NAVY WARFARE PUBLICATION

NAVY INFORMATION OPERATIONS NWP 3-13

EDITION FEBRUARY 2014

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS

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

PRIMARY REVIEW AUTHORITY:
NAVY INFORMATION OPERATIONS COMMAND
NORFOLK (NIOC-N)

URGENT CHANGE/ERRATUM RECORD		
NUMBER	DATE	ENTERED BY

0411LP1142913

INTENTIONALLY BLANK

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

21 May 2014

LETTER OF PROMULGATION

1. NWP 3-13 (FEB 2014), Navy Information Operations, is UNCLASSIFIED. Handle in accordance with the administrative procedures contained in NTTP 1-01 (APR 2005), The Navy Warfare Library.

2. NWP 3-13 (FEB 2014) is effective upon receipt and supersedes NWP 3-13 (JUN 2003), Navy Information Operations. Destroy superseded material without report.

3. NWP 3-13 (FEB 2014) provides information operations (IO) guidance to Navy commanders, planners, and operators to exploit and shape the information environment (IE) and apply information-related capabilities (IRC) to achieve military objectives. It reinforces the integrating functionality of IO to incorporate IRC and engage in the IE to provide a military advantage to the friendly Navy force. This NWP offers a framework of fundamental principles, practices, techniques, procedures, and terms that guides a commander in employing IRC to accomplish the mission.

4. NWP 3-13 (FEB 2014) is approved for public release; distribution is unlimited.

SCOTT B. JERABEK

INTENTIONALLY BLANK

February 2014

PUBLICATION NOTICE

ROUTING

1. NWP 3-13 (FEB 2014), NAVY INFORMATION OPERATIONS, provides information operations guidance to Navy commanders, planners, and operators to exploit and shape the information environment and apply information-related capabilities to achieve military objectives. This publication reinforces the integrating functionality of information operations to incorporate information-related capabilities and engage in the information environment to provide a military advantage to the friendly Navy force. It is effective upon receipt.

2. This publication replaces NWP 3-13 (JUN 2003), Navy Information Operations.

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.

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

LIST OF ILLUSTRATIONS

Page No.

INTENTIONALLY BLANK

PREFACE

Information operations is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries and potential adversaries while protecting our own. Delivering current, relevant, and accurate doctrine to Navy planners and operators is essential. There are operational and tactical implications of this revision, including potential organizational and process adjustments in the maritime operations center.

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 PRINTED COPIES

Order printed copies of a publication using the print-on-demand (POD) system. A command may requisition a publication using the standard military standard requisitioning and issue procedure (MILSTRIP) process on the Naval Supply Systems Command Web site called the Naval Logistics Library (https://nll.ahf.nmci.navy.mil). An approved requisition is forwarded to the specific Defense Logistics Agency (DLA) site at which the publication's electronic file is officially stored. Commands may also order publications through the Navy Doctrine Library System Web site (https://ndls.nwdc.navy.mil) by visiting publication-specific metadata Web pages and selecting the hyperlink on the stock number, which is linked to the Naval Logistics Library Web site. Users may be prompted to create an account to complete the ordering process. Currently, three 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 (NWDC) Web site at: https://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 the sample for urgent change recommendation message format on page 13.

ROUTINE CHANGE RECOMMENDATIONS

Submit routine recommended changes to this publication at any time by using the routine change recommendation letter format on page 14. Mail it to the address below or post 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//
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

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 PURPOSE

This Navy warfare publication (NWP) provides information operations (IO) guidance to Navy commanders, planners, and operators to exploit and shape the information environment (IE) and apply information-related capabilities (IRC) to achieve military objectives. This publication reinforces the integrating functionality of IO to incorporate IRC and engage in the information environment to provide a military advantage to the friendly Navy force.

Like all Navy doctrine, this NWP should not impede a commander's exercise of innovation and mission command. This NWP offers a framework of fundamental principles, practices, techniques, procedures, and terms that guide a commander in employing IRC to accomplish the mission.

1.2 SCOPE

This NWP provides doctrine for the planning, preparation, execution, and assessment of IO for Navy operations. This NWP applies across the levels of war, mainly directed at the operational level of war. It fits between joint force commander-level guidance in Joint Publication (JP) 3-13, Information Operations; Navy tactical-level guidance in Navy Tactics, Techniques, and Procedures (NTTP) 3-13.2, Information Operations Warfare Commander (IWC) Manual; and other information-related NTTPs. The Navy typically executes IRC at the tactical level; but operational-level synchronization can optimize IO's integrative power.

1.3 BACKGROUND

Long before man walked the Earth, the survival of thinking creatures depended on exploiting information. Successful predators developed techniques to approach their quarry without alarming them, while potential prey with the best camouflage lived long enough to pass that trait to another generation. Social animals learned the importance of using influence, prestige, and fear to advance their survival. As humans moved from hunting packs to tribes and then to nations, information advantages contributed to survival and triumph in battle.

Modern advances in technology have increased the role of information in warfare; there are many instances of maritime IO that predate electronic communications and steam propulsion. For example, Napoleon's army was a potent land force but his navy struggled to match the British Royal Navy at sea. The French invested in an extensive network of semaphore stations capable of relaying visual signals up to 200 miles in an hour. This produced an information advantage, improving Napoleon's already effective command and control (C2) and passing observation reports along the coast to alert ships and reduce the Royal Navy's ability to achieve surprise. Among the Royal Navy's commanders was Lord Thomas Cochrane of the brig HMS *Speedy*. Cochrane was especially skilled in applying deception and surprise to defeat more-capable enemies and to capture unsuspecting prize ships. In 1808, one of Cochrane's raiding parties attacked a semaphore station and set it afire as the French signalmen retreated. After the British withdrew, the French were relieved to find charred remains of their codebooks, assuming the attackers did not realize their value. In reality, Cochrane had copied the codes and passed it along to his superiors, enabling the British to decode the semaphore traffic and to insert false messages. Even in the days of fighting sail, maritime commanders integrated network intrusion, disruption, intelligence, and deception to create information effects and achieve desired goals.

The United States Navy's doctrinal concept of an integrating information function began in 1986 with a tactical memorandum on command, control, and communication countermeasures, described as the combination of electronic warfare (EW), military deception (MILDEC), operations security (OPSEC), and physical destruction. In 1989, then-Chief of Naval Operations (CNO) Admiral Carlisle A.H. Trost designated space and electronic warfare as a warfare mission area, defined in a 1992 CNO policy paper as "the destruction or neutralization of enemy space and electronic warfare targets. As warfare support, it is the enhancement of friendly force battle management through the integrated employment and exploitation of the electromagnetic spectra and the medium of space."

This integrating function was redefined through the years under terms such as "command and control warfare" and "information warfare" before becoming IO in 2005. Evolving joint and Navy doctrine has refined IO as a discrete warfare area, not just a supporting function or enabling capability, and the IE as a valuable and contested part of the battle space.

1.4 KEY DEFINITIONS

In January 2011, Secretary of Defense (SecDef) Memo 12401-10 redefined information operations as the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries and potential adversaries while protecting our own.

JP 3-13 defines these terms:

1. An information-related capability is a tool, technique, or activity employed within a dimension of the IE that may be used to create effects and operationally desirable conditions. (Chapter 3 discusses IRC in detail.)

2. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The IE includes physical, informational, and cognitive dimensions.

3. The target audience (TA) is an individual or group selected for influence. Influence is the act or power to produce a desired outcome or end on a TA.

Integration is the arrangement of military forces and their actions to create a force that operates by engaging as a whole.

Discussion of IRC and its effects sometimes requires contrast with conventional noninformation military capabilities such as bombs, missiles, and bullets. This NWP refers to lethal effects to describe the observable physical damage intentionally caused by explosions or the dynamic motion of objects, and a lethal weapon is a device designed to cause such damage. JP 1-02, Department of Defense Dictionary of Military and Associated Terms, defines a nonlethal weapon as "a weapon that is explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment."

CHAPTER 2

Information Operations Fundamentals

2.1 WAYS, ENDS, MEANS

As a model of military operations, ends are a commander's intended outcomes resulting in or supporting the desired strategic end state. Ways are the sequence of actions (methods and tactics and procedures, practices, and strategies) to achieve the ends. Means are the resources required to execute the ways such as troops, weapons systems, money, political will, and time. In this model of military operations, IRC is a means to create effects that induce an intended sequence of events that support strategic ends, either by supporting a friendly sequence of actions or undermining an adversary's sequence of actions.

The means of national power can only be effective when all elements focus on moving toward a feasible and clearly defined end state. In his book, "On War", German general and military theorist Carl von Clausewitz wrote, "War is thus an act of force to compel our enemy to do our will." Military objectives must cause a realistic change in the adversary's behavior or capability as a means to achieve that desired national/theater strategic end state; this is true whether using lethal fires or IRC. Planners must define the audience or target and how to apply IRC for the best results. MILDEC may manipulate adversary decision makers to act in a way advantageous to friendly military objectives. The general populace may be open to influences that may shift allegiance toward a more favorable leadership. A cyberspace or electronic attack might disrupt the adversary's C2. Lethal effects or military information support operations (MISO) can sap adversary combatants of their will to fight or send them into an irrational rage; friendly force planners must be careful to decide which option best suits the current mission.

Actions intended to influence a target audience focus on altering the perceptions and behaviors of leaders, groups, or entire populations to affect behaviors, protect operations, and project accurate information to achieve desired effects. These effects should result in a change in the adversary's behavior decision cycle and align with the commander's objectives.

2.2 INFORMATION SUPERIORITY

JP 1-02 defines information superiority as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." The concept should not imply an impossible goal of friendly force information perfection against total information denial for the enemy. It simply means the commander operates with less friction from the fog of war than the opposing commander does.

Just as it is impossible to sustain global maritime superiority, it is not always practical or desirable to maintain continuous information superiority. While ideal, "an uninterrupted flow of information" should not be required or even assumed. Commanders and their staffs need to make information a priority and their units must capitalize on the synergy between information and other lines of operation, apply IRC, and expend resources when it is necessary for mission success.

2.3 AUTHORITIES, RESPONSIBILITIES, AND LEGAL CONSIDERATIONS

Navy forces typically operate under a component commander or joint task force commander attached to a combatant commander (CCDR) or a subordinate joint force commander (JFC). A JFC executes unified actions to apply all of the instruments of national power to affect adversary political, military, economic, social, infrastructure, and information systems.

2.3.1 Authorities

The authority to employ IRC derives from Title 10, U.S. Code, Armed Forces. While Title 10 does not address IO separately, it provides the legal basis for the roles, missions, and organization of the Department of Defense (DOD) and the Services. Title 10, Section 16, gives command authority over assigned forces to the CCDR, which provides that individual with the authority to organize and employ commands and forces, assign tasks, designate objectives, and provide authoritative direction over all aspects of military operations.

DOD policy delegates authority to DOD components. DOD Directive 3600.01 series, Information Operations, is the principal IO policy document. Its counterpart, Chairman of the Joint Chiefs of Staff Instruction 3210.01C, Joint Information Operations Proponent, provides joint policy regarding the use of IRC, professional qualifications for the joint IO force, as well as joint IO education and training requirements. These two documents delineate the CCDR's authority to conduct joint IO and to delegate operational authority to a subordinate JFC, as appropriate.

The nature of IO is such that the exercise of operational authority inherently requires a detailed and rigorous legal interpretation of authority or legality of specific actions. Commanders at all levels should involve their staff judge advocates in the development of IO policy and the conduct of IO.

2.3.2 Responsibilities

JP 3-13 describes responsibilities for Undersecretary of Defense for Policy, Undersecretary of Defense for Intelligence, and the Joint Staff. The Joint Information Operations Warfare Center ensures IRC integration in support of IO and provide IO subject matter experts to the Joint Staff and the combatant commands (CCMD).

The Chairman of the Joint Chiefs of Staff (CJCS), as the principal military advisor to the President, Secretary of Defense, and the National Security Council, is responsible for developing and providing U.S. military policies, positions, and strategies that support DOD IO operational planning as part of the interagency process. CJCS IO functions include:

1. Validate capability based IO requirements through the Joint Requirements Oversight Council.

2. Develop and maintain joint doctrine for IO and IRC in joint operations.

3. Ensure all joint education, training, plans, and operations include, and are consistent with, IO policy, strategy, and doctrine.

The Deputy Director for Global Operations (J38) serves as the CJCS's focal point for IO and coordinates with the Joint Staff, CCMD, and other organizations that have direct or supporting IO responsibilities.

The Unified Command Plan provides guidance to CCDR and assigns missions and force structure as well as geographic or functional areas of responsibility (AORs). CCDRs integrate, plan, coordinate, and execute IO when conducting campaigns and identify and prioritize IO requirements. The CCDRs also integrate IO into appropriate security cooperation plans and activities.

In addition to these responsibilities, Commander, United States Special Operations Command is also responsible for integrating and coordinating MISO, including providing other CCDRs with MISO planning and execution capabilities. Commander, United States Strategic Command (CDRUSSTRATCOM) is responsible for acting as an advocate for joint electromagnetic spectrum operations (JEMSO), cyberspace operations (CO), and space operations. As the joint EW advocate, CDRUSSTRATCOM is focused on enhancing interoperability and providing other CCDRs with EW capabilities and expertise in support of their missions. As CO advocate, CDRUSSTRATCOM is responsible for synchronizing CO planning. CCDR's responsibilities include:

1. Plan, exercise, and conduct IO in support of national goals and objectives as directed by the Joint Strategic Capabilities Plan (JSCP).

2. Integrate capabilities into deliberate and crisis action planning to conduct IO in accordance with appropriate policy and doctrine to accomplish their Unified Command Plan-assigned missions.

3. Develop a process within the component command and joint task force (JTF) staffs that effectively integrates the various capabilities and activities to conduct IO.

4. Incorporate IO tactics, techniques, and procedures into exercises, modeling and simulation, and training events using the joint mission-essential task process.

5. Develop and support intelligence requirements information operations activities under all pertinent operational plans.

6. Develop, maintain, and prioritize IO requirements.

7. Incorporate IO into flexible deterrent options such as military exercises and shows of force.

Service component commanders derive responsibilities from their parent Service. These responsibilities include recommending to the JFC the proper employment of the Service IRC in support of joint IO. If deemed appropriate, the CCDR or JFC may also choose to conduct IO using Service component capabilities.

1. Develop IO doctrine and tactics and organize, train, and equip forces with capabilities to conduct IO. Ensure the Services' forces and planning capabilities effectively support the combatant commanders through the appropriate Service component commanders.

2. Conduct research, development, testing and evaluation, and procurement of capabilities that meet validated Service and joint IO requirements.

3. Incorporate IO into Service school curricula and into appropriate training and education activities.

Like Service component commands, functional component commands have authority over forces or—in the case of IO—IRC, as delegated by the establishing authority (normally a CCDR or JFC). Functional component commands may also be tasked to plan and execute IO as an integrated part of joint operations.

2.3.3 Legal Considerations for Information Operations

Military activities in the information environment, like all military operations, are conducted in accordance with law and policy. The conduct of IO often involves legal and policy questions requiring not just local review but often, national-level coordination and approval. The U.S. Constitution, U.S. legal codes, and international laws set boundaries and establish precedence for all military activity, to include IO. JP 3-13 provides further discussion of legal considerations in the conduct of joint IO.

