MCWP 8-10

Information in Marine Corps Operations

U.S. Marine Corps

Limited Dissemination Controls: None. Approved for Public Release.

PCN 143 000184 00

A non-cost copy of this document is available at:
https://www.marines.mil/News/Publications/MCPEL/

Report urgent changes, routine changes, and administrative discrepancies by letter or email to the Doctrine Branch at:

Commanding General
United States Marine Corps
Training and Education Command
ATTN: Policy and Standards Division, Doctrine Branch (C 466)
2007 Elliot Road
Quantico, VA 22134-5010

or by email to: Doctrine @usmc.mil

Please include the following information in your correspondence:

Location of change, publication number and title, current page number, paragraph number, and if applicable, line number
Figure or table number (if applicable)
Nature of change
Addition/deletion of text
Proposed new text.

Copyright Information

UNITED STATES MARINE CORPS

29 February 2024

Foreword

Marine Corps Warfighting Publication (MCWP) 8-10, *Information in Marine Corps Operations*, builds on the doctrinal foundation established in Marine Corps Doctrinal Publication 8, *Information*. Rapidly evolving technologies have changed the character of warfare and expanded the ability of Marines to create and exploit information advantages. Understanding this evolution and its link to enabling Marines to out-think, out-compete and out-fight our adversaries underpins the Marine Corps' ability to win the fight for information in support of the joint force. To this end, the MCWP 8-10 supports integrating the information warfighting function in all operations to make the Marine Corps a more lethal, capable and ready force.

MCWP 8-10 addresses the four functions of information (generate, preserve, deny, project) by describing a method for Marine Corps commanders and their staffs to plan and integrate information into operations and command activities. It provides the practical link connecting our maneuver warfare philosophy to the detailed tactics, techniques, and procedures found in reference or tactical publications. Further, MCWP 8-10 describes the means for *conducting* information by identifying those activities across all warfighting functions that can generate information advantages, and then presents a method to assess the effectiveness of those activities.

Overall, MCWP 8-10 provides a practical reference for Marine Corps commanders, their staffs, and personnel to better leverage the power of information to gain advantages in all types of operations and command activities. Adversaries will continue to exploit a rapidly evolving technology and global security landscape to undermine traditional joint force advantages. Marines should expect MCWP 8-10 to be revised as often as needed to keep it current and relevant.

MCWP 8-10 supersedes MCWP 3-32, *Marine Air-Ground Task Force Information Operations*, dated 1 July 2013, erratum dated 2 May 2016, and change 1 dated 4 April 2018. Reviewed and approved this date.

Todd D. McCarthy

TODD D. MCCARTHY
Colonel, U.S. Marine Corps
Director, Plans and Strategy Division, Deputy Commandant for Information

Publication Control Number: 143 000184 00

Table of Contents

CHAPTER 1. INFORMATION FUNDAMENTALS

CHAPTER 2. THE MEANS AND METHODS FOR CONDUCTING INFORMATION IN MARINE CORPS OPERATIONS

CHAPTER 3. INFORMATION PLANNING

CHAPTER 4. COMMAND AND CONTROL OF INFORMATION ACTIVITIES

CHAPTER 5. ASSESSMENT: MEASURING INFORMATION EFFECTIVENESS AND PERFORMANCE

Appendices

Glossary

References and Related Publications

CHAPTER 1.
INFORMATION FUNDAMENTALS

"Marines apply the Marine Corps information warfighting function to create and exploit information advantages on all points of the competition continuum."

—Marine Corps Doctrinal Publication 8, *Information*

Marine Corps Warfighting Publication (MCWP) 8-10, *Information in Marine Corps Operations,* expands upon Marine Corps Doctrinal Publication (MCDP) 8, *Information*, to describe how the Marine Corps information warfighting function applies to Fleet Marine Forces (FMF) and the supporting establishment, throughout   the competition continuum. MCWP 8-10 describes how to integrate the information warfighting function into planning, operations, and other command activities and discusses foundational Marine Corps information warfighting function concepts, principles, and practices. Each unit and organization should tailor the contents of this publication to meet commanders' specific mission requirements, battle rhythm events, organizational constructs, and command relationships.

INFORMATION AND THE CHANGING CHARACTER OF WARFARE

The nature of warfare remains uncertain, complex, and violent, as described in MCDP 1, *Warfighting*. However, the changing character of competition and warfare in this information age is punctuated by the diffusion of power and technology, increased potency of effects across domains, and the exponential connectivity that enables the convergence of effects. Defeating the enemy in current and future battlespaces will most likely depend on controlling information and the networks that allow information to flow more effectively than that of the enemy. Peer adversaries are increasingly capable of leveraging the global proliferation of sensors, abundant data, virtually unlimited computing power, artificial intelligence, and higher connectivity to adapt, evolve and, in some cases, transform their capabilities to offset historical US military advantages (Joint Publication (JP) 1, Volume 1, *Joint Warfighting)*.

To compete and fight effectively in changing environments, the Marine Corps is developing concepts, capabilities, formations, training, and doctrines to maintain a competitive edge. To succeed in joint warfighting, the Marine Corps must continually adapt and leverage the way information connects and converges the effects of reconnaissance and counter-reconnaissance; communications, computers, cyberspace and space operations; as well as targeting, and other information activities conducted by FMF throughout the competition continuum. An information activity refers to the employment of information capabilities to create exploitable advantages and desired effects.

A primary goal of the Marine Corps' continuous evolution and adaption is to gain information-based advantages that result in decision advantage, higher tempo, power projection, resiliency, and the disruption of the enemy system across domains, at echelon, and scaled to mission. The Marine Corps and joint force fundamentally recognize that information itself, and the ability to effectively generate, preserve, deny, and project it to gain competitive and combat power advantages, is central to the Marine Corps' contribution to joint and combined warfare. In essence, information is a form of power that must be exploited and protected to effectively compete, fight, and win in the information age.

INFORMATIONAL POWER

Power is the capacity or ability to direct or influence the behavior of others or the course of events. Warfare, and all other forms of competition, are fundamentally about the distribution and redistribution of power through a contest of wills. Information is a form of power that the United States leverages, in concert with diplomatic, military, and economic power, to influence events and achieve outcomes in support of national objectives. Applying informational power within a military context span from the strategic level of warfare to tactical unit and even individual actions throughout the battlespace.

Strategic Level Informational Power

The diplomatic, informational, military, and economic instruments of national power provide a framework that the United States uses to assess potential competitors and describe the security environment. At the strategic level, informational power refers to the use of information, narratives, and technical means to advance the Nation's interests and achieve objectives. The Marine Corps, as a component of the military instrument of power, supports advancing national objectives through the informational instrument by its presence, operations, and other actions to demonstrate resolve, or otherwise influence the perceptions, decisions, and behaviors of relevant actors.

