NAVY WARFARE PUBLICATION

INTELLIGENCE SUPPORT TO NAVAL OPERATIONS NWP 2-01

NOVEMBER 2010

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS

URGENT CHANGE/ERRATUM RECORD		
NUMBER	DATE	ENTERED BY

INTENTIONALLY BLANK

DEPARTMENT OF THE NAVY
NAVY WARFARE DEVELOPMENT COMMAND
1528 PIERSEY STREET BLDG O-27
NORFOLK VA 23511-2723

November 2010

LETTER OF PROMULGATION

1. NWP 2-01 (NOV 2010), INTELLIGENCE SUPPORT TO NAVAL OPERATIONS, is UNCLASSIFIED. Handle in accordance with the administrative procedures contained in NTTP 1-01, The Navy Warfare Library.

2. NWP 2-01 (NOV 2010), INTELLIGENCE SUPPORT TO NAVAL OPERATIONS, is effective upon receipt and supersedes NWP 2-01 (JAN 1997), INTELLIGENCE SUPPORT TO OPERATIONS AFLOAT. Destroy superseded material without report.

3. NWP 2-01 (NOV 2010), INTELLIGENCE SUPPORT TO NAVAL OPERATIONS, is a comprehensive reference detailing the intelligence support available to the operational commander. It also serves as a ready resource for the Information Dominance Corps intelligence professionals, information warfare officers, and cryptologic technicians.

4. NWP 2-01 (NOV 2010), INTELLIGENCE SUPPORT TO NAVAL OPERATIONS, is not approved for public release. Further dissemination only as directed by Navy Warfare Development Command or higher DOD authority. This determination was made August 23, 2010. Requests for this document shall be referred to Navy Warfare Development Command, 1528 Piersey Street, Norfolk, VA 23511-2723.

WENDI B. CARPENTER

INTENTIONALLY BLANK

November 2010

PUBLICATION NOTICE

ROUTING

1. NWP 2-01 (NOV 2010), INTELLIGENCE SUPPORT TO NAVAL OPERATIONS, is available in the Navy Warfare Library. It is effective upon receipt.

2. Summary. NWP 2-01 (NOV 2010), INTELLIGENCE SUPPORT TO NAVAL OPERATIONS, is a complete rewrite of NWP 2-01 (JAN 1997), INTELLIGENCE SUPPORT TO OPERATIONS AFLOAT. NWP 2-01 (NOV 2010), INTELLIGENCE SUPPORT TO NAVAL OPERATIONS, is a comprehensive reference detailing the intelligence support available to the operational commander. It also serves as a ready resource for the Information Dominance Corps intelligence professionals, information warfare officers, and cryptologic technicians.

Navy Warfare Library Custodian

Navy Warfare Library publications must be made readily available to all users and other interested personnel within the U.S. Navy. Classified Navy Warfare Library publications are to be treated in the same manner as other classified information.

Note to Navy Warfare Library Custodian

This notice should be duplicated for routing to cognizant personnel to keep them informed of changes to this publication.

INTENTIONALLY BLANK

CONTENTS

Page No.

CHAPTER 4 — SUPPORT TO NAVY INTELLIGENCE FORWARD

LIST OF ILLUSTRATIONS

Page No.

CHAPTER 2 — NAVY INTELLIGENCE ENTERPRISE

CHAPTER 3 — NAVY INTELLIGENCE OPERATIONS

PREFACE

Unless otherwise stated, masculine nouns and pronouns do not refer exclusively to men.

Report administrative discrepancies by letter, message, or e-mail to:

COMMANDER
NAVY WARFARE DEVELOPMENT COMMAND
ATTN: DOCTRINE
1528 PIERSEY STREET BLDG O-27
NORFOLK VA 23511-2723

NWDC_NRFK_FLEETPUBS@NAVY.MIL

ORDERING DATA

Order printed copies of a publication using the Print on Demand (POD) system. A command may requisition a publication using standard military standard requisitioning and issue procedure (MILSTRIP) procedures or the Naval Supply Systems Command website called the Naval Logistics Library (https://nll1.ahf.nmci.navy.mil). An approved requisition is forwarded to the specific DAPS site at which the publication's electronic file is officially stored. Currently, two copies are printed at no cost to the requester.

CHANGE RECOMMENDATIONS

Procedures for recommending changes are provided below.

WEB-BASED CHANGE RECOMMENDATIONS

Recommended changes to this publication may be submitted to the Navy Doctrine Library System, accessible through the Navy Warfare Development Command website at: http://ndls.nwdc.navy.smil.mil or https://ndls.nwdc.navy.mil.

URGENT CHANGE RECOMMENDATIONS

When items for changes are considered urgent, send this information by message to the Primary Review Authority, info NWDC. Clearly identify and justify both the proposed change and its urgency. Information addressees should comment as appropriate. See accompanying sample for urgent change recommendation format on page 13.

ROUTINE CHANGE RECOMMENDATIONS

Submit routine recommended changes to this publication at any time by using the accompanying routine change recommendation letter format on page 14 and mailing it to the address below, or posting the recommendation on the Navy Doctrine Library System site.

COMMANDER
NAVY WARFARE DEVELOPMENT COMMAND
ATTN: DOCTRINE
1528 PIERSEY STREET BLDG O-27
NORFOLK VA 23511-2723

CHANGE BARS

Revised text is indicated by a black vertical line in the outside margin of the page, like the one printed next to this paragraph. The change bar indicates added or restated information. A change bar in the margin adjacent to the chapter number and title indicates a new or completely revised chapter.

WARNINGS, CAUTIONS, AND NOTES

The following definitions apply to warnings, cautions, and notes used in this manual:

WARNING

An operating procedure, practice, or condition that may result in injury or death if not carefully observed or followed.

CAUTION

An operating procedure, practice, or condition that may result in damage to equipment if not carefully observed or followed.

Note

An operating procedure, practice, or condition that requires emphasis.

WORDING

Word usage and intended meaning throughout this publication are as follows:

“Shall” indicates the application of a procedure is mandatory.

“Should” indicates the application of a procedure is recommended.

“May” and “need not” indicate the application of a procedure is optional.

“Will” indicates future time. It never indicates any degree of requirement for application of a procedure.

FM ORIGINATOR
TO *(Primary Review Authority)*//JJJ//
INFO COMNAVWARDEVCOM NORFOLK VA//N-5//
COMUSFLTFORCOM NORFOLK VA//JJJ//
COMUSPACFLT PEARL HARBOR HI//JJJ//
(Additional Commands as Appropriate)//JJJ//
BT
CLASSIFICATION//N03510//
MSGID/GENADMIN/*(Organization ID)*//
SUBJ/URGENT CHANGE RECOMMENDATION FOR *(Publication Short Title)*//
REF/A/DOC/NTTP 1-01//
POC/*(Command Representative)*//
RMKS/ 1. IAW REF A URGENT CHANGE IS RECOMMENDED FOR *(Publication Short Title)*
2. PAGE _____ ART/PARA NO _____ LINE NO _____ FIG NO _____
3. PROPOSED NEW TEXT *(Include classification)*

4. JUSTIFICATION.
BT

Message provided for subject matter; ensure that actual message conforms to MTF requirements.

Urgent Change Recommendation Message Format

DEPARTMENT OF THE NAVY
NAME OF ACTIVITY
STREET ADDRESS
CITY, STATE XXXXX-XXXX

5219
Code/Serial
Date

FROM: *(Name, Grade or Title, Activity, Location)*
TO: *(Primary Review Authority)*

SUBJECT: ROUTINE CHANGE RECOMMENDATION TO *(Publication Short Title, Revision/Edition, Change Number, Publication Long Title)*

ENCL: *(List Attached Tables, Figures, etc.)*

1. The following changes are recommended for NTTP X-XX, Rev. X, Change X:

a. CHANGE: (Page 1-1, Paragraph 1.1.1, Line 1)
Replace "...the ~~National Command Authority~~ President and Secretary of Defense establish~~es~~ procedures for the..."
REASON: SECNAVINST ####, dated ####, instructing the term "National Command Authority" be replaced with "President and Secretary of Defense."

b. ADD: (Page 2-1, Paragraph 2.2, Line 4)
Add sentence at end of paragraph "See Figure 2-1."
REASON: Sentence will refer reader to enclosed illustration.
Add Figure 2-1 (see enclosure) where appropriate.
REASON: Enclosed figure helps clarify text in Paragraph 2.2.

c. DELETE: (Page 4-2, Paragraph 4.2.2, Line 3)
Remove "Navy Tactical Support Activity."
"...~~Navy Tactical Support Activity, and~~ the Navy Warfare Development Command ~~are~~ is responsible for..."
REASON: Activity has been deactivated.

2. Point of contact for this action is *(Name, Grade or Title, Telephone, E-mail Address)*.

(SIGNATURE)
NAME

Copy to:
COMUSFLTFORCOM
COMUSPACFLT
COMNAVWARDEVCOM

Routine Change Recommendation Letter Format

CHAPTER 1

Introduction

1.1 GENERAL

Fourteen years have elapsed since Navy Warfare Publication (NWP) 2-01, Intelligence Support to Operations Afloat (January 1997), was disseminated to the fleet. This introduction cannot begin to convey the changes that have occurred in the global security environment and the elevation of information to a "main battery" of the United States Navy's (USN's) arsenal.

Naval Intelligence has a proud and rich history extending well over 100 years; however, it is just a part of the entire Intelligence Community (IC), military and civilian, supporting America's forces. Naval forces are proud to be at the forefront of joint and combined operations, and the events of the recent decade further illustrate the indispensable role of intelligence across the range of military operations (ROMO). The success of these operations depended upon the delivery of accurate and timely intelligence to the President, the Secretary of Defense (SECDEF), the combatant commanders (CCDRs), and the aircrews and ships operating around the world.

The attacks of September 11, 2001 substantially changed the strategic landscape and shaped our national security strategy. Today, combatant commands plan for a wide range of operations against a similarly wide range of threats. The Navy continually refines its core capabilities to support those plans, and correspondingly, the IC anticipates, identifies, and seeks to understand those threats in detail. The range of threats facing planners and their executors today has grown exponentially and in an asymmetrical fashion. Decision makers rely on intelligence to provide them an operational advantage by enabling the selection of optimal courses of action (COAs) in a time-sensitive maritime environment.

1.2 PURPOSE

NWP 2-01 is a comprehensive reference detailing the intelligence support available to the naval commander in the successful planning and execution of operations.

1.3 SCOPE

NWP 2-01 is by nature a refresher and ready resource for the Information Dominance Corps (IDC) intelligence professionals, information warfare officers, and cryptologic technicians; however, the target audience is the operational commander. The publication's length and content are specifically tailored to ensure a practical and valuable reference for the operational decision maker. NWP 2-01 is the foundation for a series of proposed follow-on Navy tactics, techniques, and procedures (NTTP) publications.

1.3.1 Chapter 1 — Introduction

Chapter 1 addresses the role of intelligence within the six core capabilities of our current maritime strategy. The Navy's recent focus on information dominance (ID) and the standup of the IDC is presented. Finally, maritime domain awareness (MDA) as an outcome of intelligence gathering, production, and sharing is introduced.

1.3.2 Chapter 2 — Navy Intelligence Enterprise

Chapter 2 delineates the naval afloat and ashore billets and organizations providing direct intelligence support to the operational commander.

1.3.3 Chapter 3 — Navy Intelligence Operations

Chapter 3 defines the levels of intelligence and describes the processes by which the intelligence team optimally accomplishes the majority of its tasks. Next, the intelligence composition and organization of afloat and deployable naval assets is provided. The remainder of the chapter describes the ROMO in which the Navy must be prepared to participate.

1.3.4 Chapter 4 — Support to Navy Intelligence Forward

Chapter 4 reports on the various national, theater, joint task force (JTF), and Service intelligence organizations that make up the IC and reveals how these organizations may assist afloat and deployed naval assets. The chapter concludes by addressing interagency and multinational intelligence sharing considerations.

1.4 A COOPERATIVE STRATEGY FOR 21ST CENTURY SEAPOWER

The October 2007 Maritime Strategy of the United States (U.S.) sea services stresses an approach that integrates seapower with other elements of national power, as well as those of U.S. friends and allies. It describes the application of seapower around the world to protect the American way of life, as the United States joins with other like-minded nations to guard and sustain the global environment in which we operate. Successful implementation of this strategy assuredly requires robust intelligence integrated with maritime operations. “A Cooperative Strategy for 21st Century Seapower” calls for an expanded portfolio of six core capabilities.

1.4.1 Forward Presence

Maritime forces are forward deployed, especially in an era of diverse threats to the homeland. Operating forward enables familiarity with the environment, as well as the personalities and behavior patterns of regional actors. Should peacetime operations transition to war, environmental and adversarial understanding developed by intelligence personnel enables the warfighter to quickly engage in combat operations.

1.4.2 Deterrence

Preventing war is preferable to fighting war. Deterring aggression is viewed in global, regional, and transnational terms via conventional, unconventional, and nuclear means. The United States uses forward-stationed and rotationally-deployed forces, space-based assets, sea-based strategic deterrence, and other initiatives to deter those who wish the United States harm. Theater security cooperation (TSC), maritime ballistic missile defense, and the United States’ advantages in space and cyberspace must be protected and extended. Intelligence is crucial to the realization of these goals. For example, the intelligence team is a critical enabler in the effort to protect the force from weapons of mass destruction (WMD), providing decision makers with timely, actionable intelligence to shape appropriate actions against WMD threats. Intelligence provides warning of WMD attacks and is vital to the identification, tracking, and interdiction of adversary proliferation attempts.

1.4.3 Sea Control

The ability to operate freely at sea is one of the most important enablers of joint and interagency operations. Sea control requires capabilities in all aspects of the maritime domain as well as space and cyberspace. This combined arms approach to sea control leverages robust intelligence capabilities in order to achieve local and regional sea control and exploit the maritime domain as maneuver space. The Office of Naval Intelligence (ONI) is the reachback center of excellence on submarine proliferation, acting collaboratively with maritime intelligence operations centers (MIOCs) and operational forces.

1.4.4 Power Projection

The ability to project power ashore at the place and time of our choosing is the basis of U.S. combat credibility. It is the core capability of combat power that the Navy provides to the joint force commander (JFC). The operational intelligence team is involved in every facet of the planning, execution, and evaluation of operations that define power projection. From the intelligence specialist (IS) interpreting satellite imagery to the carrier air wing targeting officer (CVW TO) exercising every step of the joint targeting cycle, intelligence is grafted into this core competency.

1.4.5 Maritime Security

The creation and maintenance of security at sea is essential to mitigating threats short of war, including piracy, terrorism, weapons proliferation, drug trafficking, and other illicit activities. Countering these irregular and transnational threats protects our homeland, enhances global stability, and secures freedom of navigation for the benefit of all nations. U.S. maritime forces enforce domestic and international law at sea through established protocols and also join navies and coast guards around the world to police the global commons. Intelligence activities supporting this pillar of U.S. maritime strategy are very similar to those backing the forward presence capability.

1.4.6 Humanitarian Assistance and Disaster Response

Building on relationships forged in times of peace and stability, naval forces mitigate human suffering as the vanguard of interagency and multinational efforts, both in a deliberate, proactive fashion and in response to crises. The expeditionary character of maritime forces uniquely positions them to provide assistance during times of humanitarian assistance or disaster. Foreign humanitarian assistance is generally planned and executed under normal and routine conditions. Disaster response events, especially those occurring in fragile nations or ungoverned areas, require the IC to address many factors, including whether the environment is permissive, uncertain, or hostile.

1.5 INFORMATION DOMINANCE

The United States has entered into a new era that opens alternative paths to grand strategy and combined arms warfighting. Globalization and exponential growth in computing and communications capabilities have transformed the information environment from an enabling medium to a nexus of commercial, social, political, and intellectual activity. Evolution of space and cyberspace from niche warfare support applications to key domains for competition and combat reflects the increasing prominence and militarization of the information environment. While the nature of warfare endures, warfare modes are evolving to fit the unique characteristics of information age power, competition, and conflict. The globalization and explosion of information technology (IT) capabilities are making data an inexpensive commodity and leveling the playing field for command and control (C2), information access, and knowledge management.

ID is defined as superiority in the generation, manipulation, and employment of information sufficient to afford its possessors military dominance. ID reduces uncertainty, informs risk assessment, and uncovers hidden competitive options and opportunities. It aims to apply information power better than any adversary to amplify traditional naval combat capabilities and expand options for our operational commanders.

The need for a new strategy and roadmap focused on attaining ID was realized as the Navy decidedly placed information on par with platforms, treating information as a weapon across the full ROMO. As a result, information no longer represents a mere enabler of operations: it is elevated in status as a primary competitive advantage and core capability of the Navy.

The Navy must transform its strategic concepts, organizations, processes, and culture to remain a dominant force in this information age. To achieve success in 21st century warfare, the Navy created a fully integrated intelligence, information, cyberspace, C2, and network operations capability and wields it as a weapon. The Chief of Naval Operations (CNO) directed the melding of intelligence, information and network management,

communications, electronic warfare (EW), cyberspace, meteorology, and oceanography to establish an IDC ready to navigate the course ahead.

A clear course has been set to align Navy organizations to effectively operationalize cyberspace and information operations (IO) by establishing Fleet Cyber Command/Tenth Fleet (FLTCYBERCOM/COMTENTHFLT) and realigning the Office of the Chief of Naval Operations (OPNAV) staff to achieve integration and to foster innovation. The establishment of the Deputy CNO for Information Dominance (N2/N6) represents a landmark transition in the evolution of naval warfare.

The IDC was created to more effectively and collaboratively lead and manage a cadre of officers, enlisted, and civilians who possess extensive skills in information intensive fields. The naval intelligence professional is a key pillar of the IDC. The following Navy personnel comprise the IDC:

1. Information professional officers (182x, 642x, 742x designators)
2. Information warfare officers (181x, 644x, 744x designators)
3. Naval intelligence officers (183x, 645x, 745x designators)
4. Oceanography officers (180x, 646x designators)
5. Cyber warfare engineers (184x designator)
6. Space cadre (5500x, 6206x subspecialty codes or VSx AQD)
7. Aerographer's mate (AG) enlisted personnel
8. Cryptologic technician (CTN, CTM, CTR, CTI, CTT) enlisted personnel
9. Intelligence specialist (IS) enlisted personnel
10. Information technician (IT) enlisted personnel
11. Navy civilians assigned to positions in the fields of intelligence, information, counterintelligence (CI), human-derived information (HDI), meteorology, and oceanography.

The common goal of the IDC is assuring the commander and the warfighter get the right information at the right time in order to optimize perceptions and understandings which support and make more effective the processes of decisionmaking and C2.

1.6 MARITIME DOMAIN AWARENESS

The National Plan to Achieve MDA defines MDA as "the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States." The National Plan also states that the purpose of MDA is to facilitate timely, accurate decisionmaking that enables actions to defend against threats to U.S. national security interests. Effective understanding occurs when a decision maker's comprehension of relevant information allows appropriate action. The National Plan acknowledges that information requirements vary depending upon the mission or task at hand; therefore, MDA equates to a holistic understanding of the maritime environment, enabling the commander to successfully execute his assigned mission(s).

MDA for the Navy results when mission-relevant data, information, and intelligence from the United States and partners is collected, processed, exploited, shared, fused, analyzed, and disseminated to planners, watchstanders, and decision makers at the strategic, operational, and tactical levels. MDA is necessary across the full ROMO in all phases of conflict, both for routine and contingency operations. MDA includes understanding all activities

above, on, and beneath the sea, from the littoral to the open ocean. MDA is not confined to vessel tracking, anomaly detection, discovery of illicit cargo shipments, or identifying smugglers. It includes developing a deep understanding of political, social, economic, and physical trends within geographic regions and human networks.

MDA is not an end unto itself, but rather an enabler of all Navy core capabilities as described by the unified maritime strategy of the United States. It is both a physical and virtual extension of the commander's senses and is the means by which his critical information requirements are satisfied.

INTENTIONALLY BLANK

CHAPTER 2

Navy Intelligence Enterprise

2.1 INTRODUCTION

The basic elements of the Navy are the fleets, strike groups, individual ships, aircraft squadrons, and expeditionary force units. The senior intelligence officer (SIO) assigned to each unit has responsibility for the intelligence support provided to his commander and is also accountable for the training and readiness of the intelligence team. This afloat and forward-deployed cadre of naval intelligence professionals is just the tip of an elaborate support structure extending back to the CNO and the Director of Naval Intelligence. This chapter provides a description of the organic naval afloat and ashore billets and organizations providing direct intelligence support to the operational commanders.

2.2 ROLES AND RESPONSIBILITIES

2.2.1 Fleet Commander N2/N39

Commander, United States Fleet Forces Command (COMUSFLTFORCOM) and Commander, United States Pacific Fleet (COMUSPACFLT) N2/N39s are responsible for providing trained and combat ready naval forces to United States Joint Forces Command (USJFCOM) and United States Pacific Command (USPACOM), respectively. In collaboration with the Navy Cyber Forces (CYBERFOR) Assistant Chief of Staff for Intelligence/Director of Fleet Intelligence (DFI), they establish policies, set training standards, resolve manning and readiness issues, develop intelligence system requirements, and oversee fleet intelligence systems installations. The fleet commander N2/N39s validate subordinate unit requests for information (RFIs) and requests for forces (RFFs), and establish priorities and foreign disclosure policy. Additionally, COMUSPACFLT N2/N39 provides oversight of operations, establishes collection policies, provides planning and operational support to USPACOM, and maintains Navy-to-navy exchange programs with foreign intelligence organizations.

COMUSPACFLT N2/N39, as well as the other Navy component commander (NCC) N2s (Commander, United States Naval Forces, Southern Command (COMUSNAVSO); Commander, United States Naval Forces, Central Command (COMUSNAVCENT); Commander, United States Naval Forces, Europe (COMUSNAVEUR)/United States Naval Forces, Africa (COMUSNAVAF); and FLTCYBERCOM) also establish within the AOR maritime intelligence priorities, Navy intelligence reporting policy, and subordinate and staff RFI procedures. NCC N2s also validate subordinate RFIs and RFFs and provide planning and intelligence operations support to their respective geographic combatant commander (GCC). Additionally, many NCC staff N2s are dual-hatted as numbered fleet N2s (e.g., COMUSNAVSO/Fourth Fleet N2).

2.2.2 Director of Fleet Intelligence

The DFI is tasked with the mission of optimizing intelligence readiness across all Navy mission areas and serving as the operating forces' advocate in the development, integration, and fielding of intelligence, surveillance, and reconnaissance (ISR) systems. The DFI's primary responsibility is assisting and advising all fleet commanders, NCCs, and Navy type commanders (TYCOMs) on ISR readiness issues as well as working to ensure intelligence readiness for maritime operations centers (MOCs). In addition, the DFI oversees intelligence operations at CYBERFOR, which includes three primary responsibilities: performing the intelligence TYCOM mission of man, train, and equip (MT&E) of afloat intelligence forces; acting as fleet advocate for ISR capability and readiness; and executing the CNO-directed Intelligence Manpower Distribution Plan (IMDP).

2.2.3 Numbered Fleet N2

Second, Third, Fourth, Fifth, Sixth, Seventh, and Tenth Fleet N2s are responsible for supporting the intelligence requirements of forces assigned in their areas of operation (AOs). Like the fleet commander N2/N39s, the numbered fleet N2s conduct liaison with their foreign counterparts, provide guidance on foreign disclosure of intelligence, validate subordinate RFIs, and establish fleet collection policies and guidance. Fourth, Fifth, Sixth, and Seventh Fleet release a series of predeployment support messages outlining AO-specific guidance for operations, intelligence, and IO. Numbered fleet commanders are candidates for the role of JTF commander or as the JTF's NCC or functional component commander (FCC) (joint force maritime component commander (JFMCC)).

2.2.4 Numbered Fleet Cryptologist

The numbered fleet cryptologist, a special assistant to the numbered fleet N2, is responsible for assigning, tasking, prioritizing, and maintaining cryptologic resources in support of the numbered fleet commander's mission. Focused on the operational level of war, the numbered fleet cryptologist supports the MOC through the technical direction of subordinate task force cryptologic resource coordinators (CRCs) ensuring their organic cryptologic collection plans satisfy the numbered fleet commander's priority intelligence requirements (PIRs). The numbered fleet cryptologist liaises with the fleet commander and theater and national agencies to coordinate cryptologic support not attainable through the use of organic resources. The numbered fleet cryptologist also leverages several subordinate staff officers in the performance of his duties, including the fleet CRC, fleet assistant CRC, and fleet signals intelligence warfare officer (SIWO). Additionally, the numbered fleet cryptologist ensures IO core capabilities are integrated into fleet planning efforts.

2.2.5 Carrier Strike Group

A carrier strike group (CSG) is typically comprised of one CSG staff, one aircraft carrier (CVN), one air wing (CVW), and one destroyer squadron (DESRON). Each of these organizations maintains its own intelligence structure. This section discusses the duties and responsibilities of each intelligence component, except the DESRON N2, which is discussed in section 2.2.7.

2.2.5.1 CSG N2

The CSG N2 is responsible to the strike group commander for all intelligence and cryptologic personnel assigned to CSG subordinate units. When deployed, the N2 coordinates all intelligence support to operations within the strike group. Key areas of responsibility include: administrative and functional control of fleet intelligence detachment (FID) personnel; generation of operational task (OPTASK) intelligence and cryptology supplements; PIR evaluation; support to operational planning; oversight of strike group indications and warning (I&W) and reporting; and development of the strike group's intelligence integration plan. Most of these functions are performed at lower levels, either within the CSG staff or by N2 personnel of subordinate units.

When not deployed, the CSG N2 oversees the intelligence readiness and training of the units assigned to the strike group commander.

2.2.5.2 CSG Assistant N2

The CSG assistant N2 is responsible to the N2 for the orchestration of the supplementary plot (SUPPLOT) watch. Additionally, the CSG assistant N2 is responsible for coordination of intelligence production to support warfare commanders and strike group operations, intelligence inputs to the strike group commander's daily intentions message, and intelligence inputs to the warfare commander's coordination board. The CSG assistant N2 also provides coordination and intelligence support as required for all staff planning activities.

2.2.5.2.1 Collection Management

The assistant N2 and the CRC are responsible for collection management functions. One of the FID officers assigned to a strike group is trained in collection management to assist as directed by the assistant N2.

2.2.5.2.2 Supplementary Plot

SUPPLOT is the all-source intelligence fusion center onboard the CVN monitoring the geopolitical situation and foreign military operations within the AO to which a CSG is assigned. SUPPLOT provides I&W and updated situational information to the tactical flag command center (TFCC), the ship's combat direction center (CDC), and other warfare commanders via voice reports and chat in order to support warfare commanders' decisionmaking. SUPPLOT operations are the responsibility of the CSG N2; however, responsibility for the function, manning, and training of SUPPLOT is often delegated to the assistant N2.

2.2.5.3 Carrier Strike Group Cryptologic Resource Coordinator

The CSG CRC is responsible to the strike group commander for all aspects of cryptologic operations within the CSG. The CRC issues specific tasking under the cryptologic coverage plan to cryptologic units to support I&W for the strike group and meet the commander's PIRs. The CRC manages nonorganic cryptologic support from a variety of agencies. The CRC also requests and manages cryptologic direct support (DS) personnel embarked for operational training and deployment. DS personnel include a variety of CTs and information warfare officers that conduct operations in the ship's signals exploitation space (SSES) and the cryptologic analytical support element (if established).

2.2.5.4 Carrier Strike Group Deputy Information Operations Warfare Commander

The CSG deputy information operations warfare commander (DIWC) is assigned as the principal assistant to the information operations warfare commander (IWC) on all matters related to strike group IO. The DIWC is responsible for the management of the IO staff and for assisting the IWC in the coordination and planning of IO. Additionally, the DIWC ensures that strike group computer networks are defended adequately and effectively to prevent exploitation and corruption of sensitive information.

2.2.5.5 CVN Intelligence Officer

The intelligence officer assigned to an aircraft carrier, referred to as the "ship's IO," is responsible for providing intelligence support and services to the commanding officer (CO), key C2 nodes, the embarked carrier group staff, the air wing commander and his staff, and other warfare commanders as established in each strike group's integrated intelligence plan.