The staff judge advocate should be involved in IO planning and execution. Legal considerations include, but are not limited to, an assessment of:

1. The different legal limitations placed on IO in peacetime, crisis, and conflict (to include war). Legal analysis of intended wartime targets requires traditional Law of War analysis.

2. The legal aspects of transitioning from defensive to offensive operations.

3. Special protection for international civil aviation, international banking, and cultural or historical property.

4. Actions that are expressly prohibited by international law or convention. Examples include, but are not limited to:

    a. Destruction resulting from space-based attack[1]

[1] Convention on International Liability for Damage Caused by Space Objects

b. Violation of a country's neutrality by an attack launched from a neutral nation[2]

c. MISO broadcasts from the sea, which may constitute unauthorized broadcasting[3].

2.4 EMPLOYMENT OF INFORMATION-RELATED CAPABILITIES

Information is how an organization develops situational awareness, makes decisions, and executes orders. Figure 2-1 depicts the adversary decision-making process through the IE and the effects of IRC upon it.

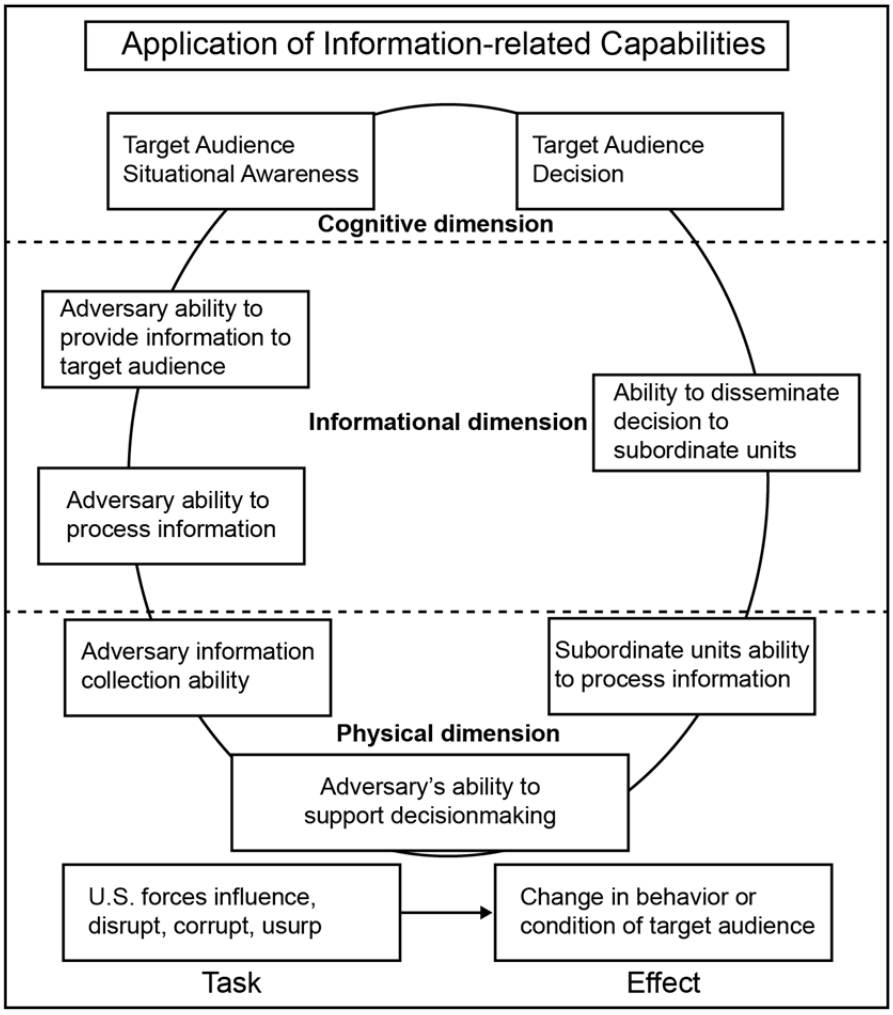


Figure 2-1. Applying Information-related Capabilities from Task to Effect

[2] Hague Convention V
[3] United Nations Convention on the Law of the Sea

2.4.1 Effects

An effect is the physical or behavioral state of a system that results from an action, a set of actions, or another effect. The success of the Navy force is defined by its ability to create the effects necessary to achieve military objectives, whether at the strategic, operational, or tactical levels. Commanders should clearly articulate the objectives or goals of a given military operation. Effects should then flow from objectives as a product of the military operations designed to help achieve those objectives.

Based on clear objectives, planners should design specific operations to achieve a desired outcome and then identify the optimum capability for achieving that outcome. There are second-order and third-order effects that should also be taken into consideration. Many of the variables in IO planning also have human dimensions that are difficult to measure, may not be directly observable, and for which it may be difficult to acquire feedback. At all times, planners should analyze effects from the point of view of the culture and social makeup of the country or location of upcoming operations. Information assessment is inherently challenging and has a lower degree of accuracy than conventional battle damage assessment. Nevertheless, the planning for IO should focus on operational objectives and the effects produced. Operational assessment allows the commander to evaluate IO and adjust specific information operations to evolving combat situations to increase its effectiveness.

Strategic effects can be created by a wide variety of military actions at all levels of war. IO can create effects at the strategic level and require coordination with other instruments of national power. In addition, tactical-level IO events have the potential to create strategic effects. Influence operations are often designed to affect a nation's leaders or population. Communications networks are often an integral part of national (strategic) infrastructure and may be vulnerable to attack. Those strategic vulnerabilities present in our adversaries may also be present at home. As a result, our strategic defense is highly dependent on the IRC that create information and maritime superiority.

IO at the strategic level of war is directed by the President or SecDef and is planned in coordination with other agencies or organizations outside the DOD. Such operations should be coordinated among supporting Navy units, the CCDR's IO team or cell, the JTF commander's IO team or cell, and other supporting components to ensure unity of effort and prevent conflict with ongoing operational-level efforts. Examples of how IO can achieve strategic effects include:

1. Promote durable relationships and partnerships to influence both friendly and adversarial behavior toward achieving national objectives.

2. Institute appropriate protective and defensive measures to ensure friendly forces can continuously conduct IO across the entire spectrum of conflict. Such measures create effects that deny adversaries knowledge of or the ability to access or disrupt friendly information operations.

3. Reduce adversary leadership resistance to U.S. national objectives by affecting their resolve or confidence.

4. Negatively impact an adversary's ability to lead by affecting their communications with their forces or their understanding of the operating environment.

5. Employ actions that reduce friendly vulnerabilities to physical and cyberspace attacks.

Operational-level effects can be created by a wide variety of military actions at all levels of war. The Service or functional component commander conducts IO within the assigned AOR or joint operation area. IO at this level uses military assets and capabilities to achieve operational effects through the design, organization, integration, and conduct of campaigns and major operations. IO plans between and among supported and supporting commands should be coordinated closely to prevent redundancy, mission degradation, and fratricide. Specific operational effects IO can achieve at this level may include:

1. Hindering an adversary's ability to strike by incapacitating their information systems and creating confusion

2. Slowing or stopping an adversary's operational tempo by causing hesitation, confusion, and misdirection

3. Reducing an adversary's command and control capability
4. Influencing adversary and neutral perceptions of leaders, military forces, and populations away from adversary objectives and toward U.S. objectives
5. Disrupting the adversary commander's ability to mass and synchronize combat power
6. Employing actions that reduce friendly vulnerabilities to physical and cyberspace attacks
7. Protecting forces during humanitarian assistance, disaster response, and noncombatant evacuation operations
8. Protecting friendly force C2 and information.

Tactical tasks are actions intended to create desired effects or preclude undesired effects supporting tactical objectives. The Navy or maritime component commander directs tactical IO execution. The primary focus of IO at the tactical level of war is to deny, degrade, deceive, disrupt, or destroy an adversary's use of information directly related to conducting military operations. Tactical IO includes protecting friendly information and information systems.

Figure 2-2 depicts three generic information tasks and possible effects and IRC used to achieve them.

2.4.2 Influence Target Audiences

A detailed understanding of adversary decision maker(s), planning, and integration with operations is required for conducting operations focused on affecting the perceptions and behaviors of leaders, groups, or populations. U.S. forces employ capabilities to affect behaviors, protect operations, communicate the commander's intent, and project accurate information to create desired effects across the cognitive dimension. Effects result in a change in behavior or a change in the adversary's decision cycle so that it aligns with the commander's objectives. The principal military capabilities to support accomplishment of influence objectives include MISO, MILDEC,

Task	Influence Target Audiences	Disrupt, Degrade Adversary Command and Control Systems	Protect Friendly Information and Information Systems
Effects	Inform and educate target audiences Influence adversary and neutral perceptions toward U.S. objectives	Exploit adversary C2 systems Disrupt adversary decision-making cycle Misdirect reconnaissance collection efforts	Assure own-force communications Deny friendly force intelligence to hostile collection
IRC	Commander's communications strategy Public affairs (PA) Engagement Military information support operations Civil-military operations Intelligence Counterintelligence	Lethal effects Electronic attack Electronic support Offensive cyberspace operations Intelligence Counterintelligence Military deception	Information assurance Electronic spectrum management Electronic protection Defensive cyberspace operations Operations security Physical security Intelligence Counterintelligence Emission control Information operations condition

Figure 2-2. Information Tasks, Effects, and Information-related Capabilities

OPSEC, counterintelligence, counterpropaganda, and public affairs. The commander's communication strategy (CCS) is one key to shaping influence operations.

Understanding the target audience is key to all influence endeavors. Logically, the first step in the influence process is to decide who or what to influence. The second step is to develop a detailed target audience analysis (TAA) that properly matches influence objectives.

The methodology to conduct TAA achieves four overarching objectives.

1. Precisely identify the optimal target audiences.

2. Measure the ability to influence an audience.

3. Identify the best process to influence that audience.

4. Produce and deploy the triggers that effectively and measurably impact the audience.

The TAA should construct a robust profile of the audience to determine how an appropriately conceived and developed message campaign can influence it. Because there is no universal model of communications applicable to all groups and cultures, tailor all communication efforts to the local dynamics with respect to the behaviors they are meant to change. Select and integrate the ways and means to achieve desired effects and influence objectives. Operations are executed and assessed to see if effects and objectives were met. Chapter 3 describes influence capabilities. See JP 3-13 for further discussion of the influence paradigm.

2.4.3 Disrupting or Degrading Adversary Command and Control Systems

The adversary force, like all organizations, relies on communications and information networks to make and implement decisions. Small cells can limit communications to face-to-face encounters and couriers; this is excellent OPSEC but limits the size and complexity of operations. Some adversaries mirror the way U.S. forces use the electromagnetic spectrum (EMS) and computer networks as the backbone of elaborate special-purpose military information architectures. Adversaries across the range of sophistication also use civilian telecommunications, particularly cell phones and the Internet, to gather intelligence, disseminate information, shape perceptions, and direct operations.

The integrated use of lethal effects, EW, and CO supported by intelligence disrupt and exploit adversary C2. The fires cell synchronizes physical attack, electronic attack (EA), and offensive cyberspace operations (OCO) against adversary C2.

2.4.4 Protect Friendly Information and Information Systems

Information and information systems protection includes active and passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information to support command and control of Navy forces. It denies enemies the opportunity to exploit friendly information and information systems for their own purposes. The secure and uninterrupted flow of data and information allows Navy forces to multiply their combat power and synchronize maritime power projection with other joint capabilities. Numerous threats to that capability exist in the operational environment. Information protection includes information assurance (IA), defensive cyberspace operations (DCO), electronic protection (EP), OPSEC, physical security, and intelligence. All these capabilities are interrelated and integrated to protect information and information systems.

INTENTIONALLY BLANK

CHAPTER 3

Information-Related Capabilities

3.1 OVERVIEW

Older definitions of IO focused heavily on a set list of core capabilities. This led to stovepipe thinking and weakened the integrating effect. As SecDef Memo 12401-10, Strategic Communication and Information Operations in the DOD, explains, "successful IO requires the identification of IRC most likely to achieve desired effects and not simply the employment of a capability. Modifying the definition also effects a needed change to the existing notion that the core capabilities must be overseen by one entity. Capability integration does not necessitate ownership."

An IRC can be effective as part of an operation if it can answer the question "Why did you do that?" with a specific effect or a military advantage that helps achieve the commander's goal and supports movement towards mission success and a desired end state.

3.2 DESCRIPTION OF INFORMATION-RELATED CAPABILITIES

An IRC is defined as a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions (JP 1-02). Planners may find the following list useful to identify traditional IRC but it should not limit one's vision of possible resources.

1. Core capabilities (including the original "five pillars")
    a. EW
    b. Cyberspace operations
    c. MISO
    d. MILDEC
    e. OPSEC
    f. PA
    g. Civil-military operations (CMO)
    h. Defense support to public diplomacy
    i. Physical (lethal) attack
    j. IA
    k. Physical security
    l. Combat camera (visual information)

m. Intelligence

n. Counterintelligence.

JP 3-13 lists the following examples of IO capabilities integrated in joint IO.

1. Strategic communication (SC), discussed in paragraph 3.2.1.
2. Joint interagency coordination group. As a capability, this allows joint commanders to interface with organizations across the diplomatic, informational, military, and economic spectrum, including other U.S. Government (USG) departments, other governments, private sector entities, and nongovernmental organizations.
3. PA, discussed in paragraph 3.2.2.
4. CMO.
5. CO, discussed in paragraph 3.2.3.
6. IA.
7. Space operations.
8. MISO, discussed in paragraph 3.2.5.
9. Intelligence.
10. MILDEC, discussed in paragraph 3.2.6.
11. OPSEC.
12. Special technical operations (STO).
13. JEMSO, which are EW and joint EMS management operations used to exploit, attack, protect, and manage the electromagnetic (EM) operational environment to achieve the commander's objectives. Traditional EW terminology best describes Navy operations, but the JEMSO construct may be more useful to operational-level planners.
14. Key leader engagement.

Within the Navy, the Information Dominance Corps has extended the IRC concept across the functions of intelligence (N2), assured C2, and meteorology and oceanography. The Center for Naval Analyses study, Structures for Information Operations Warfare Commander and Information Dominance Afloat (September 2013), examines existing models of conducting IO and the impact of adopting an information dominance warfare model. This NWP does not endorse the study's recommendations but encourages further debate and a broad vision of how the Navy integrates and employs available IRC to best satisfy mission requirements.

Recent DOD IO policy and doctrine (Secretary of Defense Memo 12401-10, JP 3-13, and DOD Directive 3600.01) stress influence at the strategic and operational levels as the focus of IO. Navy doctrine has typically emphasized the disrupt, corrupt, or usurp tactical information superiority aspects of IO as well as the protect functions. As an integrating function, IO should embrace information's impact on operations as a whole and not stress a single aspect at the cost of another. Navy planners should make IRC choices based on their echelon, mission, and available capabilities—not on a preconceived checklist.

3.2.1 Strategic Communication and Commander's Communication Strategy

Strategic communication is focused Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.