At the strategic level, the Marine Corps' theory of information in warfighting is a simple acknowledgment that the physical actions of military operations and activities are used to influence a wide range of relevant actors. The very existence of the Marine Corps sends a message to potential adversaries that there are interests over which the United States is willing to fight. Military power, throughout history, has existed to send messages to adversaries and potential adversaries, relevant observers, and allies. Leaders, nations, and states assemble military power to intimidate, challenge, and influence the behavior of relevant adversarial audiences. They also assemble military power to reassure, reinforce, and empower friendly relevant actors. At the most fundamental level, military organizations exist to convey messages—through the uniforms, ceremonies, and mere presence of forces—that emphasize power and power potential. These actions reaffirm the fundamental purpose of military power and actions; to influence and adjust the will of an opponent.

Operational and Tactical Level Informational Power

At the operational and tactical levels of warfare, the Marine Corps views informational power as applicable throughout the competition continuum. A relationship between informational power and physical power exists, such that the commander can combine both to pursue specific information advantages that help achieve objectives and other military advantages (e.g., achieve tempo or decision superiority).

The forces with the ability to manipulate, deny, or destroy the information required for the basic functioning or decision making of the enemy's or adversary's system (e.g., equipment, personnel, organizations), while preventing them from doing the same, achieves significant advantages.

When the mission does not require using combat power, Marines can still seek to gain and exploit information advantages by influencing the perceptions, decisions, and behaviors of others. This can include actions that range from conducting military demonstrations to persuading local leaders through engagements, exposing adversary malign behavior in local media, conducting civil-military operations (CMO), or by disrupting adversary communications, disinformation, and propaganda networks.

Although Marines have always used information to support military objectives, using the information warfighting function as a practical framework to think about and pursue specific information advantages is new. The information warfighting function, and its rationale for existence, are discussed in more detail later in this chapter.

INFORMATION IS A COMMON DENOMINATOR

While information describes a form of power and is a warfighting function, it has always been a critical element of competition and warfare. From conducting planning to deceiving the enemy, the act of gathering, combining, understanding, protecting, denying, and using information will always be an inherent part of every type of military operation or activity. Information can be viewed as a common denominator underpinning all that Marines and units do. The following sections discuss information from the following three perspectives:

- Information in its many forms.
- The information environment.
- The use of information within warfighting functions.

These sections also provide examples of information as a common denominator in operations.

Information in its Many Forms

All Marines use information to perform primary or supportive roles. The word information is commonly understood as a representation of an idea or thought in tangible form such as a symbol, word, image, number, or pattern. These tangible "building blocks" are the raw material of communication, human understanding, and decision making. Material can be recorded, stored, gathered, transformed, communicated, observed, combined, analyzed, or used to transfer ideas and instructions that drive decision making and action. In short, information is central to the functioning of military organizations as a system. Not all forms of information have equal utility or value, as some might be incomplete, unvalidated, or unprocessed. As such, it is intentionally transformed from one state to another to improve its utility, and in the process evolves from raw materials (signals or data), to processed or categorized data and knowledge, and ultimately into the full complexity of understanding. Figure 1-1 illustrates the primary forms of information as it evolves.

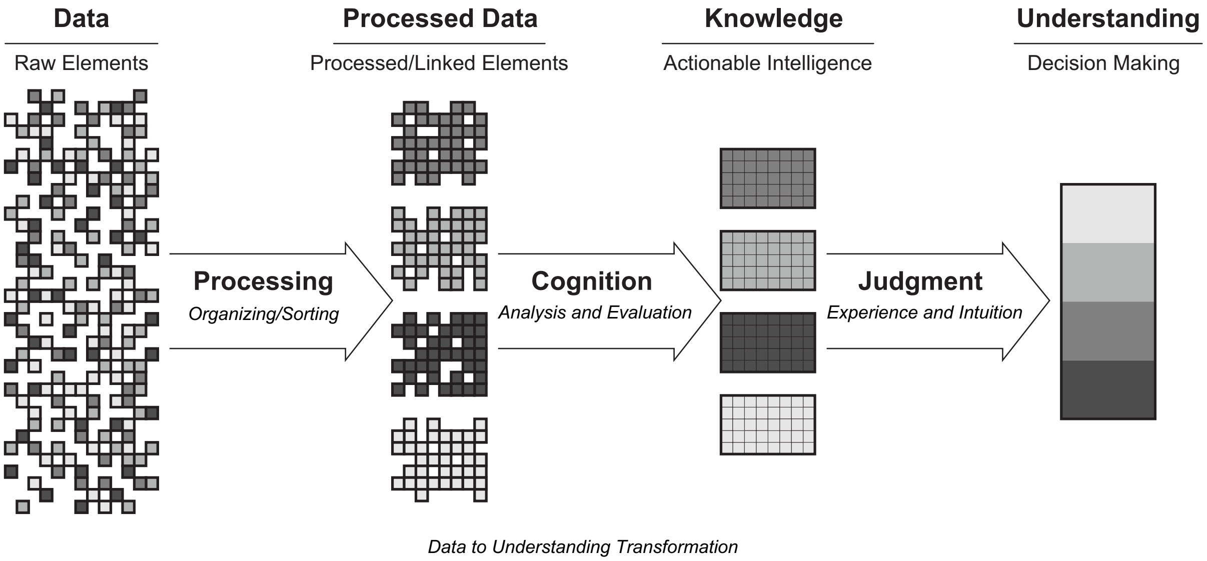


Figure 1-1. Transformation from Data to Understanding

All forms of information can have value and utility. For example, intelligence is a form of information because it involves the creation of *knowledge* about the enemy and environment to inform the commander's understanding and decision making. An operation order (OPORD) results from a planning process, which combines information with human experience and judgment to create a product that supports situational understanding, decision making, and action. Raw data, such as an intercepted-but-unanalyzed radio transmission holds potential; with context, it could heighten awareness of activity in the area.

Information Environment

Marines exist within and communicate through a modern, highly connected information environment in the performance of their duties and when off duty. Marines must consider the potential risks for any on- or off-duty communication to be seen on a global scale. The information environment includes information itself and all relevant social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information. The information environment also includes the individuals, organizations, and systems that collect, process, disseminate, or use information. As a global competitive space spanning all domains, the information environment can be thought of as an "always live" and a contested physical and cognitive maneuver space where military advantages can be gained or lost. The information environment exists in its modern form because information and the technologies of information have fundamentally changed this environment and the character of warfare.

Information and the Warfighting Functions

Warfighting functions encompass all military activities that occur in the operational environment and serve as a model for understanding the complexities of military operations. They are activities and capabilities grouped into major functional areas that aid in planning and executing operations. Warfighting functions exist to fulfill distinct purposes and are mutually supporting. Information is a common denominator of all warfighting functions because each warfighting function (including the information warfighting function) uses information, at least in part, to help fulfill its distinct purpose. The following sub-sections briefly discuss the seven warfighting functions' use of information to fulfill their objectives.

Command and Control. Command and control (C2) encompass the exercise of authority and direction by a commander over assigned and attached forces to accomplish the mission. It is how the commander determines what needs to be done and sees to it that appropriate actions are taken. The purpose of command and control is to harmonize all functions and operations into a meaningful whole. Information is central to command and control because it supplies the primary material that the commander uses to build situational awareness, inform decision making, and direct and influence action. Examples of information relevant to command and control include the common operational picture, common tactical picture, plans and orders. For further information refer to, JP 3-0, *Joint Campaigns and Operations*, and MCDP 6.