The intelligence organization varies by ship, with some ship's IOs acting as department heads (N2), while others are subordinate to the operations officer. The ship's IO directly supervises at least two divisions, OZ (ISs) and OS (CTs) divisions, each headed by a ship's company division officer. The ship's IO is responsible for the MT&E of assigned personnel and the materiel condition of spaces. Additionally, the ship's IO is assigned duties as the ship's special security officer (SSO) and may also perform duties as the ship's special access program control officer (SAPCO) managing programs for the type and fleet commander. More specifically, the ship's IO supports the CSG N2 by providing the following: access to available intelligence files within the carrier intelligence center (CVIC), briefing assistance, intelligence data in support of tactical operations (including ISR planning), and special intelligence briefs as required. Priorities are set by the CSG commander.

Whenever the air wing and group staff are embarked, the ship's IO supervises and manages a diverse team of intelligence professionals (ship's company and air wing personnel) tasked with meeting the intelligence requirements of the strike group commander, the strike group staff, the warfare commanders and coordinators, and the critical operational nodes aboard the ship (e.g., CDC, tactical action officer (TAO), and strike ops). In order to meet these requirements and those of the theater and national agencies, the ship's IO organizes the intelligence team into five functional cells:

1. SUPPLOT. Conducts all-source I&W in support of the strike group staff, the warfare commanders, and the ship's C2 nodes.

2. Strike intelligence analysis cell (SIAC). Conducts detailed all-source analysis of threat countries where missions and operations are planned/conducted and is comprised of both the target intelligence cell (TIC) and the target analysis cell (TAC).

3. Mission briefing/debriefing. Conducts briefings/debriefings of aircrews and performs combat assessments.

4. SSES. Conducts exploitation of foreign signals.

5. Multisensor interpretation (MSI). Conducts exploitation of organic and non-organic imagery.

During the early phases of the fleet readiness training plan (FRTP), the ship's IO manages the individual and team training programs of assigned intelligence and cryptologic personnel. Later, the ship's IO manages the integration of the staff, ship, air wing, and FID intelligence team to ensure proper operation of the CVIC's functional cells.

2.2.5.6 CVN OZ Division Officer/Carrier Intelligence Center Officer

The OZ division officer/CVIC officer is responsible for the oversight and management of the ISs. This includes manning and training matters, security clearance issues, and watch-standing requirements. During the training cycle, the OZ division officer monitors each division's training plan and ensure spaces and equipment are maintained at a high state of readiness. Additionally, if so designated by the ship's IO, the OZ division officer also acts as the CVN intelligence systems officer. The systems officer is CVIC's resident expert on the operation, management, and maintenance of all intelligence data processing and communications systems. This officer normally does not supervise any maintenance personnel or administrators and must maintain close coordination with the ship's IT personnel to ensure CVIC equipment is properly maintained.

2.2.5.7 CVN OS01 Division Officer/Ships Signals Exploitation Space Officer

The OS01 division officer serves as the ship's SIWO for the CVN. The OS01 division officer is responsible for the materiel condition readiness of SSES, training of assigned personnel, and all facets of cryptologic operations. These duties may include sensitive compartmented information facility accreditation, SAP/special technical operations programs, special communications systems, adjudication of special clearance issues, and operational actions as directed by the IWC and the CRC.

2.2.5.8 CVN OS02 Division Officer/Electronic Warfare Officer

The OS02 division officer serves as the EW officer ensuring the ship is prepared to execute force EW. He ensures the EW operators are supporting the correlation and fusion of organic EW data in support of the information warfare watch team. During the training cycle, the OS02 division officer monitors the division's training plan, is responsible for spaces, and ensures equipment is maintained at a high state of readiness. On many platforms, OS01 and OS02 merged, placing all CT rates under the SIWO for efficiencies in training and management within one division.

2.2.5.9 CVW Intelligence Officer

The CVW intelligence officer, more commonly known as the "CAG AI", is the SIO on the CVW staff and is directly responsible for all intelligence support to the strike warfare commander (STWC) and the CVW. The CAG AI is well versed in all aspects of intelligence support to strike aviation and has normally completed an initial tour as a squadron air intelligence officer (AI). In addition to providing direct intelligence support, the CAG AI mentors and oversees the professional development of CVW staff intelligence officers, squadron AIs, and CVW enlisted intelligence personnel to ensure readiness and training, both ashore and afloat. Additionally, the CAG AI may also perform duties as the CVW SSO, CVW command security manager, and CVW SAPCO.

During workups, the CAG AI coordinates with CVN staff on workspace and equipment issues and liaises with both the CSG N2 and CVN intelligence staff to maintain a close working relationship. While underway, the CAG AI provides executive supervision of those CVIC work centers providing direct support to the air wing and STWC. These work centers include mission briefing/debriefing and SIAC, comprised of both the TIC and the TAC.

2.2.5.10 CVW Targeting Officer

The CVW TO is the CSG/CVN/CVW intelligence staff's resident expert on intelligence support to strike mission planning, targeting, and weaponeering and is one of two CVW staff intelligence officers directly supervised by the CAG AI. The CVW TO manages the CVIC TIC work center which provides target intelligence products (e.g., mission planning folders, weaponeering solutions, etc.) to CVW strike planners. The CVW TO also oversees CVW weapon system video (WSV) download, analysis, and dissemination in support of poststrike bomb hit assessment (BHA) that feeds the battle damage assessment (BDA) process. To carry out these responsibilities, the CVW TO closely coordinates with the applicable theater joint intelligence operations center (JIOC), numbered fleet MOC targeting personnel, and with specialized targeting intelligence agencies at the national level. For day-to-day support to the STWC, the CVW TO collaborates with the CVW strike operations officer to ensure CVW assets tasked by the air tasking order or integrated tasking order (ITO) are fully supported.

With the exception of the CVW TO assigned to forward deployed naval forces in the U.S. Seventh Fleet AO, all CVW TOs are based at Naval Strike and Air Warfare Center (NSAWC) within the NSAWC Targeting Cell for formal and on-the-job training to earn the 3A1 additional qualification designator (AQD) for targeting. Homebasing at NSAWC during the postdeployment and early predeployment periods allows CVW TOs to collaborate on lessons learned and hone their expertise in targeting, weaponeering, and strike mission planning while maintaining situational awareness of the latest carrier aviation operations.

2.2.5.11 CVW Assistant Targeting Officer

The CVW assistant targeting officer (ATO) works directly for the CVW TO in the TIC. The ATO assists the CVW TO by providing target development and weaponeering support to strike planning, ensuring that relevant data from the mission briefing/debriefing cell is integrated into the planning process. Additionally, the ATO is responsible for WSV debrief to include BHA capture, production, and dissemination. The ATO also provides reachback targeting and weaponeering support for CSG, fleet, and combatant command requirements on a not-to-interfere basis with CVW tasking and requirements. As with the CVW TO billet, the ATO is based at NSAWC within the targeting cell to receive prerequisite training and mentorship in order to qualify for the 3A1 AQD.

2.2.5.12 Squadron Air Intelligence Officer

Squadron AIs are responsible for providing their squadron CO and aircrew with intelligence support needed to complete their assigned missions. Duties include maintaining an intelligence documents library, establishing and maintaining a squadron recognition and threat weapon systems training program, serving as the assistant command security manager, ensuring that squadron SSO requirements are coordinated with CVW SSO personnel, and providing intelligence support to squadron-specific missions and functions. In most cases, a squadron AI supervises at least one IS assigned to their squadron and is responsible for their professional development and training, day-to-day operations, and administrative control. Squadron AIs are typically assigned to the squadron operations department and work directly for the squadron operations officer while ashore. When afloat, squadron AIs are normally assigned to one of the CVIC work centers by the CAG AI and function under the direction of the ship's IO.

2.2.6 Expeditionary Strike Group/Amphibious Squadron

An amphibious squadron (PHIBRON) usually consists of three amphibious ships: one landing helicopter dock (LHD) or landing helicopter assault (LHA) ship, one dock landing ship (LSD), and one landing platform dock (LPD) ship. When these ships are loaded with the forces of a Marine expeditionary unit (MEU) and accompanied

by associated naval support elements, the PHIBRON is designated an amphibious ready group (ARG)/MEU. The ARG/MEU, commanded by the PHIBRON staff, is the standard rotational amphibious force deployment package.

If a requirement exists that a flag or general officer command an ARG/MEU, the formation is referred to as an expeditionary strike group (ESG), which includes an embarked flag or general officer and their associated command element (CE) staff. Regardless of the Service orientation of the commander, the CE consists of both Navy and Marine Corps personnel. Additional surface combatants may or may not be assigned to an ARG/MEU or ESG.

2.2.6.1 Expeditionary Strike Group N2

When deployed, the assigned ESG N2 is responsible for coordinating all aspects of intelligence support to operations within the group or force. Since group commanders are prime candidates for assignment as JTF commanders or as the NCC for a JTF, the N2 must be well versed in joint doctrine and procedures. When not deployed, the ESG N2 is responsible for monitoring the intelligence readiness and training of all assigned intelligence/cryptologic personnel assigned to amphibious forces on their respective coast.

2.2.6.2 Expeditionary Strike Group Assistant N2

When deployed, the ESG assistant N2 is normally assigned as the operational intelligence officer for the group. As such, the assistant N2 liaises with LHD/LHA intelligence work centers, tactical flag plot, and other composite warfare commander (CWC) C2 nodes to maintain force situational awareness.

2.2.6.3 Expeditionary Strike Group Cryptologic Resource Coordinator

When deployed, the assigned ESG CRC is responsible for coordinating all aspects of cryptologic support to operations within the group or force. When not deployed, the ESG CRC is responsible for monitoring the cryptologic readiness and training of all assigned cryptologic personnel assigned to amphibious forces on their respective coast.

2.2.6.4 Amphibious Squadron N2

PHIBRON N2s provide the ARG/MEU commander and staff with intelligence and cryptologic support necessary to carry out their assigned missions. Additionally, the N2 sets policy for and monitors the functions of the ARG/MEU's intelligence/cryptologic team to ensure the timely flow of intelligence information among the ARG/MEU units and that organically-collected intelligence is promptly and accurately reported to fleet, theater, and national agencies.

Additionally, PHIBRON N2s are responsible for the intelligence readiness and training of the units assigned to their ARG/MEU. The N2 monitors the ARG/MEU's intelligence/cryptologic training plans to ensure personnel receive required training prior to deployment. The N2 performs duties as the staff SSO. Since the PHIBRON commander is a candidate for selection as the JTF NCC or functional component commander (JFMCC) for a humanitarian relief or NEO operation, the N2 must be well versed in joint doctrine and procedures.

2.2.6.5 Amphibious Squadron Assistant N2

The PHIBRON assistant N2 is normally assigned as the ARG/MEU collection manager. As such, the assistant N2 liaises with the MEU collection manager to track and prioritize collection requirements and to task organic and nonorganic collection assets in support of the ARG/MEU commander. Additionally, dependent on the staff, the assistant N2 may stand watches in expeditionary plot (EXPLOT) or conduct the daily briefing to the ARG/MEU commander.

2.2.6.6 Amphibious Squadron Cryptologic Resource Coordinator

When deployed, the assigned PHIBRON CRC is responsible for coordinating all aspects of cryptologic support to operations within the ARG/MEU. When not deployed, the PHIBRON CRC is responsible for ensuring the cryptologic readiness and training of all assigned cryptologic personnel assigned to the ARG.

2.2.6.7 LHD/LHA Intelligence Officer

The intelligence officer assigned to the LHD/LHA, referred to as the "ship's IO," provides intelligence and cryptologic support/services so that the embarked PHIBRON staff, the embarked Marines, and his own CO and C2 cells can accomplish their assigned missions. In order to provide this support, the ship's IO manages a cadre of professional intelligence personnel, officer and enlisted, from the ship's intelligence and cryptologic divisions and the embarked tactical air control squadron (TACRON). Additionally, the ship's IO provides equipment, space, and materiel to the embarked PHIBRON N2 and MEU intelligence (S2) staffs.

When deployed, the ship's IO is responsible for the manning and management of EXPLOT, the joint intelligence center (JIC), and SSES and ensures the proper flow of information between these spaces and other C2 nodes belonging to the ship, the embarked staff, and the MEU.

During the FRTP, the ship's IO is responsible for the training of his assigned personnel and the installation of equipment and systems in his assigned spaces. The ship's IO receives support and direction in these matters from the PHIBRON N2, the TYCOM, and the fleet commander N2/N39. The ship's IO also operates as the ship's SSO and ensures all security regulations are adhered to and material is safeguarded.

2.2.6.8 LHD/LHA OZ Division Officer/Joint Intelligence Center Officer

The OZ division officer/JIC officer is responsible for the oversight and management of the ISs. This includes manning and training matters, security clearance issues, and watch-standing requirements. During the training cycle, the OZ division officer monitors the training plan and ensures spaces and equipment are maintained at a high state of readiness. Additionally, if so designated by the ship's IO, the OZ division officer also acts as the JIC intelligence systems officer. The systems officer is the JIC's resident expert on the operation, management, and maintenance of all intelligence data processing and communications systems. This officer normally does not supervise any maintenance personnel or administrators and must maintain close coordination with the ship's IT personnel to ensure JIC equipment is properly maintained.

2.2.6.9 CG, DDG, LHD, LHA, LPD Signals Warfare Officer

SIWOs are assigned aboard cruisers, flight II destroyers, and amphibious assault and docking ships. They are tasked with such duties as collecting, analyzing, exploiting, and disseminating information and intelligence as directed by the IWC, CRC, and ship's IO. The SIWO's primary responsibility is to employ communication IO systems to detect, classify, and track all targets as directed and coordinate with the ship's combat information center (CIC) to ensure their inclusion into the common operating picture. Other activities include providing equipment status to the CRC, managing the ship's emission control (EMCON)/river city bill, and providing I&W for own ship and strike group self defense. If an electronic warfare officer is assigned to the unit or strike group, he assumes the duties and responsibilities for matters pertaining to EW and works in conjunction with the ship's IO, SIWO, and collateral duty intelligence officer (CDIO) or independent duty intelligence specialist (IDIS) to optimize collection efforts.

In the event a surface strike group or a surface action group is established without a previously assigned CRC, the SIWO, as the only cryptologic support available to the DESRON staff, must be prepared to join the DESRON staff as the CRC.

2.2.6.10 Tactical Air Control Squadron Intelligence Specialist

The TACRON IS is responsible for providing the squadron CO and other squadron personnel with the intelligence support needed to complete their assigned missions. Duties include maintaining an intelligence library, establishing and maintaining a threat recognition training program, establishing a squadron security training program, and providing intelligence support to squadron evolutions.

When the TACRON is embarked, the squadron IS is assigned additional duty to the LHD/LHA ship's IO and is fully integrated into all JIC/EXPLOT evolutions.

2.2.7 Destroyer Squadron N2

The DESRON N2 is responsible for coordinating intelligence support to the DESRON commodore as the sea combat commander and is supported by the numbered fleet/CSG/ESG/ARG N2 organization. When separated from the strike group, the DESRON N2 can act as the task force intelligence officer; however, without an organic intelligence staff, the DESRON N2 relies upon reachback support to provide situational awareness to the commodore and DESRON staff.

When not deployed, the DESRON N2 is responsible for managing the readiness and training of the intelligence and cryptologic personnel assigned to ships subordinate to the commodore and works with the DESRON staff, the afloat training group, CYBERFOR N2, COMUSPACFLT Intelligence/Information Warfare Readiness Cell, and the CSG/ESG/ARG N2s to mentor and train these personnel.

2.2.8 Collateral Duty Intelligence Officer/Independent Duty Intelligence Specialist

IDISs are Chief and First Class Petty Officers assigned to cruisers, destroyers, and amphibious transport dock ships. In the case of afloat units without an IDIS assigned, the CO designates a CDIO. IDISs and CDIOs are responsible for timely and accurate intelligence collection and processing to support their commander's requirements. Activities include exploiting intelligence collection opportunities as they occur, responding to the commander's tasking for time sensitive information necessary to achieve objectives, and comprehending the specific collection requirements and essential elements of information (EEIs) contained in operation orders, operation plans (OPLANs), and OPTASKs. The IDIS/CDIO understands collection programs, standing and ad hoc collection requirements, and reporting procedures.

The IDIS/CDIO provides tailored intelligence information to the CO, TAO, warfare coordinators, and training teams. The IDIS/CDIO also trains and supports every warfare area while serving as a technical advisor on the war council and doctrine review board. Additionally, the IDIS/CDIO trains and leads the SNOOPY team. IDISs are not authorized to perform SSO or assistant SSO functions and are not qualified for duties and responsibilities of a special security assistant.

2.2.9 Shipborne Unmanned Aerial Vehicle Intelligence Detachment Officer in Charge

Three intelligence personnel are attached to ships carrying a tactical unmanned aerial vehicle (UAV) in order to conduct exploitation and dissemination of collected intelligence. The detachment consists of one officer in charge (OIC) (E-7 to O-3 intelligence officer/specialist) and two imagery analysts (E-4 to E-6) with experience exploiting full-motion video. The detachment OIC attends the Naval Collection Management Course and carries the collection management AQD. The imagery analysts hold the 3910 Navy enlisted classification (NEC) code and receive additional full motion video exploitation training through the National Geospatial-Intelligence Agency (NGA) and the Navy and Marine Corps Intelligence Training Center (NMITC).

The detachment normally works for the ship's operations officer and operates as an integral part of the ship's intelligence team, coordinating collection operations with the ship's CDIO/IDIS and CTs. Detachment personnel are assigned to the ship through individual augmentation (IA) orders and report five days prior to deployment. Subject to individual availability and scheduled training dates, the intelligence detachment embarks the ship as often as possible during the FRTP in order to maximize afloat training and integration opportunities.

2.2.10 Intelligence Specialist

Navy ISs analyze the complete spectrum of intelligence information and are a key to the successful execution of operations. They serve on afloat, deployed, and shore installations. ISs receive initial "A" (apprentice) school training and immediate follow-on "C" (classification) school training at NMITC, Dam Neck, VA. Depending upon the needs of the Navy, first tour ISs are assigned to an operational billet (e.g., squadron, ship, deployable staff, FID, etc.), a shore staff supporting the fleet, or to numerous joint commands or other intelligence organizations. ISs attend various "F" (fleet) courses to provide specialized systems and applications training during various times throughout their career. An NEC code designates an IS as a trained professional in one of five specialized areas to support the warfighter:

1. IS-3910, naval imagery interpreter. The 3910 interprets all-source imagery intelligence, operates digital imagery systems to interpret imagery, analyzes full-motion video, identifies and measures objects of intelligence interest found in imagery, prepares imagery interpretation reports, and maintains files related to imagery interpretation.

2. IS-3912, expeditionary warfare intelligence specialist. This IS provides comprehensive intelligence support to special operations forces (SOF) and expeditionary warfare operations and is specially trained to support naval and joint force operations ashore. The 3912 performs analytical assessments, all-source fusion, mission planning, and threat analysis using standardized procedures in support of special operations and expeditionary forces.

3. IS-3913, Navy tactical human intelligence (HUMINT) specialist. The 3913 supervises and conducts tactical HUMINT collection operations that include debriefings, interrogations, and elicitations in English and foreign languages for positive intelligence and force protection information; screening of HUMINT sources and documents to establish priorities for exploitation; under CI supervision, plans and participates in CI and force protection operations; coordinates the translation and exploitation of captured enemy documents, foreign language, and foreign open-source publications; and conducts liaison and coordination in foreign language with host nation (HN) agencies.

4. IS-3923, strike planning applications. The 3923 conducts tactical- and operational-level research, analysis, and dissemination in support of strike operations. He fuses multisource data into textual and graphical presentations of the battlefield and operational area to support power projection planning. This IS provides aimpoint geopositioning utilizing the Joint Service Imagery Processing System – Navy/Distributed Common Ground Systems – Navy, integrated operational and environmental intelligence information to strike planners, and target intelligence to tactical mission planners.

5. IS-3924, operational intelligence (OPINTEL) analyst. The OPINTEL analyst's core function is to provide an integrated and fused all-source intelligence picture using the Global Command and Control System – Maritime as their primary tool.

2.2.11 Cryptologic Technician

CTs perform critical missions in multiple warfare areas to support U.S. national defense and dynamic USN combat roles. The CT force is comprised of five ratings: cryptologic technician - interpretive (CTI), cryptologic technician - maintenance (CTM), cryptologic technician - networks (CTN), cryptologic technician - collection (CTR), and cryptologic technician - technical (CTT) specializing in foreign language interpretation, cryptologic system maintenance, network operations and management, signals collection and analysis, and electronic protection and attack, respectively.

1. Cryptologic technician – interpretive. CTIs conduct IO using foreign language skills and advanced computer systems; collect, analyze, and exploit foreign language communications signals of interest to identify, locate, and monitor worldwide threats; transcribe, translate, and interpret foreign language materials; prepare time-sensitive tactical and strategic reports; and provide cultural and regional guidance

in support of joint, fleet (special operations, air, surface, and subsurface), national, and multinational consumers.

Basic linguist NECs, depending on language, are CTI-9192 through CTI-9216.

2. Cryptologic technician – maintenance. CTMs perform preventive and corrective maintenance on electrical and electronic cryptologic and ancillary systems, to include cryptologic carry-on program (CCOP) equipment, used for communications, analysis, monitoring, tracking, identification, electronic attack, and physical security; install, test, troubleshoot, repair or replace cryptologic networks, physical security systems, electronic equipment, antennas, personal computers, auxiliary equipment, digital and optical interfaces, and data systems; configure, monitor, and evaluate IO systems in support of national and fleet tasking; coordinate repair of command, control, communications, computer, and intelligence systems; and prepare reports and inventories of equipment.

The following NECs comprise the CTM community:

   a. CTM-9224, AN/SQQ-124(V) Tactical Exploitation System maintenance technician. Performs organizational level maintenance on the AN/SQQ-124(V) (COBLU 1).

   b. CTM-9225, AN/SSQ-137 Ship's Signals Exploitation Equipment (SSEE) maintenance technician. The 9225 performs mobile cryptologic maintenance duties. Maintains the SSEE Increment E cryptologic system installed on U.S. naval combatants.

   c. CTM-9229, Submarine carry-on equipment technician. The 9229 performs organizational-level maintenance on submarine cryptologic carry-on equipment.

   d. CTM-9289, SRS-1 Combat Direction Finding System maintenance technician. The 9289 performs organizational-level maintenance on the SRS-1.

3. Cryptologic technician – networks. CTNs monitor, identify, collect, and analyze network information; provide data for digital network products; and conduct computer network operations worldwide to support Navy and Department of Defense (DOD) national and theater level missions. Duties include network target development; I&W; attack sensing and warning; network, software, and forensic analysis; and computer network defense (CND) operations.

The following NECs comprise the CTN community:

   a. CTN-9308, Navy interactive ON-NET (ION) operator. Navy ION operators use advanced software applications for network navigation and tactical forensic analysis.

   b. CTN-9309, Navy ION operator trainer. Navy ION operator trainers mentor ION operators and prepare them to used advanced software applications for network navigation and tactical forensic analysis.

4. Cryptologic technician – collection. CTRs operate state-of-the-art computer systems to conduct IO; collect, analyze, and exploit signals of interest to identify, locate, and report worldwide threats; and provide tactical and strategic signals intelligence (SIGINT), technical guidance, and IO support to surface, subsurface, air, special warfare units, and national consumers to maintain ID.

The following NECs comprise the CTR community:

   a. CTR-9150, AN/SSQ-137 SSEE operator. The 9150 operates the SSEE Increment E cryptologic system installed on U.S. naval combatants.

   b. CTR-9131, SRS-1 Combat Direction Finding System operator. The 9131 operates the SRS-1 equipment as an integral part of electronic warfare support (ES).

c. CTR-9147, intermediate signals analyst. The signals analyst conducts and supervises SIGINT signals search, analysis, target identification, and reporting operations. The 9147 uses cryptologic mission databases, computer-based analysis techniques, advanced modulation and multiplexing techniques, and coding theory to acquire, display, and demodulate high data rate communication systems while protecting sensitive methods and sources.

d. CTR-9138, journeyman analysis and reporting specialist. Reporters identify major SIGINT producers and consumers, perform indepth current and term analysis, report real time or historical activities for fleet or national mission support, and produce finished summary reports by integrating multisource analysis of raw or semiprocessed information and tactical analytic products.

5. Cryptologic technician – technical. CTTs operate and maintain electronic sensors and computer systems; collect, analyze, exploit, and disseminate electronic intelligence (ELINT) in accordance with fleet and national tasking; provide I&W and technical and tactical guidance to warfare commanders and national consumers in support of surface, subsurface, air, and special warfare operations.

The following NECs comprise the CTT community:

a. CTT-1702, AN/SLQ-32B(V)2 technician. The 1702 performs preventive and corrective maintenance on the AN/SLQ-32B(V)2 ES system.

b. CTT-1733, AN/SLQ-32(V)2 technician. The 1733 performs preventive and corrective maintenance on AN/SLQ-32A(V)2 and the AN/SLQ-32(V)2 ES system.

c. CTT-1734, AN/SLQ-32(V)3 technician. The 1734 performs preventive and corrective maintenance on the AN/SLQ-32A(V)3 and the AN/SLQ-32(V)3 Deceptive Electronic Countermeasures System.

d. CTT-9141, intermediate technical ELINT analysis technician. The 9141 performs measurements on noncommunications signals using analog equipment and determines required noncommunications collection and analysis procedures and priorities.

e. CTT-9102, national operational ELINT analyst. The 9102 performs analysis and reporting of all-source information for tactical and strategic commanders in support of battle force and national intelligence objectives. Analysts operate general service and sensitive compartmented information (SCI) processing, transmission, analysis, and storage systems. Although analysts primarily use ELINT data, they are trained in fusing ELINT with other intelligence disciplines.

2.2.12 Patrol and Reconnaissance Group N2

Commander, Patrol and Reconnaissance Group (CPRG) is located in Norfolk, VA and serves as the executive agent for maritime patrol force TYCOM functions, reporting directly to Commander, Naval Air Forces on TYCOM matters. The CPRG N2 is responsible for overseeing intelligence aspects of MT&E responsibilities for all maritime patrol and reconnaissance (MPR) family of system (FOS) aircraft and squadrons. The FOS is comprised of maritime patrol squadron (VP) and fleet air reconnaissance squadron (VQ) aircraft and squadrons, and beginning in 2016, the broad area maritime surveillance UAV. Additionally, the N2 provides CPRG and his staff with OPINTEL and force protection support to accomplish the force's assigned missions.

2.2.12.1 Patrol and Reconnaissance Wing Intelligence Officer

The commander, patrol and reconnaissance wing (CPRW) intelligence officers are responsible for the day-to-day supervision, training, administrative, and SSO support to assigned FOS squadron intelligence personnel. There is one O-4 and one ISC assigned per wing. There are three wings: CPRW-11 in the Atlantic (Jacksonville, FL) and two in the Pacific (CPRW-2 in Kaneohe, HI and CPRW-10 in Whidbey Island, WA). In concert with the CPRG N2, the CPRW intelligence officers develop and execute the FRTP to prepare the squadron personnel for deployment.

2.2.12.2 Maritime Patrol and Reconnaissance Squadron Intelligence Officer

The VP squadron AI is normally a first tour junior officer with three ISs assigned. The AI provides the squadron CO and squadron personnel with intelligence support and training enabling them to complete their assigned missions. Additionally, the AI supervises the ISs assigned to the squadron and ensures that they receive professional development and training.

The VQ SIO is normally an O-4 with five first tour junior officers, eight ISs, and thirteen CTs assigned. The SIO supervises three divisions to execute the personnel security, IT, and intelligence support functions.

Under the FOS concept, the VP and VQ squadron intelligence officers and enlisted personnel integrate into the tactical operations center and mobile tactical operations center to provide OPINTEL and photographic support to all FOS squadrons.

2.2.13 Naval Special Warfare Command N2/N39

The Naval Special Warfare Command (NSWC) N2 is responsible to the Commander, NSWC for all operational intelligence issues as well as worldwide personnel, training, and materiel matters affecting intelligence professionals within the command. NSWC is operationally subordinate to United States Special Operations Command and administratively reports directly to the CNO.

The NSWC N39 is responsible to the Commander, NSWC for all tactical IO and SIGINT issues as well as worldwide personnel, training, and material matters affecting all information warfare officers and CTs within the command.

