (Joint Pub 1-02)

**Telemetry Intelligence (TELINT):** Technical intelligence derived from the intercept, processing, and analysis of foreign telemetry. Telemetry intelligence is a category of foreign instrumentation signals intelligence. (Joint Pub 1-02)

**Unintentional Radiation Intelligence (RINT):** Intelligence derived from the collection and analysis of non-information-bearing elements extracted from the electromagnetic energy unintentionally emanated by foreign devices, equipment, and systems, excluding those generated by the detonation of nuclear weapons. (Joint Pub 1-02)

**Validation:** A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. (Joint Pub 1-02)

**Weaponeering:** The process of determining the quantity of a specific type of lethal or nonlethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapon effect, munitions delivery accuracy, damage criteria, probability of kill, and weapon reliability. (Joint Pub 1-02)

# SUGGESTED FOLLOW-ON READINGS

Joint Publication 2-0, "Joint Doctrine for Intelligence Support to Operations" (Washington, D.C.: Joint Chiefs of Staff, 1993).

Joint Publication 2-02, "Joint Tactics, Techniques and Procedures for Intelligence Support to Joint Task Force Operations" (Washington, D.C.: Joint Chiefs of Staff, 1993 (Proposed Publication-Secret Noforn)).

Naval Doctrine Publication 1, "Naval Warfare" (Washington, D.C.: Department of the Navy, 1994).

Fleet Marine Force Manual 3-20, "Commander's Guide to Intelligence" (Washington, D.C.: Department of the Navy, 1991).

Fleet Marine Force Manual 3-21, "MAGTF Intelligence Operations" (Washington, D.C.: Department of the Navy, 1991).

Fleet Marine Force Manual 3-25, "Counterintelligence" (Washington, D.C.: Department of the Navy, 1991).

Field Manual 34-1, "Intelligence and Electronic Warfare Operations" (Washington, D.C.: Department of the Army, 1993).

Field Manual 34-130, "Intelligence Preparation of the Battlefield" (Washington, D.C.: Department of the Army, 1994).

Handel, Michael I., ed. Intelligence and Military Operations. (London, England, Frank Cass & Co., Ltd., 1990).

Handel, Michael I., ed. Leaders and Intelligence. (London, England, Frank Cass & Co., Ltd., 1989).

Handel, Michael I., ed. War, Strategy and Intelligence. (London, England, Frank Cass & Co., Ltd., 1989).

Holmes, W. J. Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific during World War II. (Annapolis, MD: Naval Institute Press, 1979).

Layton, Edwin T., et al. And I Was There: Pearl Harbor and Midway-Breaking the Secrets. (New York, NY: William Morrow and Co., 1985).

Wohlstetter, Roberta. Pearl Harbor: Warning and Decision. (Stanford, CA: Stanford University Press, 1962).

Naval Doctrine Command was established by the Department of the Navy in 1993. Its primary missions are to develop naval concepts and integrated naval doctrine; provide a coordinated Navy-Marine Corps voice in joint and multinational doctrine development; and address naval and joint doctrine with respect to training, education, operations, exercises, simulations, and war games. To ensure doctrine remains relevant we encourage your feedback on this publication and other doctrinal issues. Address your comments to:

Commander, Naval Doctrine Command
1540 Gilbert Street
Norfolk, VA 23511-2785

Additional copies of this publication may be obtained through the following distribution centers:

Navy Publications and Forms Directorate
5801 Tabor Avenue
Philadelphia, PA 19120-5099
re: SN 0700LP0000200

Marine Corps Logistics Base Atlantic
Warehouse 1221, Section 5, M/F: Pubs Stock
Albany, GA 31704-5001
re: PCN 14100020000

This publication may be purchased by non-government personnel by writing to: ASO/NPFD Attn: Cash Sales Code 1013, 5801 Tabor Avenue, Philadelphia PA 19120-5099 or National Technical Information Services, 5285 Port Royal RD., Springfield, VA 22161, Attn: Military Publication