Maneuver. Maneuver is the employment of forces in an operational area, through movement in combination with fires and information, to achieve a position of advantage with respect to an adversary or enemy (*DoD Dictionary of Military and Associated Terms*, hereafter referred to as *DoD Dictionary*). The purpose of maneuver is to create or exploit positional advantage to enable mission accomplishment or other forms of advantage—such as superior tempo or psychological effects. Information is a primary consideration of maneuver in so far that the latter encompasses actions that seek to mask, manipulate, or amplify the information (i.e., signatures) of the maneuvering force. Examples of information relevant to maneuver include the visible attributes of the maneuvering force such as presence, posture, and profile.

Fires. Fires is "the use of weapon systems or other actions to create specific lethal or nonlethal effects on a target" (*DoD Dictionary*). The purpose of fires is to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight. Information is a primary consideration of fires intended to deny the adversary's ability to gather, process, understand, or use information. Fires may also be used to create psychological impacts. For fires to be effective, fires personnel require trusted access to accurate targeting information to plan and conduct fire missions. For further information refer to, JP 3-09, J*oint Fire Support*, and MCWP 3-31.

Intelligence. Intelligence is "the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (*DoD Dictionary*). The purpose of intelligence is to inform decision making and to support force protection. Information is central to the intelligence warfighting function because it is the primary material collected, processed, and transformed into higher levels of relevant and actionable knowledge to inform decision making. Examples of information relevant to intelligence include raw sensor data and collections information gathered across all intelligence disciplines. For further information refer to JP 2-0, *Joint Intelligence*, and MCWP 2-10, *Intelligence Operations*."

Logistics. Logistics is "planning and executing the movement and support of forces" (*DoD Dictionary*). It is the aspect of military operations that deals with the procurement, transportation, and maintenance of military materiel, facilities, and personnel. The purpose of logistics is to provide the force with the physical means of waging war and to regenerate combat power.

Information is a primary consideration of logistics regarding the ability to mask, manipulate, or amplify the information (signatures) of the logistics force. Additionally, logistics personnel also require trusted logistics information (maintenance status, levels of supply, forecasted requirements) to plan and conduct logistics operations. For further information refer to MCDP 4, *Logistics*, and JP 4-0, *Joint Logistics*.

Force Protection. Force protection encompasses all efforts to secure and defend the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area to maintain mission effectiveness. The purpose of force protection is to safeguard friendly centers of gravity (COGs) and to protect, conceal, reduce, or eliminate critical vulnerabilities. Information is a primary consideration of force protection because Marines seek to deny an opponent information (i.e., indicators) about the protected force. Additionally, force protection personnel require trusted, threat-informed intelligence to plan and conduct force protection. For further information refer to MCDP 1-2, *Campaigning*.

Information. The information warfighting function includes the material and actions taken to generate, preserve, deny, and project informational power to increase and protect competitive advantage or combat power potential within all domains of the operational environment. The purpose of the information warfighting function is to create and exploit information advantages. Information of any kind, ranging from raw data to knowledge and understanding, is the material generated, preserved, denied, and projected through the information warfighting function during operations.

INFORMATION WARFIGHTING FUNCTION

The Marine Corps information warfighting function is a framework used to support planning and to conduct operations that leverage information for advantage. Information described as a warfighting function is a distinct idea from information itself (as illustrated in Figure 1-1). Two questions must be answered to help Marines develop an understanding of the information warfighting function. First, how can information be a warfighting function? Second, why did the Marine Corps establish information as a warfighting function?

How Can Information be a Warfighting Function?

Information can only be a warfighting function when it is viewed as a framework of activities like the other warfighting functions. Just as Marines conduct fires, maneuver, or command and control, Marines conduct four information function activities: generate, preserve, deny, and project information.

Why Did the Marine Corps Establish Information as a Warfighting Function?

In 2019, the Marine Corps established the information warfighting function after adopting the joint force’s 2017 rationale used to establish the information joint function. The Marine Corps accepted the Chairman of the Joint Chiefs of Staff assertion of the need for a “philosophical change in how the joint force uses information to achieve strategic and operational objectives.”

This philosophical change is oriented on resolving the longstanding shortcomings of information operations that limited the joint force's ability to compete below the level of armed conflict and engage transregional, multi-domain, and multi-functional threats facing the joint force.

Information operations were often viewed as separate operations rather than activities integrated into the overall joint effort. Additionally, all military capabilities have informational potential. However, information operations focused solely on the employment of information-related capabilities (now referred to as information capabilities or activities), effectively ignoring the inherent information attributes of military operations and other activities. Additionally, information operations principally focused on adversary decision making and behavior, ignoring other relevant actors that shape the strategic and operational environment.

By accepting the joint force's rationale, the Marine Corps established the information warfighting function. With this change, there is an enduring requirement for commanders to make information a primary consideration throughout the planning process and during operations. Further, there is a requirement for the Marine Corps to create formal doctrine (such as MCWP 8-10), consider new formations and capabilities, as well as establish training and education programs to ensure that Marines know how to conduct information warfighting function activities in a manner that satisfies the rationale stated above.

Information Warfighting Function Doctrine Logic

The information warfighting function is organized around a simple doctrine logic illustrated in Figure 1-2.

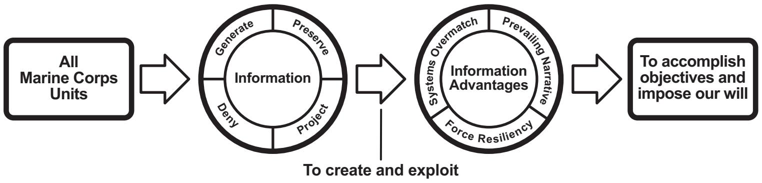


Figure 1-2. Information Warfighting Function Doctrine Logic.

The doctrine logic provides a practical framework that any Marine or Marine Corps unit or organization can apply. All Marine Corps units can generate, preserve, deny, and project information. The goal is to do these four functions deliberately to create and exploit information advantages that support accomplishing mission objectives and imposing our will over an opponent. The following sections discuss the four functions of information and the three types of information advantages (systems overmatch, prevailing narrative, and force resiliency) illustrated in Figure 1-2.

Functions of Information. Just as there are functions of logistics and functions of intelligence, there are functions of information. The following four functions of information are what make the information warfighting function a warfighting activity.

<u>Generate Information</u>. Generating information is the act of creating or obtaining the information needed to understand the situation, make decisions, direct actions, and conduct assessments. Marines and Marine Corps units and organizations generate large amounts of information, including intelligence information to perform their missions and conduct unit activities.

Information generation includes any process or capability involved in collecting, gathering, accessing, combining, processing, storing, or displaying the information needed to plan and conduct operations, support decision making, or perform any mission, task, or support activity. Information generation activities include, but are not limited to, the following:

- Collect data and information to feed the intelligence cycle (e.g., reconnaissance).
- Develop intelligence products.
- Provide situational awareness (multi-domain or all-domain), to include information environment and electromagnetic spectrum (EMS) awareness.
- Gain and maintain physical or virtual access to information, systems, and networks.
- Access, gather, and process friendly force reporting and status information.
- Develop plans, orders, tasks, and instruction.
- Conduct analysis and develop assessments, estimates, reports, and briefs.
- Acquire or create visual information.