SC is a national strategic-level initiative of the USG under the auspices of the Department of State. The Joint Staff director of communication provides SC guidance to the CCMD via different products, such as guidance for development of the theater campaign plan, JSCP tasking, or a warning order (WARNORD), that specifically directs crisis action planning. These products facilitate planning during the initiation phase in the joint operation planning process (JOPP). (JOPP is covered in chapter 5.) Navy commanders synchronize maritime operations toward a unified action supporting SC.

Although lethal weapons can create significant influence effects, IRC—such as PA, MISO, and defense support to public diplomacy—can prove invaluable to inform and influence.

The CCDR develops a theater campaign plan containing theater security cooperation guidance, which should include long-term information objectives during phase 0 operations throughout the AOR.

A JFC develops a CCS based on the SC guidance, narratives, themes, and messages. CCS is a commander's strategy for coordinating and synchronizing themes, messages, images, and actions to support strategic communication-related objectives and ensure the integrity and consistency of themes and messages to the lowest tactical level through integrating all relevant communication activities.

In support of the JFC strategy, Navy planners conduct detailed mission analysis and operational-level planning to develop a maritime strategy that describes the Navy role in the overarching plan. Using the maritime operations center (MOC) construct of cross-functional team (CFT), missions are developed across the three planning horizons—future plans, future operations, and current operations—to fully integrate IRC.

A recent example of the Navy's successful employment of CCS was evidenced during Operation UNIFIED RESPONSE following the 2010 Haiti earthquake. As part of the plan to contribute to UNIFIED RESPONSE, each afloat unit embarked Navy PA professionals to provide near-real-time coordination while underscoring the critical role the sea service played in providing humanitarian assistance and disaster relief. Although not a combat operation, the effect was significant in achieving broader strategic objectives and building international consensus to the relief effort.

3.2.2 Public Affairs

PA is directed toward the external and internal public with interest in the DOD. PA conducts three basic functions: public information, command information, and community engagement activities. These functions support the commander's intent and concept of operations (CONOPS). PA performs a primary coordination role of public information in the military.

PA supports Navy operations by communicating factual and accurate unclassified information about military activities to various audiences. The timely release of official information aids in the pursuit of unified action while bolstering public support. Credible, well-timed information can mitigate the impact of an adversary's efforts. PA personnel at all levels offer invaluable advice to leaders on the possible outcomes of military actions, identify the potential impact on the public information realm, and serve as key resources to assess achieving desired effects. For more information on PA, refer to JP 3-61, Public Affairs.

3.2.3 Cyberspace Operations

Cyberspace is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks,

computer systems, and embedded processors and controllers. CO is the employment of cyberspace capabilities in which the primary purpose is to achieve objectives in or through cyberspace. A cyberspace capability is a device, computer program, or technique—including any combination of software, firmware, or hardware—designed to create an effect in cyberspace.

3.2.3.1 Cyberspace Domain and Information Environment

Cyberspace crosses geographic and geopolitical boundaries. Much of it resides outside U.S. control and it is tightly integrated with the operation of national critical infrastructures and key assets as well as with the conduct of commerce, governance, and national security. CO integrates with other capabilities to gain and protect an operational advantage and to place adversaries at a disadvantage. The Navy needs assured security within its networks. Commanders seek to gain and retain the degree of freedom of action in cyberspace that is required at a particular place and time to accomplish mission objectives, yet still deny the same freedom to adversaries. Commanders should also be prepared to operate in a degraded or denied cyberspace.

3.2.3.2 Cyberspace Functional Operations

United States Strategic Command (USSTRATCOM), United States Cyber Command (USCYBERCOM), and Fleet Cyber Command (FLTCYBERCOM)/Commander, 10th Fleet (COMTENTHFLT) plan, coordinate, synchronize, and conduct activities to direct operations and defense of specified DOD networks. They also prepare for and conduct military operations in support of the JFC's mission. Timely intelligence and threat indicators from traditional and advanced sensors, vulnerability information from DOD and non-DOD sources, and accurate assessment inform CO missions.

CO includes OCO, DCO, and DOD information network operations. The successful execution of CO requires the synchronized employment of offensive and defensive capabilities underpinned by effective and timely operational preparation of the environment and secure operation of supporting data networks.

DOD information network operations include the employment of manual and automated methods to preserve and sustain the availability, confidentiality, integrity, and nonrepudiation of military information networks. They are actions taken to design, build, secure, operate, maintain, and sustain DOD networks. These include proactive actions that address the entire DOD information network, including such actions as configuration control and patching, IA measures, user training, physical security and secure architecture design, operation of host-based security systems and firewalls, and encryption of data at rest. The U.S. military reliance on cyberspace is well understood by adversaries. For that reason, JFC planning to ensure resiliency in the face of cyberspace threats is essential.

OCO is categorized as the employment of cyberspace operations to support the JFC operational requirements and the defense of DOD networks. OCO conduct activities that actively gather information, manipulate, disrupt, deny, degrade, or destroy computers, information systems, or networks through cyberspace.

Support operations involve forces and actions required to operate, sustain, and secure the DOD information network as well as cyberspace activities that support all military operations. Support operations do not include DCO in response to specific threats directed at the DOD information network but rather those that constitute steady-state IA to establish and operate secure networks. For additional information, see JP 3-12, Cyberspace Operations.

3.2.3.3 Command and Control of Cyberspace Operations

CO requires a coordinated effort to synchronize forces toward a common objective. The C2 structure simultaneously supports actions at the theater or joint operations area level and at the global level. Global CO should be integrated and synchronized with capabilities under control of the JFC. Command and control of forces that conduct most CO activities, as defined by the execute order, authorizes actions based on threats that meet particular conditions and triggers (executed either manually or automatically); the nature of the threat requires an

immediate response. These conditions are addressed by the campaign/operation plans that include DCO, OCO, and DOD information network operations. The affected CCDR is the supported commander for CO in their AOR.

A secure, resilient, and flexible C2 architecture enables commanders to maintain unity of effort in employment of their forces at the critical times and places. CO requires coordination of theater operations with global operations, creating a dynamic supported/supporting C2 arrangement. The supported commander integrates CO into specific joint operations, campaign plans and CONOPS, operation plans (OPLANs), and operation orders. C2 of DOD information network operations and DCO may require predetermined and preauthorized actions based on meeting particular conditions and triggers.

The Navy likely enters a conflict as part of a joint or combined task force, not as a single-Service force. The specific C2 elements the JFC selects depends on the type and scale of operation, the cyberspace presence or sophistication of the adversary, and the types of cyberspace targets identified.

CO planners face the same considerations and challenges that are present in planning for military operations as well as some unique considerations. A full understanding of an adversary's posture and capabilities in cyberspace involves not only understanding the underlying network infrastructure but also requires profiles on system users and administers a clear understanding of what friendly forces and capabilities might be targeted and how and an understanding of applicable domestic, foreign, and international laws and policy. CO planners use JOPP to implement the JFC's guidance and intent.

Targeting is included in the coordination of CO. Targeting integrates and synchronizes fires within joint operations through the process of selecting and prioritizing desired effects and matching the appropriate capabilities to those effects, given operational requirements and limitations; targeting links the desired effects of fires to specific tasks at the joint force component level. Planners should specify the scope, level, start time, and duration of the desired effects. Targets are selected from the three components of cyberspace, including physical network, logical network, and cyber-persona. The process identifies and coordinates multiple activities across multiple components.

Cyberspace capabilities operate and create effects within cyberspace. They may be as simple as the type of computer operating system being used by an adversary or as complex as the exact serial number of the latest update installed, what system resources are available, or what other applications are expected to be running (or not running) when the cyberspace capability executes on target. CO planners work with the supported command to identify, validate, and vet targets for OCO and enabling operations. Using available all-source analysis and the JFC's normal targeting processes, the targeting staffs develop and maintain the joint integrated prioritized target list and supporting documents.

CO capabilities are typically integrated with the commander's other capabilities to gain the advantage, to protect and maintain that advantage, and to place adversaries at a disadvantage. Commanders seek to gain and retain the degree of freedom of action in cyberspace required at a particular place and time to accomplish mission objectives, yet deny the same to adversaries. They are also prepared to operate in a degraded or denied cyberspace.

3.2.4 Electronic Warfare

EW is military action involving the use of EM and directed energy to control the EMS or to attack the enemy. EW consists of three divisions: EA, EP, and electronic warfare support (ES). Figure 3-1 provides an overview, and the following sections describe the specific functional areas of EW.

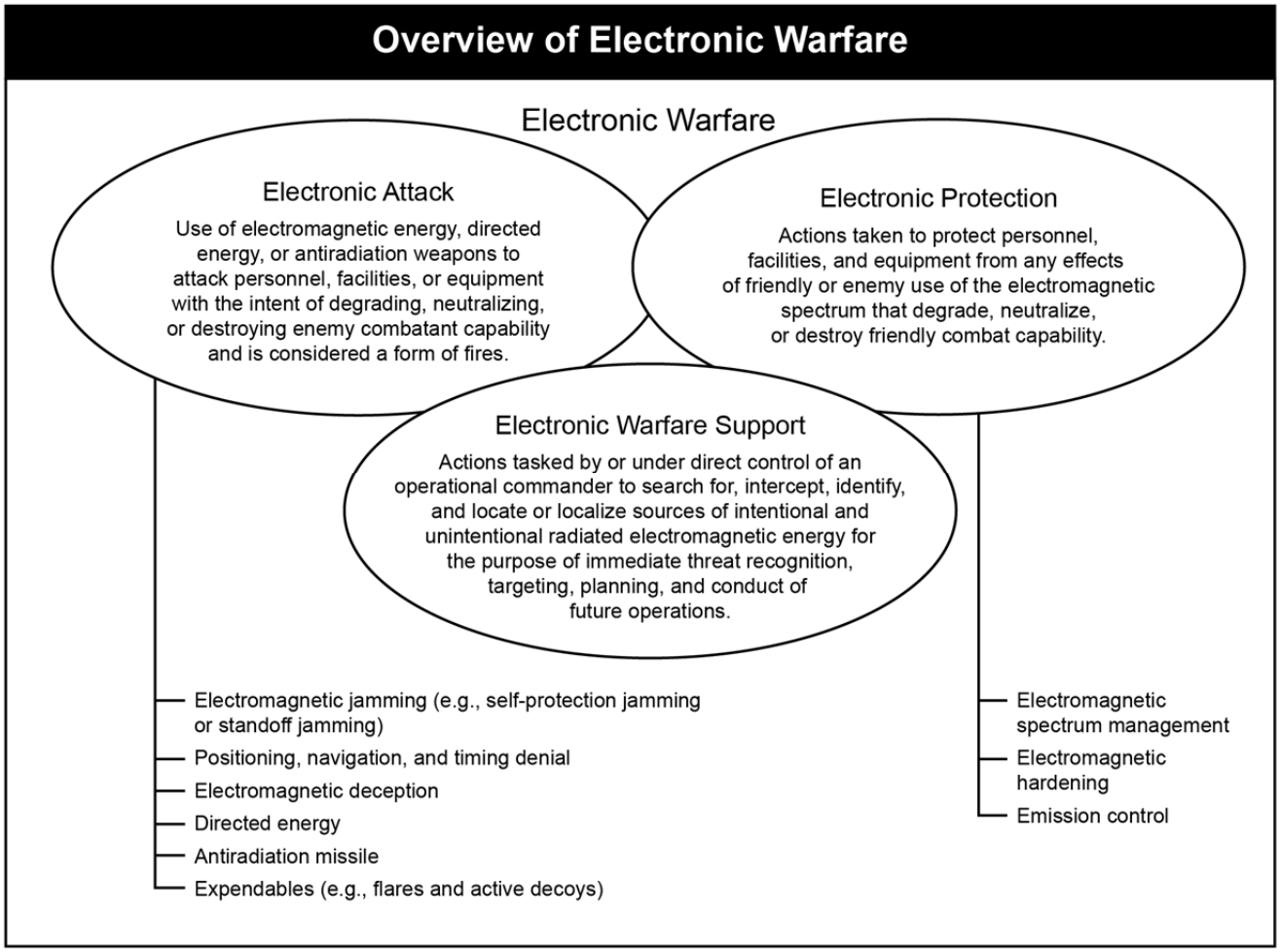


Figure 3-1. Overview of Electronic Warfare

3.2.4.1 Electronic Warfare Support

ES involves actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, threat avoidance, targeting, planning, and conduct of future operations. ES responds to and supports immediate operational requirements. ES is the Navy's most powerful tool to assess the EM environment for timely information vital to mission success.

ES and signals intelligence (SIGINT) often share the same or similar assets and resources and may be tasked simultaneously to collect information that meets both requirements. Under certain circumstances, data collected for intelligence may meet immediate operational requirements. Information collected for ES purposes is normally also processed by the appropriate parts of the intelligence community for further exploitation after the operational commander's ES requirements are met. As such, information collected from the EMS may serve two purposes: as ES, unprocessed information used by operational forces to develop and maintain situational awareness for an operationally defined timeframe or particular campaign phase; as SIGINT, retained and processed under appropriate intelligence authorities in response to specified intelligence requirements. In cases in which planned ES operations conflict with intelligence collection efforts, the commander with tasking authority (i.e., JFC, joint force maritime component commander (JFMCC), or tactical commander) decides which mission has priority.

3.2.4.2 Electronic Protection

EP involves actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, or enemy use of the EMS as well as natural phenomena that degrade, neutralize, or destroy friendly combat capability. EP focuses on system or process attributes or capabilities. Inherent hardware features minimize the impact of unplanned or undesired EM signals on an EM-dependent system's operation. EP processes are designed to eliminate, reduce, or mitigate the impact of the same unplanned or undesired EM signals. These features and processes combine to allow friendly capabilities to function as intended in contested and congested EM operating environments.

EP includes actions taken to ensure friendly use of the EMS, to include:

1. Frequency agility in a radio
2. Variable pulse repetition frequency in radar
3. Receiver/signal processing
4. Spread spectrum technology
5. Spectrum management processes
6. Frequency coordination measures (e.g., joint restricted frequency list)
7. Global Positioning System antijam measures
8. Selective opacity (i.e., the phenomenon of not permitting the passage of EM radiation) of optical apertures
9. Emission control (EMCON) procedures
10. Wartime reserve modes.

EP is not force protection or self-protection. EP is use of EM energy or physical properties to preserve an EMS-dependent system from direct or environmental EM effects, thereby allowing the system to continue operating against both enemy EA and friendly EM interference. For example, a platform may deploy a decoy (flare, chaff, or active radio frequency) to misdirect an incoming missile. This is EA, since the decoy attacks the missile's ability to use the EMS to reach the intended target. If a missile's guidance system employs flare rejection or chaff discrimination logic or operates radar outside the frequency range of active decoys, those are examples of EP as they ensure the missile's use of the EMS. Although defensive EA actions and EP protect personnel, facilities, capabilities, and equipment, EP protects from the effects of EA (friendly or adversary) or electromagnetic interference, while defensive EA is primarily used to protect against lethal attacks by denying adversary use of the EMS to target, guide, or trigger weapons.