2.2.13.1 Naval Special Warfare Group N2/N39

The naval special warfare group N2 is responsible for intelligence personnel issues, training, and materiel matters related to supporting sea, air, and land (SEAL) teams, special boat teams (SBTs), and/or SEAL delivery vehicle (SDV) teams within the echelon III claimancy. Naval special warfare (NSW) groups are force provider organizations, operationally aligned to support designated combatant commands, but under the command and control of NSWC.

The NSW Group N39 is responsible for information warfare officer and CT issues, training, and materiel matters related to supporting SEAL teams and SBTs within the echelon III claimancy.

2.2.13.2 SEAL Team/Squadron Intelligence Officer

The SEAL team intelligence officer provides tailored intelligence support to their CO and team members while in the continental United States (CONUS). When deployed, the team is designated as a naval special warfare squadron (NSWRON). While in the CONUS, SEAL teams are operationally and administratively subordinate to the NSW group. When deployed, NSWRON operational command passes to the NSW unit based in the supported CCDR’s AOR.

2.2.13.3 Naval Special Warfare Support Activity Information Warfare Officer

The NSW support activity (SUPPACT) information warfare officer provides tactical IO consisting primarily of EW, computer network operations, and SIGINT support to the CO and SEAL team members.

2.2.13.4 Naval Special Warfare Unit Intelligence Officer

The NSW Unit intelligence officer provides intelligence and cryptologic support to the unit’s CO and members and supports NSWRON units under the operational command of the unit. Operationally, NSW units are subordinate to the theater special operations command (TSOC). Administratively, units are subordinate to the NSW group.

2.2.14 Navy Expeditionary Combat Command N2

The Navy Expeditionary Combat Command (NECC) serves as a single functional command to centrally manage the current and future readiness, resources, and MT&E of the Navy expeditionary force. Intelligence capabilities within the NECC force are aligned to provide tactically-focused force protection and I&W intelligence information to operating expeditionary forces. The NECC N2 is responsible for providing force-wide policy and guidance to ensure integration and interoperability of expeditionary intelligence and tactical IO capabilities. NECC N2 interacts with intelligence and IO community managers to optimize force manpower for IS-3912s, IS-3913s, CTs specially trained for expeditionary missions, naval intelligence officers, and information warfare officers.

Each of these specializations require particular skills and equipment training, some within intelligence and IO training pipelines, and some available only through other Service or commercial sources. NECC N2 coordinates with various resource sponsors and NECC components to ensure the greatest possible commonality of intelligence and IO equipment and training for the expeditionary force.

2.2.15 Mine Warfare Staff N2

The Naval Mine and Anti-Submarine Warfare Command (NMAWC) sources the mine warfare commander (MIWC) and is prepared to deploy and assume duties as the mine warfare (MIW) commander, task force (CTF) or commander, task group (CTG) to the numbered fleets. The MIWC N2 performs the functions of a CTF N2 in addition to supporting NMAWC as the Navy's center of excellence for MIW planning and analysis and developing TTPs for mine operations and countermeasures. The Mine Countermeasures Squadron (MCMRON) FIVE and SEVEN staff N2s are responsible for providing the staff and the CDIO with information on the mine and general threat information about their operating area, force protection information, and knowledge of intelligence collection and reporting requirements. Additionally, the MCMRON staff N2 reviews OPLANs involving mine operations and assists the staff in operational planning.

2.2.16 Naval Strike and Air Warfare Center N2

NSAWC is the Navy's center of excellence for aviation strike warfare training including strike intelligence training and air combat tactics development. The NSAWC N2 provides full spectrum strike intelligence training to CVW intelligence teams and supports intelligence and targeting activities related to integrated strike warfare, maritime/overland air superiority, strike fighter employment, airborne battle management, combat search and rescue, close air support, and associated support missions. The NSAWC N2 hosts the strike FID, providing precise aimpoint geopositioning training, certification, and administrative support to deploying NEC code 3923 ISs. The NSAWC Targeting Division (N22), which consists of CVW TOs and aimpoint geoanalysts, including the FID, is responsible for providing reachback targeting, weaponeering, and aimpoint graphic support to CSG and fleet commanders. The NSAWC N2 also maintains oversight over the reserve targeting officer program which provides additional trained targeting personnel to support CVW and fleet targeting requirements.

2.3 FLEET INTELLIGENCE DETACHMENT

The FIDs provide operationally ready intelligence professionals to the fleet in the critical, high demand skill areas of imagery interpretation and strike support to CSG/ESG/ARGs. The CNO-approved concept moved those ship's company intelligence billets holding the most perishable skill sets from CVN/LHA/LHDs to intelligence centers where the skills are applied daily. The FID at the ONI Nimitz Operational Intelligence Center provides 1630 officer and IS-3910 support, and the FID at NSAWC provides IS-3923 support. FID augmentation is event-focused and driven by specific skill sets for validated operational requirements levied by numbered fleet, CSG, and ARG commanders. When not embarked, FID personnel provide remote real time intelligence support to deployed operating forces, receive sustainment training/qualifications, and share lessons learned. CYBERFOR reviews requirements ensuring permanent manning plus FID augmentation achieve an intelligence complement as indicated in Figure 2-1.

	Permanent Manning Basic Allowance			FID Complement			Deploying Complement		
	Officer	ISCS	NEC 3924	Officer O-1 to O-3	NEC 3910	NEC 3923	Officer O-1 to O-3	IS	Total
CVN	1 x O-5 1 x O-3	1	9	2	4	4	4	18	22
LHD/LHA	1 x O-4 1 x O-2	1	8		4	2	2	15	17

Figure 2-1. Fully Implemented Intelligence Manpower Alignment, Carrier Strike Group/Amphibious Ready Group

FID personnel are ordered temporary additional duty (TAD) to the CSG/ESG/ARG N2 no later than five working days prior to the first scheduled event/underway period. Approved events and waiver processes will be promulgated via message and instruction. Once a FID is assigned, replacement of personnel is not authorized without DFI approval. Gaining commands are responsible for providing fitness report and evaluation inputs in the form of performance information memorandums to the FID directors and integrating FID personnel into professional development programs to the greatest extent possible.

2.4 FLEET INTELLIGENCE ADAPTIVE FORCE

The Fleet Intelligence Adaptive Force (FIAF) provides the Navy with the ability to rapidly redistribute resources between MOCs and address in-theater crisis/emergent intelligence demand signals. The FIAF provides a ready pool of Navy intelligence professionals to support combatant command IA requirements, enhance intelligence capabilities at the MOCs, provide support to FRTP events and exercises, and respond to emergent Navy intelligence requirements.

The FIAF consists of seven CYBERFOR detachments collocated at six numbered fleets and Pacific Fleet MOCs manned with 140 billets (19 x 1630s and 121 x ISs) aligned administratively to CYBERFOR and operationally to the MOC to which they are collocated. The majority of the FIAF billets are aligned to COMUSPACFLT, Second Fleet, Third Fleet, and Fourth Fleet against the following priority order requirements: validated joint and Navy-to-Navy IAs, federated MOC OPINTEL support, CVN/LHA/LHD exercise/surge augmentation, and VP surge support. Alignment of the majority of the FIAF billets to CONUS-based MOCs is designed to relieve intelligence personnel IA sourcing from aircraft carriers and large deck amphibious ships. Smaller numbers of FIAF billets are aligned to Fifth Fleet, Sixth Fleet, and Seventh Fleet against the following priority order requirements: increasing number of analytical subject matter experts capable of filling emergent Navy assignments in theater, building and maintaining intelligence readiness, and augmenting command ship exercise/surge requirements in theater.

The DFI chairs, at least on an annual basis, a fleet intelligence augmentation planning board to develop, maintain, and articulate future FIAF requirements. Board participants include fleet stakeholders involved in the requirements process such as NCCs, numbered fleet N2s, and affected TYCOMs. The board identifies and prioritizes anticipated FIAF requirements, reviews the FIAF concept of operations (CONOPS) for currency and return on investment, and makes recommendations for changes in manpower or training requirements across the seven FIAFs. Effective management of FIAF personnel requires the designation of two CONUS-based employment categories. The employment categories are defined by their eligibility for IA deployment under COMUSFLTFORCOM IA business rules. Specifically, employment category I personnel are eligible for IA deployment whereas employment category II personnel are not. MOC N2s provide daily tasking for all FIAF personnel regardless of employment category; however, decisions regarding TAD, deployment, and IA management are divided as follows: CYBERFOR N2/DFI approves deployments, TAD/temporary duty (TDY),

and IA for employment category I, and the MOC N2 approves deployments and TAD/TDY for employment category II. To maintain accurate accountability and employment of FIAF personnel, the DFI publishes a monthly report designating the employment dategory status of all FIAF personnel.

The FIAF is a flexible capability enabling Naval Intelligence to respond to validated current and emergent IA requirements, provide forward MOCs onsite expertise to increase intelligence readiness of deploying naval forces, and enhance enterprise-wide intelligence readiness by delivering remote support from multiple locations.

2.5 CRYPTOLOGIC DIRECT SUPPORT

IO and cryptologic DS is a flexible system based on operational requirements whereby personnel and equipment are managed in centralized pools and allocated to forward deployed units based on validated numbered fleet and CCDR requirements. Cryptologic and IO personnel are concentrated at the fleet information operations centers (FIOCs). These activities are collocated with National Security Agency (NSA) activities to leverage national systems and training, providing personnel an environment that allows them to maintain currency and proficiency when not deployed. Tailored support teams are nominated and provided to tactical and operational-level units based on procedures set forth in the COMUSFLTFORCOM global augmentation policy.

The FIOCs are responsible for providing trained augmentees in response to fleet requirements. FIOC support continues for the duration of the deployment through a system of reachback support, managed by the nondeployed FIOC DS personnel. This reachback support allows the DS system to leverage the expertise resident at regional FIOCs and decrease the manning footprint at sea.

Requests for DS are initiated by the CRC, validated by numbered fleets, approved by fleet commanders, and then tasked to the FIOC for sourcing.

For further information on DS manning, refer to the annual IO and cryptologic global augmentation policy message. For 2009, the PLA, DTG, and subject are: COMUSFLTFORCOM NORFOLK VA, 232017Z OCT 09, SUBJ: INFORMATION OPERATIONS AND CRYPTOLOGIC GLOBAL AUGMENTATION POLICY.

2.6 CRYPTOLOGIC CARRY-ON PROGRAM

In addition to permanently installed IO systems, CRCs and numbered fleet N2s can request temporary equipment installations through the CCOP. CCOP systems and services provide an invaluable force multiplier to the fleet through timely and accurate I&W data and threat geolocation information which are vital to the time-sensitive targeting process as well as maintaining situational awareness during peacetime and conflict. CCOP capabilities range from complete suites designed to augment tactical cryptologic platforms without a permanent cryptologic system installed to unique, and sometime ad hoc, hardware and/or software applications that enhance or fill a gap in the permanent system capabilities. CCOP allows for the rapid insertion of both software and hardware capabilities as necessary to sustain IO support and keep pace with emerging technologies. COMUSFLTFORCOM is the executive agent for the CCOP program. CCOP equipment requests are initiated by the CRC, validated by numbered fleets, approved by fleet commanders, and sent to the respective platform TYCOM for tasking to Navy information operations commands (NIOCs) for installation.

For further information on CCOP, refer to the annual IO and cryptologic global augmentation policy message. For 2009, the PLA, DTG, and subject are: COMUSFLTFORCOM NORFOLK VA, 232017Z OCT 09, SUBJ: INFORMATION OPERATIONS AND CRYPTOLOGIC GLOBAL AUGMENTATION POLICY.

INTENTIONALLY BLANK

CHAPTER 3

Navy Intelligence Operations

3.1 INTRODUCTION

As demonstrated during Operations Enduring Freedom and Iraqi Freedom, deployed naval forces predominantly operate for a JFC's maritime commander. Naval forces are usually the first to arrive at the scene of any world crisis and are prepared to conduct a broad range of military and humanitarian assistance operations.

This chapter first defines the levels of intelligence and the processes used to assess an adversary's capabilities and COAs. Next, the intelligence structure of our major deployable naval forces and the joint organization they may support or manage is described. The chapter concludes with the types of naval warfare and joint operations that the naval intelligence professional supports.

3.2 LEVELS OF INTELLIGENCE

The three levels of war are strategic, operational, and tactical, providing a doctrinal perspective that clarifies the links between strategic objectives and tactical actions. Each level of war has a corresponding level of intelligence operations. This construct of strategic, operational, and tactical levels of intelligence aids the commander and the intelligence team in visualizing the flow of intelligence from one level to the next. As a tool for the naval commander, NWP 2-01 firmly resides in the realm of tactical intelligence; however, familiarity with strategic and operational intelligence is essential.

3.2.1 Strategic Intelligence

National strategic intelligence is produced for the President, Congress, SECDEF, senior military leaders, and the CCDRs. It is used to develop national strategy and policy, monitor the international situation, prepare military plans, determine major weapon systems and force structure requirements, and conduct strategic operations. Strategic intelligence operations also produce the intelligence required by CCDRs to prepare strategic estimates, strategies, and plans to accomplish missions assigned by higher authorities.

Theater strategic intelligence supports joint operations across the ROMO and determines the current and future capabilities of adversaries that could affect the national security and U.S. or allied interests. Theater strategic intelligence includes determining when, where, and in what strength the adversary will stage and conduct theater level campaigns and strategic unified operations.

3.2.2 Operational Intelligence

Operational intelligence is used to describe intelligence support to theater operational forces. It is primarily used by CCDRs and subordinate JFCs and their component commanders. Operational intelligence focuses on adversary military capabilities and intentions. It helps the JFC and component commanders keep abreast of events within their area of interest and helps commanders determine when, where, and in what strength the adversary might stage and conduct campaigns and major operations. During counterinsurgency and counterterrorism operations, operational intelligence is increasingly concerned with stability operations and has a greater focus on political, economic, and social factors.

Within the operational arena, operational intelligence addresses the full ROMO, facilitates the accomplishment of theater strategic objectives, and supports the planning and conduct of joint campaigns and subordinate operations.

It focuses on providing the JFC information required to identify adversary centers of gravity (COGs) and provides relevant, timely, and accurate intelligence and assessments. Operational intelligence also includes monitoring terrorist incidents and natural or manmade disasters and catastrophes.

3.2.3 Tactical Intelligence

Tactical intelligence focuses on combat intelligence, which is used by commanders, planners, and operators for planning and conducting battles, engagements, and special missions. Relevant, accurate, and timely combat intelligence allows tactical units to achieve positional and informational advantage over their adversaries. Precise threat and target status reporting, in particular, is essential for success during actual mission execution.

Tactical intelligence addresses the threat across the ROMO. Tactical intelligence operations identify and assess the adversary's capabilities, intentions, and vulnerabilities, as well as describe the physical environment. It seeks to identify when, where, and in what strength the adversary will conduct tactical-level operations. Tactical intelligence is the mainstay of the naval intelligence professional, and this is why naval intelligence personnel are assigned to individual ships, squadrons, and units. They are in place to provide direct intelligence support to the warfighter.

3.3 INTELLIGENCE PROCESS

The intelligence process provides the basis for common intelligence terminology and procedures and consists of six interrelated categories of intelligence operations. Intelligence operations are wide ranging activities conducted by the intelligence team for the purpose of providing the commander with relevant, accurate, and timely intelligence. The six categories of intelligence operations are: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. This intelligence process (see Figure 3-1) greatly simplifies a dynamic and complex process, and in many situations, the various intelligence operations occur simultaneously with one another or may be bypassed altogether. For example, a request for imagery generates planning and direction but this may not involve new collection, processing, or exploitation if the request is satisfied from archival imagery.

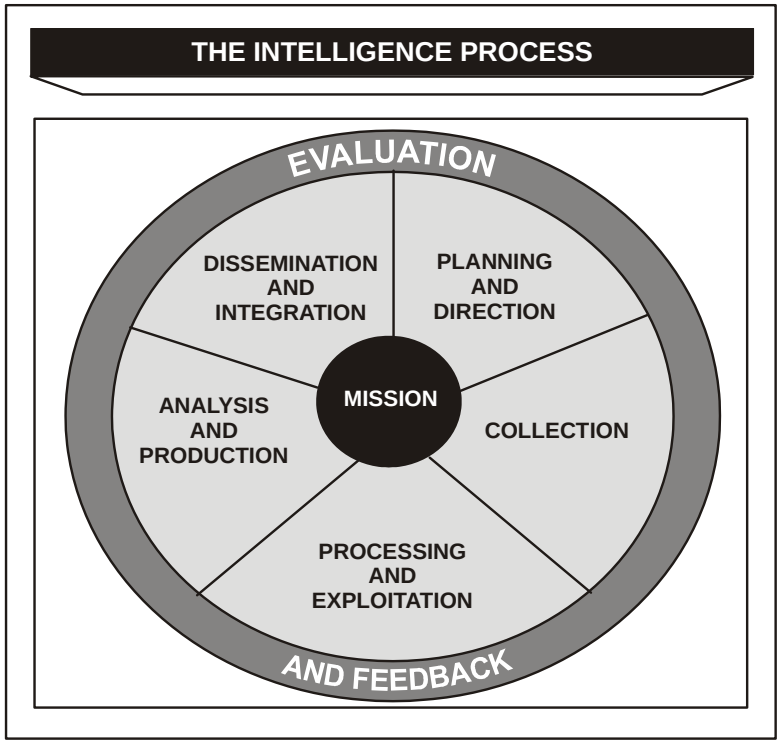

Figure 3-1. The Intelligence Process

3.3.1 Planning and Direction

During mission analysis for naval operations, the force staff identifies significant gaps in what is known about the adversary and other relevant aspects of the operational environment and formulates intelligence requirements. All staff sections may recommend intelligence requirements for designation as PIRs – a priority for intelligence support that the commander and staff need; however, the N2 has overall staff responsibility for consolidating PIR nominations and for making an overall staff recommendation to the commander regarding their approval. Ultimately, the commander designates PIRs, which together with friendly force information requirements constitute the commander's critical information requirements (CCIRs). Based on identified intelligence requirements (to include PIRs), the intelligence staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). A subset of information requirements that are related to and would answer a PIR are known as EEIs. Figure 3-2 illustrates how information requirements (including EEIs) are formulated from, and are intended to answer, intelligence requirements (including PIRs).

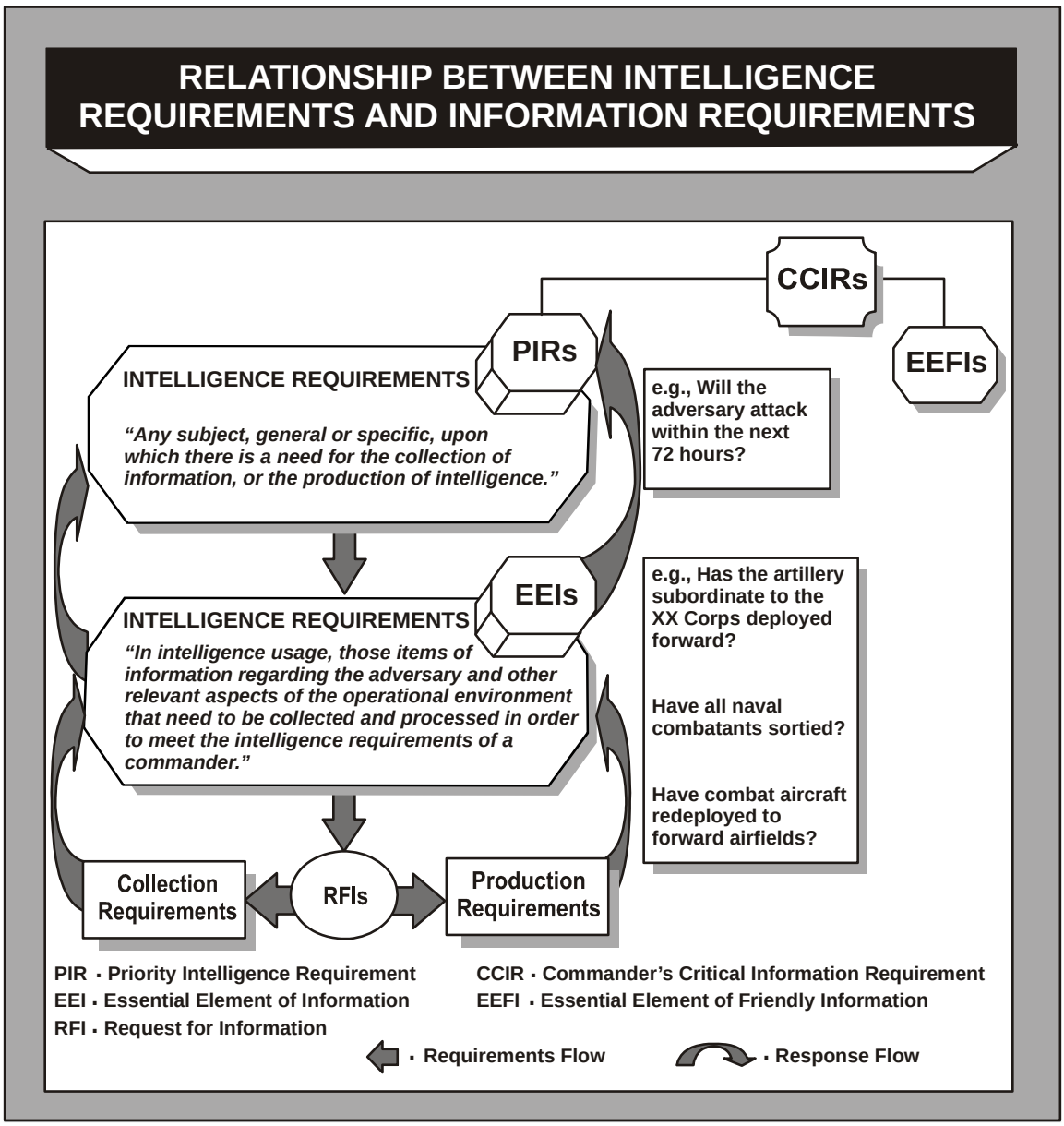

Figure 3-2. Relationship Between Intelligence Requirements and Information Requirements

Once intelligence requirements and information requirements are established, intelligence personnel review existing intelligence databases for answers to the requirements. If the intelligence does not already exist, they issue RFIs and initiate the development or revision of a collection plan. An RFI is a specific time-sensitive ad hoc requirement for information or intelligence products and is distinct from standing requirements or scheduled intelligence production. An RFI is initiated at any level of command and is validated in accordance with the higher echelon's procedures. An RFI leads to either a production requirement if the request is answered with information on hand or a collection requirement if the request demands collection of new information. Collection planning and requirement management are major activities during planning and direction.

3.3.2 Collection

Collection involves tasking organic and supporting collection resources to gather information. The collection process determines what is available to support decisionmaking. Since few collection requirements are met fully by organic assets alone, collection resources available at the theater and national level are normally 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. Collected data is distributed via appropriately classified channels to processing and exploitation elements.

3.3.3 Processing and Exploitation

During processing and exploitation, raw collected data is converted into forms that can be readily used by commanders, intelligence analysts, and other consumers. Processing and exploitation includes first phase imagery exploitation, data conversion and correlation, document translation, and signal decryption, as well as reporting the results of these actions to analysis and production elements. Processing and exploitation may be performed by the same element that collected the data.

An example of processing and exploitation occurs when the technical parameters (frequency, pulse repetition frequency, and bandwidth) detected by an ELINT collection system are compared and associated with the known parameters of a particular radar system. Rather than having to deal with raw ELINT data, the analyst is provided with the identity of the radar.

3.3.4 Analysis and Production

During analysis and production, intelligence is produced from the information gathered by the collection capabilities assigned or attached to the force and from the refinement and compilation of intelligence received from subordinate units and external organizations. All available processed information is integrated, evaluated, analyzed, and interpreted to create products that satisfy the commander's PIRs or RFIs. Intelligence products are presented in many forms such as oral presentations, hard copy publications, or electronic media. Intelligence production for joint operations is accomplished by units and organizations at every echelon. Whereas collection, processing, and exploitation are primarily performed by specialists from one of the major intelligence disciplines, analysis and production is done primarily by all-source analysts that fuse together information from all intelligence disciplines. The product resulting from this multidiscipline fusion effort is known as all-source intelligence.

3.3.5 Dissemination and Integration

The goal of dissemination and integration is to provide the right amount of appropriately classified intelligence when, where, and how it is needed to ensure its use by the commander or warfighter. Dissemination is carried out through a variety of means. The means are determined by the needs of the user and the implications and criticality of the intelligence. Briefings, video teleconferences, telephone calls, facsimile transmissions, electronic messages, web pages, and network access to computer databases are all means of dissemination. The diversity of dissemination paths reinforces the need for communications and computer systems interoperability among joint and multinational forces, component commands, DOD organizations, and the interagency community.

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.

3.3.6 Evaluation and Feedback

During evaluation and feedback, intelligence personnel at all levels assess how well each of the various types of intelligence operations are performed. Commanders and operational staff elements must provide feedback. When areas are identified that need improvement, the necessary changes are made. Evaluation and feedback may also serve to refine collection requirements and priorities in phased operations. Evaluation and feedback are continuously performed during each step of the intelligence process. Intelligence planners, collectors, analysts, and disseminators coordinate and cooperate to determine if any of the various intelligence operations require improvements.

For further information on the intelligence process, refer to JP 2-0, Joint Intelligence.

3.4 INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

Intelligence preparation of the operational environment (IPOE) is the analytical process used by intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the commander's decision-making process. It is a continuous process that involves four major steps: defining the total operational environment, describing the impact of the operational environment, evaluating the adversary, and determining and describing adversary potential COAs. The IPOE process assists commanders and their staffs in achieving information superiority by identifying adversary COGs, focusing intelligence collection at the right time and place, and analyzing the impact of the operational environment on military operations.

The IPOE process provides a disciplined methodology for applying a holistic view of the operational environment to the analysis of adversary capabilities and intentions. The process is both continuous and cyclical in that IPOE is conducted both prior to and during an operation as well as during planning for follow-on missions. The most current information available regarding the adversary situation and the operational environment is continuously integrated throughout the IPOE process. Although some aspects of the IPOE process may require adjustment depending on the type of mission, the basic process remains the same throughout the ROMO. Figure 3-3 graphically depicts the basic IPOE process.

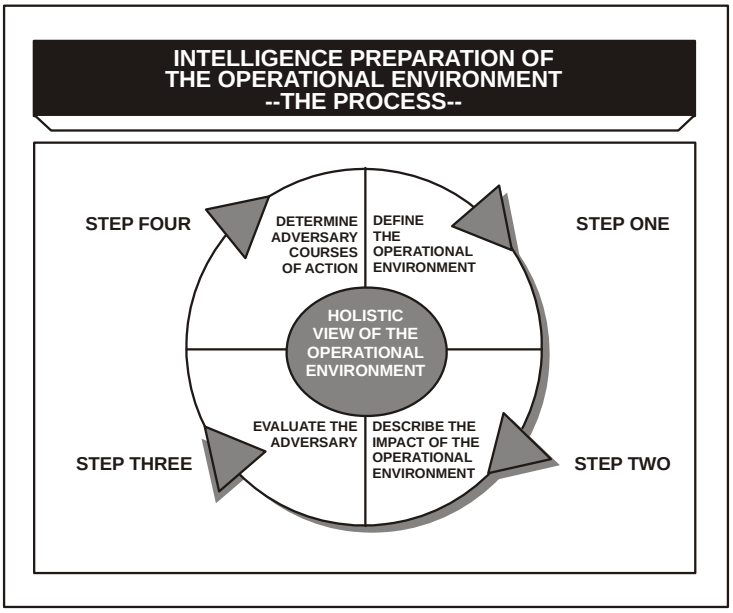

Figure 3-3. Intelligence Preparation of the Operational Environment — The Process

3.4.1 Define the Operational Environment

In the first step of the IPOE process, the force staff assists the commander and component commanders in defining the operational environment by identifying those aspects and significant characteristics that are relevant to the force's mission. The N2 staff works with other force and component command staff elements to formulate an initial survey of adversary and other relevant characteristics that may impact both friendly and adversary operations. Successfully defining the command's operational environment is critical to the outcome of the IPOE process. Failure to focus on the relevant characteristics of the operational environment leads to wasted time and effort.