Preserve Information. Preserving information is the act of preventing the loss, corruption, or destruction of friendly force information against external and internal threats. This requires constant vigilance by maintaining, protecting, defending, and securing the systems, software, and networks that store, process, or communicate information needed to plan, conduct, and coordinate operations. All Marines and Marine Corps units and organizations have a role in preserving the information generated in support of planning and operations. Typical information preservation tasks include but are not limited to the following (many of which are common to other warfighting functions):

- Assure C2 and critical systems, including cybersecurity and defensive cyberspace operations (DCO).
- Conduct fires or other offensive actions (e.g., offensive cyberspace operations [OCO]) to counter enemy attacks targeting friendly information, communications, intelligence, or C2 nodes.
- Conduct physical security and implement redundant and distributed data storage.
- Exercise information discipline and good cyberspace hygiene.
- Routinely practice continuity of operations.
- Maintain unit histories.

Deny Information. Marines engage opponents to deny their ability to gather, fuse, process, display, understand, or use the information needed to make decisions, generate effects, or act in a coordinated fashion. This includes concealing, misrepresenting, or altering information; or disrupting, destroying, or preventing the acquisition of information the enemy or adversary needs to function, understand the situation, and make decisions. Information denial activities can involve a range of actions from across Marine Corps warfighting functions, such as employing fires to destroy enemy collection or C2 capabilities. Information denial activities can also be used to support maneuver through operations security (OPSEC) or concealment. All Marines and Marine Corps units and organizations can conduct or support information denial activities. The following are typical examples of denying information:

- Conduct OPSEC and signature management (SIGMAN).
- Deceive adversary decision-makers or foreign intelligence entities (also referred to as FIEs) by—
  - Supporting joint military deception (MILDEC) under approved authorities.
  - Conducting tactical deception (TAC-D).
  - Conducting deception in support of operations security (DISO).
- Attack and exploit networks, systems, and information.
- Practice information discipline in public spaces and social media.
- Counter enemy propaganda and foreign malign influence through informing and influencing activities.
- Conduct counter-reconnaissance operations.

Project Information. Projecting information is the act of communicating, transmitting, or delivering information of any type to inform, influence, or deceive an observer or targeted system. Information projection activities range from using official communication to informing allies and the US population of Marine Corps activities to using TAC-D in support of ground force maneuver. Typical information projection tasks include but are not limited to the following:

- Conduct military exercises with allies and partners.
- Conduct humanitarian assistance distribution.
- Conduct CMO and key leader engagements (KLEs).
- Conduct shows of force, military demonstrations, or freedom of navigation operations.
- Leverage other inherent informational aspects of military operations (including presence, posture, and profile).
- Conduct public affairs activities to inform domestic and international audiences.
- Conduct offensive cyberspace operations (OCO) to attack and exploit networks, systems, and information.
- Publish command activities to communicate a command narrative.
- Conduct military information support operations (MISO) to influence foreign target audiences.
- Conduct deception activities to affect enemy and adversary decision makers' perception and behavior.

Information Advantages. An information advantage is an exploitable condition that results when one side can generate, preserve, deny, or project information more effectively than the other. By applying the functions of information in combination with other warfighting functions during operations, Marines can generate effects that result in information advantages.

Marines must understand that an information advantage is not an end state or objective unto itself. Instead, like other advantages (e.g., air superiority), information advantages are often temporary conditions exploited to achieve or pursue other objectives. Using the air superiority example, Marines exploit this advantage in the air domain to conduct other missions and achieve objectives —most often in other domains—such as when providing close air support for troops in contact. There are three primary types of information advantages that define a minimum set, or grouping of advantages that Marines should consider in planning and aim to achieve. The three basic types of information advantage are: *systems overmatch, prevailing narrative*, and *force resiliency*.

Systems Overmatch. Systems overmatch refers to the technical advantage one side has over another, yielding fires, intelligence, maneuver, logistics, force protection, or C2 advantages. The warfighting functions and systems used to perform these functions, depend on assured access to trusted information, whether that information is accessed through distant remote servers, or retained locally. The same holds true for our enemies and adversaries and their respective functions and systems. By denying, degrading, manipulating, or destroying the information flowing to or within an enemy's systems (e.g., weapons systems, intelligence, C2 systems) Marines can sow doubt or confusion, or disrupt the enemy's ability to function in a cohesive way.

Disrupting, manipulating, or destroying information or information-dependent systems involve ongoing offensive and defensive actions in the battle for systems overmatch. These actions, combined with influence activities, deception, and supporting actions, can result in significant military advantages. History is full of examples of one side achieving exploitable systems overmatch conditions that resulted in other advantages such as tempo, precision, or the ability to mass overwhelming firepower. Operation DESERT STORM, which occurred from 1990-1991, provides a primary example of systems overmatch. The United States and its allies achieved systems overmatch early in the conflict, resulting in overwhelming information superiority that was exploited to apply overwhelming firepower, speed, and precision in battle. Once the ground war started, Iraqi defenses collapsed in less than 96 hours.

Prevailing Narrative. A prevailing narrative is a critical type of information advantage that Marines seek to create and exploit. Narratives are essential underpinnings to every operation and activity because they give meaning to a set of interpreted facts. The prevailing narrative is credible and resonates the most with the intended audience. The crafter's goal is to achieve a prevailing narrative that results in a public opinion or perception advantage by eliciting trust, establishing credibility, and fostering belief in the friendly force's presence, mission, and objectives. If this already exists or is achieved, the prevailing narrative becomes exploitable; popular trust can result in popular support for the unit's presence and mission. The prevailing narrative between any two opponents can be compelling, might not be entirely truthful, and can lead to the success or failure of one side over another. For example, several negative prevailing narratives about US involvement in Vietnam eroded US popular support. The loss of popular support undermined the tactical and operational successes and ultimately led to the United States' withdrawal from the conflict.

Force Resiliency. From an information perspective, resiliency embodies a Marine or a unit's ability to resist, counter, and prevail against enemy and adversary reconnaissance, technical disruptions, and foreign malign influences, such as misinformation and disinformation. In short, Marines resist, counter, and prevail against any threat that targets their systems and psyche. Technical resiliency involves the capabilities and tactics, techniques, and procedures (TTP) used to recover from systems outages, and attacks against data, networks, and information systems. Psychological resiliency involves the capabilities and TTP Marines use to recognize when they are being targeted by foreign malign influence activities, then mentally isolate and block those activities, and carry on with the mission. Both technical and psychological resiliency are exploitable advantages when one side experiences less disruption than the other, resulting in minimal loss of speed, focus, mass, or cohesion relative to the other.