3.2.4.3 Electronic Attack

Electronic attack refers to the division of EW involving the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (see JP 3-09, Joint Fire Support). EA includes actions taken to prevent or reduce an enemy's effective use of the EMS through employment of systems or weapons that use EM energy (e.g., jamming in the form of EM disruption, degradation, denial, and deception). EA includes both active EA, in which EA systems or weapons radiate in the EMS, as well as passive EA (nonradiating/re-radiating) such as chaff. It also includes employment of systems or weapons that use radiated EM energy (to include directed energy) as their primary disruptive or destructive mechanism. Examples include lasers, electro-optical, infrared, and radio frequency weapons such as high-power microwave or those employing an electromagnetic pulse.

3.2.4.4 Electromagnetic Battle Management

Electromagnetic battle management (EMBM) is the dynamic monitoring, assessing, planning, and directing of JEMSO in support of the commander's scheme of maneuver. EMBM proactively harnesses multiple platforms and diverse capabilities into a networked and cohesive sensor/decision/target/engagement system and protects friendly use of the EMS while strategically denying benefits to the adversary.

Once a plan is approved and an operation is under way, the preponderance of EW staff effort shifts to EMBM. EMBM includes continuous monitoring of the EM operating environment, EMS management, and dynamic reallocation of EW assets based on emerging operational issues. Normally, personnel on watch in the joint operations center perform this monitoring. These watch personnel, stationed at a dedicated EW watch station, are normally tasked to alert other EW or staff personnel to carry out specific coordinating actions, including preplanned responses consistent with established rules of engagement. For more information about EW, refer to JP 3-13.1, Electronic Warfare, and NTTP 3-51.1, Navy Electronic Warfare.

3.2.5 Military Information Support Operations

MISO are planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, and individuals in a manner favorable to the originator's objectives. Specifically trained Service members conduct these operations.

MISO plays a fundamental role in a commander's communication efforts through the planned use of directed programs specifically designed to support USG and DOD activities and policies. MISO practitioners follow a deliberate process that: 1) aligns a commander's objectives with an analysis of the environment; 2) selects a relevant target audience and develops focused, culturally and environmentally attuned messages and actions; 3) employs sophisticated media delivery means; and 4) produces observable, measurable behavioral responses. When viewed as part of a joint operation, MISO provides fundamental capability sets to support campaign objectives through appropriate planning and execution of component tactical actions.

There is a basic distinction between psychological impact and MISO. Military actions, such as strikes or shows of force, have a psychological impact; however, they are differentiated from MISO unless their specified purpose is to influence a target audience's perceptions and subsequent behavior.

MISO, in conjunction with SC and PA, establish and reinforce foreign perceptions of U.S. military, political, and economic power and resolve. In conflict, MISO can degrade the enemy's relative combat power, reduce civilian interference, minimize collateral damage, and maximize local support for operations.

The principal considerations for effective MISO employment include early planning and sustained employment; integration of MISO with the communication strategies of the USG and multinational partners; use of indigenous assets, command emphasis, and resourcing; responsive MISO approval process; and quantifiable and timely assessment criteria.

At the operational level, MISO plays a central role in achieving the commander's information objectives by shaping, inducing, or influencing an adversary's attitudes and behavior. The CCDR's or component commander's J39 staff section is the nexus of IO synchronization in plan development and assessment.

From a maritime perspective, the MOC IO cell identifies and draws on available dissemination assets, product reproduction capabilities, and planning resources. The IO cell collaborates with joint MISO experts, civil affairs representatives and, in some cases, State Department representatives to identify maritime audiences, develop themes and products, and plan dissemination.

PA and MISO activities are separate and distinct functions that support and reinforce one another. Doing so requires coordination and synchronization. Commanders ensure that appropriate coordination between MISO and PA activities is consistent with DOD principles of information, policy or statutory limitation, and security.

The following factors should be considered when synchronizing strategic communication, communication strategy, PA, and IO:

1. Unity of effort among disparate communities

2. Maintain good situational awareness among stakeholders

3. Coordinate activities to avoid or mitigate unintended consequences.

For more information on MISO, refer to JP 3-13.2.

3.2.6 Military Deception

MILDEC is the collective term for actions intended to mislead adversary decision makers, thereby causing the adversary to take specific actions or inactions that contribute to the accomplishment of the friendly mission. MILDEC may be employed at the strategic, operational, or tactical levels; can be incorporated into a supported or supporting operation; and can be performed in every phase of military operations. When successfully executed, MILDEC is invaluable in saving lives and resources and can expedite the end of hostilities.

MILDEC targets enemy decision makers. MILDEC goals and objectives contribute to the success of the commander's mission. The deception objective is a concise statement of what the MILDEC causes the adversary to do or not do. It is expressed in terms of the adversary's action or inaction, which directly leads to the purpose or condition stated in the MILDEC goal. The deception target is the adversary decision maker with the authority to make the decision that achieves the deception objective to reinforce or change their behavior in our favor.

Successful MILDEC execution includes thorough planning and attention to detail. In addition to a detailed series of event coordination, a detailed knowledge of the adversary's decision makers and their authorities, behaviors (expected reactions), and tactics is critical. To conduct a MILDEC operation, planners develop:

1. Deception mission analysis

2. Deception planning guidance

3. Staff deception estimate

4. Commander's deception estimate

5. CJCS estimate review, if required

6. Deception plan development

7. Deception plan review and approval.

Deception event sequence, synchronization, and timing must work in concert so the adversary has the time to observe, analyze, and decide on a course of action (COA) based on those observations. Six principles provide guidance for planning and executing MILDEC.

1. Focus. The deception must target the adversary decision maker capable of causing the desired action or inaction.

2. Objective. To shape a decision maker's perception, causing the adversary to take (or not take) specific actions.

3. Centralized planning and control. More than in many other military activities, MILDEC should be centrally planned and directed. Consistency is crucial to success.

4. Security. Deny adversary's knowledge of a force's intent to deceive and execution of that intent.

5. Timeliness. A deception operation requires careful timing.
6. Integration. Fully integrate each MILDEC with the operation it supports.

MILDEC can achieve different objectives in support of the desired ends.

1. Mask friendly maneuver
2. Reinforce enemy perception of friendly strengths, weaknesses, and intentions
3. Distract the enemy
4. Overwhelm adversary intelligence collection and analysis capabilities
5. Disrupt their decision-making process (render adversaries unable to decide or force a quick response)
6. Create false appearances of friendly capabilities (strengths/weaknesses)
7. Force an unanticipated maneuver/reaction
8. Force the adversary to cancel a planned action
9. Confuse the enemy as to your force strength, activity, location, timeline, equipment, or intent
10. Disrupt your enemy's ability to synchronize or coordinate a counterattack
11. Demoralize the enemy
12. Increase your enemy's proverbial fog of war
13. Achieve surprise.

The MOC IO cell includes a MILDEC planner who is responsible for incorporating MILDEC into operational-level plans.

CHAPTER 4

Information Operations Organizational Relationships and Forces

4.1 ADMINISTRATIVE AND OPERATIONAL RELATIONSHIPS

Navy forces typically operate under a component commander or joint task force commander as assigned/attached to a CCDR or a subordinate JFC. A JFC uses the concept of unified actions—the synchronization, coordination, and/or integration of activities of Governmental and nongovernmental entities with military operations to achieve unity of effort—to apply all of the instruments of national power (diplomatic, information, military, and economic) to affect adversary capabilities and behavior.

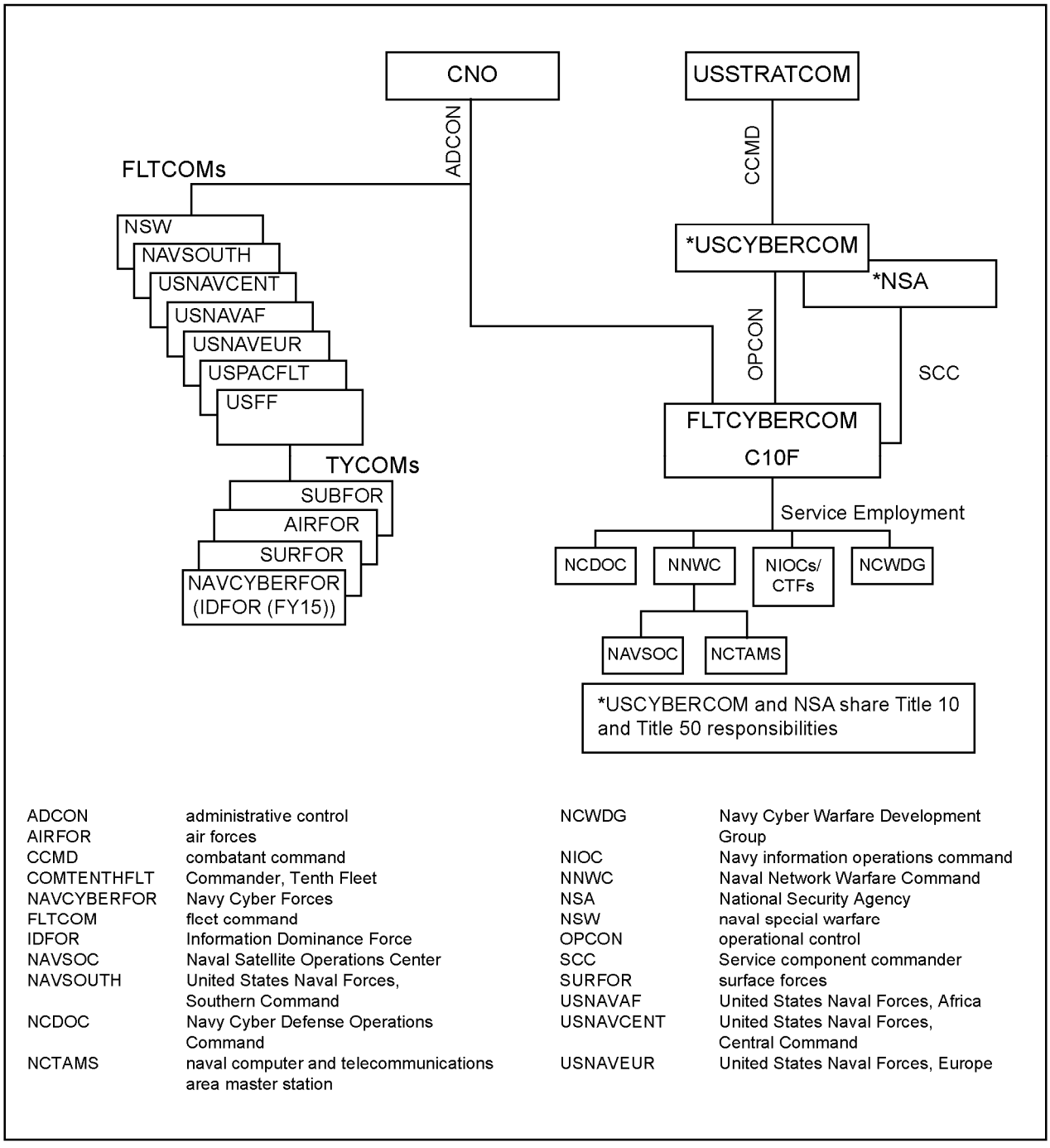
Force providers organize, man, train, and equip Navy forces so that they are ready to deliver IRC to achieve desired effects and attain a commander's objectives. They are assigned to force employers who determine IO objectives to support the commander's plan and plan, integrate, and employ IRC to achieve desired effects and objectives in joint operations. Navy commanders perform C2 functions for all roles of warfare. At the operational level, Navy component commanders (NCCs) or numbered fleet commanders (NFCs) command assigned forces and carry out C2 functions through the MOC to dynamically plan, direct, monitor, and assess operations. The MOC IO cell plans, integrates, and coordinates the employment of IRC.

4.1.1 U.S. Fleet Forces Command and U.S. Pacific Fleet

Administratively, NFCs, United States Fleet Forces Command (USFF), and United States Pacific Fleet (USPACFLT) serve as the Navy component command to CCDR. USFF supports both the CNO and CCDR worldwide. USFF also provides responsive, relevant, sustainable Navy forces that are ready for tasking to United States Northern Command through Commander, Task Force EIGHT ZERO. The command provides operational and planning support to CCMD and integrated warfighter capability requirements to the CNO.

In collaboration with USPACFLT, USFF organizes, mans, trains, maintains, and equips Navy forces; develops and submits budgets; and executes readiness and personnel accounts to develop required and sustainable levels of fleet readiness. Additionally, USFF serves as the unified voice for fleet training requirements and policies to generate combat-ready Navy forces per the fleet response plan using the fleet training continuum (FTC).

Navy forces proceed through the basic and integrated training phases of the fleet response training program. USFF and its subordinates provide the training means and coordinate with Commander, Navy Cyber Forces (NCF) and other type commanders (TYCOMs) to train and assess the readiness of personnel and forces to deploy ready to employ their IRC to achieve desired effects. Figure 4-1 illustrates the alignment of Navy IO organizations.



ADCON	administrative control	NCWDG	Navy Cyber Warfare Development Group
AIRFOR	air forces	NIOC	Navy information operations command
CCMD	combatant command	NNWC	Naval Network Warfare Command
COMTENTHFLT	Commander, Tenth Fleet	NSA	National Security Agency
NAVCYBERFOR	Navy Cyber Forces	NSW	naval special warfare
FLTCOM	fleet command	OPCON	operational control
IDFOR	Information Dominance Force	SCC	Service component commander
NAVSOC	Naval Satellite Operations Center	SURFOR	surface forces
NAVSOUTH	United States Naval Forces, Southern Command	USNAVAF	United States Naval Forces, Africa
NCDOC	Navy Cyber Defense Operations Command	USNAVCENT	United States Naval Forces, Central Command
NCTAMS	naval computer and telecommunications area master station	USNAVEUR	United States Naval Forces, Europe

Figure 4-1. Navy Administrative and Operational Alignment

4.1.2 U.S. Fleet Cyber Command/U.S. Tenth Fleet

FLTCYBERCOM is an echelon II command and reports as the Navy component command to USSTRATCOM and USCYBERCOM. USCYBERCOM and the National Security Agency (NSA) are commanded by the same person, which helps in coordinating Title 10 and Title 50, War and National Defense, responsibilities and authorities. Navy operational cyberspace forces are assigned to the echelon III COMTENTHFLT, who is dual-hatted as Commander, FLTCYBERCOM. Several organizations are operationally assigned to COMTENTHFLT: Navy Cyber Defense Operations Command, Navy Network Warfare Command, Navy information operations commands (NIOCs), Navy Cyber Warfare Development Group, Naval Satellite Operations Center, and naval computer and telecommunications area master stations.

FLTCYBERCOM serves as the central operating authority for Navy networks, SIGINT, IO, EW, and space capabilities in support of forces afloat and ashore. It directs Navy CO globally to deter and defeat aggression and ensures freedom of action to achieve military objectives in and through cyberspace. As COMTENTHFLT, the command provides operational support to Navy commanders worldwide supporting information and computer, EW, and space operations. In addition to joint and Service reporting, the command also serves as the Navy's Service Cryptologic Element, reporting to the Central Security Service.