3.4.2 Describe the Impact of the Operational Environment

The second step of the IPOE process evaluates the impact of the operational environment on adversary, friendly, and neutral military capabilities and broad COAs. All relevant physical and nonphysical aspects of the operational environment are analyzed by IPOE analysts, command personnel, and geospatial intelligence (GEOINT) analysts to produce a geospatial perspective. Likewise, a systems perspective is developed through the analysis of relevant sociocultural factors and system/subsystem nodes and links. Products developed during this step might include overlays and matrices that depict the military impact of geography, meteorological and oceanographic factors, demographics, and the information environment. Other products include assessments of sociocultural factors and network analysis diagrams associated with adversary and neutral political, military, economic, social, information, and infrastructure systems.

3.4.3 Evaluate the Adversary

Evaluating the adversary identifies and evaluates the adversary's capabilities and limitations, current situation, COGs, and the doctrine, patterns of operation, and TTP employed by adversary forces, absent those constraints identified during step two. During this step, models are developed that portray how adversary forces normally execute military operations or how they reacted to specific military situations in the past. The IPOE analyst must take care not to evaluate the adversary's capabilities by mirror imaging U.S. joint and Service doctrine. In many cases the doctrine of potential adversaries is embryonic or nonexistent.

3.4.4 Determine and Describe Adversary Courses of Action

The first three steps of the IPOE process help to provide commanders, subordinate commanders, and their staffs with a holistic view of the operational environment by analyzing the impact of the operational environment, assessing adversary doctrine and capabilities, and identifying adversary COGs and decisive points. The fourth step in the IPOE process, determining adversary COAs, builds upon this holistic view to develop a detailed understanding of the adversary's probable intent and future strategy. The process provides a disciplined methodology for analyzing the set of potential adversary COAs in order to identify the COA the adversary is most likely to adopt, and the COA that is most dangerous to the friendly force or to mission accomplishment.

3.4.5 Special Considerations

Naval forces conduct IPOE to develop a holistic view of the operational environment and assess adversary potential COAs in a wide variety of situations across the ROMO. Within the context of IPOE, the commander and N2 must apply the term "adversary" broadly, to refer to those organizations, groups, decision makers, or even physical factors that can delay, degrade, or prevent the joint force from accomplishing its mission. For example, during some crisis response and limited contingency operations, such as homeland defense, disaster relief, and civil support, the IPOE "adversary" may actually be a condition or situation, such as a hurricane with its related flooding, the outbreak of a disease pandemic with its associated vectors, or the starvation faced by famine-struck refugees. During military engagement, security cooperation, and deterrence operations, the "adversary" may range from smugglers and drug cartels to insurgents and terrorists. Identifying and conducting an IPOE analysis of these types of nontraditional adversaries presents a far greater challenge than the analysis of the more conventional "force-on-force" adversary normally associated with major operations and campaigns.

For further information on IPOE, refer to JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

3.5 INTELLIGENCE ORGANIZATION

When naval units deploy or conduct an operation, the individual ship, squadron, staff, and air wing intelligence personnel must coalesce to become part of a larger intelligence organization. In most cases, these intelligence professionals provide vital Service-specific intelligence and analysis to a JFC and J2. In some instances, however, they are called upon to support operations as the nucleus of a J2 organization or as a single Service. This section describes the structure of these intelligence organizations and how they align themselves to most optimally support the operational decision maker.

3.5.1 Joint Task Force/Joint Force Maritime Component Commander/Navy Component Commander

A JTF is a joint force that is constituted and so designated by a JTF-establishing authority (e.g., the SECDEF, a CCDR, a subordinate unified commander, or an existing commander, joint task force (CJTF)) to conduct military operations or support to a specific situation. It usually is part of a larger national or international effort to prepare for or react to that situation. In most instances, the JTF-establishing authority is a CCDR. The JFC is ultimately responsible to the establishing authority for JTF actions. Figure 3-4 illustrates a possible JTF organization.

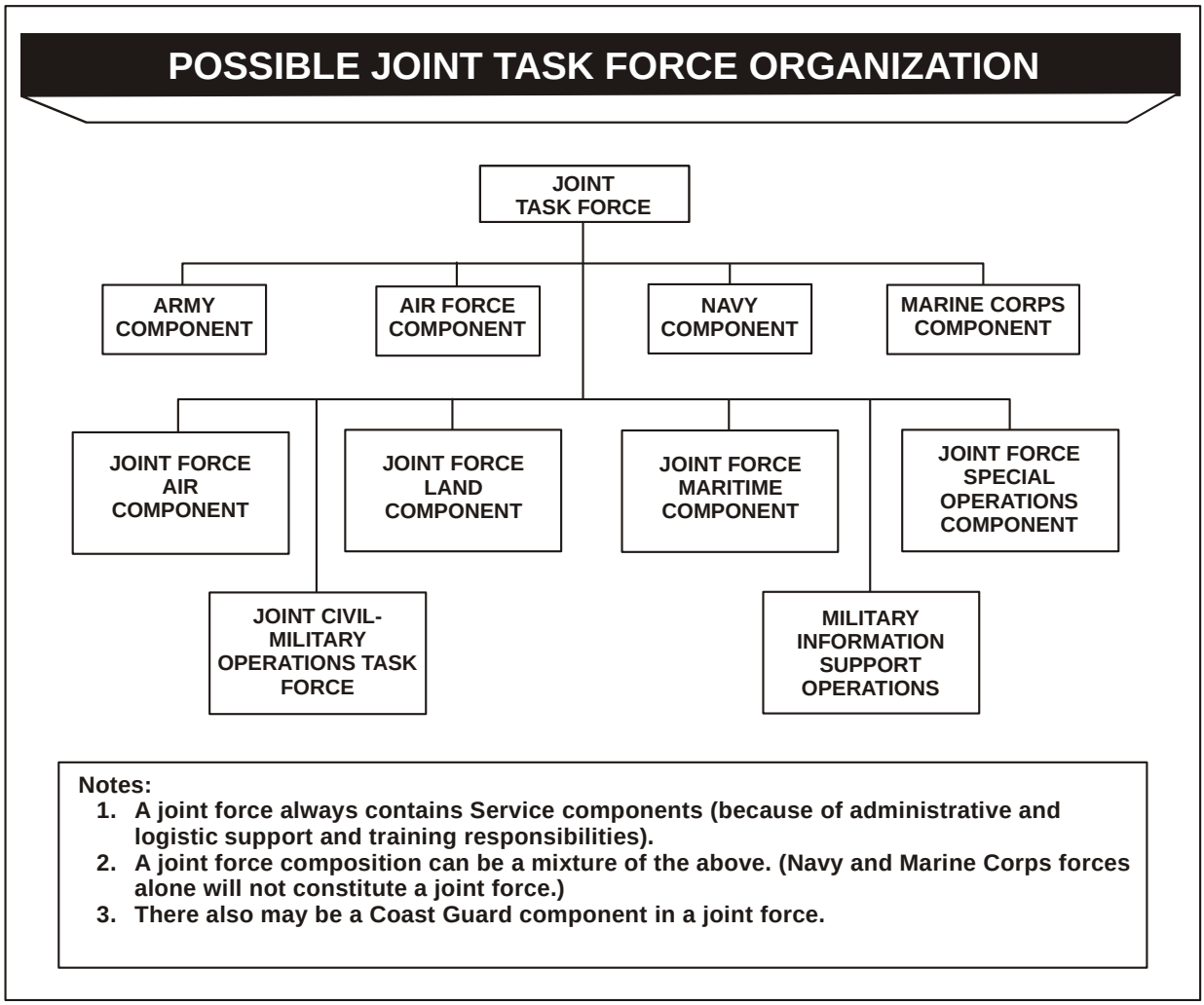

Figure 3-4. Possible Joint Task Force Organization

The preferred option for organizing a JTF headquarters (HQ) is to form it around a combatant command's Service component HQ or the Service component's existing subordinate HQ (such as a numbered fleet, numbered air force, marine expeditionary force, or army corps) that includes an established command structure. In some cases, the CCDR may designate the standing joint force HQ (core element) as the core HQ element and augment it with additional Service functional experts. As a third option, a CCDR may initially deploy a combatant command assessment team, or like organization, as the JTF core element. This third option is likely employed in a location where no military presence currently exists. Figure 3-5 depicts a typical JTF staff organization.

The primary role of the joint force J2 is to provide intelligence support to the JFC. The J2 additionally acts as a broker of intelligence support for those in subordinate commands as well as the executive agent for intelligence support tasks that may be required by the JFC CONOPS or directed by higher authority. The J2 has primary responsibility for coordinating the intelligence effort across the force. Based on JFC guidance, the J2 develops

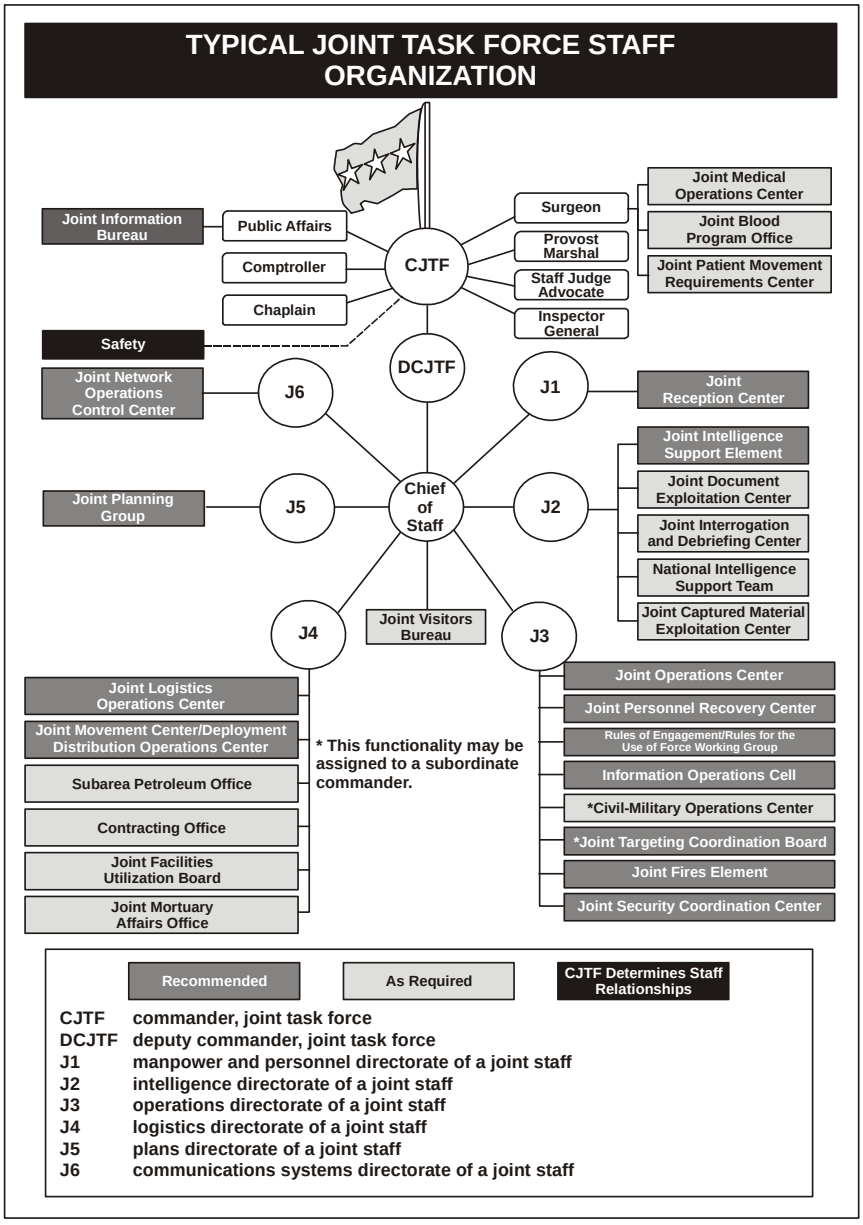

Figure 3-5. Typical Joint Task Force Staff Organization

intelligence and reconnaissance plans for component operations and provides feedback to the JFC on intelligence-related issues affecting joint operations. The J2 defines intelligence responsibilities and PIRs of tactical forces.

The size and composition of the joint force J2 staff is dependent upon the joint force organization and scope of the operation. Normally, the J2 requires access to national, theater, and tactical intelligence systems/data. The joint force J2 staff also requires the ability to conduct core analysis, I&W, collection management, targeting, and systems and administrative support.

When a Service component commander is activated as a JFC, the core intelligence staff normally becomes responsible for operational-level intelligence matters. Because such responsibility can be a significant expansion of the scope and depth normally executed, augmentation of the J2 staff is likely required. The J2 and staff must understand the intelligence requirements of the JFC and the subordinate component commands so they can focus on the timely integration and synchronization of relevant all-source intelligence into joint force operations. The overall objective is to provide the JFC with accurate, timely, and relevant knowledge about the threat and the surrounding environment. Figure 3-6 portrays a notional subordinate JTF intelligence organization. Additional information concerning the JTF J2 support to the JFC is available in section 4.4.1.

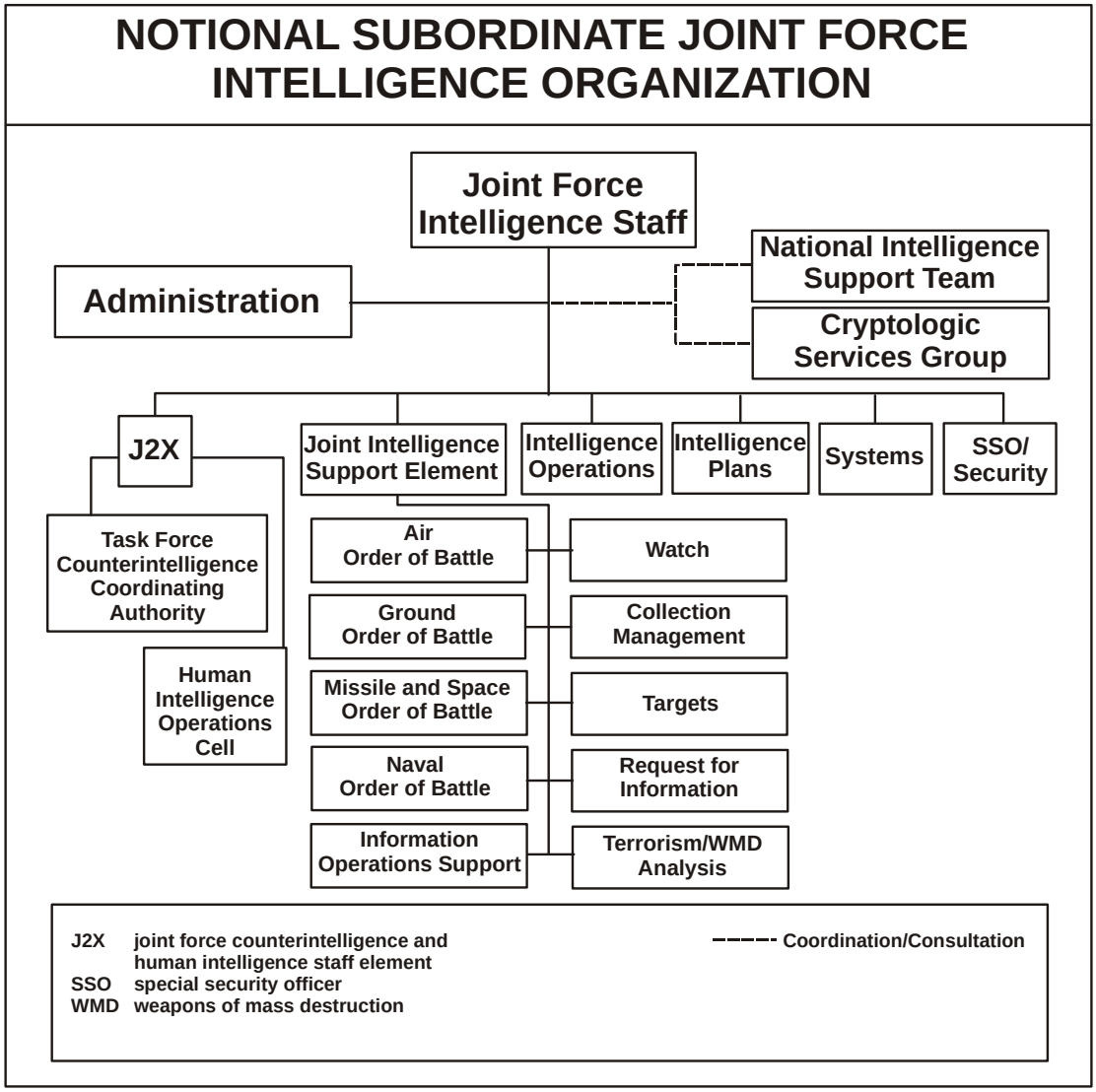

Figure 3-6. Notional Subordinate Joint Task Force Intelligence Organization

The JFC conducts maritime operations through either a Service component construct (NCC) or an FCC (JFMCC). Joint doctrine establishes the advantages for each model; however, examination of the last 20 years reveals that in most cases the JFC opts for the FCC and designates a JFMCC.

The JFMCC is the JFC's maritime warfighter. The JFC normally designates a JFMCC to command and control joint maritime operations. As a functional component commander, the JFMCC has command authority over assigned and attached forces and forces/assets made available for tasking to perform operational missions.

JFMCC responsibilities include planning, coordination, allocation, tasking, and synchronization of joint maritime operations based on the JFC's CONOPS and maritime apportionment decisions. The authority and command relationships of the JFMCC are established by the JFC. The JFMCC typically exercises operational control over assigned and attached forces. Additionally, the JFMCC may exercise tactical control over other military capabilities/forces made available for tasking. The JFC may also establish a support relationship between components to facilitate operations. The JFMCC executes or contributes to the operational functions supporting JFC goals. These operational functions apply in varying degrees across the ROMO, including those that involve multinational forces and interagency support. Figure 3-7 depicts a notional JFMCC functional organization.

A typical JFMCC J2 organization consists of an intelligence watch, intelligence plans, intelligence analysis, collections, cryptology, CI, and intelligence systems cells. Augmentation requirements are determined by the nature of the contingency, specific skills required to execute the mission, and the depth of intelligence capability in the existing staff. Numbered fleet and CSG/ESG/ARG N2s should be prepared to function as a JTF/JFMCC J2.

The JFC may conduct operations through Service component commanders or, at lower echelons, Service force commanders. This relationship is appropriate when stability, continuity, economy, ease of long-range planning, and the scope of operations dictate organizational integrity of Service forces for conducting operations. An NCC assigned to a CCDR consists of the NCC and the Navy forces that are assigned to that CCDR.

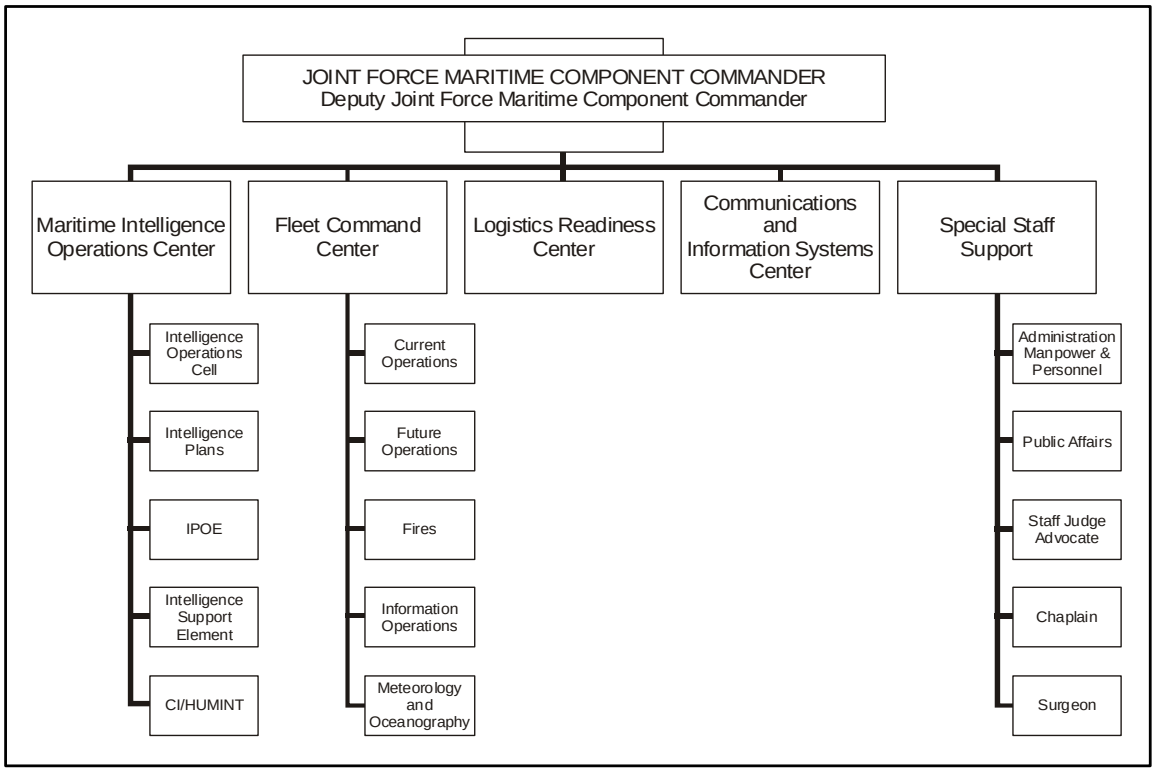

Figure 3-7. Notional Joint Force Maritime Component Commander Functional Organization

When a command is designated as the NCC to multiple CCDRs, the NCC and only that portion of the NCC's assets assigned to a particular CCDR are under the command authority of that particular CCDR. The JFC may provide NCCs command authority over Navy forces assigned or attached to the JFC. In addition to fulfilling any designated command authorities, Service component commander responsibilities derive from their Service's support function.

For further information on JTF, JFMCC, and NCC, refer to NWP 3-32, Maritime Operations at the Operational Level of War; NTTP 3-32.1, Maritime Operations Center; JP 3-32, Command and Control for Joint Maritime Operations; and JP 3-33, Joint Task Force Headquarters.

3.5.2 Maritime Intelligence Operations Center

The primary intelligence support mechanism for the MOC is the MIOC. The MIOC is responsible for attaining, maintaining, and sharing intelligence-related situational awareness. The MIOC is an all-source intelligence organization whose operations and schedule are driven by the needs of the commander and the established MOC battle rhythm. Its primary function is to satisfy the commander and staff's requirements by planning, conducting, collecting, analyzing, and disseminating reliable and timely intelligence. These actions are centered on adversary intentions, I&W, IO, targeting, and assessment. Intelligence must perform as an operational element in the monitoring, assessing, planning, and directing processes. While intelligence is an operational function in and of itself, it also has a supporting role in the planning and execution for all other operational functions.

The most visible component of the MIOC is an I&W watch that is charged with building situational awareness of the adversaries' disposition and activities, conducting predictive analysis of his impending operations, and communicating that intelligence through reports and continuous input to the common operational picture. A successful I&W watch is one that can both communicate intelligence to the rest of the staff and communicate staff requirements back to the rest of the MIOC and intelligence staff.

The MIOC maintains elements that provide support to both the cells within the MIOC as well as the staff members and functions throughout the MOC organization, such as the special security functions and foreign disclosure functions. The MIOC may also include staff that provides support specifically to the functioning of the MIOC, such as intelligence administration support and intelligence systems support.

The MIOC organization and location differ at each command and vary between operations. Locating the I&W watch in the fleet command center is considered best practice, but when that is not possible, there is a greater requirement on watchstanders to achieve the necessary level of information exchange.

For further information on MIOC, refer to NTTP 3-32.1, Maritime Operations Center.

3.5.3 Carrier Strike Group

The CSG intelligence organization provides accurate and timely intelligence support to the strike group commander, the embarked staff, the air wing, and critical warfighting centers of the ship. The intelligence organization is composed of staff, air wing, DESRON, and ship personnel synthesized into functional work centers providing I&W, intelligence collection requirements management, strike planning, and OPINTEL support to sea control, air and missile defense, IO, special operations, MIW, noncombatant evacuation operations (NEO), and other mission areas.

1. See Figure 3-8 – Carrier Strike Group Operational Organization.

2. Process. The carrier intelligence organization is a composite organization composed of staff, air wing, DESRON, and ship's personnel. The CSG N2 is the SIO and manager of the organization. Throughout the FRTP, the N2 ensures air wing, ship, DESRON, and other strike group intelligence personnel receive necessary training, that work center procedures are established, and that personnel are trained in their underway positions. Once underway, the N2 sets the organization's priorities, establishes overarching policy and procedures, and ensures that CVIC's numerous internal and external customers receive the intelligence support they need to accomplish their assigned missions.

   The ship's IO is primary overseer of the group N2's guidance and priorities. With the primary assistance of the CAG AI, the ship's IO supervises the overall MT&E of the personnel and systems assigned to the ship. Two CVIC work centers, MSI and SSES, are supervised by the ship's IO. The CSG assistant N2 is in charge of SUPPLOT, and the CAG AI is responsible for SIAC and mission briefing/debriefing operations. One of the intelligence team's major functions is to ensure that CVIC work centers maintain a coherent flow of intelligence information between CVIC, CSG, CVN, CVW, DESRON, and other internal C2 nodes.

3. Coordination. The carrier conducts numerous intelligence activities such as imagery interpretation and reporting, intelligence production, strike planning, and providing I&W to other U.S., coalition, and allied operational units. As such, CVIC needs to maintain close liaison with other fleet assets, naval shore commands, and joint intelligence and operational commands.

   As the strike group intelligence officer, the N2 is responsible for providing intelligence support to all strike group assets, including those without assigned intelligence personnel. The CSG N2 must establish formal and informal strike group RFI procedures so that intelligence personnel operating independently—CDIOs, IDISs, and DESRON N2s—can receive tailored support from CVIC. If CVIC is unable to provide the desired assistance, then established theater RFI procedures can be initiated.

   Depending on the mission, CVIC must also maintain close liaison with fleet and theater I&W watches, naval intelligence reachback agencies, and specialized national or theater targeting/analytical centers. Normally, informal data exchanges can be easily conducted between CVIC watches and these other sites; however, care must be exercised to adhere to established theater RFI procedures.

4. Work centers.

   a. SUPPLOT. This cell is an all-source I&W center supporting the battle watch officer in the TFCC, the TAO in CIC or CDC, and the assigned CWCs. SUPPLOT fuses organic and nonorganic SIGINT, imagery intelligence (IMINT), and HUMINT information, analyzes this data, and provides the decision makers with a detailed all-source assessment on the threat faced by strike group assets. SUPPLOT maintains close contact with the ship's SSES, CIC or CDC (air, surface, subsurface, and EW modules),

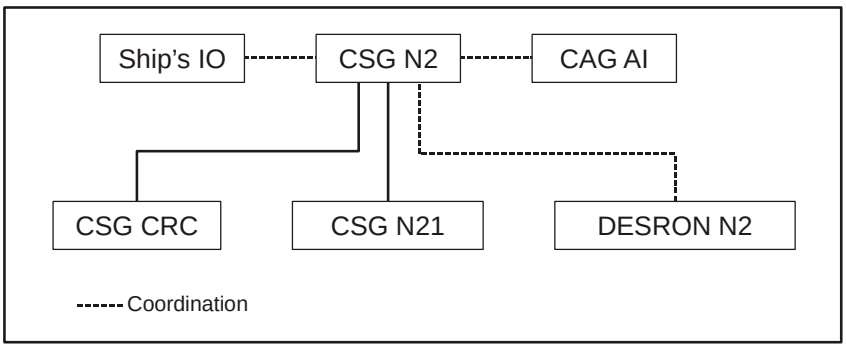

Figure 3-8. Carrier Strike Group Operational Organization

bridge watchstanders, lookouts, and the embarked staff and warfare commanders/coordinators. SUPPLOT is led by the CSG assistant N2 and manned by a combination of ship, air wing, and DS personnel.

b. SIAC. SIAC is comprised of two cells, the TIC and the TAC. SIAC TIC is responsible for conducting target development, weaponeering, electronic and hardcopy target material production, target list management, and STWC coordination in support of CVW deliberate/dynamic targeting, contingency planning, and maritime interdiction. SIAC TIC is comprised of the CVW TO, the CVW ATO, and a cross section of ship, squadron, and NSAWC FID personnel.