INFORMATION IN A COMBINED ARMS FUNCTIONAL APPROACH

The speed, reach, and persistent nature of information in the modern information environment not only makes the world a "smaller place," but also compresses the levels of warfare and erases the traditional notion of battlespace boundaries. Information in today's highly connected world also impacts the foundational concept of combined arms. MCDP 1 states, "Combined arms is the full integration of arms in such a way that to counteract one, the enemy must become more vulnerable to another." Marines pose the enemy not just with a problem, but with a dilemma—a no win situation. The concept of combined arms remains as applicable today as in any previous century. However, if the historical frame for understanding combined arms involved combining supporting arms and organic fires to defeat enemies in battle, then the current frame for understanding a combined arms functional approach must involve combining supporting arms and organic fires with maneuver and information to create dilemmas not only against enemies in battle, but also competitors throughout the competition continuum. Figure 1-3 illustrates a model for information in a combined arms functional approach.

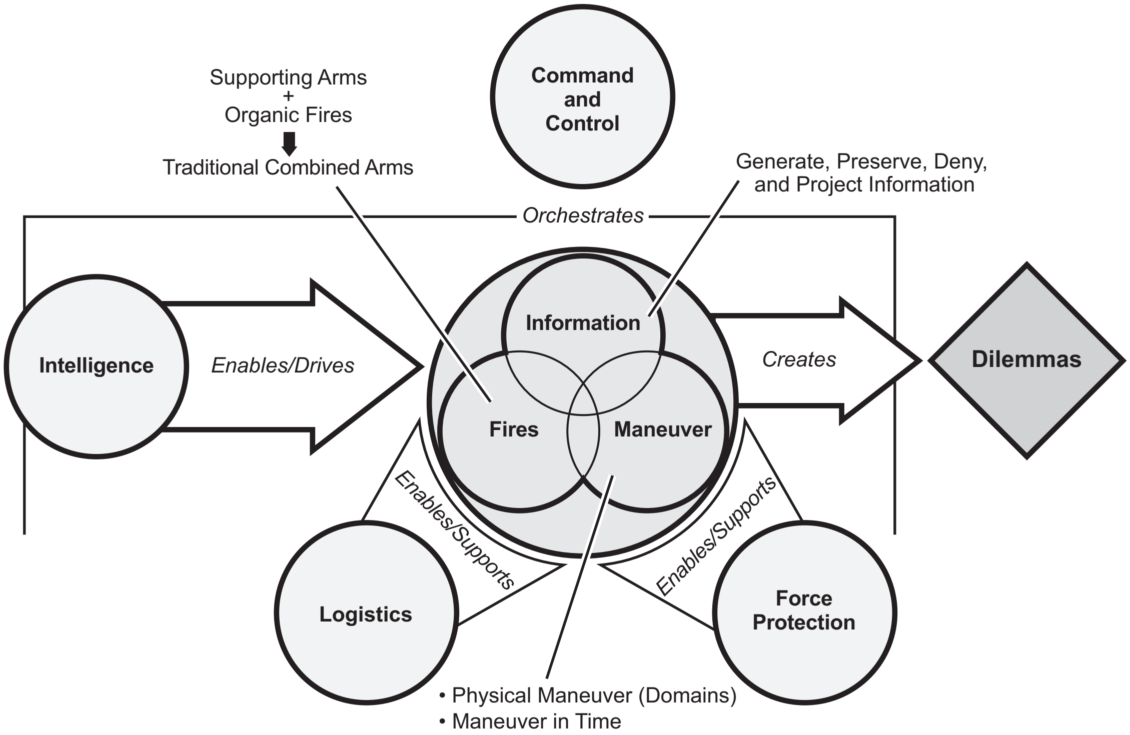


Figure 1-3. Information in a Combined Arms Functional Approach.

Marines should understand that an expanded concept for combined arms is to use a functional approach to competition and warfare by involving all warfighting functions to create, enable, or support an array of dilemmas or other effects. At the model's core are the fires, maneuver, and information warfighting functions. They generate direct, first-order effects when applied in operations. Intelligence sits at the left side of the model to indicate its role in identifying opportunities to create dilemmas; thus, effectively driving or critically enabling, the creation of dilemmas and the activities of the other warfighting functions.

Marines conduct counterintelligence activities to deny or disrupt an opponent's ability to gather information or otherwise develop intelligence about friendly forces. Such activities align under the information warfighting function as information denial. Command and control sit at the top of the model because it is used to orchestrate and harmonize the timing, tempo, and focus of combining the other warfighting functions to create dilemmas. Logistics and force protection sit at the flanks of the model to illustrate their enabling and supporting roles in creating dilemmas. Objectives are indicated at the right side of the illustration to denote the purpose and orientation of the entire model.

Information sits at the core of Figure 1-3 because, like the other warfighting functions at the model's core, information is used to create first-order effects (particularly information generation, denial, and projection activities). Combining information activities with fires and maneuver at the right time and place can create dilemmas. For example, when a target system analysis reveals an exploitable vulnerability in an enemy integrated air defense system (IADS), Marines could execute a combined electromagnetic and cyberspace attack (information projection) at a specific time to blind the enemy (information denial) and cover friendly maneuvering forces in the attack. The dilemma in this example involves a cascade of events that starts with degraded enemy situational awareness, which then leads to increased uncertainty and a paralyzed enemy vulnerable to destruction. The specific dilemma to the enemy is: react while blinded and increase visibility and exposure to additional forms of attack or do nothing and await destruction by the maneuvering force in the attack. Additional examples of creating dilemmas with information, fires, and maneuver include, but are not limited to, the following:

- Electromagnetic attacks to steer enemy units onto exploitable radio frequencies to render the enemy units vulnerable to physical attack, intelligence collection, or usurpation of command and control through projections of false orders.
- Denial of service attacks against enemy media operations steers repair personnel to a site, rendering them vulnerable to physical attack from aircraft.
- KLE succeeds in obtaining a persuasive local leader's willingness to echo friendly narrative, which renders enemy and adversary recruitment efforts less effective.
- Public communication and media engagements can expose an adversary's or enemy's actions and counter their influences to advance friendly narratives while simultaneously degrading enemy or adversary narratives.
- Stand-in forces' messaging and maneuvers stimulate a competitor's military and political system and either influence them to adopt a less aggressive posture or force them to reveal crucial information about their intentions and capabilities through their responses to our operations, activities, and investments.

COMPETING AND FIGHTING FOR INFORMATION

Marines apply the information warfighting function through a combined arms functional approach to gain information and other advantages over rivals throughout the competition continuum. The United States' rivals range from peer competitors to violent non-state actors. These actors increasingly integrate military force, ambiguous or dual-use activities, and information along with other instruments of national power to create dilemmas for the United States through combinations of lethal and nonlethal effects. Some adversaries have the strategic depth to wage protracted competition and warfare against the United States. Access to advanced technologies in a highly connected world allow some rivals to compete and fight over time with greater sophistication and less constraint from geographic, legal, or moral boundaries and factors. As a result, Marines today face an increasingly interconnected and complex operational environment with simultaneous combinations of cooperation, competition below armed conflict, and armed conflict (see JP 3-0). A good example of this is the competition for key maritime terrain in the South China Sea.