4.1.3 Navy Cyber Forces Command

Type commanders man, train, and equip their assigned forces. Both USFF and USPACFLT have air, surface, and subsurface TYCOMs. NCF is the TYCOM for afloat Navy cyber forces and is assigned under USFF and supports USPACFLT. NCF has subordinate and supporting commands that assist in the scheduling, planning, and execution of requisite cyberspace training. NCF works closely with the air, surface, and subsurface TYCOMs who own the platforms to monitor and ensure that assigned units are properly manned for operational readiness. They coordinate with the Bureau of Naval Personnel to ensure manning levels are met. NCF further monitors the material readiness of their assigned forces. They coordinate with maintenance facilities and other technical support to maintain the material readiness of all equipment/assets in the highest state of readiness. Training is critical for the readiness and ability of forces to employ IO capabilities. As the complexity of the equipment and the sophistication of tactics continue to rise, the need for maximum effectiveness in the use of that equipment mandates thoroughly trained operators who are prepared to respond when needed.

These organizations carry out a number of supporting tasks important to the Navy force ability to accomplish assigned tasks and missions. The tactics for all IRC should be developed and exercised to effectively deliver the right capability at the right time and place to achieve the desired results. Extensive intelligence and targeting support should also be carried out and integrated into the FTC so Navy forces are fully ready to employ their IRC when they report for duty.

4.2 COMMAND AND CONTROL STRUCTURE FOR INFORMATION OPERATIONS

At the operational level, NCC and NFC provide maritime capabilities in support of the CCDR and JFCs. Figure 4-2 provides the organizational alignment for the numbered fleets and the combatant commands.

The NFC prepares IO plans to protect the information grids, shape the operating environment, and exploit adversary vulnerabilities. The NFC employs tactical assets in the form of a carrier strike group (CSG), amphibious ready group (ARG), or independent units within the theater. These assets shape the theater in support of the unified combatant commander's theater campaign plan (TCP) and provide IO support to joint planning and operations.

COMTENTHFLT provides manning and equipment augmentation and reachback support to the NFC and their forces to support the effective employment of IRC for the assigned missions and tasks. COMTENTHFLT ensures coordination with intelligence activities and IO to protect the information and information systems to support Navy forces and the ability to employ IRC.

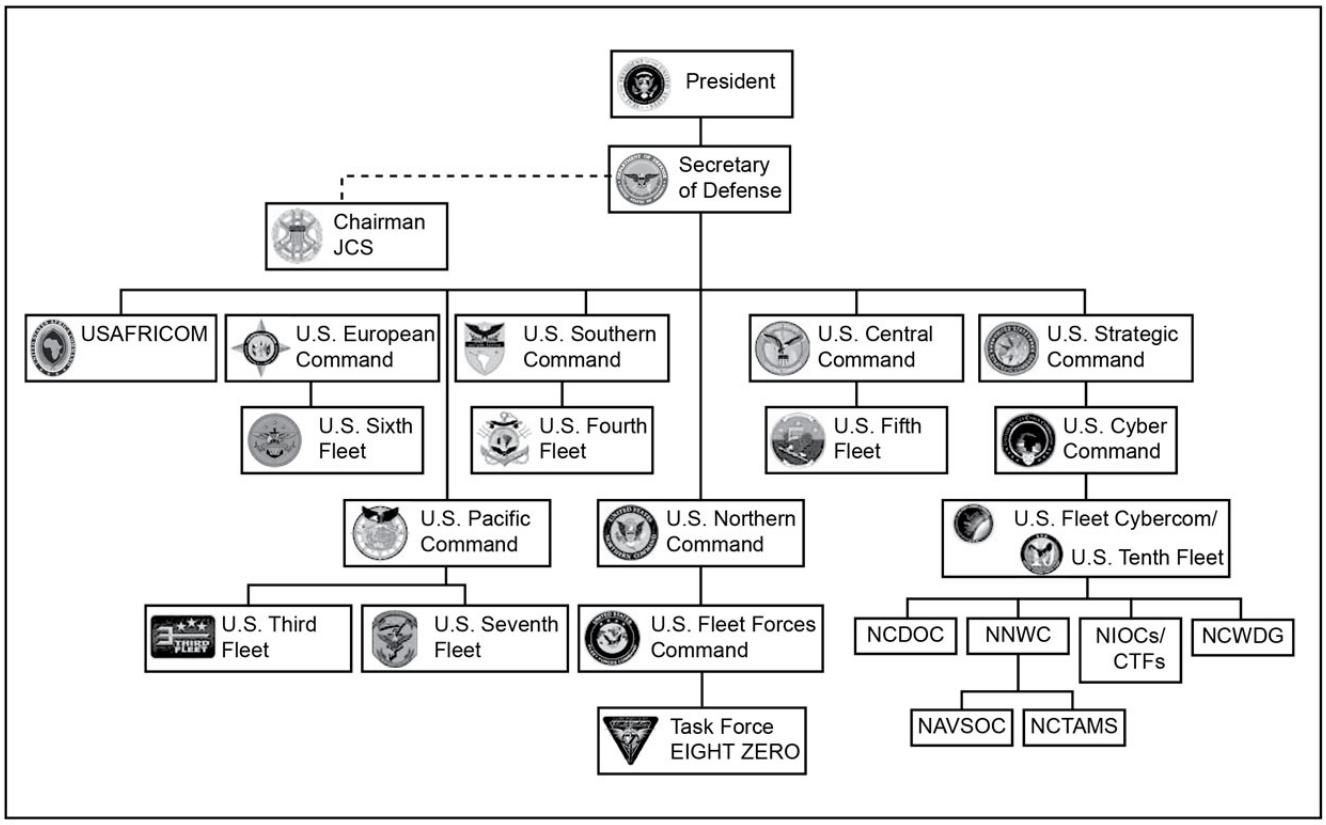


Figure 4-2. Organizational Alignment for Numbered Fleets and Combatant Commands

4.3 INFORMATION OPERATIONS COMMAND AND CONTROL ROLES AND RELATIONSHIPS

In consultation with subordinate commanders, the NFC/NCC determines the IRC/forces necessary to meet operational requirements. The NFC/NCC's daily guidance and event-based campaign plan drive these requirements. The IO cell integrates, coordinates, synchronizes, and deconflicts the use of IRC to support actions to achieve desired effects in support of the commander's plan. IO planners task available forces/capabilities in support of the plan. The intent is that IRC be apportioned to accomplish the tasks and objectives in support of the maritime commander's plan. Capabilities not required by the Navy component are made available for tasking by the JTF to support the JFC's mission and campaign plan.

In peacetime, the major command (such as USFF) or the numbered fleet MOC has a standing IO staff, typically designated N39, along with an IO cell staffed across disciplines as required by operations to plan IO and coordinate IRC. The MOC IO cell integrates into the structure within the MOC. The IO cell provides the IO expertise to plan, employ, and assess IO and employs IRC prior to the initiation of hostilities, transition to conflict, and reconstitution. The JFMCC IO cell has representation as appropriate within each planning cell throughout the MOC.

During peacetime, the MOC coordinates (when tasked) with Service-, joint-, and national-level organizations to plan and achieve effects to deter or, if deterrence fails, influence, shape, and prepare the operating environment for effective follow-on maritime operations. To maintain proper expertise, the N39/IO cell also trains and exercises to support the MOC's wartime missions. In addition, N39 develops and reviews the IO portion of operational plans and uses existing intelligence analysis to support peacetime operations through transition to conflict while maintaining close working relationships with external IO-related activities. Successful military operations carefully integrate all IRC to support the commander's objectives and plans. The N39/IO cell chief considers the use of all IRC to support other lines of operation as well as IO as a line of operation when appropriate.

During the transition to conflict, reconstitution phases of a campaign plan, and upon full activation of the MOC, the N39/IO cell provides the Navy's key IO expertise. The MOC typically is the main organizational structure through which the full set of IRC are integrated and synchronized through IO. Based on the commander's direction and guidance, the N39/IO cell supports the design and execution of portions of the campaign that use IO and the IRC to accomplish the commander's objectives. The IO team's primary focus is to plan and integrate IRC into the commander's maritime operation plan (OPLAN) and is closely associated with STO.

IO cell members within the MOC integrate IO planning, execution, coordination, targeting, monitoring, adjustment, and assessment. They work within the MOC organization to develop rules of engagement (ROE) necessary to support IO and fuse target nominations into attack plans and tasking orders. The IO cell should ensure the ROE and IO operating requirements and authorizations are considered. The IO cell should coordinate IO-specific intelligence requests and requirements with the N2. The fusion of the IO cell's disciplines into the MOC promotes timely integration of IRC with other force options into maritime operations and the air tasking order (ATO) planning and execution processes.

4.3.1 Numbered Fleet Commander

The IO coordination and integration process for the Navy, Service, or functional component commander or a NFC serving as a JTF commander may include:

1. The JFC develops theater campaign objectives and normally designates a joint force IO officer for broad IO oversight functions. When designated, the joint force IO officer heads the JFC J39/IO cell.

2. The JFC IO team (composed of select representatives from each staff element, Service component, and supporting agencies responsible for integrating the capabilities and disciplines of IO) develops IO options in support of JFC objectives. Detailed execution is left to the components to accomplish through tactical actions and tasks. The component commanders should set the priority, effects, and timing for all IO in the overall operation.

3. Navy and other components address component objectives and the desired effects required to achieve them. The JFC designates primary and supporting components.

4. The MOC IO team completes maritime component tasks, as determined by the JFC's objectives, the component objectives, and the commander's intent for planning and integration. The IO team helps integrate IRC into the maritime OPLAN and ATO.

5. The MOC IO cell members meet regularly to develop and coordinate IO in the COAs. The IO cell should seamlessly integrate the planning results through the MOC CTF into the maritime OPLAN and the ATO/tasking process for commander's approval.

The IO cell should ensure the ROE and operating requirements and authorizations, such as special target lists, are considered. The team should coordinate and follow up on IO-specific intelligence requests and requirements through the N2/staff and stay in contact with the appropriate assets to resolve problems and coordinate requirements and tasking. Likewise, the team chief should help ensure target deconfliction.

The NFC's MOC IO cell, at the operational level of war:

1. Prepares IO plans to shape the operational environment

2. Protects information, information systems, and Navy and DOD networks

3. Disrupts adversary C2

4. Exploits adversary vulnerabilities

5. Ensures the most effective use of EMS resources.

The NFC's IO cell maintains awareness of all IRC in military operations. The NFC employs tactical assets, such as CSGs, ESGs, and ARGs, within the theater in support of the unified combatant commander's TCP. The NFC may serve as the Navy component commander or JFMCC during major combat operations supporting a JFC.

Only the NFC has the authority to reassign, redirect, or reallocate a subordinate's forces. When a subordinate unit (such as a CSG or ARG) does not have the organic IRC to support an assigned mission, the IO cell coordinates tasking of available IRC based on the NFC's/NCC's IRC apportionment decision.

4.3.2 Numbered Fleet Commander Maritime Operations Center Information Operations Cell

The MOC is the organizational and procedural means by which the NFC carries out C2 of assigned forces and coordinates with higher authority to support assigned missions. The mission of the MOC IO cell is to coordinate and integrate employment of IRC during military operations. The IO cell within a MOC functions as the core organizational construct for an NCC, NFC, or JFMCC to support operational-level IO planning, execution, and assessment. The MOC IO cell can also serve as the core construct for a JTF joint IO cell. The MOC IO cell coordinates with other component operations centers.

The MOC has a permanent IO staff billeted according to the role being filled, the mission, overall manning of the command, and the commander's desires. It can be augmented in response to the changing complexity of operations. The IO staff forms the core of the IO cell, a more fluid organization that stands up as needed, and may draw on MOC assets in response to any aspect of an operation.

The IO staff and select command representatives or liaison officers make up the IO cell. The IO cell provides planners to the operational planning teams made up of future plans and future operations cells. The IO cell maintains a presence in current operations. The IO cell meets to ensure IO-related activities developed across the operational planning teams do not conflict and can be supported with available assets. The IO cell ensures the plan incorporates all the salient IO capabilities, needs, and details and ensures the IO actions are integrated with the overall maritime and JTF scheme of maneuver. The IO representative to the operational planning teams provides guidance to the specialists within the IO cell to develop actions to support the scheme of maneuver. The IO cell integrates these actions into composite plans and, with the IO cell chief's approval, presents the IO plan to future plans and operations cells as required.

The combination of qualified MOC IO staff, augmentation, potential cyberspace support elements, and reachback to FLTCYBERCOM/COMTENTHFLT allows IO to integrate dynamically into the MOC. This ensures the MOC IO cell is supported by and supports military operations as required. IO cell functions include:

1. Support current operations. Perform continuous planning, execution, and assessment of integrated IO and IO-related activities in support of the combatant commander's goals and objectives. Also, direct the execution of IO activities in support of the current scheme of maneuver and to achieve information superiority.

2. Integrate and coordinate IO into the campaign plan. As the experts in IO, the cell recommends priorities to achieve IO objectives identified during the planning process and coordinates plans with higher headquarters, other components and subordinates, and assigned assets or units. Members also participate in targeting board and fires cell to prioritize, nominate, and deconflict targets and to provide alternative means to prosecute targets.

3. Conduct assessment. Using measures of effectiveness (MOEs) and measures of performance (MOPs), evaluate and compare the target's behavior against expectations and, if required, determine how to modify plans or how to reengage the target for the desired effect.

The IO cell develops and synchronizes IO plans and supports planning efforts within future plans and operations, current operations, assessment cells, and other CTF as required to support the mission. The IO cell consists of the IO cell chief, the IO officer, and personnel with expertise in the areas of planning, targeting, and IRC. These unique skill sets, along with an IO support team as shown in figure 4-3, should be present in or readily available to the IO cell. The Operations officer is key to integrating IO into future and current operations and is responsible for balancing the resource requirements within the staff during selection and execution of a course of action.