   SIAC TAC is an all-source analytical cell supporting the STWC. SIAC personnel analyze organic and nonorganic imagery, SIGINT, HUMINT, open source reports, and postmission and in-flight reports to provide aircrew with the most current and accurate information and assessments. SIAC is led by a squadron AI and manned by a combination of NSAWC FID and air wing ISs and CTs.

c. Mission briefing/debriefing. This cell provides two major functions. First, it provides a detailed intelligence, weather, and operational briefing for all missions prior to launch. The briefing is normally conducted while the crews are in their ready room via the ship's secure closed-circuit television (SCCTV) system.

   Second, the cell conducts a detailed debrief of all returning missions. This debrief includes operational and intelligence-related information such as an initial assessment of strike damage, ordnance performance, observed adversary activity, observed merchant ships and neutral combatants, the functioning of all systems, and fuel/weapons status. The cell incorporates most of this information into a mission report required by the joint air operations center (JAOC). Additionally, the debriefing cell internally coordinates with SUPPLOT, SIAC, and SSES to ensure that relevant debrief information is included in their assessments. The mission briefing/debriefing cell is normally manned entirely by squadron AIs/ISs and 1-2 SCCTV technicians.

d. MSI. MSI performs imagery analysis of organic (shared reconnaissance pod (SHARP) and handheld photography) and nonorganic (national, coalition, and commercial) imagery. In addition to general imagery analysis, MSI is heavily involved in strike warfare planning, to include target analysis, aimpoint geopositioning, and initial BDA. These activities are conducted for tactical aircraft and cruise missiles. MSI is normally manned by a combination of ONI, FID, and air wing personnel.

e. SSES. SSES provides real time SIGINT tactical support using organic and nonorganic resources in response to national, theater, and fleet cryptologic requirements. Operationally, SSES responds to cryptologic tasking from the CRC/IWC providing tactically relevant time-sensitive I&W data extending beyond the horizon.

3.5.4 Expeditionary Strike Group/Amphibious Ready Group/Marine Expeditionary Unit

The amphibious intelligence organization provides accurate and timely intelligence support to the group commander, the embarked staff, and critical warfighting centers of the command ship. The intelligence organization provides I&W, intelligence collection requirements management, strike planning, and OPINTEL support to sea control, air and missile defense, special operations, MIW, NEO, and other mission areas.

1. Process. The amphibious intelligence organization is a composite organization composed of staff, MEU, PHIBRON, IDISs, and ship's company personnel. When embarked, the ESG/ARG N2 is the SIO and manager of the organization. The ESG/ARG N2 sets the organization's priorities, establishes overarching policy and procedures, and ensures the numerous internal and external customers receive the intelligence support they need to accomplish their assigned missions.

   The LHD/LHA ship's IO supervises the overall MT&E of the personnel and systems assigned to the ship. The PHIBRON N2 and MEU S2 are in charge of EXPLOT, SSES, the imagery processing interpretation

center (IPIC), and the United States Marine Corps (USMC) intelligence watch, while the ESG/ARG N2 is in charge of the JIC. One of the intelligence team's major functions is to ensure that all work centers maintain a coherent flow of intelligence information between external and internal C2 nodes.

2. Coordination. The ESG/ARG/MEU conducts numerous intelligence activities such as imagery interpretation and reporting, intelligence production, strike planning, and providing I&W to other U.S. coalition and allied operational units. As such, the JIC needs to maintain close liaison with other fleet assets, naval shore commands, and joint intelligence and operational commands.

   As the amphibious group SIO, the N2 is responsible for providing intelligence support to all strike group assets, including those without assigned intelligence personnel. The ESG/ARG N2 must establish formal and informal strike group RFI procedures so that intelligence personnel operating independently can receive tailored support from the JIC. If the JIC is unable to provide the desired assistance, then established theater RFI procedures can be initiated.

   Depending on the mission, the JIC must also maintain close liaison with fleet and theater I&W watches, naval intelligence agencies, and specialized national or theater targeting/analytical centers. Normally, informal data exchanges can be easily conducted between JIC watches and these other sites; however, care must be exercised to adhere to established theater RFI procedures.

3. Work centers.

   a. EXPLOT. This cell is an all-source I&W center supporting the battle watch officer and the CWCs. EXPLOT constantly monitors organic and nonorganic SIGINT, IMINT, and HUMINT information, analyzes this data, and provides the decision makers with a detailed all-source assessment on the threat faced by strike group assets.

   b. JIC. The JIC conducts long-term intelligence analysis, production, and dissemination in support of ESG/ARG/MEU requirements. Additionally, the JIC provides aircrew mission brief/debrief support for Navy air assets and the embarked MEU air combat element. The JIC is normally augmented during C2X, JTFEX, and deployment by an embarked CYBERFOR FID consisting of two IS-3923 strike analysts.

   c. IPIC. IPIC performs imagery analysis of organic and nonorganic imagery. In addition to general imagery analysis, IPIC is heavily involved in strike warfare planning, to include target analysis, aimpoint geopositioning, and initial BDA. These activities are conducted for tactical aircraft and cruise missiles. IPIC is normally manned during C2X, JTFEX, and deployment by an embarked CYBERFOR FID consisting of four IS-3910 imagery interpreters and sometimes augmented by MEU personnel.

   d. SSES. SSES provides real time SIGINT tactical support using organic and nonorganic resources in response to national, theater, and fleet cryptologic requirements. Operationally, SSES responds to cryptologic tasking from the CRC/IWC providing tactically relevant time-sensitive I&W data extending beyond the horizon.

3.5.5 Destroyer Squadron

The DESRON N2 provides intelligence support to the DESRON staff and the squadron's IDISs and CDIOs. CDIOs are normally junior surface warfare officers or senior enlisted and have limited formal intelligence training or experience. The DESRON intelligence organization receives most of its support from the CSG/ESG/ARG. In

some instances, CSGs establish specialized MIO support cells to assist the DESRON commander in assigned missions. When the DESRON operates independently of the CSG/ESG/ARG, the CSG/ESG/ARG N2 coordinates with the DESRON's numbered fleet N2 to establish policy guidelines on the support process for the DESRON N2. Figure 3-9 depicts the standard DESRON intelligence organization.

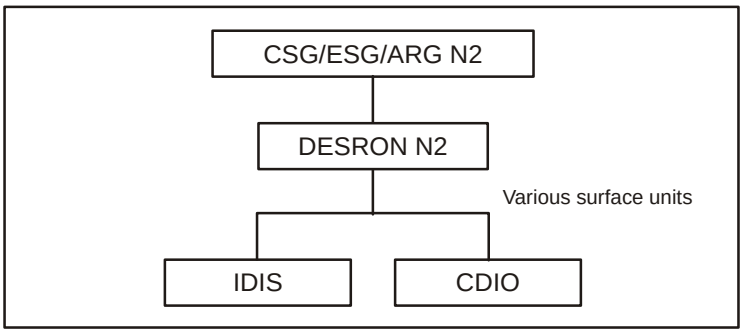

Figure 3-9. Destroyer Squadron N2 Organization

3.5.6 Maritime Patrol and Reconnaissance

Administratively, MPR squadrons and their intelligence personnel report to their respective wing commander. A VP squadron has one junior intelligence officer and three ISs. A VQ squadron has one O-4, five first tour junior officers, eight ISs, and 13 CTs assigned. The MPR wing N2 provides day-to-day intelligence mentoring and training, as well as SSO and administrative support to squadron intelligence personnel. The CPRG serves as the executive agent for TYCOM (Commander, Naval Air Forces) maritime patrol functions and also schedules and coordinates global deployment of maritime patrol platforms. The CPRG N2 oversees the intelligence aspects of MPR MT&E, essentially functioning as a TYCOM N2.

Operationally, deployed MPR squadrons fall under a task force commander (e.g., CTF 57, CTF 67, and CTF 72). These staffs are responsible for planning and executing MPR missions in a specific AO or functional role.

When deployed, operational and intelligence support is provided by an AO-specific tactical operations center (TOC). TOCs are command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) centers manned by a combination of permanently assigned and deployed personnel. Deployed squadron intelligence personnel integrate themselves into the TOC organization.

1. See Figure 3-10 – Maritime Patrol and Reconnaissance N2 Organization.

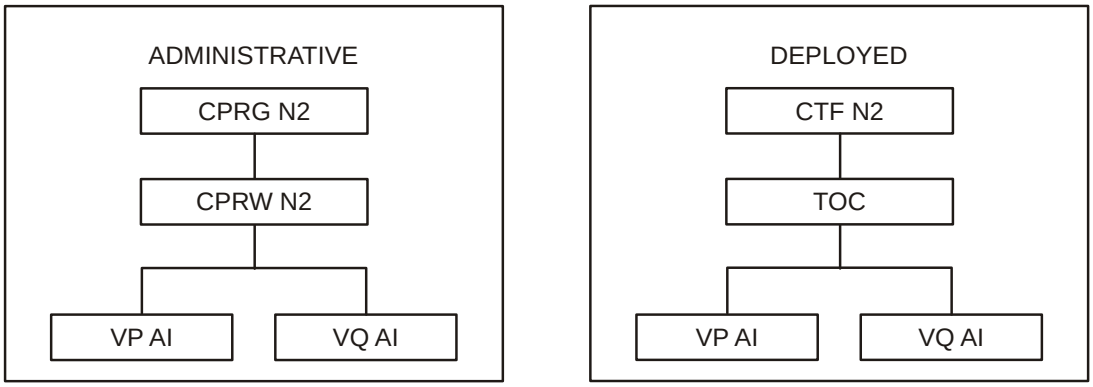

Figure 3-10. Maritime Patrol and Reconnaissance N2 Organization

2. Process. TOCs provide tactical-level C4ISR and mission support to aircrew. They are the MPR equivalent to the CVN's CDC and CVIC. Congruent to its planning and execution role, TOCs perform correlation of mission and sensor data for each of the FOS platforms. The TOCs supply fleet and JFCs, via the MOC, with synthesized information required to inform decisions. TOCs simultaneously publish raw sensor data to the MOC and interagency databases for further analysis and dissemination within the IC. The TOC monitors theater intelligence summaries, event-by-event reporting, and specialized reports from the ONI merchant watch to provide mission-specific information to flight crews. The TOC also transfers MPR imagery reports and OPINTEL to theater and national customers for use in further analysis to satisfy PIRs.

3. Coordination. The TOC maintains close coordination with its respective CTF operations cell. The CTF provides mission assignments in response to fleet, theater, and national requirements. The TOC intelligence personnel maintain close liaison with the numbered fleet N2, the theater JIOC, and the ONI watch/merchant shop.

3.5.7 Naval Special Warfare

NSW forces deploy to theaters as NSW squadrons (e.g., a SEAL team augmented with NSW mobility and logistics capability, a mobile communications team, explosive ordnance disposal, and a tailored intelligence cross functional team). The organic SEAL team intelligence department and cross functional team, in conjunction with the Naval Special Warfare Mission Support Center (NSW MSC), ONI's Kennedy Irregular Warfare Center, and theater NSW units, provide intelligence support to the deployed force. In CONUS, the organic team intelligence department, in conjunction with the NSW group N2 and SUPPACT, provide the team with intelligence support.

NSW forces rely on intelligence support from the NSW MSC, the field support team, and augmentation from Kennedy Irregular Warfare Center. Additional support can also be obtained from a CCDR's JIOC and the Special Operations Command Global Mission Support Center. Deployed NSW forces request and receive intelligence support directly from the NSW MSC via reachback communications or from supporting theater intelligence capabilities such as the TSOC or a subordinate TSOC combined joint special operations task force. CONUS forces request and receive theater-related intelligence support from theater JIOCs via the TSOC. Intelligence support for CONUS-based exercises or nontheater deployments is requested through the NSW MSC, the Kennedy Center, or NSW SUPPACTs.

3.5.8 Navy Expeditionary Forces

NECC provides highly adaptive, tailored forces to CCDRs and NCCs in the following areas: riverine forces, explosive ordnance disposal, naval construction forces, maritime civil affairs, maritime security forces, expeditionary logistics, mobile diving and salvage, expeditionary training, and combat camera. These forces operate in close proximity to HN forces and populaces and hold specific intelligence and IO requirements to support their unique missions. Most expeditionary units are assigned organic intelligence resources and are augmented by Navy Expeditionary Intelligence Command (NEIC) capabilities. These forces are generally supported by specially trained 1610s, 1630s, IS-3912s, IS 3913s, and specialized CT personnel.

3.6 INTELLIGENCE AND THE RANGE OF MILITARY OPERATIONS

The ROMO is divided into three major categories: major operations and campaigns; crisis response and limited contingency operations; and military engagement, security cooperation, and deterrence. Intelligence is critical in all naval and joint operations. During major operations and campaigns, intelligence identifies enemy capabilities, helps identify the COGs, projects probable COAs, and assists in planning friendly force employment. In crisis response and limited contingency operations, intelligence provides assessments that help the JFC decide which forces to deploy; when, how, and where to deploy them; and how to employ them in a manner that accomplishes the mission. Finally, during military engagement, security cooperation, and deterrence activities, intelligence operations seek to provide the national leadership with the information needed to realize national goals and objectives while providing military leadership with the information needed to accomplish missions and implement the national security strategy.

The most important role of intelligence in military operations is to assist commanders and their staffs in understanding and visualizing relevant aspects of the operational environment. This includes determining adversary capabilities and will, identifying adversary critical links, key nodes, high-value targets and COGs, and discerning adversary probable intentions and likely COAs. Visualization of the operational environment requires a thorough understanding of the characteristics of the operational area and the current dispositions and activities of adversary and neutral forces. It requires knowing the adversary's current and future capability to operate throughout the operational environment based on a detailed analysis of the impact of weather, geography, and other relevant considerations. Most important, visualization requires understanding the adversary's objectives, identifying how the adversary might fulfill those objectives, and determining the adversary's readiness to achieve the objectives. Together, all these factors make a critical contribution to the JFC's capability to achieve information superiority; however, intelligence must also enable the JFC to know the potential and probable future state of events well in advance of the adversary. This knowledge allows the JFC to better predict the adversary's future COA and scheme of maneuver and to anticipate adversary actions and plan detailed countermeasures.

3.6.1 Major Operations and Campaigns

When required to achieve national strategic objectives or protect national interests, the United States' national leadership may decide to conduct a major operation or campaign involving large-scale combat, placing the United States in a wartime state. In such cases, the general goal is to prevail against the enemy as quickly as possible, conclude hostilities, and establish conditions favorable to the HN and the United States and its multinational partners. Establishing these conditions often requires naval and joint forces to conduct stability operations to restore security, provide essential services and humanitarian relief, and conduct emergency reconstruction. Major operations and campaigns typically include multiple phases (e.g., Operations DESERT SHIELD and DESERT STORM [1990-1991] and Operation IRAQI FREEDOM [2003]). Some specific crisis response or limited contingency operations may not involve large-scale combat but could be considered major operations or campaigns depending on their scale and duration (e.g., Tsunami relief efforts in Indonesia or Hurricane Katrina relief efforts in the United States, both in 2005).

Major operations and campaigns are almost exclusively joint endeavors and usually employ multiple naval mission areas. Section 3.7 describes those major mission areas of naval operations and briefly introduces how naval intelligence supports them.

3.6.2 Crisis Response and Limited Contingency Operations

A crisis response or limited contingency operation can be a single small-scale, limited-duration operation or a significant part of a major operation of extended duration involving combat. The associated general strategic and operational objectives are to protect U.S. interests and/or prevent surprise attack or further conflict. A limited contingency operation in response to a crisis includes all of those operations for which joint operation planning is required and an OPLAN or operation order is developed. The level of complexity, duration, and resources depends on the circumstances. Included are operations to ensure the safety of American citizens and U.S. interests while maintaining and improving the United States' ability to operate with multinational partners to deter the hostile ambitions of potential aggressors (e.g., JTF SHINING HOPE in the spring of 1999 to support refugee humanitarian relief for hundreds of thousands of Albanians fleeing their homes in Kosovo). Many of these operations involve a combination of military forces and capabilities in close cooperation with other government agencies (OGAs), intergovernmental organizations, and nongovernmental organizations.

Intelligence provides assessments that help the JFC decide which forces to deploy; when, how, and where to deploy them; and how to employ them in a manner that accomplishes the mission. The intelligence requirements in support of crisis response and limited contingency operations such as NEOs; peace operations; foreign humanitarian assistance; recovery operations; consequence management actions associated with chemical, biological, radiological, nuclear, and high-yield explosives; strikes and raids; homeland defense; and civil support are similar to those required during major operations. During disaster relief operations, intelligence can play an important role in surveying the extent of damage and can assist in planning for the deployment of relief forces. Intelligence is essential to protect joint forces participating in these operations. While intelligence efforts are supporting peacekeeping operations, intelligence must also provide the JFC with I&W of any possible escalation

of violence and a firm basis upon which to develop necessary OPLANs. Intelligence professionals providing support for homeland defense and civil support shall comply with intelligence oversight policies and regulations. Intelligence activities carried out as part of civil support operations should be reviewed by competent legal authority.

3.6.3 Military Engagement, Security Cooperation, and Deterrence

These ongoing and specialized activities establish, shape, maintain, and refine relations with other nations and domestic civil authorities. The general strategic and operational objective is to protect U.S. interests at home and abroad. Military engagement is the routine contact and interaction between elements of the Armed Forces of the United States and those of another nation's armed forces, or between foreign and domestic civilian authorities or agencies to build trust and confidence, share information, coordinate mutual activities, and maintain influence. Security cooperation involves all DOD interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and friendly military capabilities for multinational operations, and provide U.S. forces with peacetime and contingency access to an HN. Security cooperation is a key element of global and theater shaping operations and a pillar of WMD nonproliferation. Deterrence helps prevent adversary action through the presentation of a credible threat of counteraction.

Maintaining a forward presence enables U.S. forces to gain regional familiarity and develop a common understanding of important cultural, historical, interpersonal, and social differences. Activities such as professional military exchanges, forward basing, and cooperative relationships with multinational partners enhance U.S. forces' ability to shape potential military engagement, security cooperation, and deterrence operations, gain an understanding of multinational tactics and procedures, enhance information sharing, and establish mutual support with host country nationals. Intelligence support is essential to activities such as emergency preparedness, arms control verification, combating terrorism, counterdrug operations, enforcement of sanctions and exclusion zones, ensuring freedom of navigation and overflight, nation assistance, protection of shipping, shows of force, and support to insurgency and counterinsurgency operations.

3.7 CORE NAVAL MISSION AREAS

3.7.1 Composite Warfare Commander Concept

The officer in tactical command (OTC) of any naval task organization can create a composite warfare organization whenever and to whatever extent required, depending upon the composition and mission(s) of the force, the environment in which the force is operating, and the nature and severity of the threat. The OTC may retain CWC command functions; however, the OTC and CWC are always separate and distinct even when the same commander fills both roles. The OTC may assign CWC command functions to a subordinate commander. In the case of a widely disbursed force, the OTC may designate sector CWCs. The CWC controls warfare commanders by providing guidelines for operational conduct and using command by negation.

The composite warfare construct allows the OTC to assign some or all of the command functions associated with warfare commander and coordinator duties and supports the execution of a decentralized command philosophy. The OTC and/or CWC may choose to activate all commanders and coordinators or activate only a few of them. Flexibility of implementation, reinforced by clear guidance to subordinates, and use of command by negation is key to decentralized control of the tactical force. The composite warfare organization enables offensive and defensive combat operations against air, surface, undersea, electronic, and land-based threats.

The CWC is the officer to whom the OTC has assigned all of his authority and assigned functions for the overall direction and control of the force. The OTC retains the power to negate any particular action by the CWC. Subordinate to the CWC are five warfare commanders: air missile defense commander (AMDC), antisubmarine warfare commander (ASWC), information operations warfare commander (IWC), strike warfare commander (STWC), and the surface warfare commander (SUWC).

The warfare commanders are responsible for collecting and disseminating information and, in certain situations, are assigned authority to respond to threats with assigned assets.

For further information on the CWC concept, refer to NWP 3-56, Composite Warfare Commander's Manual.

3.7.2 Strike Warfare/Targeting

Targeting has not changed in its basic form for centuries; however, the transformation of warfighting doctrine and tactics has drastically altered how the targeting end state is reached. Targeting is defined as "the process of selecting and prioritizing targets and matching the appropriate response to them, taking into account operational requirements and capabilities." Effective targeting is distinguished by the ability to generate the type and extent of effects necessary to facilitate the realization of the commander's objectives. Joint Publication 3-60, Joint Targeting, serves as the overarching guidance for developing AO and fleet-specific targeting doctrine and TTPs.

Targeting encompasses many disciplines. The application of military power is primarily an operations function, yet the extensive intelligence support required means that both operations and intelligence must work together to focus on achieving the commander's objectives. It is the function of targeting to efficiently achieve those objectives within the parameters set by the OPLAN, rules of engagement (ROE), and law of armed conflict (LOAC). TTPs for targeting span the full range of lethal, nonlethal, kinetic, and nonkinetic applications of force. In achieving the commander's objectives, targeting is concerned with producing specific effects (effects-based targeting). Targeting analysis considers all possible means to achieve desired effects, drawing from any available forces, weapons, and platforms.

3.7.2.1 Effects-Based Targeting

The ability to rapidly collect, share, access, and manipulate information is essential in achieving superiority over an adversary. Understanding the adversary's operational objectives, intentions, decision cycle, expectations, and needs through observation and analysis enable the use of varied means to produce effects against the enemy's critical vulnerabilities. The diligent application of the IPOE process by the intelligence team allows the commander to achieve critical battlespace awareness. Targeting effects are the cumulative results of actions taken to engage geographical areas, complexes, installations, forces, equipment, leadership, functions, perception, or information by lethal and nonlethal means. Targeting effects are categorized as either direct or indirect. Direct effects are the immediate, first-order consequences of action unaltered by intervening events or mechanisms; they are usually immediate and easily recognizable. Indirect effects are the delayed and/or displaced second and third-order consequences of action.

3.7.2.2 Joint Targeting Cycle

The purpose of the joint targeting process is to provide the commander with a methodology linking objectives with effects throughout the battlespace to reach a desired end state. It provides a logical progression and ensures consistency with the commander's objectives. The targeting process seeks to achieve effects in a systematic manner and is delineated by the targeting cycle as shown in Figure 3-11.

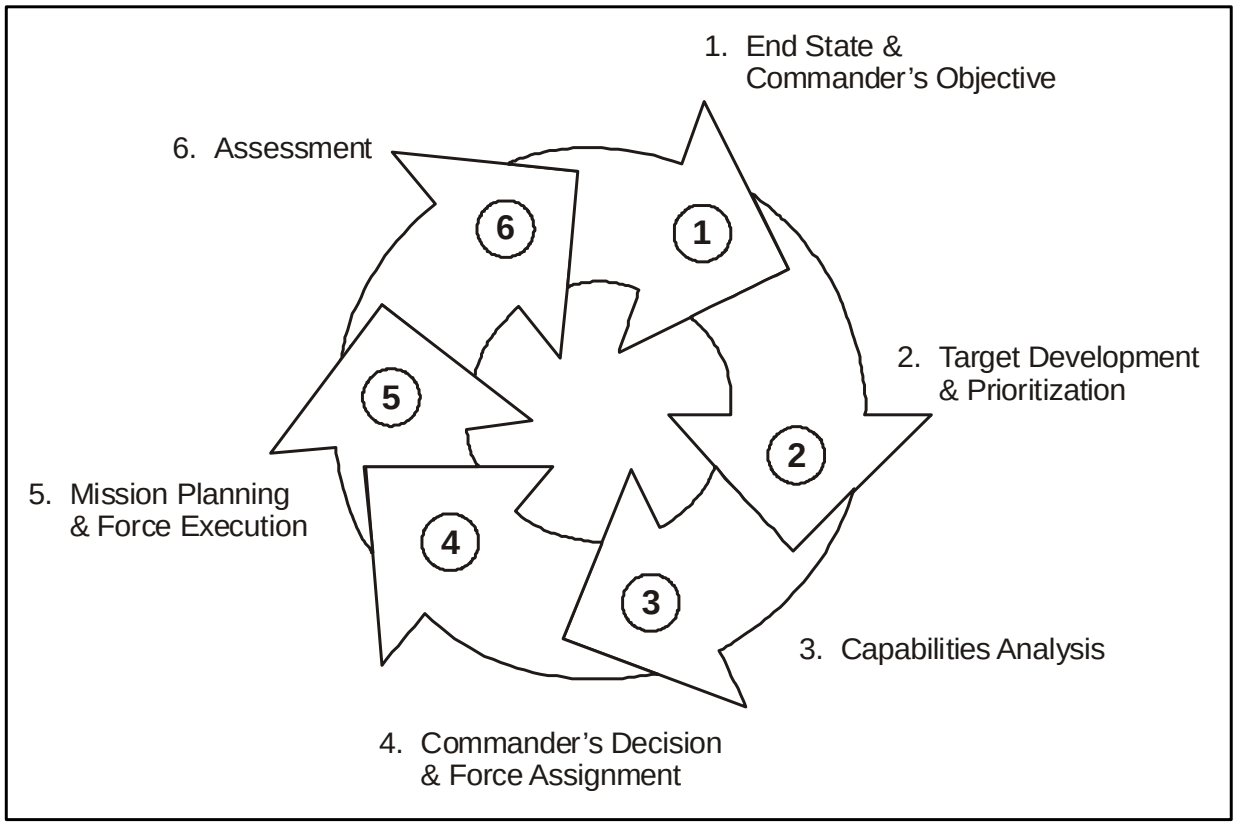

Figure 3-11. The Joint Targeting Cycle

Commanders must understand joint targeting in order to comply with senior level of command objectives, guidance, and intent; focus on adversary's COGs; coordinate, synchronize, and deconflict attacks; rapidly respond to time-sensitive targets (TSTs); minimize duplication of effort; expeditiously assess executed operations; and fully integrate all capabilities available.

The targeting cycle is an iterative process that methodically analyzes, prioritizes, and assigns forces against adversary targets systematically to achieve the appropriate effects. The targeting cycle is not time dependent, and steps may occur concurrently. It provides a helpful metric to describe the steps that must be satisfied to successfully conduct targeting. Though often reduced to a flowchart, it is important to acknowledge that targeting is also an art. The art of targeting seeks to achieve desired effects with the least risk, time, and expenditure of resources.

3.7.2.2.1 Phase 1 — End State and Commander's Objectives

The objectives support the President and SECDEF's desired end state for the conduct of military actions, while the guidance provided with the objectives stipulates particular conditions related to the execution of operations (e.g., limitations on collateral damage). Taken together, the end state and objectives embody the commander's intent for military operations. End state and objectives drive the subsequent phases of the targeting cycle. Clear, quantifiable, and achievable end state and objectives enable the successful realization of national security goals through a targeting solution.

3.7.2.2.2 Phase 2 — Target Development and Prioritization

Critical to the entire targeting process is the establishment of intelligence requirements. Targeting professionals must work closely with collection managers to ensure that target development, pre- and poststrike requirements, and any changes that occur throughout the targeting cycle are integrated into the collection plan. It is vitally

important to understand that target development always approaches adversary capabilities from the perspective of how those capabilities are supported by target systems. A target system is most often considered as a collection of assets directed at performing a specific function (e.g., air defense system) and being broadly geographically bounded. Target development reveals the relationship between these multiple target systems and their components (targets). This process is referred to as "nodal analysis."

Integral to target development is target validation. Target validation determines whether a target is a viable element of the target system. Equally important in target validation is determining whether it is a lawful target under the LOAC and ROE. Once potential targets are identified and validated, they are nominated through the proper channels. The net result of target development is to produce from the approved targets a target nomination list (TNL) that identifies those elements that most closely support the JFC's objectives and were vetted through all associated commanders and agencies. The nomination list also includes specific functional outcomes that must be created at each target to achieve objectives as well as any stipulations that may affect how those functional outcomes may be created (e.g., collateral damage). This is critical in order to frame the force estimation performed in the next phase and to facilitate the assessment of success achieved at the conclusion of operations.

The following are the varying authorities, groups, and products related to the validation, nomination, and prioritization processes:

1. Coalition command authority. If the United States is operating as a member of a coalition force, other members of the coalition may have political, economic, military, or informational concerns that also affect targeting operations.