Maritime Reconnaissance and Counterreconnaissance

To counter rival campaigns and effectively compete, Marines implement a competition mindset that puts into practice a range of operations and activities that integrate physical actions and information activities to gain advantages, influence rivals, and reinforce alliances and partnerships. While Marines compete for any advantage (e.g., technological, placement or access, position on key terrain), they also compete and fight for information. The information fight entails Marines conducting reconnaissance and counterreconnaissance throughout the competition continuum. Reconnaissance and counterreconnaissance involve a constant cycle of detection, surveillance, obfuscation, deception, denial, analysis, and assessment of effectiveness. This cycle also entails operations and activities that Marine Corps units perform; thus, making reconnaissance and counter-reconnaissance primary operational activities Marines conduct throughout the competition continuum to gain an information advantage and influence potential adversaries in support of the combatant commander (CCDR) objectives. Reconnaissance and counterreconnaissance are distinct mutually supporting activities contributing to the fight for information.

Maritime Reconnaissance. Maritime reconnaissance includes all efforts to help the fleet locate the enemy or adversary sufficiently to deliver decisive effects. From key maritime terrain and seaward littoral operating areas, FMF conduct multi-domain reconnaissance operations to fight for information and conduct operational preparation of the environment. Maritime reconnaissance activities include baselining adversary and host-nation population patterns of life, identifying key infrastructure and maritime terrain, and conducting network development and engagement activities using clandestine and overt operations. Marines use the opportunity to learn while conducting operations and focus collections to identify adversary activity, provide early warnings for the fleet and joint force, develop intelligence to support naval information warfare activities and joint operations in the information environment (OIE). Maritime reconnaissance is also conducted to trigger counterreconnaissance operations and to assess operational effectiveness. While the above describes how reconnaissance generates information to support decision making, the act of conducting reconnaissance itself may be a form of information projection—particularly if reconnaissance activities are conducted in the open (e.g., visible patrolling). When this occurs, intelligence activities are used to project information by sending a message through presence and profile.

Fight for Information in the South China Sea

The widespread improvement of intelligence, surveillance, and reconnaissance (ISR) and targeting capabilities by peer competitors is a fundamental characteristic of a mature precision strike regime. Rivals use advanced surveillance and targeting capabilities as a hedge against long held US power projection advantages. This provides them the cover needed to pursue coercive strategies against neighboring countries who are often allies or partners of the United States. There is no clearer example of this than the People's Republic of China's (PRC)'s efforts to work under the protection of their strike capabilities to undermine the US strategy and change the balance of power in East Asia.

The PRC's actions serve as prime examples of using a combined arms functional approach below the threshold of armed conflict. Specifically, the PRC is applying a concept called the "Three Warfares" in the South China Sea. Marines should understand the Three Warfares as the PRC's comprehensive approach to competition that combines the informational effects of public opinion and media warfare, psychological warfare, and legal warfare with overt and ambiguous physical actions to advance territorial claims. The PRC's strategy is to leverage systems overmatch (advanced surveillance, targeting, and strike capabilities) with coercive actions (e.g., illegal fishing) to control the narrative and achieve objectives while thwarting its competitors' ability to respond.

Specifically, the dilemma works like this: The United States and partner nations can either physically engage PRC "civilian" fishing vessels enforcing territorial claims and risk war, or stand by and watch the PRC incrementally advance its claims and change the balance of power in the region toward its favor. In addition to using fishing boats to assert claims, the PRC has physically "maneuvered" by building key maritime terrain in the form artificial islands in the disputed seas—all despite continual international condemnation. These deliberate, persistent, and incremental efforts are conducted under cover of their strike capabilities, which includes the People's Liberation Army Navy operating in over-the-horizon "overwatch" positions.

In addition to the above, the PRC engages in aggressive media messaging through regional and global news outlets and digital media to promote its narrative of rightful historical claim. Even though this narrative is not accepted by most political leaders in the international community, it is consistent and has become normalized. The PRC's observed behavior in the South China Sea demonstrates a combined arms functional approach as an effective way of combining civil-military fusion, posturing, influence, and legal obfuscation to buy China time and space, which serves to further strengthen its position and prevent counteractions by its neighbors. The PRC's combined arms functional approach has significantly challenged the ability of China's neighbors to effectively oppose the PRC's pursuit of a territorial *fait accompli*.

As an element of the joint force, FMF contribute to day-to-day competition activities between the United States and its rivals and potential adversaries. This requires adopting a continuous view of aggressive rival actions seeking to make incremental progress toward their strategic goals below the threshold of armed conflict—such as those of the PRC describe above. It also requires deliberately integrating physical actions and information to create effects throughout the competition continuum. Marines today recognize that, even during "peacetime," each engagement, operation, and exercise conducted must not only fulfill specific training objectives but must also send the right message to potential adversaries, as well as to allies and partners. Additionally, peacetime activities can be used to satisfy national intelligence requirements, create dilemmas for adversaries, and to shape the operational environment if conflict is unavoidable.

Maritime Counterreconnaissance. Maritime counter-reconnaissance contributes to the fight for information by denying or deceiving the adversary's ability to collect information on FMF, and joint forces. Counter-reconnaissance imposes costs and sows doubt to cause inaction or to trigger the threat to culminate short of its objective. Additionally, counter-reconnaissance operations can be used to create de-escalation options to quell rising political tensions. During competition, counter-reconnaissance operations are used to influence adversary decision-makers to think that the cost of continuing their operations or activities is too high. In the event of conflict, counter-reconnaissance operations are conducted to screen the FMF as it maneuvers to establish sea control and sea denial through surface, aviation, and subsurface fires.

Narrative Competition

Competing and fighting for information embodies engaging in narrative competition on a day-to-day basis. Strategic competition between rivals involves competing narratives. Marine Corps units at all levels need to understand the overarching strategic narrative, nest command narratives, and unit activities within the higher-level narrative framework. Commands and units should also seek to understand the narratives already present in the region in which they are stationed or operating, and which narratives are favored by rivals and competitors. Marine Corps units must avoid actions and messages that are inconsistent with the command's preferred narrative. A command narrative explains the purpose and intent of the unit's posture and presence over the duration of the unit's mission. Command narratives provide a point of focus for planning and directing unit operations and activities. A command narrative is different than a commander's intent. The narrative is intended to reach all relevant actors, which includes but is not limited to the following:

- Competitor, enemy leader, or troops.
- Host nation population groups.
- Ally and partner leaders.
- Marines of a unit.
- Internal and external audiences.

The goal of a commander is to make the command's narrative the prevailing narrative. A strong command narrative anchors and guides all exercises, operations, and public communication activities that a unit performs throughout the competition continuum. Furthermore, a command narrative transcends specific unit missions, and should be tailored and adjusted as the mission progresses and the situation or environment changes. An effective command narrative is foundational to operations and provides greater understanding, credibility, and context to the unit's presence and mission. When done well, the command narrative aligns command personnel with a common purpose, enables mission tactics related to information, assures partners and allies, and deters and undermines competitors and adversaries. Actions are the strongest reinforcement of a narrative, so commanders should emphasize consistency between command narrative and force actions. See Appendix D for more information about command narrative.