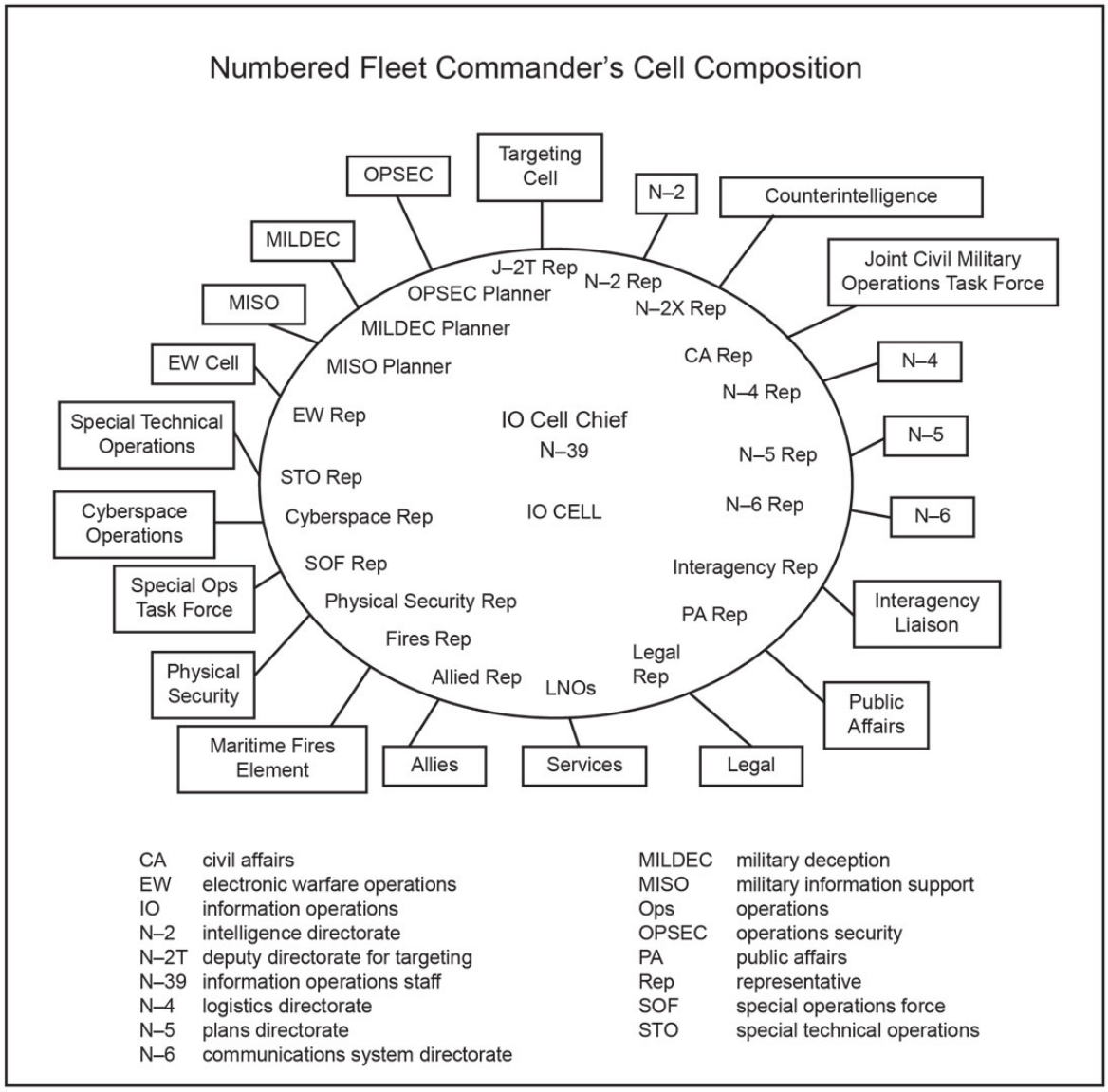


Figure 4-3. Notional Information Operations Cell Composition

IO planners work closely with various staff and warfare area planners to identify target audiences and target sets that can be affected with IRC to support the full range of the maritime commander's objectives. The MOC receives information from a broad range of sources, including national, operational, and tactical units and sensors that can be used as the basis for the assessment, planning, execution, and changes in force employment during environment shaping or upon execution of an OPLAN.

The IO cell responsibilities listed below vary with the complexity and level of operations and the role of the staff as either a Service or functional component command. The IO cell:

1. Coordinates the overall IO portion of the plan for the NFC.

2. Protects the force against hostile information, information systems, and electronic attacks as well as hostile propaganda and deception.

3. Directs maritime force IRC to support the NFC's concept of operations.

4. Integrates IO into all force plans and evolutions and coordinates this effort with JTF, subordinate headquarters, and other components.

5. Controls force emitters and releases control of applicable systems through EMCON guidance to subordinate commanders.

6. Controls all force information and information systems and releases control of applicable systems through information operations condition (INFOCON) guidance to subordinate commanders.

7. Maintains, protects, and shapes the desired force operations profile and signature and ensures the development of favorable tactical situations.

8. Directs maritime force IRC.

9. Uses information provided by theater and national assets to task and direct forces in support of IO.

10. Directs assets involved in environment awareness and shaping efforts, IO support to tactical missions, and IO execution and monitoring, to include targeting assets, directing units in localization and engaging information targets, and countersurveillance and countertargeting.

11. Coordinates with PA, visual information, and CMO to ensure their efforts are compatible with IO for operational effectiveness (e.g., protecting critical operational indicators and countering adversary propaganda).

12. Presents targets that require lethal engagement to achieve IO objectives to the appropriate joint boards, centers, and cells. This includes target nominations to the joint target list, maritime target list, and draft joint integrated prioritized target list.

13. Coordinates with theater IO cell to recommend or deconflict targets for information attack and to determine potential effects of theater IO activities on force operations.

14. Provides joint targeting coordination board (JTCB) with liaison officers knowledgeable on targets nominated by the IO cell and IO weapons capabilities.

15. Coordinates planning of airborne EW operations with the electronic warfare coordination cell (EWCC).

16. Determines assignment of jamming control authority in conjunction with JTF IO and joint force air component commander (JFACC) EWCC.

17. Conducts effects assessment of IO capabilities and operational assessment of IO support to the commander and JTF IO cell objectives.

18. Provides input to the commander's objectives, guidance, and intent.

4.3.3 Composite Warfare Commander

The officer in tactical command (OTC) assigns the composite warfare commander (CWC) authority and ascribed functions for the overall direction and control of the force. The OTC retains the power to negate any particular action by the CWC. The OTC may designate more than one CWC in a maritime OA. For example, with multiple CSGs or ARGs operating within a maritime OA, each group may have its own CWC. In some cases, they may all operate under a single CWC.

The CWC has five subordinate warfare commanders.

1. Air and missile defense commander

2. Antisubmarine warfare commander

3. Information operations warfare commander (IWC)

4. Strike warfare commander

5. Surface warfare commander.

Refer to NWP 3-56, Composite Warfare Doctrine, for further information about the CWC construct.

4.3.4 Information Operations Warfare Commander

Under the direction of the CWC, the IWC shapes and assesses the IE, achieves and maintains information superiority, develops and executes IO plans in support of CWC objectives, and supports other warfare commanders. As such, the IWC is responsible to the CWC for all IO within the strike group. The IWC also integrates IO into all plans and evolutions and coordinates this effort with theater, fleet, and JTF IO planners and disseminates IO data to the force.

The IWC also ensures targeting board awareness of IO objectives to maximize mission effectiveness of IRC and supporting lethal and nonlethal effects. The IWC coordinates with the MOC IO cell to recommend or deconflict targets for attack and to determine potential effects of theater IO activities on CSG and ARG operations.

The IWC is responsible to the strike group commander for planning and executing IRC, including protecting the force against hostile operations within the EMS and cyberspace. The IWC establishes and maintains the tactical picture through spectrum awareness, mission-oriented planning, and directing and monitoring plans. The IWC assists the commander to control all force emitters and information systems by recommending and executing EMCON, River City, and INFOCON.

Typical functions the CWC assigns to an IWC include:

1. Assist OTC or CWC in force IO planning and integration.

2. Assist OTC or CWC in force EW planning and integration.

3. Coordinate and control force ES assets and ensure ES information dissemination within the force.

4. Coordinate and control force EA assets.

5. Recommend the force EMCON profile to OTC, including responding to changes in the tactical situation. This includes coordinating with the antisubmarine warfare commander to manage acoustic emissions.

6. Assist OTC or CWC to establish a communications security own force monitoring plan.

7. Formulate and promulgate, as force spectrum manager, the force afloat EMS operations program.

8. Coordinate with airspace control authority, air resource element coordinator, and helicopter element coordinator for support aircraft.

9. Coordinate with the cryptologic resource coordinator for the employment of ES and SIGINT equipment in support of force tactical intelligence requirements.

10. Direct the use of force expendable decoy resources.

11. Develop preplanned responses for countersurveillance, counterinfluence, and countertargeting.

12. Integrate real-time ES contact reports with indications and warnings to recommend force defensive measures and readiness conditions to OTC or CWC.

13. Monitor force actions and communications to ensure alignment with previously directed SC objectives.

Refer to NTTP 3-13.2, Information Operations Warfare Commander Manual, for further information.

4.3.5 Carrier Strike Group and Amphibious Ready Group Commanders

The CSG and ARG employ individual unit or small group tactics to execute IRC as tasked by the NFC or Navy/naval/maritime component commander. The CSG and ARG units routinely execute operational environment (OE) shaping plans developed by the NFC. They share the information derived from conducting OE awareness with other force consumers through the DOD information networks.

The Navy normally organizes assigned/attached forces as part of a task force, typically aligned through an NFC. The afloat senior commander is normally designated as the OTC or CWC. As part of a joint command structure, the NFC may be designated as a JTF commander or a JFMCC under a CCDR, JFC, or commander of another JTF. Further, an NCC may also be tasked as a JFMCC or be assigned by the CCDR to provide Service support to a JFC or a joint task force commander.

An IO team from Navy Information Operations Command-Norfolk (NIOC–N), VA, or NIOC San Diego, CA, supports the ARG and embarked Marine air-ground task force (MAGTF) commander with IO planning and execution. Augmentees from FLTCYBERCOM activities may be part of the afloat IO planning team and support for ARG IO evolutions. During open-ocean transits and approaches to the littorals, the ARG planning team focuses on exchanging current IO data with the appropriate theater MOC IO cell and other ARGs and units to maintain a current regional picture for the ARG commander. During littoral operations, the planning team focuses on EMCON support to amphibious operations and defense of the amphibious task force. This shift in focus requires a shift in reporting priorities and liaison efforts from the EW modules of other ARG ships to MAGTF elements located ashore or afloat.

CHAPTER 5

Information Operations and Planning

5.1 INTRODUCTION

The planning process allows the commander and staff to plan and execute operations effectively, to ensure that the employment of forces is linked to objectives, and to integrate IO seamlessly with the actions of a joint force. The planning process assists commanders and their staffs in analyzing operational environment effects and distilling a multitude of planning information in order to provide the commander with a coherent framework to support decisions. The process is thorough and helps apply clarity, sound judgment, logic, and professional expertise.

Just as all maritime operations are integrated within the broader context of joint operations and campaigns, so IO is integrated with joint planning to ensure a successful military operation, setting the necessary conditions for the strategic end state. It is critical that Navy efforts correctly align maritime forces and their capabilities with joint requirements.

The Navy's core capabilities across the phases of an operation are shown in figure 5-1. IRC can support all the Navy's core capabilities and should be identified and developed during planning, execution, and transitions between phases. IRC can be included along the planning horizons for current operations, future operations, and future plans.

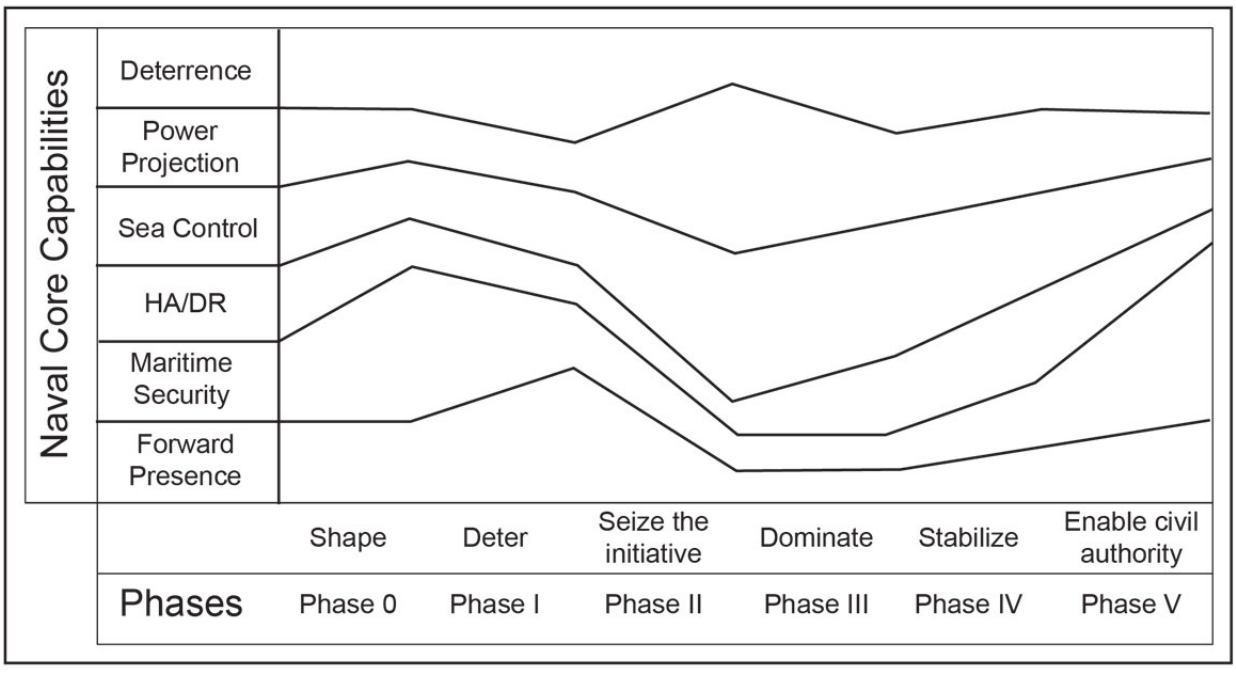


Figure 5-1. Notional Application of Navy Core Capabilities Across the Six-phase Campaign Model Continuum

The Navy force provides unique options to the joint commander, each useful in executing IO, including:

1. Forward deployment and prompt response
2. Sustained presence
3. A maneuverable base with freedom of movement in international waters
4. A scalable force with flexible capabilities.

5.2 OPERATION PLANNING

Operational-level planners should have a thorough knowledge of JP 5-0, Joint Operation Planning, and NWP 5-01, Navy Planning. Prior to developing any operational plan, it is necessary to understand strategic guidance and the sources of strategic direction. Planners should derive purpose and focus from all available sources, including the JSCP, Guidance for Employment of the Force, Global Force Management Implementation Guidance, and others. Strategic guidance provides the shape of the desired strategic and military end states to a plan or order. This process enables unified action, a concept describing the synchronization, coordination, and integration of the activities of Governmental and nongovernmental entities with military operations to achieve unity of effort. For additional information on unified action, see JP 1.

Operation planning has a close relationship with policy and strategic guidance. Comprehensive policy can clarify planning. Consequently, deliberate or crisis action planning correctly informs policy. The planning process provides a common basis for discussion, execution, and change for the joint force, its subordinate and higher headquarters, the joint planning and execution community, and national leadership. It establishes the necessary scope and scale to enable inclusion of IRC into a plan in order to develop an integrated product to meet the commander's intent.

5.2.1 Applicability to Navy Planners

Effective Navy planners are knowledgeable in joint planning and are experts in how the Navy's unique maritime capabilities can contribute to joint mission success. Further, they comprehend the necessity to integrate IO and IRC throughout plan development, supported by IO planners, when even greater expertise is required.

The JFMCC is the JFC's maritime warfighter, designated to control joint operations at sea. The authority for operational-level planning and employment of maritime forces and assets rests with the JFMCC.

JFMCC planning duties and responsibilities may include, but are not limited to:

1. Develop a maritime OPLAN to best support joint force objectives
2. Develop maritime COAs within the framework of the JFC-assigned objective mission, the forces available, and the commander's intent
3. Coordinate JFMCC planning with higher, lower, adjacent, and multinational headquarters
4. Determine JFMCC forces required and coordinate deployment planning in support of the selected COAs
5. Coordinate the planning and execution of maneuver operations with other missions.

Members of the MOC N39 cell and subsequently formed operational planning teams (OPTs) benefit from this knowledge and approach.