2. Joint targeting steering group (JTSG). The JTSG assists the commander in developing targeting guidance and reconciling competing requests for assets. If a commander has more than one JTF operating in theater requiring targeting support resources, the JTSG can assist the commander and/or the J3/J5 in deciding how limited assets and resources are deployed.

3. JIOC/joint intelligence support element (JISE). The JIOC/JISE forwards from the JFC targets deemed to be critical, high payoff targets of strategic military or political importance. The JIOC/JISE develops targets based on the JFC's targeting guidance and priorities and consolidates them with targets received from higher HQ.

4. Service and/or functional components. Components submit their target nominations to the JFC's designated representative, usually the J3. The components are represented on the joint targeting coordination board (JTCB).

5. Joint fires element (JFE). If assigned, the JFE is the principal joint fires advisor to the JFC. It serves as the focal point for fires planning, coordination, synchronization, and execution. The JFE compiles and publishes the JFC's no-strike/protected target list. The JFE also serves as the executive agent for the JTCB and coordinates with component representatives and JFC staff members as well as provides administrative support to run the JTCB.

6. JAOC. The JAOC is the hub for air-delivered joint fires for the JFC. The JAOC, through the targeting effects team (TET), generates a recommended joint integrated prioritized target list (JIPTL). The JIPTL serves as the basis for the targeting efforts of the joint force air component commander (JFACC), his staff, and supporting commanders. The TET also recommends an apportionment of air assets to use for executing the JIPTL on a daily basis. Both the recommended apportionment and JIPTL go to the JTCB for review and discussion before they are sent forward for JFC approval.

7. TET. This may be a standing cell where component representatives reside to provide input to the targeting process, or it may be a meeting that convenes on a periodic basis (at least once daily). The board links targets to commander's guidance, deconflicts and coordinates target nominations, prioritizes targets into a JIPTL, makes a recommendation for apportionment of air assets to engage targets, and provides other

targeting support requiring component input at the JFACC level. The TET is usually chaired by the deputy JFACC and comprised of representatives from plans, operations, and intelligence.

8. JIPTL. The JIPTL is a prioritized listing of targets based on component and JTF target priorities. The number of available strike assets is estimated along with the ability to service the targets on the list so a "cut line" may be established. The cut line delineates which targets will most likely be struck with projected resources. The cut line is an important concept since targets below the line are not serviced. Components must be ready to justify and/or reprioritize target nominations relative to the cut line.

9. Naval and amphibious liaison element (NALE). The NALE represents the JFMCC in the JAOC. Maritime component requests for actions involving air forces under control of the JFACC are coordinated through this element.

10. JTCB. The focus of the JTCB is on the operational level of war. The primary concern is the employment of operational fires and shaping the JTF battlespace in the joint operating area.

3.7.2.2.3 Phase 3 — Capabilities Analysis

Coincident with the determination of targets and desired outcomes for those targets, it is necessary to select the most appropriate forces to apply against them. The purpose of this phase in the cycle is to weigh the relative efficacy of the available forces as an aid to achieving the objectives. These estimates build upon the analysis performed in target development and may be generated using mathematical models such as those embedded within the Joint Munitions Effectiveness Manuals. It is critically important to stress that all estimates generated during this phase are situational, reflecting the pairing of particular forces against particular targets, under particular conditions of employment.

3.7.2.2.4 Phase 4 — Commander's Decision and Force Alignment

A TNL and associated forces are vetted through the appropriate coordinating bodies representing the joint force components to ensure that the commander's objectives, guidance, and intent are met and that the chosen application of effort results in minimal operational conflict. This TNL comprises targeting recommendations compiled by the commander's designated targeting representative. The commander then approves the JIPTL, or elements thereof, and tasking orders are prepared and released to the executing components and forces.

3.7.2.2.5 Phase 5 — Mission Planning and Force Execution

Upon receipt of tasking orders, detailed planning must be performed for the execution of operations. The joint targeting process supports this planning by providing tactical-level planners with direct access to detailed information on the targets, supported by the nominating party's analytical reasoning that linked the target with the desired effect during Phase 2. During execution, the battlespace changes as the adversary responds and deviates from friendly force predictions. The joint targeting process monitors these changes in order to allow commanders to maintain the initiative through flexibility.

3.7.2.2.6 Phase 6 — Assessment

The goal of assessment is to determine the poststrike status of a target. If the desired effect is not reached, then a reattack recommendation, which requires immediate action, may be warranted. Conversely, it may be decided to fold the target back into the targeting process for reevaluation. These determinations are accomplished through BDA and a munitions effectiveness assessment (MEA).

BDA considers three aspects: physical damage assessment, functional damage assessment, and target system assessment. First phase BDA is usually derived from a single source based on visual observation of the target or from weapons monitoring equipment. Every ship's intelligence center is capable of performing first phase BDA; however, in some operating environments, senior levels of command do not authorize BDA reporting from tactical units. When this is the case, the tactical unit instead makes a BHA rather than BDA. Second phase BDA

reviews initial BDA reports and draws on all-source ISR and operational data to assess functional damage to a target. Third phase BDA requests and fuses supplemental BDA to provide an estimate of the extent and expected duration of degradation to the capabilities of the targeted system.

Conducted concurrently and interactively with BDA, MEA is the assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and recommend any required changes to the methodology, tactics, weapon system, munitions, fusing, and/or weapon delivery parameters to increase force effectiveness. MEA is primarily the responsibility of operations with required inputs and coordination from the intelligence team.

3.7.2.3 Time-Sensitive Targeting Cycle

The TST cycle is a slight variation of the joint targeting cycle. All six phases of the joint targeting cycle contribute to the process; however, TST is executed in a shortened turnaround cycle iteratively between Phases 5 and 6 of the joint targeting cycle. The key to successful TST prosecution is frontloading as much of the target development and commander's decision process as possible to enable speedy force execution. This dynamic process is illustrated through studying the time-sensitive strike kill chain: find, fix, track, target, engage, and assess.

For further information on the joint targeting cycle, refer to JP 3-60, Joint Targeting.

3.7.3 Surface Warfare

Surface warfare operations are conducted to neutralize enemy naval surface forces and merchant vessels. The SUWC is usually located on a vessel fitted with a robust intelligence, cryptologic, and communications capability. The SUWC employs aircraft, surface forces, and subsurface forces to accomplish surface warfare operations. These forces may fall under the direct control of the SUWC or may be under the control of another warfare commander.

The principal role of intelligence in support of the SUWC is to characterize the threat and classify all threat targets that may enter the detection range of the U.S. or coalition naval force. Intelligence correlates and fuses all-source data, including intentions, to determine the threat, threat direction, and operational characteristics of the threat platform before the threat platform is detected by own forces. Intelligence organizations supporting the STWC and the air resource element coordinator must ensure that the SUWC is aware of the results from all strike and surveillance missions.

3.7.4 Air Warfare

Air warfare (AW) operations are conducted with the intention to destroy or neutralize enemy aircraft or missiles in the atmosphere, including nullifying or reducing their effectiveness. The Navy's role in AW is dynamic, reflecting shifts in operating environment, mission, potential enemies, and the threat. Assured access to the maritime domain is one of the key pillars of the U.S. maritime strategy. As the Navy adapts to an increasingly lethal and complex set of threats, resources and efforts must be focused to achieve maximum effect. It is in this complicated domain that the Navy must operate to assure access and project power. The AMDC is responsible for those measures taken to defend a maritime force against attack by air and ballistic missile threats launched from aircraft, ships, submarines, and land-based sites.

Increasingly, sea-based forces operate near shore, projecting air and missile defense overland in order to defend critical assets ashore. The previous AW environment that relied on distances to separate and deconflict operations has been replaced by a complex, overlapping, and time-constrained battlespace. The threat has also evolved rapidly and now includes continually improving manned and unmanned aircraft as well as large numbers of sophisticated cruise and ballistic missile systems. Proliferation of these systems combined with advances in adversary technology, operational sophistication, and ISR employment could challenge the Navy's ability to ensure access and project power. The mission has expanded to meet the increased threat, and in addition to

defending maritime forces, Navy AW assets must now defend the sea base, joint forces ashore, our global allies, and the homeland.

Ensuring an integrated joint and maritime ISR effort is a critical requirement, but it is also challenging. Long range aircraft, antiship cruise missile, and ballistic missile threats to maritime forces can be launched against maritime forces hundreds of miles from the coast. A critical challenge for the fleet is ensuring that joint ISR priorities reflect the threat these weapons pose to fleet and joint operations. MOC ISR planners develop ISR requirements based on the mission and operational environment. They then determine which requirements fleet assets can accomplish and which to submit to the JFC as PIR recommendations. Those that are retained are issued in the form of tasks to specific fleet units.

3.7.5 Amphibious Warfare

An amphibious warfare (AMW) operation is launched from the sea against a hostile or potentially hostile shore. An AMW operation is directed by a CCDR, a subunified commander, or a JTF commander. An AMW operation requires extensive air participation and is characterized by closely integrated efforts of forces trained, organized, and equipped for different combat missions. The salient features of an AMW operation are mobility and flexibility, exploiting the element of surprise and capitalizing on enemy weaknesses by projecting and applying combat power at the most advantageous location and time. The mere threat of an amphibious landing can induce enemies to divert forces, build defensive positions, allocate major resources to coastal defense, or disperse forces. AMW operations are designed to achieve one or more of the following objectives: prosecute further combat operations; obtain an advanced naval, land, or air base site; deny use of an area or facilities to the enemy; and fix enemy forces and attention, providing opportunities for other combat operations.

Forces assigned to conduct an AMW operation are organized as an amphibious task force (ATF), or when the criteria for a JTF are met, a joint amphibious task force. Successful accomplishment of the ATF mission is dependent on timely and accurate intelligence. The ATF N2 coordinates the collection process up, down, and across echelons to ensure integration of effort, expeditious collection, and rapid processing, analysis, and dissemination of intelligence to the afloat and landing force commanders.

3.7.6 Antisubmarine Warfare

Antisubmarine warfare (ASW) operations are conducted with the intention of denying the enemy effective use of submarines. Under the CWC concept, the OTC is responsible for the defense of maritime forces. The CWC/OTC may delegate those responsibilities pertinent to ASW to the ASWC. The ASWC is responsible for the protection of the force against hostile submarines, for planning and managing the employment of ASW forces (air, surface, and subsurface), and for collecting, evaluating, and disseminating ASW surveillance information to the CWC and the force. In a CSG, the ASWC is normally located in the ASW module of the CDC. Intelligence support to the ASWC is provided by the DESRON N2. The DESRON N2 works closely with the CSG intelligence team. Operational and tactical intelligence support is designed to detect, classify, target, and engage all hostile subsurface threats before they reach maximum effective weapons release range. This multisource information is normally provided by SUPPLOT. Intelligence must define the capabilities, operating ranges, patterns, and force sustainability of enemy submarines.

3.7.7 Mine Warfare

Intelligence support to MIW is fundamentally no different than intelligence support to any other warfare discipline. It involves all-source, fused assessment, timely I&W, IPOE, etc. At the same time, owing to the particular requirements of this warfare area, it embraces some specific considerations. Transformation of Navy doctrine, planning, and staff organization are driving an increased requirement for mine-related intelligence. Chief among these are elevation of the MIWC within the CWC CONOPS, approaching introduction of a family of organic mine countermeasures (MCM) capabilities into the CSG/ESG/ARG (projected incremental IOC 2012-2017), and an improving ROE climate geared toward accommodating the potentially enormous value of mining as a warfighting option. Intelligence support to the strike group MIWC is provided by the DESRON N2. The

DESRON N2 works closely with the CSG/ESG/ARG intelligence team. Intelligence support to NMAWC's deployable (CTF-level) MIWC is provided by the NMAWC/MIWC battle staff N2.

MIW encompasses three segments: MCM, mining, and countermining. Each of these areas poses intelligence requirements, yet common threads run through each of these segments. For example, the value of careful IPOE work cannot be understated.

3.7.8 Naval Special Warfare

NSW operations are typically performed independently; however, they are increasingly conducted in conjunction with conventional military operations. The primary goal is to achieve a political or military objective where a conventional force requirement does not exist or might adversely affect the overall strategic outcome. NSW operations are usually conducted in a low-profile manner that typically aim to achieve the advantages of speed, surprise, and violence of action against an unsuspecting target. NSW operations are typically carried out with limited numbers of highly trained personnel that are able to operate in all environments, utilize self-reliance, are able to easily adapt and overcome obstacles, and use unconventional combat skills and equipment to complete objectives. NSW operations are supported by specific, tailored intelligence.

The NSW MSC provides the reachback capability to collect, process, and disseminate intelligence products that respond to specific information requirements of forward deployed NSW forces engaged in operations across the ROMO. The mission support center is designed to operate from CONUS and support the NSWRON, SBT, and SDV team commanders. Special Operations Mission Planning Environment-Maritime (SOMPE-M) is forward deployed with the NSW forces and connects to SOF or Service communications systems. SOMPE-M provides connectivity between deployed NSW forces and the NSW MSC via the SECRET Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS) connectivity.

3.7.9 Expeditionary Warfare

Expeditionary warfare (EXW) operations are conducted by maritime forces in the littoral, riparian, or coastal environments. They are conducted at the very edge of the maritime environment or ashore which bridge the critical gap between the maritime component and the land component. EXW operations can include any or all of the following capabilities: riverine operations, explosive ordnance disposal, mobile diving and salvage, naval construction, expeditionary security (ports and harbors), maritime civil affairs, foreign military training, expeditionary logistics, expeditionary intelligence, and combat camera.

EXW operations can span all phases of operations at any level of warfare. Expeditionary forces are typically present in an area during the earliest stages of engagement providing training and assistance to HN militaries and civilian populaces. Expeditionary forces are deployed across the globe and can provide access very rapidly and for sustained periods. In addition to their warfare capabilities, expeditionary forces posses extensive capabilities to support humanitarian assistance and disaster relief (HA/DR).

3.7.10 Irregular Warfare

The USN counters irregular challenges through a flexible, agile, and broad array of multi-mission capabilities that are employed across the full ROMO in concert with joint, other government organizations (OGOs), and international partners. The USN will enhance proficiency and effectiveness in security force assistance, maritime security, stability operations, ID, and other force applications as necessary to support U.S. and partner counterinsurgency, counterterrorism, and foreign internal defense. These operations enhance regional security and stability and serve to dissuade, deter, and when necessary, defeat irregular threats.

Irregular threats in the maritime theater include terrorism, insurgency, and illicit activities which weaken governance and eventually, regional security. Intelligence support to confronting irregular challenges includes persistent ISR and assessments of operational areas and environments that may serve as safe havens for irregular threats.

The Navy Irregular Warfare Office works closely with the USN, other Services, DOD, OGOs, and the United States Special Operations Command to integrate intelligence, plans, strategy, and programs for irregular warfare and confronting irregular challenges.

3.7.11 Information Operations

IO are actions taken to affect adversary information and information systems while defending one's own information and information systems. IO is described as the integrated employment of EW, computer network operations, psychological operations, military deception, and operations security to influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking while protecting our own. In its broadest sense, IO is the coordinated use of information in support of national security objectives.

Intelligence support is vital to IO planning. Effective execution also depends on intelligence to provide measures of effectiveness. Fundamental to achieving an effective IO strategy is the ability to develop detailed, usable knowledge of the strengths and vulnerabilities of potential adversaries. This ability requires the best intelligence available to friendly forces, including not only information on adversary weapons, C2 systems, and combat and information systems, but also an understanding of how potential adversaries think and plan for conflict and how friendly IO efforts might shape such thinking and planning.

Provision of primary sources of information rests heavily on defense and national intelligence agencies. At the operational level, naval forces must be trained, equipped, and employed with surveillance and reconnaissance assets that provide the force commander a clear, accurate, and timely picture of the battlespace. Intelligence support is critical to coordinate IO requirements and to effectively task organic, theater, and national assets.

At the CSG staff level, the IWC may be the senior information warfare officer, while at the ESG/ARG staff level, the IWC is the senior information warfare officer. The IWC plans, monitors IO threats, directs IO assets, and keeps operational commanders informed. The IWC identifies intelligence requirements and issues RFIs via the same procedures used by other warfare commanders.

For further information on IO, refer to JP 3-13, Information Operations.

CHAPTER 4

Support to Navy Intelligence Forward

4.1 INTRODUCTION

With the deliberate increase in "jointness" following the Goldwater-Nichols Act of 1986 and the 15 March 1991 SECDEF Memorandum, Strengthening Defense Intelligence, the establishment of the JICs resulted in Naval Intelligence disestablishing its extensive support structure centered on the fleet intelligence centers and Ocean Surveillance Information System nodes. Those organizations were specifically manned with resident intelligence and cryptologic personnel to provide intelligence support to afloat and deployed forces. The JIC (now referred to as JIOC) concept fuses the main support capabilities of all Service, combat support agency, and combat units into a one stop shopping center for intelligence support. Establishment of the JIOC replaced a maritime-focused Navy watch floor with a joint facility responsible for intelligence support to all areas of warfare. JIOCs provide all-source analysis, collection management, and targeting support for all forces in the GCC's AOR. Afloat and deployed naval forces rely on these organizations and the structure behind them to satisfy their intelligence requirements. In reality, a particular JIOC is not expected to resolve every RFI, so it coordinates support from other intelligence organizations above and below its echelon. To effectively operate in today's information-rich environment, the commander must understand the national, theater, JTF, and Service intelligence support available to his organic intelligence team.

4.2 NATIONAL LEVEL SUPPORT

Backing up the theater JIOCs is a vast array of organizations and agencies that conduct intelligence activities considered necessary for the protection of the national security of the United States. At the core of this structure is the U.S. IC. The IC is defined in the National Security Act of 1947, amended by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, and guided by Executive Order 12333, as updated in 2008. It refers to those Executive Branch agencies and organizations that are funded in the National Intelligence Program (NIP). The IC consists of 16 member organizations. These organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements. The national intelligence organizations routinely provide support to the JFC while continuing to support national decision makers. Included in the IC are the Service intelligence organizations; however, they are detailed in section 4.5 of this chapter.

The IRTPA established the office of the Director of National Intelligence (DNI) to oversee IC budgeting, appointment of IC agency heads, IC personnel policies, tasking for collection and analysis, foreign liaison, and protection of intelligence sources and methods.

4.2.1 Department of Defense Intelligence and Combat Support Agencies

4.2.1.1 National Joint Operations and Intelligence Center

The National Joint Operations and Intelligence Center (NJOIC) is an integrated Joint Staff J2/3/5 element that monitors the global situation on a 24/7 basis and provides the Chairman of the Joint Chiefs of Staff (CJCS) and the SECDEF a DOD planning and crisis response capability. The intelligence component of the NJOIC maintains an alert center that consists of the Deputy Director for Intelligence, regional desks corresponding to each GCC, and representatives from each Service intelligence staff element, the intelligence combat support agencies, and the Central Intelligence Agency (CIA). The Alert Center is an all-source, multidiscipline intelligence center providing defense intelligence situational awareness, I&W, and crisis management intelligence support to the President, the

SECDEF, the Joint Chiefs of Staff (JCS), combatant commands, deployed forces, the Services, and other intelligence consumers during peace, crisis, and war. It provides planning, management, and infrastructure for intelligence working groups and intelligence task forces which provide direct intelligence support during major conflicts. The Defense Intelligence Agency (DIA) maintains a direct support element at the NJOIC tailored to the current global situation and operations tempo. In conjunction with the Defense Intelligence Operations Coordination Center (DIOCC), the NJOIC coordinates the intelligence response to immediate crises and contingencies.

4.2.1.2 Defense Intelligence Agency

DIA is an intelligence combat support agency. The Director, DIA reports to the SECDEF through the CJCS. DIA's mission is to satisfy the military and military-related intelligence requirements of the SECDEF, the CJCS, and the DNI, and provide the military intelligence contribution to the National Foreign Intelligence Program (NFIP) and CI. DIA serves as the DOD lead for coordinating intelligence support to meet combatant command requirements. DIA also leads efforts to align ISR activities, and links and synchronizes national, defense, and military intelligence. DIA also provides analytical and operational support in areas such as CI, counterterrorism, counterdrug operations, computer network operations, personnel recovery, proliferation of WMD, United Nations peacekeeping and coalition support, MASINT, NEO efforts, I&W, targeting, BDA, current intelligence, collection management, intelligence architecture and systems support, and document and media exploitation capability. The Director, DIA is dual-hatted as the Director, DIOCC and also serves as the Commander, Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance (JFCC-ISR) under the United States Strategic Command (USSTRATCOM).

4.2.1.3 Defense Intelligence Operations Coordination Center

The DIOCC is responsible for integrated intelligence operations and collection. The DIOCC's primary functions are serving as the DOD lead for collection management and intelligence planning and providing support to combatant command JIOCs and JTFs. The Director, DIOCC serves concurrently as the Director, DIA and the JFCC-ISR. The DNI established the National Intelligence Coordination Center (NIC-C) at the DIOCC. This is the DNI's central node for deconflicting U.S. and DOD intelligence activities.

4.2.1.4 National Security Agency/Central Security Service

NSA is an intelligence combat support agency under the SECDEF and is also a member of the IC under the DNI. The Director, NSA, exercises operational control over the United States Cryptologic System (USCS). The Director is the principle SIGINT advisor to the SECDEF, the DNI, and the JCS, and is designated as the national manager responsible for securing the government's national security telecommunications and information systems. USCS is the term that describes both the SIGINT and information assurance activities of the U. S. Government.

The Central Security Service (CSS) is comprised of the Service cryptologic elements of the military Services. NSA/CSS is a unified organization structured to provide for the SIGINT mission of the United States and to ensure the protection of national security systems for all departments and agencies of the U.S. Government. The Director, NSA is also Commander, United States Cyber Command, a sub unified command subordinate to USSTRATCOM. NSA provides direct support to the combatant command JIOCs through the CSS.

4.2.1.5 National Geospatial-Intelligence Agency

NGA is an intelligence combat support agency under the SECDEF and is dual-tasked as a member of the IC under the DNI. The Director, NGA serves as the functional manager for GEOINT and is the principle GEOINT advisor to the DNI, SECDEF, CJCS, and the CCDRs. As functional manager, NGA develops strategic guidance and procedures, sets tradecraft standards, and ensures coordination across intelligence disciplines and IC elements. NGA conducts GEOINT analysis to combine IMINT and geospatial information to produce tailored, actionable intelligence to support customers across a broad range of the DOD and the U.S. Government. NGA provides direct support to the combatant command JIOCs and the DIOCC.

4.2.1.6 National Reconnaissance Office

The Director, National Reconnaissance Office (NRO), reports to both the DNI and the SECDEF. NRO is responsible for integrating unique and innovative space-based reconnaissance technologies and the engineering, development, acquisition, and operation of space reconnaissance systems. NRO activities provide support to I&W, monitoring arms control agreements, enabling spaceborne access to denied areas, and the planning and execution of military operations.

4.2.2 Nonmilitary Members of the Intelligence Community

4.2.2.1 Director of National Intelligence

The DNI serves as the head of the IC. The DNI also acts as the principle advisor to the President, the National Security Council, and the Homeland Security Council for matters related to national security. Recognizing the heightened role of DOD as both a producer and primary consumer of intelligence, the DNI subsequently appointed the Undersecretary of Defense for Intelligence (USD(I)) as his Deputy Director for Intelligence. The DNI is responsible for the performance of the nation's intelligence capability, even though it is dispersed across six governmental departments.

4.2.2.2 Central Intelligence Agency

The CIA's primary areas of expertise are in HUMINT collection, all-source analysis, and the production of political and economic intelligence. The Director, CIA, also serves as the national HUMINT manager and the National Clandestine Service Director. The CIA has three Deputy Directors: Deputy Director for Intelligence, Deputy Director for Science and Technology (S&T), and Deputy Director for Support. CIA is the largest producer of all-source national security intelligence to senior U.S. policymakers and provides extensive political and economic intelligence to DOD senior decision makers. CIA also oversees the Open Source Intelligence Center.

4.2.2.3 Department of State

The State Department Bureau of Intelligence and Research (INR) performs intelligence analysis and produces studies on a wide range of political and economic topics essential to foreign policy determination and execution. The INR coordinates programs for intelligence, analysis, and research and produces intelligence studies and current intelligence analyses for the Secretary of State and other State Department policymakers, including ambassadors, special negotiators, country directors, and desk officers. INR is also responsible for policy and coordination of intelligence activities in support of diplomacy and conducts open source public opinion surveys, polls, and media trend analyses.

4.2.2.4 Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) is an intelligence and law enforcement agency. It is responsible for understanding threats to our national security and penetrating national and transnational networks that desire and are capable of harming the United States. The FBI coordinates these efforts with its IC and law enforcement partners. It focuses on terrorist organizations, foreign intelligence services, WMD proliferators, and criminal enterprises. The principal investigative arm of the Department of Justice, the FBI has primary responsibility for CI and counterterrorism operations conducted in the United States. CI operations contemplated by any other organization in the United States must be coordinated with the FBI. Any overseas CI operation conducted by the FBI must be coordinated with the CIA.

4.2.2.5 Department of Treasury

The Department of Treasury analyzes foreign intelligence related to U.S. economic policy and participates with the Department of State in the overt collection of general foreign economic information.

4.2.2.6 Department of Energy

The Department of Energy (DOE) analyzes foreign information relevant to U.S. energy policies and nonproliferation issues and the national science laboratories under its authority. The DOE formulates energy policy for the United States and has a system of national laboratories and technical centers which conduct energy-related research in the national interest. The Office of Intelligence and Counterintelligence directs the development of the DOE's policy, plans, and procedures relating to arms control, nonproliferation, export controls, and safeguard activities. It provides access to the DOE's energy information and technical expertise to the rest of the IC. Additionally, this office is responsible for managing the Department's research and development (R&D) program for verifying and monitoring arms implementation and compliance activities and for providing threat assessments and support to HQ and field offices.

4.2.2.7 Department of Homeland Security

The Department of Homeland Security's (DHS) Office of Intelligence and Analysis provides I&W support to the Homeland Security Advisory System, assesses the scope of terrorist threats to the U.S. homeland, and integrates terrorist-related information from DHS components, OGAs, and private sector entities. The Office of Intelligence & Analysis focuses on threats related to border security; chemical, biological, radiological, and nuclear issues, to include explosives and infectious diseases; critical infrastructure protection; extremists within the homeland; and travelers entering the homeland.

4.2.2.8 United States Coast Guard

The United States Coast Guard (USCG), a component of the DHS, operates as both an armed force and a law enforcement organization. The USCG's Maritime Intelligence Fusion Centers Atlantic and Pacific operate under the direction of the Assistant Commandant for Intelligence and serve as the central hub for collection, fusion, analysis, and dissemination of maritime intelligence and information to Coast Guard operating units, DHS, and all members of the IC including DOD and key decision makers at the national level.

The USCG has unique missions and responsibilities that make it a significant player in several national security issues. To accomplish these diverse objectives, the USCG intelligence program consists of two distinct elements — the National Intelligence Element and the Law Enforcement Intelligence Program. The National Intelligence Element conducts activities as described in Executive Order 12333 and the National Security Act of 1947 and is a part of the IC. USCG intelligence efforts support counterdrug operations, alien migration interdiction operations, living marine resource enforcement, MIO, port safety, counterterrorism, coastal and harbor defense operations, and environmental protection.

The United States Coast Guard Intelligence Coordination Center (ICC) is a tenant command within theUSN's National Maritime Intelligence Center (NMIC) in Suitland, MD and maintains a 24-hour intelligence watch, providing I&W input to the NMIC. The ICC acts as the strategic center with ties to both national intelligence agencies and the HQ-level law enforcement intelligence activities. The ICC supports strategic analysis, manages Coast Guard collection, and provides national imagery exploitation support, including tactical support to operational commanders.

The United States Coast Guard Investigative Service (CGIS) is a federal investigative and protective agency chartered to conduct internal and external criminal and personnel security investigations, assist in providing personal security protection, and conduct CI investigations. Responsibilities include criminal investigations of maritime crimes, investigating fraud, personal protection services, and security background investigations. CGIS CI and intelligence operations focus on drug smuggling, environmental crimes, illegal immigration by sea, and assistance as required by other federal law enforcement agencies.