All-Domain Command and Control and Assessment

A critical component of competing and fighting for information is conducting all-domain command and control. In the joint community, joint all-domain command and control is the art and science of decision making to rapidly translate decisions into action and leverage capabilities across all domains and with mission partners to achieve operational and informational advantage in both competition and conflict. All-domain command and control consists of the ability to sense, make sense of, and act across all domains, the EMS, and the broader information environment. It also implies that these contested spaces can and must be viewed as an integrated whole, akin to a 21st century single-battle concept—where actions in any one domain can affect actions in any other domain; and actions at one position on competition continuum can affect the conditions faced during a shift to another point on the continuum.

The ability to conduct all-domain command and control is an essential requirement for conducting 21st century combined arms. It embodies a feedback loop spanning domains to provide an integrated picture that informs decision making and assessment. All domain command and control requires the commander to understand threats, vulnerabilities, and opportunities in all domains in a manner that provides insight, and enables commanders to take actions relevant to their level of command in any or all domains. For more information about all-domain command and control and its relationship to information in Marine Corps operations, refer to Chapter 4. For additional information about assessments, refer to Chapter 5.

Joint Operations in the Information Environment

The Marine Corps is an integral part of the joint force—whether in support of day-to-day campaigning and integrated deterrence, or in support of major combat operations. Marines must understand how the joint force approaches the fight for information. The joint force fights for information by applying the information joint function. Like the Marine Corps, the joint force integrates its information function with all its other functions in operations to achieve objectives throughout the competition continuum.

A primary task of the information joint function is to leverage information to affect the behavior of opponents and other relevant actors. This involves planning and conducting joint OIE tasks. Joint OIE tasks are military actions involving the integrated employment of multiple information forces. This entails Active Component and Reserve Component forces of the Services specifically organized, trained, and equipped to create effects in the information environment. Joint OIE tasks aim to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and by protecting friendly information, information networks, and information systems. Joint OIE tasks leverage information ultimately to influence the will of adversaries and other relevant actors by affecting their awareness, understanding, and ability to act, while protecting joint force will, awareness, understanding, and ability to act in and through the information environment.

Joint OIE tasks are conducted as an integral part of all operations and campaigns and help shape the information environment for future operations. As such, joint forces will always be conducting one or more joint OIE tasks to remain continuously engaged in and through the information environment. Joint OIE tasks are conducted in support of all operations and may be a main effort or supporting effort. The Marine Corps does not use OIE terminology in Service doctrine but does recognize OIE as a joint force construct. As such, the Marine Corps provides information forces to CCDRs and joint task forces (JTFs) for employment in joint OIE. Information forces include Marines and Marine Corps units organized and equipped to employ specialized information capabilities that can be used by the joint force commander (JFC) to enable joint OIE tasks. Marines should familiarize themselves with joint OIE tasks because they help to plan or conduct them. Refer to JP 3-04, *Information in Joint Operations*, to learn more about joint OIE.

CHAPTER 2.
THE MEANS AND METHODS FOR CONDUCTING INFORMATION IN MARINE CORPS OPERATIONS

> *"The next fight will be a battle of signatures. Assume everything we do can and will be observed. On tomorrow's battlefield, to be seen is to be targeted, to be targeted is to be engaged, to be engaged is to be killed, at range and with precision!"*
>
> —Gen. Robert B. Neller, 37th Commandant of the Marine Corps

The information warfighting function is planned, executed, and assessed in operations by all Marine Corps units. Some of the means and methods used to conduct information activities in Marine Corps operations are organic to all types of Marine units and organizations. Other means and methods are provided by specialized information units and organizations (e.g., Marine expeditionary force information group [MIG]), which can be organic to FMF units or available through reachback support from joint, interagency, intergovernmental, or multinational partners. Table 2-1 summarizes the means and methods of conducting information activities in Marine Corps operations.

Table 2-1. The Means of Conducting Information Activities.

Inherent Informational Aspects of Military Operations and Activities	Specialized Information Capabilities and Activities
• Applicable to all units and personnel. • Most prevalent means of conducting information activities. • Examples include, but are not limited to— ♦ Physical attack. ♦ Presence. ♦ Posture. ♦ Profile. ♦ All other informational effects of conducting operations or other activities.	• Applicable to specialized information units and organizations. • Specialized information activities employ specific information capabilities to create or maintain exploitable information advantages or desire effects. • Examples include but are not limited to— ♦ Cyberspace operations. ♦ Influencing. ♦ Informing. ♦ Deception activities.

GENERAL INFORMATION ACTIVITIES

Inherent Informational Aspects of Marine Corps Operations and Activities

Every action a Marine Corps unit or individual Marine takes or does not take has the potential to communicate a message. Those actions and inactions are the features and details that an observer interprets to assign meaning to the observed activity. The inherent informational aspects of Marine

Corps operations and activities must be understood, synchronized, and leveraged as an integral part of planning and operations. This must be based on an informed understanding of the operational environment and identification of the effects desired. For example, the physical fires generated by a unit have inherent informational aspects, as do the presence, posture, and profile of Marine Corps forces. Similarly, all Marine Corps units generate signatures (technical, administrative, and physical) that need to be identified, understood, and managed through OPSEC and SIGMAN. All observed Marine activities are either consistent, inconsistent, irrelevant, or worse, contradictory to a prevailing narrative. The inherent informational aspects of operations and activities provide opportunity to create advantages by positively impacting the decisions and behaviors of relevant actors in a manner beneficial to friendly force outcomes.

Fires and Maneuver

Fires and maneuver can support the Marine Corps information warfighting function. Physical attack against enemy sensors, reconnaissance assets, communications relays, communication systems, or C2 nodes can be used to deny an enemy and adversary friendly information or the opportunity to observe or report on Marine Corps, joint, or multinational forces and activities. A physical attack can have psychological impacts on individuals at, or in the vicinity of a strike, but can also send other kinds of messages (i.e., revealing a capability or exposing an enemy vulnerability). Discriminate use of precision fires communicates concern for the safety and well-being of noncombatants while striking at our enemies. Complementing physical actions with immediate and deliberate messaging (e.g., MISO series) or other complementary information activities can result in clearer and more effective communication, ultimately affecting the enemy or other relevant actor's decision calculus and narrative in a manner that proves beneficial to Marine Corps, joint, or multinational forces.

Presence, Posture, and Profile

The physical presence of Marines in an area, what they are doing, and how they present themselves, is a form of information projection. It is the commanders' responsibility to make their intent clear and to ensure it is being met when it comes to presence, posture, and profile. Whether intended or not, Marines' presence, posture, and profile communicate a message that affects the decision making of observers. Marines must, therefore, always consider what message is being communicated   and ensure they are consistent with mission objectives, narrative, and intent.

Presence. Presence refers to a unit's physical or virtual existence. Presence can be a physical location (e.g., a Marine expeditionary unit [MEU] arriving at a foreign port) or virtual communication (a command's social media postings). Presence, or the absence of such, also communicates a message. For example, the mere presence of forces in a contested littoral or maritime environment sends the following message to adversaries: "We are here. We are the right combination of resilient and hard to detect. This allows us to remain here, and we see you." The presence of Marines in such an environment also provides the opportunity for generating information in the form of intelligence collection and reconnaissance.