5.2.2 Operational Design

Operational design is the conception and construction of the framework that underpins a campaign or major OPLAN and its subsequent execution. The modern OE is characterized by complexity and uncertainty and compels solutions that stress innovation and agility. Effective operational design requires the ability to comprehend imprecise information, ambiguity, and continual plan refinement while developing branch plans and sequels for future operations.

Joint and Navy doctrine emphatically state a commander's role in operational design. The commander is the central figure in operational design, not just because of the commander's education and experience, but also because the commander's judgment and decisions are required to guide the staff through the process. Generally, the more complex a situation, the more critical a commander's early involvement becomes as the plan takes shape.

A commander's wisdom is essential to developing the operational approach, which is necessary to establish the necessary conditions for COA development. This applies to the JFC and to the JFMCC as well. In a nuanced and complex OE, which includes the maritime segment of the joint operations area, considering, evaluating, and employing IRC along with their relevance to the ends, way, and means, are fundamental actions for the commander and planning staff.

The commander's intent is essential for the planning team. This brief statement includes the purpose and the desired end state and addresses risk. It reflects an understanding of the strategic direction, the OE, and any impediments (i.e., risk and uncertainty) to mission accomplishment.

Planners apply elements of operational design to provide the conceptual framework that underpins the operation or campaign plans and their subsequent execution. The application of operational design and operational art refines the problem and further reduces uncertainty while adequately ordering complex problems to allow facilitating more detailed planning. Additionally, it connects strategy and tactics by accounting for operational-level plans, orders, and assessment. Operational design may precede the planning process and offer initial planning considerations that include military end state, center of gravity, lines of effort, decisive points, etc.

5.2.3 Operational Art

Operational art is the cognitive approach by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means.

In spite of the way it is always presented and taught, combat planning does not lend itself to cookbook solutions, scientific models, or simple linear processes. Developing a solution requires study of the interplay of hundreds, if not thousands, of independent variables—some easily predicted, some wildly unexpected. An adaptable enemy does not fall victim to the same tactic more than once.

It is critical for staff planners to comprehend the elements of operational art and assist the commander as necessary. The use and application of operational art is a commander's technique. It is the creative thinking used to design strategies, campaigns, and major operations and to organize and employ military force. It allows commanders to understand the challenges facing them and to conceptualize approaches for achieving their strategic objectives. The thought process helps commanders and their staffs to lessen the ambiguity and uncertainty of a complex operational environment, understand the military problem set, and visualize how best to effectively employ the military element of national power in order to accomplish an assigned mission. This is the essence of operational art and, when employed correctly, it enables pursuit of unified action.

Operational design extends operational art's vision with a creative process that helps commanders and planners answer the ends–ways–means risk questions. The elements of operational design are individual tools that help the JFC and staffs visualize and describe the broad operational approach. Operational art, operational design, and operation planning processes form a synergy to produce the plan to underpin a joint operation.

5.2.4 Intelligence Support

IO, like all other military activities, benefits from robust intelligence support. Information operations intelligence integration (IOII) is the integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the information environment. IOII uses a joint concept explored further in JP 3-13.

IOII is critical to the planning, execution, and assessment of IO and the use of IRC. SIGINT is a category of intelligence comprising, either individually or in combination, all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.

IO requires unique and detailed intelligence never before asked of intelligence collection agencies and activities. Intelligence preparation of the operational environment is vital to successful IO. Support from non-DOD and non-U.S. sources may also be required. Commanders dedicate intelligence personnel and capabilities to support IO planning and execution to ensure IO activities and IRC effectively support operations.

The combatant command's IO cell is the primary focal point for supporting the JTF and component commanders with IO products that support IO planning, execution, and assessment. It provides analysis of an adversary's IO capabilities and intentions and helps support the indications and warning process. A CCDR can request a national intelligence support team stand-up, composed of intelligence and communications experts from other intelligence agencies as required.

Cyber intelligence is the tracking, analyzing, and countering of digital security threats. This type of intelligence is a blend of physical espionage and defense with modern information technology. Cyber intelligence efforts help combat computer viruses, hackers, and terrorists who use the Internet to gain sensitive information. Aggressively fighting these threats is as significant a part of this field as protecting parties from them. Intelligence activities are critical to IO planning, execution, and assessment. Commanders draw on the resources they need to conduct effective IO in support of the CCDR and put it to best use.

5.2.5 Operation Planning Process

The joint operation planning process is an orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best course of action, and produce a joint OPLAN or order. JOPP is an iterative process that structures the efforts of the commander and staff to develop plans appropriate to the military problem set at hand. Planners at all echelons apply analytical rigor and follow developmental steps to ensure a familiar and repeatable process and develop unity of effort. The principles of JOPP are relevant and adhered to during deliberate planning as well as crisis action planning, with the amount of time available for planning being the key distinction between the two.

Within the Navy, commanders are expected to operate independently while following their superior commander's intent; to act when an opportunity presents itself and to feel comfortable in conditions of ambiguity. These are attributes honed by mutual trust and confidence and years of experience at sea. This description of disciplined initiative is also known as mission command in joint doctrine. While the concept may be new to other Services, it is how the Navy has historically commanded. To ensure that planning does not stifle mission command, Navy planning focuses more on the purpose of operations rather than the details of how subordinates execute the tasks and avoids overly restrictive command and control concepts. The commander's intent cannot be a staff product; rather, if must be a true embodiment of the commander's vision and the centerpiece of the commander's discussions with subordinate commanders. Nonetheless, the terminology, products, and concepts of the Navy planning process are consistent with joint planning and joint doctrine and are compatible with other Services' doctrine.

Collecting information and building situational awareness to support the commander's planning and decision-making process supports the initiation of planning and is critical to all steps in the process. The following vignette provides a framework and context to step through the milestones in the planning process (figure 5-2).

Operation Synergy

In response to a crisis in Country TEAL, the Commander, U.S. Ocean Command (CDRUSOCEANCOM, the geographic combatant command in whose area of responsibility TEAL is located), received a CJCS planning order to develop courses of action based on staff estimates. TEAL's government has traditionally countered U.S. initiatives to establish normal diplomatic relations and has a long history of arms purchases from Country ORANGE, to include antiship cruise missile and ballistic missile components. After recent elections, significant numbers of citizens who supported the opposition party were killed by TEAL's armed forces, producing regime instability and a growing humanitarian crisis. CDRUSOCEANCOM's Navy component command is Commander, U.S. Eleventh Fleet (COMELEVENTHFLT). ELEVENTHFLT's additional responsibilities include a be-prepared-to function to serve as a JTF headquarters and JFMCC. Since TEAL is an island nation, a plan that focuses on a maritime-centric COA receives particular scrutiny.

The desired political goal is to end the humanitarian crisis and keep hostilities from spreading through the region by restoring regime stability while encouraging future strides toward democracy and openness to U.S. diplomacy. The CCDR's vision for military objectives in the information environment includes both immediate tactical elements to ensure a military advantage and long-term influence elements to shape a more positive narrative. The JFMCC forces include Navy ships and aircraft with immense combat power along with IRC. There is a challenge for the members of the OPT in the JFMCC (MOC) IO cell in their deliberations to develop a line of operation that involves integrating disparate capabilities into a plan and then coordinating and synchronizing their use during the plan's execution; in other words, identifying the intended effects and aligning the appropriate capabilities to achieve those effects.

There are essentially three broad tasks to consider and each includes numerous subordinate activities:

1. Protect friendly information and information systems. Both pro-regime and antiregime elements, in theater and globally, oppose U.S. involvement in the dispute, and both sides have shown skill and enthusiasm in attacking the Navy in the information environment. Possible IRC to counter these attacks include an effective OPSEC posture and efficient IA and DCO techniques.
2. Disrupt or degrade adversary C2 systems. The JFMCC can de-escalate internal violence and protect U.S. forces by attacking the adversary's C2 nodes using lethal fires and IRC, including EA and OCO, and executing MILDEC.
3. Influence a target audience(s). The JFMCC's plan contains a significant influence dimension and considers identifying key adversary operational- and tactical-level decision makers and leadership. Exploring the method to develop encounters and perceptions necessary to shape deeds that support achieving the desired military end state is essential, (e.g., key leader engagement, MILDEC, defense support to public diplomacy, etc.). This dimension also contains use of MISO with the aim of altering TA behavior and developing and implementing an effective commander's communication strategy to align key themes and messages to support the desired outcome.

Because of careful evaluation of available IRC and their judicious employment, the JFMCC planners brief COMELEVENTHFLT)/JFMCC and CDRUSOCEANCOM on the approach and objectives, seeking guidance and the authority to continue to plan development to respond to the crisis in TEAL. As the operation progresses and knowledge of the joint OE becomes clearer, the plan must be refined, integrate the available IRC in every phase to deliver an operational advantage that conforms with strategic guidance, and consistent with the goals of the U.S. strategic end state.

Figure 5-2. Example: Planning Process

5.2.5.1 Planning Initiation

Planning initiation is the critical first step in the planning process, whether in deliberate planning or in response to an emerging situation in crisis action planning. The JFC typically provides initial planning guidance based on current understanding of the operational environment, the problem, and the initial operational approach for the campaign or operation. It could specify time constraints, outline initial coordination requirements, or authorize movement of key capabilities within the JFC's authority. Receipt of the JFC's initial planning guidance is essential for JFMCC and other component commanders to begin their respective staff planning tasks in response to an initiating directive (e.g., a WARNORD or other planning document).

5.2.5.2 Mission Analysis

As the name implies, the mission analysis portion of planning is an intensely methodical review of the operation. This is a time for the commander and staff to carefully study the assigned tasks and identify other tasks, resources, and coordination requirements necessary for mission accomplishment. If appropriate IRC were not considered before this point in the planning sequence, this is a critical time to begin the integration process by identifying candidates for inclusion in each phase of the operation. When the commander is tasked, planners consider the following questions:

1. What is the purpose of the assigned mission?
2. What tasks must my command perform to accomplish the mission?
3. What are the limitations on my force's actions?
4. What assets are needed to support my operation?

Staff mission analysis activities, whether accomplished in the mission analysis process by members of joint planning group (JPG) or OPT, may include:

1. Analyze higher headquarters planning activities and strategic guidance
2. Review commander's initial planning guidance, including initial understanding of the operational environment, of the problem, and description of the operational approach
3. Determine known facts and develop planning assumptions
4. Determine and analyze operational limitations
5. Determine specified, implied, and essential tasks
6. Develop mission statement
7. Conduct initial force allocation review
8. Develop risk assessment
9. Develop mission success criteria
10. Develop commander's critical information requirements
11. Prepare staff estimates
12. Prepare and deliver mission analysis brief
13. Publish commander's updated planning guidance.

This is joint doctrine common to all Services and a process that is relevant to all circumstances; it may be truncated or modified based on time constraints. Mission analysis concludes with a formal briefing and issuing the commander's refined planning guidance containing:

1. Approved mission statement
2. Key elements of the OE

3. Clear statement of the problem to be solved
4. Key assumptions
5. Key operational limitations
6. Discussion of the national strategic end state
7. Termination criteria
8. Military end state
9. Military objectives
10. Commander's initial thoughts on the conditions necessary to achieve objectives
11. Acceptable or unacceptable levels of risk in key areas
12. The commander's operational approach.

5.2.5.3 Course of Action Development

A COA is a unique choice presented to the commander to accomplish an assigned mission. To be complete, a COA should be based on the operational approach and include the fundamental answers of who, what, where, when, why, and how an action takes place. Similarly, the essential tasks from the draft mission statement are common to all COAs. As with mission analysis, COA development draws on key inputs to influence a number of outputs. COAs may be separate and distinct throughout the operational domains (air, land, maritime, space, and cyberspace), the information environment, or through some combination.

JP 5-0 and NWP 5-0 cover techniques to develop COAs. IRC may be best coordinated by using the joint functions of C2, intelligence, fires, movement and maneuver, protection, and sustainment. Each of these functional areas provides sufficient opportunity to address inclusion of specific IRC and the role that maritime forces assume in their eventual execution. Additionally, Navy planners should consider three key questions during COA development to best employ assigned maritime forces and nest the plan under a broader joint construct:

1. How do land forces, maritime forces, air forces, and special operations forces integrate across the joint functions to accomplish their assigned tasks?
2. What are the major ways in which space operations can support operations across the joint functions?
3. How can the joint forces conduct IO to support joint operations?

Apply a validity test to each tentative (i.e., an option not yet approved or working) COA using the following assessment criteria: adequate, feasible, acceptable, distinguishable, and complete.

5.2.5.4 War Gaming

War gaming facilitates COA analysis and, depending on the time available, can be accomplished through a range of options. War gaming techniques generally begin with a detailed narrative to describe how events unfold; the "sketch note," which adds an operational sketch and commentary to the graphic; and a computer-assisted modeling and simulation undertaking. Any option is appropriate and is evaluated against an adversary's most probable and most dangerous COA.

The war game represents an ideal opportunity to include IRC using the aforementioned criteria. While techniques to conduct the war game may vary—including a red cell to offer an opposing view along with a white cell chaired

by a senior staff leader to ensure objectives are met and efficiency is retained throughout the process—they are key components to success when evaluating the results.

5.2.5.5 COA Comparison

The next step in COA development is to compare possible COAs but not against one another. Rather, evaluate each independently against the desired mission outcome within the given established criteria. There are numerous approaches to conduct a comparison, but the most important consideration is the element of consistency in evaluation. The goal is to create a matrix using numerical (and possibly weighted) criteria to aid the commander's selection of the COA best suited to accomplish the assigned mission.

5.2.5.6 COA Approval

It is prudent and customary to conduct a formal briefing for the commander and headquarters staff to select a COA for approval. This presentation provides the commander with an opportunity to obtain responses to any unanswered questions, include additional guidance from higher headquarters, or alter the approach if required. Once a decision is made on a COA, refined planning commences. It informs a decision statement to facilitate the JFC's commander's estimate and plan or order development.

5.3 TARGETING

The purpose of targeting is to achieve specific desired effects at the strategic, operational, and tactical levels of war. A target is a specific area, object, audience, function, or facility subject to military action on which an effect is directed. Targeting is a process of matching a target in the cognitive, informational, or physical domain with lethal or nonlethal capabilities. Targeting involves giving the commander recommendations for an attack on targets that may help achieve military objectives and providing options to achieve desired effects.

Clear objectives and commander's guidance are the foundations of the targeting process. Objectives are developed, and commander's guidance is normally provided, at the national, theater, and component levels. At the operational level, IO targeting nominations originate from IO planners integrated into the MOC and JTF targeting processes for approval and coordination. They are significantly influenced by in-depth intelligence analysis. IO planners use established targeting processes and methodologies to recommend targets for which IO can be used to support the theater campaign plan. Some other considerations include:

1. Early identification of critical elements with respect to specific targets is essential for successful IO. Understanding the nature of the threat helps defend and protect against adversary IO.

    a. Employ IRC to achieve military objectives when appropriate. IRC may target a key element of a specific, critical adversary target set.

    b. Understanding the nature of the threat helps defend and protect against adversary IO. An IO threat should be defined in terms of a specific adversary's intent, capability, and opportunity to influence the elements of the friendly information environment critical to achieving objectives.

    c. An IO threat is an adversary that is organized, resourced, and motivated to affect decision makers. Hackers, criminals and organized crime, insiders, industrial and economic espionage, and, in some cases, terrorism constitute a general threat to the protected information environment. This general threat requires monitoring for indications of a specific IO threat and subsequently may require additional defensive IO measures.