The National Response Center (NRC) serves as the central national point of contact for reporting environmental intelligence data for all oil, chemical, radiological, and biological discharges into the environment in the United States and its territories. The NRC gathers and distributes intelligence data for federal onscene coordinators and serves as the communications and operations center for the deployable National Response Team.

4.2.2.9 Drug Enforcement Administration

The Drug Enforcement Administration (DEA) enforces laws and regulations governing narcotics and controlled substances, chemical diversion, and trafficking. It is also the lead agency overseas for counterdrug law enforcement activities and investigations. DEA makes ancillary contributions to the national IC via efforts to build legal cases against narcotics traffickers. DEA-collected and produced information is valuable in homeland security efforts due to the traditional close association between narcotics trafficking and illegal alien smuggling. This results in DEA information potentially having significant value in counterterrorism applications.

4.3 THEATER-LEVEL SUPPORT

Joint intelligence organizations are directly responsible for providing the combatant command and subordinate joint force with a common, coordinated intelligence picture by fusing national and theater intelligence and law enforcement/CI information into all-source estimates and assessments. The JIOCs are charged with providing operational- and tactical-level support to all components and subordinate units. Naval assets should expect and receive I&W support, general military intelligence, targeting materials, NEO support, terrorism analysis, and collection management support. Additionally, the joint community has established other support centers specializing in one core area that provide the commander with focused information and products.

4.3.1 Combatant Command J2

The combatant command J2 assists the commander and staff in developing strategy, planning theater campaigns, and organizing the command relationships of theater intelligence assets for effective joint and multinational operations. Additionally, the J2 is responsible for determining the requirements and direction needed to ensure unity of the intelligence effort supporting the commander's objectives. The J2 provides higher echelons, up to and including the NJOIC, and subordinate commands with a common, coordinated, all-source intelligence picture in the form that the primary user of the information requires and at the point in time that it is needed. The J2 accomplishes this by employing joint force intelligence resources and identifying and integrating intelligence from additional intelligence resources such as national intelligence capabilities and component command intelligence assets. The J2 also fuses information into the all-source picture that is derived from law enforcement/CI organizations.

4.3.2 Combatant Command Joint Intelligence Operations Center

Each combatant command and United States Forces Korea, a subunified command under USPACOM, operate JIOCs to focus the application of theater and national intelligence capabilities in support of the command mission. The JIOC is the focal point for the combatant command's intelligence planning, collection management, analysis, and production effort, and is organized in a manner best suited to satisfy the CCDR's intelligence requirements. The combatant command JIOC is the first stop for component or subordinate JTFs seeking intelligence support. If the JIOC cannot meet the CCDR's requirements, the JIOC forwards an RFI to the DIOCC, or to subordinate command levels using the Community Online Intelligence System for End Users and Managers RFI management system. In some cases, the JIOC may also seek to ensure timely support by submitting requests to IC production centers through the national agency representatives to the command.

4.3.3 Cruise Missile Support Activity

Cruise Missile Support Activity (CMSA) Atlantic and Pacific (PAC) are joint activities subordinate to USPACOM and USJFCOM, respectively. CMSAs were created to conduct Tomahawk-land attack missile (TLAM) mission feasibility, weaponeering, and route planning for the JCS and CCDRs. CMSAs rapidly respond to emergent tasking and ensure updated/new missions are transmitted to afloat launch platforms. Both CMSAs work closely with the Navy's undersea and surface warfare communities and with the TLAM program management office to ensure weapons tactics and communications systems meet joint requirements.

4.3.4 Joint Warfare Analysis Center

A component of USJFCOM, Joint Warfare Analysis Center (JWAC) is a science and engineering institution that uses social and physical science techniques and engineering expertise to assist warfighters in support of our national security. JWAC provides CCDRs, the JCS, and others with effects-based, precision targeting options for selected networks and nodes. Areas of expertise include analysis of a threat country's C2; lines of communication; and petroleum/oil/lubricant, electrical, and telecommunications infrastructure. Additionally, JWAC uses target data and weapons capability to determine BDA and the potential for collateral damage. JWAC supports current military operations, OPLAN/concept plan (CONPLAN) development, and major exercises.

4.3.5 Missile and Space Intelligence Center

The Missile and Space Intelligence Center is DIA's center of excellence for S&T intelligence on guided missiles, directed energy weapons, selected space programs/systems, and related C2 systems. Its missile focus is on surface-to-air missiles (SAMs), short-range ballistic missiles with ranges less than 1,000 kilometers, antitank guided missiles, and missile defense systems.

4.3.6 Joint Information Operations Warfare Center

The Joint Information Operations Warfare Center (JIOWC) plans, integrates, and synchronizes IO in direct support of JFCs and serves as the USSTRATCOM lead for enhancing IO across the DOD. JIOWC's mission is to assist in planning, coordinating, and executing IO. The center deploys IO planning teams worldwide to deliver tailored support and sophisticated models and simulations to JFCs and the Joint Staff.

The JIOWC provides direct command and control warfare tactical and technical analytical support to operational commanders. It supports the integration of IO throughout the planning and execution phases of operations. Direct support is provided to unified commands, JTFs, the Services, and subordinate commanders. Support is also provided to the SECDEF, the Joint Staff, the Services, and other government agencies. The JIOWC maintains specialized expertise in command and control warfare systems engineering, operational applications, capabilities, and vulnerabilities.

4.3.7 Joint Personnel Recovery Agency

The Joint Personnel Recovery Agency (JPRA) is charged with coordinating and advancing capabilities for military, civil, and diplomatic efforts to obtain the release or recovery of captured, missing, or isolated U.S. personnel from uncertain or hostile environments and denied areas. JPRA is a subordinate activity of USJFCOM. The goals of the JPRA include returning isolated U.S. personnel to friendly control, denying enemies of the United States a potential source of intelligence, preventing the exploitation of captured U.S. personnel in propaganda programs, and maintaining the morale of U.S. fighting forces and the national will. JPRA's core capabilities consist of providing personnel recovery guidance; developing, conducting, and supporting personnel recovery education and training; providing support to operations, exercises, and deploying forces; and ensuring that personnel recovery remains viable through the adaptation of lessons learned, R&D, and other validated inputs.

4.4 JOINT TASK FORCE SUPPORT

JTFs may take many forms and sizes and may be employed across the ROMO in air, land, and maritime environments. The specific organization and staffing of a JTF varies based on the mission assigned, the operating environment, the makeup of enemy forces, and the time available to reach the desired end state. When fully formed, the JTF staff is composed of appropriate members in key positions of responsibility from each Service or functional component having significant forces assigned. The CJTF makes the final decision on the composition of the JTF HQ to include the establishment of boards, centers, cells, and bureaus.

In the past, CCDRs designated naval commanders as CJTFs. Numbered fleet and CSG/ESG/ARG N2s must prepare to function as a JTF J2.

4.4.1 Joint Task Force J2

The JTF J2 assists the JFC in developing strategy, planning operations and campaigns, and tasking intelligence assets for effective joint and unified operations. Additionally, the J2 is responsible for determining the requirements and direction needed to ensure unity of the intelligence effort and to support the commander's objectives. The JTF J2 provides higher echelons and subordinate commands with a single, coordinated intelligence picture by fusing national and theater intelligence into all-source estimates and assessments. The J2's responsibility also includes applying national intelligence capabilities, optimizing the utilization of joint force intelligence assets, and identifying and integrating additional intelligence resources. The scope of needs, resources, and procedures depends on the mission, nature, and composition of the force. To plan, coordinate, and execute required intelligence operations, JTF J2s are responsible for the following:

1. Provide threat assessments and warning. The J2 is responsible for analyzing all relevant aspects of the operational environment, determining adversary capabilities, and estimating adversary intentions. The J2 provides the resulting threat assessments and warning to the joint force and its components.

2. Participate in all decisionmaking and planning. Using IPOE as a basis, the J2 participates in the JFC's decision-making and planning processes from the time that operations are first contemplated or directed until the completion of the operation. The JFC and the J2 must conduct continuous dialog concerning the adversary's relative strengths, weaknesses, and ability to prevent the joint force from accomplishing its mission.

3. Synchronize intelligence with operations and plans. The J2 must ensure that intelligence collection, processing, exploitation, analysis, and dissemination activities are planned, sequenced, and timed to support the commander's decision-making process and to meet the requirements of planners.

4. Formulate concept of intelligence operations. To communicate guidance and requirements to higher and lower echelons of command, the JTF J2 develops and disseminates a concept of intelligence operations.

5. Develop detailed intelligence annexes. The JFC's PIRs and the results of wargaming serve as the basis for the intelligence annex of each directed OPLAN and CONPLAN. The annex lists the JFC's PIRs and supporting information requirements, identifies the intelligence forces available for the operation, resolves shortfalls, and assigns or recommends tasks.

6. Integrate national and theater intelligence support. The J2 must plan for integrating national and theater intelligence elements and products into the joint force intelligence structure. National and theater intelligence organizations make operations feasible that could not be accomplished without their access, capability, capacity, or expertise.

7. Exploit combat reporting from operational forces. Forward and engaged combat forces have a responsibility to report information that can be integrated with intelligence obtained from reconnaissance and surveillance assets.

8. Organize for continuous operations. Intelligence organizations should be structured for continuous day/night and all-weather operations. The J2's concept of intelligence operations should provide for continuity of support even if communications are severely stressed or temporarily lost.

9. Ensure accessibility of intelligence. The J2 must ensure that intelligence is readily accessible throughout the joint force while still adhering to security standards (e.g., security clearance and need-to-know requirements).

10. Establish a joint intelligence architecture. A truly joint intelligence infrastructure must be created to provide the best possible intelligence to the JFC. It must be constructed to ensure protection of information and intelligence from inadvertent disclosure and guarantee integrity of the data and assured access to all sources.

4.4.2 Joint Intelligence Support Element

At the discretion of the JFC, a JISE may be established during the initial phases of an operation to augment the joint force J2 element. Under the direction of the joint force J2, a JISE normally manages the intelligence collection, production, analysis, and dissemination for a joint force. The joint force J2 defines the JISE functions, responsibilities, and its relationship with the J2 staff. In many cases, specific responsibilities may be shared between the J2 staff and the JISE.

The size and organization of the JISE is determined by the JFC based upon the recommendation of the J2 and available resources. Personnel and equipment requirements for the JISE, including augmentation, are submitted to the combatant command. Resources are provided through the RFF process.

When formed, the JISE may be collocated with the joint force J2 element in the joint operations area (JOA) or may operate in a "split base" mode. In this mode, the JISE operations and personnel are divided between two locations: with the joint force J2 in the JOA and at a location outside the JOA, possibly at the joint force's home base. Split base operations may reduce the number of personnel deployed in the JOA, thus reducing the attendant communications systems infrastructure required.

At the operational level, a JISE is normally established; however, a JIOC may be formed at the direction of the JFC based on the scope, duration, and mission of the unit or JTF. The decision to establish a fully-manned JIOC may require augmentation and should be approved by the CCDR.

4.4.3 Joint Force Counterintelligence and Human Intelligence Staff Element

During joint operations, CI and HUMINT efforts both complement each other and overlap to some degree. To help ensure that these staff elements are in a position to accomplish their necessary goals, the JFC normally establishes a joint force counterintelligence and human intelligence staff element (J2X). The mission of the J2X is to coordinate, synchronize, leverage, manage, and deconflict all DOD CI, protection activities, HUMINT, and other activities involving human sources in the JOA throughout all phases of operations. A J2X should be established in joint force structures at every echelon including combined and multinational force commands. All DOD CI and HUMINT elements conducting activities occurring in, transiting through, or impacting upon the operating area must coordinate and deconflict these activities directly with the force J2X.

4.4.4 National Intelligence Support Team

At the request of a CCDR, the DIOCC coordinates the deployment of a national intelligence support team (NIST) to support a JTF commander. The NIST is a nationally sourced team composed of intelligence analysts and communications experts from DIA, CIA, NGA, NSA, and other IC agencies as required. During crisis or contingency operations, it provides commanders with a tailored, national-level, all-source intelligence team, ranging from a single agency element with limited ultra-high frequency voice connectivity to a fully equipped, multiagency team with Joint Deployable Intelligence Support System (JDISS) and JWICS video-teleconferencing capabilities.

A NIST typically supports intelligence operations at the JTF HQ and is traditionally collocated with the JTF J2; however, the DIOCC portion of the NIST has the capability to go forward as required. Current modes of operation rely on both agency and command-provided communications (equipment and bandwidth) to support deployed NIST elements.

The NIST provides commanders with analytical expertise, I&W, and special assessments. Targeting support is also available when the USJFCOM Quick Reaction Team is present. In direct support of the JTF, the NIST performs functions as designated by the JTF J2, provides access to national databases, and facilitates RFI management.

For further information on JTF Support, refer to JP 2-0, Joint Intelligence, and JP 3-32, Command and Control for Joint Maritime Operations, Change 1.

4.5 SERVICE COMPONENT SUPPORT

With the advent of the JIOCs, Service intelligence centers were directed by Congress to concentrate on S&T analysis of potential threat systems, long term trend analysis, and weapons tactics. The Service centers' assessments of foreign threats or weapons capabilities are used to improve existing U.S. weapons capabilities or to justify the development of an entirely new weapons platform. By their nature, however, the Service S&T centers retain areas of expertise that can be used to support operational forces, both individually and in a joint environment.

4.5.1 United States Navy

The Director of Naval Intelligence is the Navy's intelligence executive to the CNO and the OPNAV staff. As such, he exercises overall authority through the Department of the Navy (DON) on matters pertaining to intelligence, cryptology, CI, and special security. The Director of Naval Intelligence manages the Navy portion of the NFIP, sets Naval Intelligence policy, and directs Naval Intelligence planning and programs.

4.5.1.1 Office of Naval Intelligence

ONI, located within the NMIC in Suitland, MD, is the nation's center of excellence for maritime-related intelligence. ONI's primary mission is to provide maritime intelligence to key strategic, operational, and tactical decision makers. This mission includes intelligence production on seaborne terrorism, weapons and technology proliferation, and narcotics and smuggling activities that directly supports joint warfighters, the Navy, and civil and national decision makers and agencies.

4.5.1.1.1 Nimitz Operational Intelligence Center

The Nimitz Operational Intelligence Center functions to meet the increasing demand for rapid access to OPINTEL by aligning with globally-netted MOCs. The Nimitz center is composed of cells and detachments that support numbered fleets and naval warfare enterprises.

The Nimitz center performs the nation's substantive analysis on worldwide maritime weapons systems. Areas of interest include characteristics and performance data, tactics, and operational doctrine on non-U.S. maritime platforms and systems that U.S. forces may encounter around the world. Inside the Nimitz center are three specialized divisions to assess adversary capabilities, doctrine, and TTPs: SPEAR (air warfare), SWORD (undersea warfare), and SABER (surface/littoral operations).

During the FRTP and deployment, Nimitz Operational Intelligence Center can provide the following type of support to naval operations:

1. ONI overview briefing. This briefing provides CSG/ESG/ARG commanders and senior intelligence personnel with an overview of ONI capabilities and the support that it can provide to the force.

2. SPEAR/SWORD/SABER briefings. Briefings consist of operations and tactics in the air, undersea, and surface environments. SPEAR/SWORD/SABER divisions are manned with warfare specialists and intelligence personnel to more realistically analyze platform capabilities and tactics.

3. Naval Intelligence Task Force-Maritime Security (NITF-MS). The nation's premier analytical cell for civil maritime trade and smuggling, NITF-MS is actively involved with the USCG on issues related to U.S. port security including the tracking of suspicious cargo and analyzing shipping/trading companies and vessels for terrorist links. NITF-MS also analyzes alien smuggling, fishery operations, arms smuggling and weapons proliferation, piracy, and port capabilities. NITF-MS maintains the SEAWATCH database, providing merchant ship locations and movements, the Merchant Ship Characteristics Database, and AMIDSHIPS, an extensive database of merchant ship blueprints and photography. NITF-MS databases and analysts are essential for naval forces conducting MIO.

4. MIO briefings. These briefings provide tailored information about maritime sanctions enforcement to include current policy, smuggling activity/patterns, and intelligence support available to the CSG/ESG/ARG or DESRON while underway.

5. Driftnet fishing briefings. ONI can provide briefing material on illegal driftnet fishing activity, recognition features, fishing vessel characteristics, and DOD reporting criteria. ONI can also provide hardcopy briefing books for specific Pacific and Mediterranean areas.

6. IO/C4ISR threat briefings. Briefings include detailed information on threats to DON computer networks and EW systems, satellite communications vulnerabilities, Global Positioning System jamming capability, and all-source analysis on select target countries.

7. Naval forces modernization briefing. These briefings provide a broader analysis of select threat countries. Briefers provide analysis of the country's doctrine and strategy, its military capabilities and vulnerabilities, and the country's leadership and make projections and estimates about the target country's potential threat to U.S. interests.

8. Country and regional political/military briefings. These briefings provide "scene setters" for deploying commanders and intelligence personnel. Briefings cover long term and current political/military developments, naval modernization, and trends in all fleet AOs.

9. Cryptologic Services Group. The Cryptologic Services Group coordinates all ONI requests for SIGINT data and assists and advises the ONI Global Maritime Watch.

10. ONI Detachment, Newport. The Newport Detachment provides wargaming support to the Naval War College through scenario and opposition force development.

4.5.1.1.2 Farragut Technical Analysis Center

The Farragut Technical Analysis Center is focused on foreign S&T research, development, and proliferation. The Farragut center's mission is to deliver knowledge of current and future foreign navy capabilities to enable long range planning and research, guide future acquisitions, and prevent technological surprise. The Farragut center consists of the following departments and services:

1. Strategic Assessments (TAC-01). TAC-01 leads ONI's foreign naval capabilities projections efforts and coordinates across the IC on relevant issues in support of many customer sets, primarily those in the DON R&D, test and evaluation, acquisition, plans, and policy communities.

2. Platforms (TAC-02). TAC-02 monitors surface, subsurface, and aircraft developments around the world and produces the Navy's platform databases and recognition guides.

3. Weapons (TAC-03). TAC-03 monitors worldwide naval-specific weapons development to include naval ballistic missiles, cruise missiles, and SAM systems. Additionally, they monitor naval guns, torpedoes, mines, rockets, and the potential transfer of these weapons systems around the world. TAC-03 also maintains a foreign material exploitation laboratory to analyze these materials.

4. Information Dominance (TAC-04). TAC-04 provides all-source threat analysis of foreign CNA and CNE capabilities against Navy networks and networked systems in support of long term information assurance and CND.

5. C4ISR/IO (TAC-05). TAC-05 has three divisions that monitor and analyze naval radars, electro-optical devices, underwater sensors, and command, control, communications, computers, and intelligence (C4I) systems.

6. Acoustic Intelligence (ACINT) Shipriders (TAC-06). TAC-06 can provide subsurface and surface ships with highly skilled ACINT specialists for critical evolutions during the FRTP and deployment. TAC-06 ACINT specialists provide assistance to sonar watchstanders, real time assessments of acoustic signatures, and recommendations on sonar operations.

4.5.1.1.3 Kennedy Irregular Warfare Center

The Kennedy Irregular Warfare Center functions to meet the expanding demands of NSWC and NECC. It is comprised of two cells: a deployed forces cell which embeds into NSWRONs and a global analysis cell which provides all-source OPINTEL reachback and imagery services to expeditionary forces.

4.5.1.1.4 Hopper Information Services Center

The Hopper Information Services Center provides mission-related IT services and ensures the rapid and reliable delivery of intelligence to operational forces and intelligence customers worldwide through service oriented architecture. The Hopper center manages naval SCI networks and provides program management of the JDISS.

For further information on ONI, refer to ONI Customer Handbook 2010.

4.5.1.2 Navy Expeditionary Intelligence Command

To optimize NECC's ability to execute its MT&E responsibilities, specialized tactical intelligence and tactical IO capabilities are assigned to NEIC. NEIC is an echelon IV command assigned to NECC providing tactically-focused intelligence and IO capabilities to CCDRs, JFMCC and coalition force maritime component commanders (CFMCCs), NCCs, numbered fleet commanders, and the NECC force. NEIC capabilities are organized, trained, equipped, and deployed as cohesive units of action, providing specific, specialized services. NEIC provides the following specific capabilities:

1. Navy tactical HUMINT capabilities. Tactical HUMINT capabilities are a managed activity under the direction of the NEIC CO. Authority to conduct tactical HUMINT operations is derived from USD(I) direction. Oversight, policy, guidance, and authorities are provided or delegated through SECNAV, the Director of Naval Intelligence Deputy Director for Human-Derived Information (OPNAV N2X), USFF, and NECC. Operational authority is derived from the supported CCDR through the existing command structure. Tactical HUMINT collectors are DOD-certified to supervise and conduct HDI/Human-Enabled Information collection operations. HUMINT collectors are one of the primary means for interaction with local populations in support of the commander's requirements.

2. Maritime interception operations-intelligence exploitation team (MIO-IET). MIO-IET capabilities are a managed activity under the direction of the NEIC CO. Authority to operate MIO-IETs is derived from USD(I) direction. Oversight, policy, guidance, and authorities are provided through SECNAV, OPNAV N2X, USFF, and NECC. Operational authority is derived from the supported CCDR through the existing command structure. The MIO-IET program was established to provide fleet MIO boarding teams with the requisite expertise to recognize and exploit intelligence opportunities using a variety of techniques in collaboration with theater and national intelligence centers to support CCDR, JFMCC, CFMCC, NCC, and numbered fleet commander operational requirements. MIO-IET intelligence and tactical IO personnel are certified to conduct visit, board, search, and seizure (VBSS) level II/III boardings and are trained to integrate into fleet VBSS parties.

3. Expeditionary intelligence support element (EISE). EISE is a managed activity under the direction of the NEIC CO. EISE provides qualified naval intelligence officers and IS-3912s to deploy in support of the full range of expeditionary missions. EISE personnel complete baseline expeditionary intelligence training and enhance organic intelligence capability to facilitate expeditionary operations.

4. Expeditionary tactical information operations support (ETIOS). ETIOS capabilities are a managed activity under the direction of the NEIC CO. ETIOS personnel conduct real time or near real time collection

operations enabling force protection and I&W and provide analytic support to deployed forces. ETIOS personnel search, intercept, identify, exploit, and direction-find communications and noncommunications transmissions. ETIOS personnel are trained and equipped to exploit the EM spectrum in the expeditionary and fleet operating environments.

4.5.1.3 Fleet Cyber Command/COMTENTHFLT

FLTCYBERCOM and COMTENTHFLT were created as part of the CNO's vision to achieve information integration and innovation necessary for warfighting superiority across the full spectrum of military operations in the maritime and cyberspace domains. This initiative supports the Navy's move from platform-centric to information-centric processes. The new FLTCYBERCOM and COMTENTHFLT are headquartered at Fort George G. Meade, MD, taking advantage of existing infrastructure, communications support, and expertise.

FLTCYBERCOM serves as the NCC to United States Cyber Command. Its mission is to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support IO and space planning and operations; to deliver integrated cyber, IO, cryptologic, and space capabilities; and to deliver global Navy cyber network common operational requirements.

The mission of COMTENTHFLT is to serve as the numbered fleet for FLTCYBERCOM and operationally employ Navy cyber, IO, and SIGINT forces and to coordinate with coalition naval forces and JTFs to execute the full spectrum of cyber, IO, and SIGINT capabilities and missions across the cyber, EM, and space domains.

4.5.1.3.1 Naval Network Warfare Command

Subordinate to United States Cyber Command, Naval Network Warfare Command (NNWC) directs the operations and security of the Navy's portion of the Global Information Grid. NNWC ensures the delivery of reliable and secure net-centric and space warfighting capabilities in support of strategic, operational, and tactical missions across the Navy.

4.5.1.3.2 Navy Information Operations Commands

NIOCs provide SIGINT and IO expertise and equipment to fleet air, surface, subsurface, expeditionary, and special warfare forces. Where applicable, they are collocated with NSA/Cryptologic Support System components. The NIOCs, Navy information operations detachments, and theater-focused FIOCs support a myriad of maritime, joint theater, and national missions within the SIGINT and IO arenas, providing reachback support to maritime commanders.

4.5.1.3.3 Navy Cyber Forces

CYBERFOR is the TYCOM for cryptology, SIGINT, cyber, IO, intelligence, networks, and space disciplines. CYBERFOR reports to COMUSFLTFORCOM.

As the TYCOM, CYBERFOR's mission is to manage the manpower, training, modernization, and maintenance of C2 architecture and networks, cryptologic and space-related systems, and intelligence and IO activities. CYBERFOR is headquartered at Joint Expeditionary Base, Little Creek-Fort Story in Virginia Beach, VA. Location in a fleet concentration area ensures CYBERFOR's close linkage with those it supports. CYBERFOR coordinates with COMUSFLTFORCOM, COMUSPACFLT, and the platform TYCOMs for surface, air, and subsurface forces to coordinate MT&E issues such as IA and DS requirements, CCOP equipment installation, Navy tactical task list generation and maintenance, and personal qualification standards and job qualification requirements review and maintenance.

4.5.1.4 Naval Criminal Investigative Service

Naval Criminal Investigative Service (NCIS) is a federal law enforcement agency that protects and defends the DON against terrorism and foreign intelligence threats, investigates major criminal offenses, enforces the criminal laws of the United States and the Uniform Code of Military Justice, assists commands in maintaining good order and discipline, and provides law enforcement and security services to the Navy and Marine Corps on a worldwide basis. NCIS programs and operational activity complement other efforts within the DON to defend against espionage, terrorism, subversion, sabotage, criminal activity, and major security violations.

With over 150 offices worldwide and agents assigned to interagency task forces, CCDR and joint staffs, selected USN ships and staffs, and Marine Corps elements, NCIS activities keep the supported commanders apprised of potential threats. NCIS leverages organic investigative and analytic capabilities as well as liaison relationships to identify, neutralize, and/or exploit potential breaches of security. NCIS also provides a comprehensive briefing program to educate military and civilian personnel on threats posed by foreign intelligence and security services (FISS) and terrorist groups.

4.5.1.4.1 Combating Terrorism

The NCIS Combating Terrorism Program includes offensive (counterterrorism) and defensive (antiterrorism/force protection) capabilities employed to oppose terrorism throughout the entire threat spectrum. Activities also include the collection, processing, and analysis of information that is further integrated with theater and national sources to produce all-source intelligence products that support naval force commanders and their staffs. NCIS special agents and analysts work closely with operational planning staffs within the Navy, Marine Corps, and joint commands. To facilitate this strategy, NCIS assigns trained personnel to other law enforcement and intelligence agencies to include the FBI, CIA, and NSA.

Naval forces in transit are supported by agents assigned to OCONUS NCIS field offices or force protection detachments which are manned jointly by NCIS, Air Force Office of Special Investigations (AFOSI), and Army Criminal Investigations Command.

4.5.1.4.2 Counterintelligence

Within the DON, NCIS has primary jurisdiction for CI and investigative matters with the exception of combat and contingency-related CI responsibilities of the Marine Corps. NCIS provides a full range of CI services encompassing four primary mission areas: collection, analysis and production, operations, and investigations. NCIS accomplishes its mission through proactive and reactive programs in support of DON and national-level requirements. NCIS also provides personnel to develop and implement CI plans in support of DON, theater, and DOD CI objectives during wartime, contingencies, and exercises. NCIS is responsible for providing CI support to the DON R&D and acquisition community. NCIS has dedicated CI assets and programs in support of R&D, technology protection, critical program information, and infrastructure protection.

4.5.1.4.3 Multiple Threat Alert Center

The Multiple Threat Alert Center (MTAC) serves as the focal point within the DON for single-source evaluation, all-source analysis, and dissemination regarding asymmetric terrorist, FISS, cyber, and criminal threats impacting the DON. Additionally, MTAC serves as the 24/7 operations center for NCIS activities worldwide. MTAC maintains awareness of Navy and Marine Corps operations and liaises with national, theater, and tactical operations and intelligence watch centers to identify and warn of location-specific threats.

4.5.1.4.4 Human-Derived Information

HDI is defined as the “activities related to the conduct of the collection of intelligence information through humans. It includes the following forms of information: CI, force protection, research and technology protection, and law enforcement.” HDI encompasses all information derived from individuals.

Deputy CNO for Information Dominance (OPNAV N2/N6) has designated NCIS the mission manager for Navy HDI. This designation does not extend to tactical control of Navy and Marine Corps tactical HUMINT/CI teams.