2. C2 remains a substantial target for IO. Commercial communications systems linked to friendly and adversary C2 systems offer unique challenges to offensive targeting and defensive protection.

3. Examples of key areas of warfare support comprising potential offensive target sets and requiring protection include, but are not limited to logistics, intelligence, and non-C2 communications systems. An adversary's offensive capabilities may target friendly commercial infrastructures, just as friendly offensive capabilities may target an adversary's commercial infrastructures.

Targeting is a familiar process for JFMCC staffs, similar to offering excess sorties to the JFACC staff for additional mission availability to be apportioned in the ATO. Sequential tasking provides the commander with supplemental capability to facilitate mission accomplishment. Within the MOC N39 IO cell, similar opportunities exist to integrate IRC into the JPG/OPT planning sequence. These may represent a distinct line of operation or a line of effort and may fall into a special technological capability based on the nature of employment.

A target is an entity or object considered for possible engagement or action. It may be an area, complex, installation, force, equipment, capability, function, individual, group, system, entity, or behavior identified for possible action to support the commander's objectives, guidance, and intent. JP 3-60, Joint Targeting, describes four principles that are applied throughout the targeting cycle to create desired effects while diminishing undesired collateral effects.

1. Focused. The function of targeting is to achieve the JFC's objectives through target engagement within the parameters set by the CONOPS, the operational limitations within the plans and orders (to include fragmentary orders), the ROE, the Law of War, and agreements concerning the sovereignty of national territories. Every target nominated should contribute to attaining the JFC's objectives.

2. Effects-based. The art of targeting seeks to create desired effects with the least risk and least expenditure of time and resources.

3. Interdisciplinary. Joint targeting entails participation from all elements of the JFC's staff, component commanders' staffs, other agencies, departments, organizations, and multinational partners. IO expert participation is central for processes involving IRC and lethal effects on information systems and is useful in ensuring lethal actions are aligned with the commander's influence objectives.

4. Systematic. The joint targeting cycle is designed to create effects in a systematic manner. It is a rational, iterative process that methodically analyzes, prioritizes, and assigns assets against targets systematically.

IO planners consider all instruments of the adversary's national power to determine how best to achieve stated objectives by affecting information and information systems. Successful integration of IRC into the targeting process is fundamental to the success of the campaign. IO may call for targeting adversary human decision processes (human factors), information, and information systems used to support decisionmaking or adversary morale with a variety of lethal and nonlethal means. The selection of IO actions should be consistent with national objectives, applicable international conventions, ROE, and other guidance.

The joint force IO cell is another source for target requirements and should be closely integrated to deconflict redundant targeting, consider intelligence gain versus loss assessments, and provide inputs to the restricted target list and no-strike list. IO planners coordinate and integrate IO at all levels. Most destructive IO attacks either support strategic attacks or are considered strategic attacks or interdiction operations themselves. Therefore, planners, operators, and targeteers should carefully consider prospective IO target nominations when making apportionment decisions.

The maritime targeting cell includes IO planners who assist the staff planners in developing the JFMCC input to the joint integrated prioritized target list and in issuing subsequent task orders. The IO planners conduct frequent liaison with the JTCB IO planner counterparts to coordinate and synchronize target selection planning.

The JFMCC staff is responsible for identifying potential target sets to be presented and adjudicated at the JFC's JTCB. With respect to specific IO-related targets, the JFMCC assigns the nomenclature of high-value and high-payoff as applicable to those candidate targets. Target sets in which lethal effects may have desired IO results may include microwave towers or communications antennae and power generators or transformers.

Similarly, IRC, like OCO and EA, can disrupt adversary systems, impacting combat capabilities in the physical domain.

Figure 5-3 identifies the six phases of the joint targeting cycle. It is imperative the JFMCC planners comprehend the entire cycle and the specific requirements associated with each of the phases to ensure IRC are correctly identified, considered, war-gamed, and ultimately written into the plan from the operational to tactical level. For additional information on targeting, refer to NTTP 3-13.1 and JP 3-60.

5.4 ASSESSMENT

Assessment is a continuous process that measures the overall effectiveness of employing joint force capabilities during military operations, the determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. Assessment considerations are identified during mission analysis. As the commander's critical information requirements are developed, key indicators are derived from identifying essential information that ultimately measures progress made (or lost) towards an objective.

A measure of effectiveness (MOE) is a criterion used to assess changes in system behavior, capability, or OE that ties to measuring the attainment of an end state, achievement of an objective, or creation of an effect. A measure of performance (MOP) is a criterion used to assess a friendly action that ties to measuring task accomplishment.

Both MOP (task assessment: Are we doing things right?) and MOE (Are we doing the right things?) are important to the commander. Establish decisive points based on progress made in the areas of through monitoring and evaluating and then recommending or directing action. Altering the collection plan, adjusting MOE indicators, or changing IRC employment are viable options based on the assessment of progress. A detailed, practical discussion of assessment contained in JP 5-0, Appendix D, may help create the JFMCC IO assessment plan. See NTTP 3-32.01, Operational Assessment, for additional information.

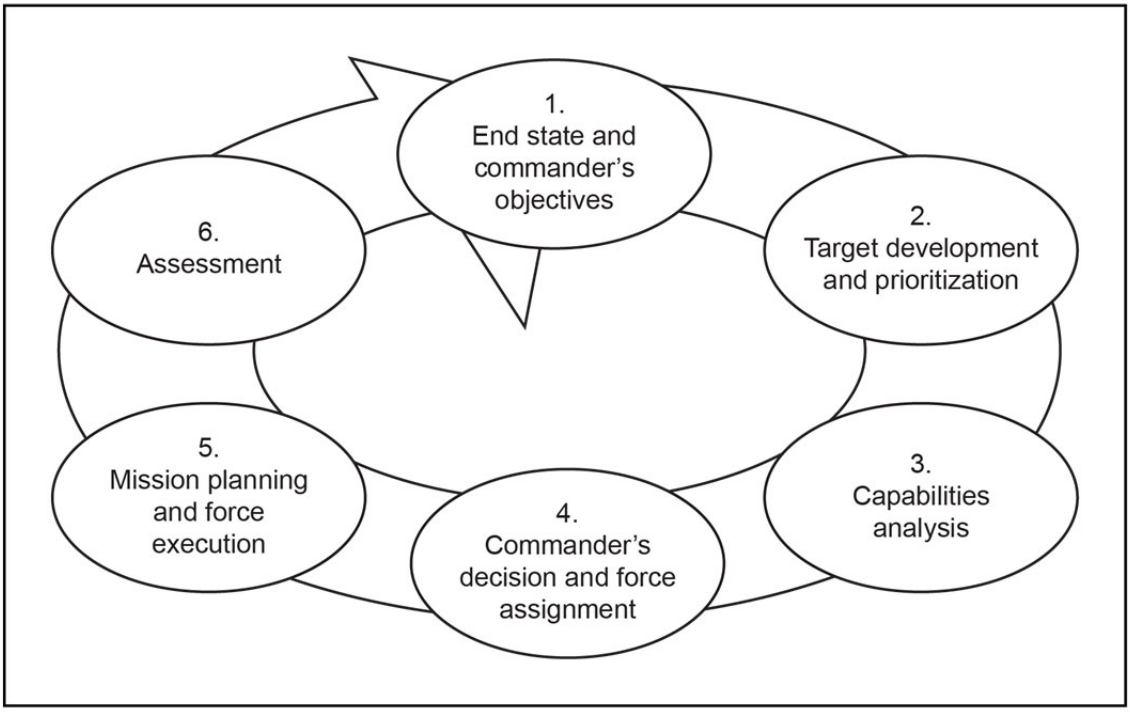


Figure 5-3. Six Phases of the Joint Targeting Cycle

5.5 COORDINATION WITH PARTNERS

Although the Navy is always prepared to undertake unilateral military action, coordination with navies of other nations has become typical. Multination participation can be vital for mission accomplishment and can strengthen partnerships. This participation may include long-standing alliances, such as the North Atlantic Treaty Organization, or a hybrid coalition of nations with conflicting histories and interests but working together for a specific common purpose.

5.5.1 Multinational and Coalition Considerations

IO concepts, doctrine, procedures, and capabilities are recognized by U.S. allies and coalition members. Naturally, there are disparate views based on national interests, interpretation, doctrine, and culture, which require coordination and conflict resolution on friction points by the multinational force commander and staff. Navy planners would be wise to recognize that coalition capabilities complement U.S. expertise, forming synergy by the significant regional and operational acumen they contribute.

The NATO alliance has a substantive and authoritative IO policy. It is based on the premise that civil-military cooperation is founded in close, interactive relationships among partner nation militaries. NATO military public information and IO have a definitive relationship. Although there is a distinct separation in function, plans and actions are well coordinated. Formalized terms of reference provide overarching guidance and consensus where possible. For additional information, see AJP 3-10, Allied Joint Doctrine for Information Operations.

5.5.2 Interorganizational Coordination

Interorganizational coordination is defined as the interaction among elements of the DOD; engaged U.S. Government agencies; state, territorial, local and tribal agencies; foreign military forces and government agencies; intergovernmental organizations; nongovernmental organizations; and the private sector. With the amalgamation of disparate cultures, objectives, resources, talent, and experience coming together to contribute a solution to a complex problem set, near-precise and consensus-level guidance is essential. Joint doctrine exists to provide such a foundation for coordination of military activities within the military end state.

The significance for JFMCC planners is that, while interagency coordination primarily takes place at the CCDR headquarters, additional coordination may be required at the component command level. Depending on the scenario and phase of an operation, maritime forces and capabilities may be assigned additional tasks to achieve military and strategic end states. Some organizations' representatives are present in the OE prior to and following military activities and their livelihood and purpose may be impacted by planned operations or by unintended consequences. This is particularly true for nongovernmental organizations and private sector interests, many of which prefer not to coordinate actions, fearing that their objectives may be jeopardized by close association with military actors. For additional information, see JP 3-08, Interorganizational Coordination during Joint Operations.

INTENTIONALLY BLANK

REFERENCES

NTTP 3-13.2, Information Operations Warfare Commander Manual

NTTP 3-51.1, Navy Electronic Warfare

NWP 3-53, Navy Psychological Operations

NWP 3-56, Composite Warfare Doctrine

SecDef Memo 12401-10, Strategic Communication and Information Operations in the DOD

JP 3-08, Interorganizational Coordination during Joint Operations

JP 3-09, Joint Fire Support

JP 3-12, Cyberspace Operations

JP 3-13, Information Operations

JP 3-13.1, Electronic Warfare

JP 3-60, Joint Targeting

JP 3-61, Public Affairs

JP 5-0, Joint Operation Planning

Center for Analyses Study, Structures for Information Warfare and Information Dominance Afloat (September 2013)

Chairman of the Joint Chiefs of Staff Instruction 3210.01 series, Joint Information Operations Policy

DOD Directive 3600.01 series, Information Operations

Title 10, U.S. Code, Armed Forces

Title 50, U.S. Code, War and National Defense

INTENTIONALLY BLANK

GLOSSARY

functional component commands. A command normally, but not necessarily, composed of forces of two or more Military Departments which may be established across the range of military operations to perform particular operational missions that may be of short duration or may extend over a period of time. See also component; Service component command. (JP 1-02. Source: JP 1)

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02. Source: JP 3-13)

information operations-information-related capability. A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. Also called IRC. (JP 1-02. Source: JP 3-13)

integration. 1. In force protection, the synchronized transfer of units into an operational commander's force prior to mission execution. (JP 1-02. Source: JP 1) 2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 1-02. Source: JP 1)

strategic level of war. The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives. See also operational level of war; tactical level of war. (JP 1-02. Source: JP 3-0)

target audience. An individual or group selected for influence. Also called TA. (JP 1-02. Source: JP 3-13)

INTENTIONALLY BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AOR	area of responsibility
ARG	amphibious ready group
ATO	air tasking order
C2	command and control
CCDR	combatant commander
CCMD	combatant command
CCS	commander's communication strategy
CDRUSSTRATCOM	Commander, United States Strategic Command
CJCS	Chairman Joint Chiefs of Staff
CMO	civil-military operations
CNO	Chief of Naval Operations
CO	cyberspace operations
COA	course of action
COMTENTHFLT	Commander, Tenth Fleet
CONOPS	concept of operations
CSG	carrier strike group
CTF	cross-functional team
CWC	composite warfare commander
DCO	defensive cyberspace operations
DOD	Department of Defense
EA	electronic attack
EP	electronic protection
EM	electromagnetic
EMBM	electromagnetic battle management
EMCON	emission control

EMS	electromagnetic spectrum
ES	electronic warfare support
EW	electronic warfare
EWCC	electronic warfare coordination cell
FLTCYBERCOM	Fleet Cyber Command
FTC	fleet training continuum
IA	information assurance
INFOCON	information operations condition
IO	information operations
IOII	information operations intelligence integration
IRC	information-related capability
IWC	information operations warfare commander
JEMSO	joint electromagnetic spectrum operations
JFACC	joint force air component commander
JFC	joint force commander
JFMCC	joint force maritime component commander
JOPP	joint operation planning process
JP	joint publication
JPG	joint planning group
JSCP	Joint Strategic Capabilities Plan
JTCB	joint targeting coordination board
JTF	joint task force
MAGTF	Marine air-ground task force
MILDEC	military deception
MISO	military information support operations
MOC	maritime operations center
MOE	measure of effectiveness
MOP	measure of performance

NATO	North Atlantic Treaty Organization
NCC	Navy component commander
NCF	Navy Cyber Forces
NFC	numbered fleet commander
NIOC	Navy Information Operations Command
NTTP	Navy tactics, techniques, and procedures
NWP	Navy warfare publication
OCO	offensive cyberspace operations
OE	operational environment
OPLAN	operation plan
OPSEC	operations security
OPT	operational planning team
OTC	officer in tactical command
PA	public affairs
ROE	rules of engagement
SC	strategic communication
SecDef	Secretary of Defense
SIGINT	signals intelligence
STO	special technical operations
TA	target audience
TAA	target audience analysis
TCP	theater campaign plan
WARNORD	warning order
USCYBERCOM	United States Cyber Command
USFF	United States Fleet Forces Command
USG	United States Government
USPACFLT	United States Pacific Fleet
USSTRATCOM	United States Strategic Command

INTENTIONALLY BLANK

LIST OF EFFECTIVE PAGES

Effective Pages	Page Numbers
FEB 2014	1 thru 14
FEB 2014	1-1, 1-2
FEB 2014	2-1 thru 2-8
FEB 2014	3-1 thru 3-10
FEB 2014	4-1 thru 4-10
FEB 2014	5-1 thru 5-12
FEB 2014	Reference-1, Reference-2
FEB 2014	Glossary-1, Glossary-2
FEB 2014	LOAA-1 thru LOAA-4
FEB 2014	LEP-1, LEP-2

INTENTIONALLY BLANK

NWP 3-13
FEB 2014