4.5.2 United States Marine Corps

HQ, United States Marine Corps Intelligence Department is responsible for policy, plans, programming, budgets, and staff supervision of intelligence and supporting activities within the United States Marine Corps. The department supports the Commandant of the Marine Corps in his role as a member of the JCS, represents the Service in joint and IC matters, and exercises supervision over the Marine Corps Intelligence Activity (MCIA). The department has Service staff responsibility for GEOINT, advanced geospatial intelligence, SIGINT, HUMINT, MASINT, and CI and ensures there is a single synchronized strategy for the development of the Marine Corps ISR Enterprise.

4.5.2.1 Marine Corps Intelligence Activity

The MCIA is the United States Marine Corps' Service intelligence center. It is primarily located at Quantico, VA and Fort Meade and Suitland, MD and has a detachment at the National Ground Intelligence Center (NGIC) in Charlottesville, VA. Unique among Service production centers, tailored products are the largest percentage of MCIA's efforts that support operating forces.

MCIA strives to tailor its intelligence production toward specific operational needs through its more than 25 types of intelligence products and services. MCIA leverages the analysis of other national or defense intelligence agencies or organizations to meet the needs of more than 570 customers including all branches of Service, government entities, and coalition partners. MCIA provides HQ, Marine Corps; USMC components; and other customers with the following types of support: threat assessments, estimates, and intelligence for planning and decisionmaking; intelligence support for doctrine and force structure development; systems and equipment acquisition; wargaming; training; predeployment planning; and exercise support.

4.5.3 United States Air Force

HQ, United States Air Force is the focal point for the end-to-end functional management of all Air Force ISR capabilities. The Air Force participates in the preparation of joint and national intelligence estimates and develops and implements the Air Force policies and guidance for developing, managing, and operating Air Force ISR activities.

4.5.3.1 Air Force Intelligence, Surveillance, and Reconnaissance Agency

The Air Force ISR Agency's mission is to organize, train, equip, and present assigned forces and capabilities to conduct ISR for CCDRs and the nation. The agency also implements and oversees execution of Air Force HQ policy and guidance to expand Air Force ISR capabilities to meet current and future challenges.

The 480th ISR Wing, 70th ISR Wing, 361st ISR Group, National Air and Space Intelligence Center (NASIC), and the Air Force Technical Applications Center are aligned under the Air Force ISR Agency. The agency is also responsible for mission management and support of SIGINT operations for 24th Air Force and the 12th Air Force's 55th Wing. In addition, the agency provides guidance to 22 Air National Guard units with ISR responsibilities. The Air Force ISR Agency further supplies mission management and support for specific intelligence operations within all of these organizations. Mission support includes organizing, training, and equipping the Service's cryptologic elements.

4.5.3.2 National Air and Space Intelligence Center

NASIC, headquartered at Wright-Patterson Air Force Base (AFB), OH, is the primary DOD producer of foreign air and space intelligence. NASIC develops its products by analyzing all available data on foreign aerospace forces and weapons systems to determine performance characteristics, capabilities, vulnerabilities, and intentions. NASIC assessments are often an important factor in shaping national security and defense policies. As the DOD

experts on foreign aerospace system capabilities, the center also supports weapons treaty negotiations and verification. Since 1961, the center's mission and resources have expanded to meet the challenge of worldwide technological developments and the accompanying national need for aerospace intelligence. In recent years, the emphasis has increasingly shifted toward evaluation of worldwide aerospace systems and the production of tailored, customer-specific products.

4.5.3.3 Air Force Office of Special Investigations

AFOSI provides professional investigative service to commanders of all Air Force activities. AFOSI identifies, investigates, and neutralizes criminal, terrorist, and espionage threats to Air Force and DOD personnel and resources.

The command focuses on five priorities: develop and retain a force capable of meeting Air Force needs, detect and provide early warning of worldwide threats to the Air Force, identify and resolve crime that threatens Air Force readiness or good order and discipline, combat threats to information systems and technologies, and detect and defeat fraud impacting force acquisitions and base-level capabilities.

In addition to HQ, AFOSI has eight field investigations regions, seven of which are aligned with Air Force major commands. While the regions serve the investigative needs of those aligned major commands, all AFOSI units and personnel remain independent of those commands, and their chains of command flow directly to AFOSI HQ. Such organizational independence ensures unbiased investigations. The single region not aligned with a major command provides CI and security program management for special access programs under the Office of the Secretary of the Air Force.

4.5.4 United States Army

The Army Deputy Chief of Staff for Intelligence (DCSINT) is responsible to the Chief of Staff, Army, for long-range planning and policy guidance on all matters relating to Army intelligence, including CI and many aspects of security policy. The DCSINT manages the Army's portion of the NIP, all Military Intelligence Program funding, Army departmental-level general military and S&T intelligence production missions, intelligence readiness training, the Army language program, and the Army Foreign Material Program. The DCSINT also serves as the DOD executive agent for commercial linguist support to the Services/CCDRs. The DCSINT supervises the Army's Intelligence and Security Command (INSCOM) and has operational control over its departmental production resources.

4.5.4.1 United States Army Intelligence and Security Command

INSCOM, headquartered at Fort Belvoir, VA, is the Army's principal intelligence command. All intelligence disciplines and capabilities not assigned to Corps and below are assigned to INSCOM. The command provides multidiscipline intelligence and IO support to Army commanders at all echelons. As the Army's force projection intelligence command, INSCOM provides a Theater Intelligence Brigade that directly supports each Army component commander in each of the GCCs. These brigades perform continuous IPOE to ensure Army commanders' situational awareness of potential adversaries in the theaters in which they operate or to which it might deploy forces. In addition, INSCOM serves as the Army's Service Cryptologic Authority and provides Army personnel in direct support of NSA and the regional SIGINT operations centers. The 902nd MI Brigade, Ft. Meade, MD, provides CI support to Army forces, combat support agencies, installations, and designated contractor facilities throughout the CONUS. The 1st Information Operations Command, Ft Belvoir, VA, provides IO support to Army communications networks and Army commands across the tactical to strategic spectrum.

4.5.4.2 National Ground Intelligence Center

NGIC is the Army's S&T intelligence center and is subordinate to INSCOM. NGIC produces all-source intelligence on foreign ground force systems, technology, organization, doctrine, strategy, and tactics in accordance with DIA's delegated production program. Like the other Service S&T centers, NGIC supports national decision makers, the acquisition community, and operational forces and executes the Army portion of the

DOD Foreign Material Acquisition Program. Although primarily located in Charlottesville, VA, NGIC also has satellite facilities at the Washington Navy Yard, Aberdeen Proving Grounds, and Fort Meade, MD. It also maintains strategic military intelligence detachments located around the country composed of Army reservists who contribute to the Army analysis and production program. To facilitate sharing of information, the MCIA maintains a contingent at NGIC.

4.6 INTELLIGENCE SHARING AND COOPERATION

Operations with a wide variety of partners, both United States and multinational, are becoming the norm, making intelligence sharing with interagency and multinational allies and partners increasingly important. In operations involving interagency, intergovernmental, nongovernmental, or multinational partners, one of the most critical functions of the JTF is establishing a common view of the problem and shared situational awareness among all partners. Although intelligence sharing is accomplished at all levels during crises, in most operations the requirement expands with proximity to the operational forces. For this reason, it is imperative that the JFC and his subordinate forces understand the limits and restrictions on information sharing.

The majority of operations conducted today involve intelligence sharing to some degree. The required amount of intelligence shared varies widely based on the nature of the military operation. In general, combat operations with multinational military coalitions require much more robust intelligence sharing than humanitarian or peacekeeping operations. The J2 must scale the organization's capability to provide intelligence sharing accordingly.

The foreign disclosure officer (FDO) of the combatant command is the key element in any intelligence sharing plan with interagency, intergovernmental, nongovernmental, or multinational partners. The FDO is versed in all relevant national disclosure policy and can guide the JFC and staff in information releasability and proper intelligence sharing procedures. The FDO provides staff review and advises the JFC on the approval of sanitized or downgraded military intelligence products. In the absence of an onsite FDO, intelligence products that require sanitization or downgrading for release to third parties are referred to the producing agency or coordinated through the RFI process. Since the process is time consuming, the JFC should request deployed FDO support to satisfy timely intelligence sharing requirements.

Intelligence and cryptologic professionals must coordinate with an FDO via their chain of command for policy and guidance on sanitizing and downgrading classified products. Writing for release is a critical step in expediting the downgrading or sanitization of intelligence products. Prepare products at an uncaveated level to the greatest extent possible. Cleary indentify material not authorized for release utilizing portion marking, fully footnote all derived classified information, and provide tear line information at a releasable level.

For further information on foreign disclosure policy and writing for release, refer to the DON Foreign Disclosure Manual.

4.7 NEW CHALLENGES IN THE NAVAL INTELLIGENCE COMMUNITY

The advent of the information age presents new challenges for the U.S. intelligence apparatus. While it allows sharing of information and analysis promptly and in large quantities, it also complicates the quest for relevant, accurate intelligence in a timely fashion. The sheer volume of available information alone can overwhelm even the most advanced collection mechanisms and associated workforce. Thus, the imperative for the professional is to develop and employ sophisticated approaches to gathering and providing pertinent intelligence in support of commander's guidance and intent. Just as importantly, the speed by which assessments reach the right commanders and decision makers is the backbone of ID and knowledge superiority.

As new capabilities are fielded and legacy capabilities are upgraded, the IC must determine methods to incorporate and synergize information from the various sensors towards a holistic assessment. This especially includes the incorporation and employment of unmanned vehicles and systems in the physical domains alongside capabilities in the virtual domain of cyberspace. While these new and improved sensors bolster the collection manned systems provide, it is critical to the successful intelligence operation that collected data is merged with

intelligence at the MOC to ensure the most complete intelligence available is accessible for the commander's consumption and utilization. The increased amount of available information necessitates the MOC as a focal point for its analysis and synthesis into finished intelligence products.

Perhaps now, more than ever, in this era of globalization, there must be a significant investment in cultural intelligence and awareness. In consonance with "A Cooperative Strategy for 21st Century Seapower," partnerships and relationships with foreign nations is at the crux of success. These associations largely hinge on the U.S. forces respect and understanding of a state's people and its culture and sensitivities. The function of intelligence for this mission is to support the accuracy and provision of this awareness. Additionally, it must furnish assessments of the interactions to ensure the U.S. approach is effective and its objectives are obtained. This role is squarely aligned with the duties of the IC and elemental to success in this regard.

This constraint becomes most evident when confronting irregular challenges ashore, in the littorals, and on the open ocean. The rapidity with which these sorts of threats can materialize and deploy drastically shortens the timeline normally associated with traditional nation-state force-on-force conflicts. As such, the intelligence required to support understanding of the irregular environment must be quickly aggregated with a speed uncommon to traditional processes. Additionally, the provided intelligence must extend beyond the military capabilities of the adversary and into the ethnic and cultural sensitivities of the combatant and populace alike to support nonkinetic and IO tactics.

The advances in warfare and technology present a wealth of new challenges for the IC; however, each challenge is an opportunity to evolve the intelligence profession to meet the requirements of the changing security environment. These opportunities must be met head-on by a trained cadre of professionals that make best use of the emerging sensor systems, increased collection capabilities, and innovative Navy organizational structures such as the MOC and the IDC. It is only through the effective employment of all facets of the intelligence mechanism that Naval Intelligence can remain preeminent in its contribution to meeting national objectives.

INTENTIONALLY BLANK

REFERENCES

JP 3-32, Command and Control for Joint Maritime Operations, (Incorporating Change 1, 27 May 2008), 8 August 2008

JP 3-33, Joint Task Force Headquarters, 16 February 2007

NTRP 3-20.6.06, CV/CVN Class Tactical Publication (U), July 2005

NTTP 1-10.1, Force Tactical Action Officer (FTAO) (U), March 2005

TACMEMO, CLF/CPF 3-03.1-03, Strike Planning Cell, 4 April 2003

NWP 3-51.1, Navy Electronic Warfare (U), February 2006

NTTP 3-13.2, Navy Information Operations Warfare Commander's Manual (U), May 2006

SECNAVINST 5430.107, Mission and Functions of the Naval Criminal Investigative Service, 28 December 2005

SECNAVINST 3850.2C, Department of the Navy Counterintelligence, 20 July 2005

DIRNAVCRIMINVSERV WASHINGTON DC, 161801Z APR 2009, HUMAN DERIVED INFORMATION STRATEGY

NAVADMIN 169/08, 161250Z JUN 08, STAND-UP OF INTELLIGENCE TYCOM FUNCTIONS WITHIN NAVAL NETWORK WARFARE COMMAND (NETWARCOM)

CNO MEMO, Fleet Cyber Command/Tenth Fleet and Navy Cyber Forces Implementation Plan and Command Relationships Directive, 29 January 2010

NAVADMIN 159/09, 280239Z MAY 09, INTELLIGENCE MANPOWER ALIGNMENT

COMNAVNETWARCOM, 021248Z OCT 09, FLEET INTELLIGENCE MANPOWER DISTRIBUTION POLICY FOR INTELLIGENCE DETACHMENT TEAMS

The Concept of Operations for Fleet Maritime Domain Awareness (Fleet MDA CONOPS), 13 March 2007

Navy Maritime Domain Awareness Concept 2007, 29 May 2007

A Cooperative Strategy for 21st Century Sea Power, October 2007

TACMEMO 3-13.3-05 Communications Electronic Warfare for Surface Units (U), December 2005

Navy Enlisted Manpower and Personnel Classifications and Occupational Standards, July 2010

COMUSFLTFORCOM, 232017Z OCT 09, INFORMATION OPERATIONS (IO) AND CRYPTOLOGIC GLOBAL AUGMENTATION POLICY (GAP)

CNO WASHINGTON DC, 300017Z MAR 07, CRYPTOLOGIC CARRY-ON PROGRAM (CCOP) FUNCTIONAL MANAGER DESIGNATION

Cryptologic Carry-On Program (CCOP) Business Plan, Version 1.0 (U), May 2007

JP 2-0, Joint Intelligence, 22 June 2007

JP 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations (U), 13 June 2006

U.S. Fleet Cyber Command/U.S. Tenth Fleet Web site, http://www.fcc.navy.mil/

United States Navy Web site, http://www.navy.mil/search/display.asp?story_id=50853

Headquarters, U.S. Marine Corps Intelligence Department Web site,
http://hqinet001.hqmc.usmc.mil/dirint/default.html

Marine Corps Intelligence Activity Web site (U),
http://www.mcia.ic.gov/portal/page/portal/CommandPortalV1/CommandInformation/CommandHistory

Headquarters, U.S. Air Force DCOS for ISR Web site (U),
http://www.intelink.ic.gov/sites/a2/aboutus/Shared%20Documents/mission.aspx?PageView=Shared

United States Air Force official Web sites, http://www.af.mil/information/factsheets/factsheet.asp?id=9438 and
http://www.af.mil/information/factsheets/factsheet.asp?fsID=145

NWP 3-32, Maritime Operations at the Operational Level of War (with Erratum 11/18/2008), October 2008

NTTP 3-32.1, Maritime Operations Center (thru Change 1 February 2010), October 2008

OPNAVINST 5450.77, Missions, Functions, and Tasks for U.S. Fleet Forces Command (USFLTFORCOM), 16 July 2007

OPNAVINST 5450.337, Missions, Functions, and Tasks of Commander, U.S. Pacific Fleet, 19 November 2007

OPNAV Notice 5400.7407, “Establishment of U.S. Fleet Cyber Command and Recommissioning of U.S. Tenth Fleet” at Fort George G Meade, MD, 19 January 2010

JP 3-13, Information Operations, 13 February 2006

United States Navy Expeditionary Combat Command Force Operational Concept, 1 August 2007

Navy Expeditionary Combat Command Expeditionary Intelligence Concept of Operations, 26 November 2007

COMNECC INST 3880.1, NECC Force Management of Expeditionary Intelligence and Tactical Information Operations Capabilities, 1 September 2009

Memo for the Information Dominance Corps, 2 November 2009, VADM Dorsett

NAVADMIN 316/09, 292237Z OCT 09, ESTABLISHMENT OF THE DEPUTY CHIEF OF NAVAL OPERATIONS FOR INFORMATION DOMINANCE (N2/N6)

Information Dominance: A Vision for the U.S. Navy, 30 October 2009, CNO

OPNAVINST 5300.12, The Information Dominance Corps, 6 October 2009

Taking Joint Intelligence Operations to the Next Level, Joint Force Quarterly, December 2007, Tyler Akers

JP 2-01.3, Joint Intelligence Preparation of the Operational Environment, 16 June 2009

JP 2-01, Joint and National Intelligence Support to Military Operations, 7 October 2004

JP 3-60, Joint Targeting, 13 April 07

NDP 2, Naval Intelligence, 30 September 1994

JP 3-0, Joint Operations (Incorporating Change 2, 22 March 2010), 17 September 2006

JP 5-0, Joint Operations Planning, 26 December 2006

JP 1, Doctrine for the Armed Forces of the United States (Incorporating Change 1, 20 March 2009), 14 May 2007

Navy Enlisted Manpower and Personnel Classifications & Occupational Standards, NAVPERS 18068F, http://www.npc.navy.mil/ReferenceLibrary/NEOCS/

OPNAVINST C3501.2K, Mission Areas and Required Operational Capability/Projected Operational Environment Statements (U), 22 January 2010

NWP 3-56, Composite Warfare Commander's Manual, August 2001

ONI Handbook 2010, Office of Naval Intelligence, 2010

Department of the Navy Foreign Disclosure Guide (Incorporating Change Transmittal 1), September 2007

COMUSFLTFORCOM NORFOLK VA, 132118Z JAN 09, EXPEDITIONARY STRIKE GROUP (ESG) WAY AHEAD (U)

COMUSFLTFORCOM NORFOLK VA, 092342Z MAR 09, EXPEDITIONARY STRIKE GROUP (ESG) WAY AHEAD SECOND IN A SERIES (U)

Naval Network Warfare Command Web site, http://www.netwarcom.navy.mil/

National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security, October 2005

The U.S. Navy's Vision for Confronting Irregular Challenges, January 2010

INTENTIONALLY BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACINT	acoustic intelligence
AFB	Air Force Base
AFOSI	Air Force Office of Special Investigations
AG	aerographer's mate (USN rating)
AI	air intelligence officer
AMDC	air missile defense commander
AMW	amphibious warfare
AO	area of operation
AOR	area of responsibility
AQD	additional qualification designator
ARG	amphibious ready group
ASW	antisubmarine warfare
ASWC	antisubmarine warfare commander
ATF	amphibious task force
ATO	assistant targeting officer
AW	air warfare
BDA	battle damage assessment
BHA	bomb hit assessment
C2	command and control
C4I	command, control, communications, computers, and intelligence
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAG AI	CVW intelligence officer
CCDR	combatant commander
CCIR	commander's critical information requirement

CCOP	cryptologic carry-on program
CDC	combat direction center
CDIO	collateral duty intelligence officer
CE	command element
CFMCC	coalition force maritime component commander
CGIS	United States Coast Guard Investigative Service
CI	counterintelligence
CIA	Central Intelligence Agency
CIC	combat information center
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	commander, joint task force
CMSA	cruise missile support activity
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	Chief of Naval Operations
CO	commanding officer
COA	course of action
COG	center of gravity
COMTENTHFLT	Commander, Tenth Fleet
COMUSFLTFORCOM	Commander, United States Fleet Forces Command
COMUSNAVAF	Commander, United States Naval Forces, Africa
COMUSNAVCENT	Commander, United States Naval Forces, Central Command
COMUSNAVEUR	Commander, United States Naval Forces, Europe
COMUSNAVSO	Commander, United States Naval Forces, Southern Command
COMUSPACFLT	Commander, United States Pacific Fleet
CONOPS	concept of operations
CONPLAN	concept plan

CONUS	continental United States
CPRG	Commander, Patrol and Reconnaissance Group
CPRW	commander, patrol and reconnaissance wing
CRC	cryptologic resource coordinator
CSG	carrier strike group
CSS	Central Security Service
CT	cryptologic technician
CTF	task force commander
CTG	task group commander
CTI	cryptologic technician – interpretive
CTM	cryptologic technician – maintenance
CTN	cryptologic technician – networks
CTR	cryptologic technician – collection
CTT	cryptologic technician – technical
CVIC	carrier intelligence center
CVN	aircraft carrier, nuclear
CVW	carrier air wing
CWC	composite warfare commander
CYBERFOR	Navy Cyber Forces
DCSINT	**[**Army] Deputy Chief of Staff for Intelligence
DEA	Drug Enforcement Administration
DESRON	destroyer squadron
DFI	Director of Fleet Intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIOCC	Defense Intelligence Operations Coordination Center
DIWC	deputy information warfare commander
DNI	Director of National Intelligence

DOD	Department of Defense
DOE	Department of Energy
DON	Department of the Navy
DS	direct support
EA	electronic attack
EEFI	essential elements of friendly information
EEI	essential element of information
EISE	expeditionary intelligence support element
ELINT	electronic intelligence
EM	electromagnetic
EMCON	emission control
EP	electronic protection
ES	electronic warfare support
ESG	expeditionary strike group
ETIOS	expeditionary tactical information operations support
EW	electronic warfare
EXPLOT	expeditionary plot
EXW	expeditionary warfare
FBI	Federal Bureau of Investigation
FCC	functional component commander
FDNF	forward deployed naval forces
FDO	foreign disclosure officer
FIAF	Fleet Intelligence Adaptive Force
FID	fleet intelligence detachment
FIOC	fleet information operations center
FISS	foreign intelligence and security services
FLTCYBERCOM	Fleet Cyber Command
FOS	family of systems

FRTP	fleet readiness training plan
GCC	geographic combatant commander
GEOINT	geospatial intelligence
HA/DR	humanitarian assistance/disaster relief
HDI	human-derived information
HN	host nation
HQ	headquarters
HUMINT	human intelligence
I&W	indications and warning
IA	individual augmentee
IC	Intelligence Community
ICC	United States Coast Guard Intelligence Coordination Center
ID	information dominance
IDC	Information Dominance Corps
IDIS	independent duty intelligence specialists
IMDP	Intelligence Manpower Distribution Plan
IMINT	imagery intelligence
INR	State Department Bureau of Intelligence and Research
INSCOM	US Army Intelligence and Security Command
IO	information operations
ION	interactive ON-NET
IPIC	imagery processing interpretation center
IPOE	intelligence preparation of the operational environment
IRTPA	Intelligence Reform and Terrorism Prevention Act
IS	intelligence specialist
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
ITO	integrated tasking order

IW	irregular warfare
IWC	information operations warfare commander
J2X	joint force counterintelligence and human intelligence staff element
JAOC	joint air operations center
JATF	joint amphibious task force
JCS	Joint Chiefs of Staff
JDISS	Joint Deployable Intelligence Support System
JFACC	joint force air component commander
JFC	joint force commander
JFCC-ISR	Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance
JFE	joint fires element
JFMCC	joint force maritime component commander
JIC	joint intelligence center
JIOC	joint intelligence operations center
JIOWC	Joint Information Operations Warfare Center
JIPTL	joint integrated prioritized target list
JISE	joint intelligence support element
JMPS	Joint Mission Planning System
JOA	joint operations area
JPRA	Joint Personnel Recovery Agency
JTCB	joint targeting coordination board
JTF	joint task force
JTSG	joint targeting steering group
JWAC	Joint Warfare Analysis Center
JWICS	Joint Worldwide Intelligence Communications System
LHA	landing helicopter assault
LHD	landing helicopter dock

LOAC	law of armed conflict
LPD	landing platform dock
LSD	dock landing ship
MASINT	measurement and signature intelligence
MCIA	Marine Corps Intelligence Activity
MCM	mine countermeasures
MCMRON	mine countermeasures squadron
MDA	maritime domain awareness
MEA	munitions effectiveness assessment
METOC	meteorological and oceanographic
MEU	Marine expeditionary unit
MIO	maritime interception operations
MIOC	maritime intelligence operations center
MIO-IET	maritime interception operations-intelligence exploitation team
MIW	mine warfare
MIWC	mine warfare commander
MOC	maritime operations center
MPR	maritime patrol and reconnaissance
MSI	multisensor interpretation
MT&E	man, train, and equip
MTAC	Multiple Threat Alert Center
N2	Navy intelligence
NALE	naval and amphibious liaison element
NASIC	National Air and Space Intelligence Center
NCC	Navy component commander
NCIS	Naval Criminal Investigative Service
NEC	Navy enlisted classification
NECC	Navy Expeditionary Combat Command

NEIC	Navy Expeditionary Intelligence Command
NEO	noncombatant evacuation operation
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NIC-C	National Intelligence Coordination Center
NIOC	Navy information operations command
NIP	National Intelligence Program
NIST	national intelligence support team
NITF-MS	Naval Intelligence Task Force-Maritime Security
NJOIC	National Joint Operations and Intelligence Center
NMAWC	Naval Mine and Anti-Submarine Warfare Command
NMIC	National Maritime Intelligence Center
NMITC	Navy and Marine Corps Intelligence Training Center
NNWC	Naval Network Warfare Command
NRC	National Response Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSAWC	Naval Strike and Air Warfare Center
NSW	naval special warfare
NSWC	Naval Special Warfare Command
NSW MSC	Naval Special Warfare Mission Support Center
NSWRON	naval special warfare squadron
NTTP	Navy tactics, techniques, and procedures
NWP	Navy warfare publication
OGA	other government agency
OGO	other government organization
OIC	officer in charge

ONI	Office of Naval Intelligence
OPINTEL	operational intelligence
OPLAN	operation plan
OPNAV	Office of the Chief of Naval Operations
OPNAV N2/N6	Deputy CNO for Information Dominance
OPNAV N2X	Director of Naval Intelligence Deputy Director for Human-Derived Information
OPTASK	operational task
OTC	officer in tactical command
PHIBRON	amphibious squadron
PIR	priority intelligence requirement
R&D	research and development
RFF	requests for forces
RFI	request for information
ROE	rules of engagement
ROMO	range of military operations
S&T	science and technology
S2	MEU intelligence
SAM	surface-to-air missile
SAPCO	special access program control officer
SBT	special boat team
SCCTV	secure closed-circuit television
SCI	sensitive compartmented information
SDV	SEAL delivery vehicle
SEAL	sea, air, and land
SECDEF	Secretary of Defense
SHARP	shared reconnaissance pod
SIAC	strike intelligence analysis cell

SIGINT	signals intelligence
SIWO	signals intelligence warfare officer
SIO	senior intelligence officer
SOF	special operations forces
SOMPE-M	Special Operations Mission Planning Environment-Maritime
SSEE	ship's signals exploitation equipment
SSES	ship's signals exploitation space
SSO	special security officer
STWC	strike warfare commander
SUPPACT	support activity
SUPPLOT	supplementary plot
SUWC	surface warfare commander
TAC	target analysis cell
TACRON	tactical air control squadron
TAD	temporary additional duty
TAO	tactical action officer
TDY	temporary duty
TET	targeting effects team
TFCC	tactical flag command center
TIC	target intelligence cell
TLAM	Tomahawk-land attack missile
TNL	target nomination list
TO	targeting officer
TOC	tactical operations center
TSC	theater security cooperation
TSOC	theater special operations command
TST	time-sensitive target
TYCOM	type commander

UAV	unmanned aerial vehicle
U.S.	United States
USCG	United States Coast Guard
USCS	United States Cryptologic System
USD(I)	Undersecretary of Defense for Intelligence
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USN	United States Navy
USPACOM	United States Pacific Command
USSTRATCOM	United States Strategic Command
VBSS	visit, board, search, and seizure
VP	patrol squadron
VQ	fleet air reconnaissance squadron
WMD	weapons of mass destruction
WSV	weapon system video

INTENTIONALLY BLANK

LIST OF EFFECTIVE PAGES

Effective Pages	Page Numbers
NOV 2010	1 thru 14
NOV 2010	1-1 thru 1-6
NOV 2010	2-1 thru 2-16
NOV 2010	3-1 thru 3-26
NOV 2010	4-1 thru 4-18
NOV 2010	Reference-1 thru Reference-4
NOV 2010	LOAA-1 thru LOAA-12
NOV 2010	LEP-1, LEP-2

INTENTIONALLY BLANK

NWP 2-01
NOV 2010