Posture. Posture refers to a unit's capabilities and readiness for action. Marines can have a high or low security posture. A scenario where all personnel in a unit are maintaining full body armor, weapons systems in the most ready and appropriate conditions, and using body language that messages intent for action displays an active, aggressive, and high security posture. In contrast, a unit that is without full body armor, weapons down, and relaxed body language shows a lower security posture. Posture, as a form of information projection, communicates a desire, will, and attitude that is instrumental to supporting a Marine Corps, joint, or multinational narrative. Posture is also a key component in support of the Marine Corps force protection warfighting function.

Profile. Profile describes the size of presence and how locals perceive the unit. It reflects the posture and character of the unit, number of patrols it conducts, and how those activities are conducted. Are Marines a constant friendly presence or a hostile and anxiety-producing group that thunders through a few times a week? Are locals afraid to interact with the unit, or are they warm and welcoming? Is the unit viewed as a source of security, an economic opportunity, or an occupying force? Profile contributes to the unit's reputation in operations. Managing profile is yet another way Marines can project information and create or exploit advantages related to prevailing narrative or force resiliency.

SPECIALIZED INFORMATION ACTIVITIES

Inform Activities

Inform activities are those taken to communicate accurate and timely information to domestic, international, and internal Marine Corps audiences to build support for operational and institutional objectives. Inform activities use public communication, engagement, and visual media to counter disinformation, correct misinformation, and put Marine Corps operations, activities, and policies in context. Such communication is subject to OPSEC, statutory limitations, propriety, and the safety of personnel. At a minimum, conducting successful inform activities depends on the following key factors:

- Granted and delegated authority to publicly communicate. This includes the authority to release information on military operations and actions.
- A thorough understanding of the relevant society, culture, population perceptions, current prevailing narrative(s), and the media environment.
- Alignment with the United States Government (USG) strategic narrative.
- Close coordination with operational planners to prevent inadvertent disclosures of critical information.
- Close coordination with influence and deception planners to deconflict activities and avoid interfering with friendly communication.

Communication Strategy and Operations. Communication strategy and operations (COMMSTRAT) leads an expansive public communication mission for the Marine Corps. At all echelons of command, COMMSTRAT synchronizes, plans, and conducts information activities that advance FMF, Service, and ultimately, joint force, Department of Defense (DoD), and USG objectives by building public trust and strengthening essential relationships—all vital to public support, political will, and ultimately, success in the operational environment. Communication strategy and operations authority to engage and compete directly, daily, and globally with any audience, through various platforms, makes it a unique capability.

Adopting a competition mindset ensures COMMSTRAT's full integration into all aspects of staff planning. Participation ensures communication considerations shape operational planning, and COMMSTRAT actions are closely coordinated so they effectively contribute to desired operational objectives. Through a prevailing narrative, COMMSTRAT has a critical role in sustaining advantages by increasing knowledge, putting actions in context, providing transparency, and facilitating accurate perceptions through proactive, closely coordinated, and synchronized releases of accurate information, and through thoughtful in-person engagements. These actions also bolster public support, reassure allies and partners, and help deter or dissuade potential adversaries.

Communication strategy and operations is integral to the accomplishment of all Marine Corps operations through public affairs and combat camera (COMCAM) activities. The synergy of activities, when integrated with other operations and activities, is integral to the Marine Corps' ability to gain and exploit information advantages throughout the competition continuum. Communication strategy and operations plans and executes public affairs activities, which include the proactive, coordinated, and synchronized (or deliberately timed) release of accurate information to internal, domestic, and international audiences. Communication strategy and operations plans and executes COMCAM activities that provides imagery and product support to aid the commander, staff, and other information capabilities in operational decision making, planning and execution.

Both activities involve the acquisition, creation, and distribution of visual information, but their actions differ in purpose. For public affairs, visual information is created for public release under public affairs authorities. For COMCAM, visual information is created in various formats to support operations, and for public release by other information capabilities under their authorities.

Public Affairs Activities. The Marine Corps must take proactive measures to communicate with global audiences, providing context to the Marine Corps' mission, specialization, and operations. A function of command, public affairs is a strategic capability vital to meeting this objective. Public affairs activities include communication activities directed toward publics and stakeholders critical to mission success, public trust, and organizational fidelity. In execution of public affairs, COMMSTRAT drives and manages the daily release of truthful information and imagery to the range of audiences (US, foreign, friendly, neutral, adversary). They synchronize tactical military objectives and national strategic objectives by leading the development of communication strategies, narratives, and detailed communication plans and public affairs guidance with the staff and other information capabilities, and with higher, adjacent, and subordinate commands. Additionally, COMMSTRAT personnel advise the commander and staff on communication strategy matters and provide counsel on proposed courses of actions (COAs), policy decisions, and their impact on key publics.

Engagement is an essential component of public affairs activities, and COMMSTRAT personnel engage with key publics through various means to include the traditional media, social media, entertainment productions, official websites, as well as community outreach and face-to-face communication. Engagement also occurs through the public dissemination of communication and visual information products like written articles, photographs, videos, and graphics.

Department of the Navy (DON) and DoD policies outline the general authorities for COMMSTRAT personnel to release information and imagery. In general, commanders have release authority for their command and its actions and delegate this authority to their senior COMMSTRAT officer. Higher headquarters (HHQ) withholds or restricts release authority based on mission requirements. It is not uncommon for the White House, DoD, or US embassies to maintain release authority for issues or activities that incur risk that an operational unit does not own.

Public affairs activities support the accomplishment of the following:

- Providing accurate, timely, and truthful information to audiences.
- Maintaining the Marine Corps' reputation as a respected professional organization, a responsible steward of resources, and a military Service that contributes daily to the US achieving national strategic and military objectives while encouraging and enabling allies and partners.
- Ensuring trust and confidence in the US population, allies and partners, and internal audiences.
- Deterring and dissuading adversaries.
- Correcting misinformation and counter disinformation.
- When applicable, synchronizing capabilities that contribute to defense support, public diplomacy, and to optimize the effects and achievement of mission objectives.

Combat Camera Activities. In support of all operations, COMMSTRAT provides the Marine Corps' COMCAM capability. Combat camera helps conceptualize, acquire, create, reproduce, transmit, disseminate, and manage visual information in support of operational and planning requirements during wartime operations, worldwide crises, contingencies, humanitarian operations, joint exercises, and other events throughout the competition continuum. Visual information incorporates various visual media, with or without sound, that includes still and motion photography, audio video recordings, graphic arts, broadcast journalism products, photojournalism products, and visual presentations. Communication strategy and operations personnel are the primary suppliers of complex operational imagery, support to special missions, and documentation operations in areas of conflict.

Commanders and staffs must plan, task, sustain, and employ COMMSTRAT to support all mission functions where information advantages can be realized. Like public affairs, COMCAM is applicable across the competition continuum. Specifically, it provides visual information to the whole staff, including support to intelligence, operations, and other information capabilities.

The COMMSTRAT operations personnel who are specifically employed to conduct COMCAM activities intended to aid internal decision-making and provide staff support, do not possess their own public release authority. Visual information to be shared publicly in support of public affairs objectives must be reviewed and cleared for public release through public affairs authorities. Release of COMCAM imagery can also occur under authorities granted to other information activities. For example, psychological operations (PSYOP) personnel conducting MISO activities may be able to release COMCAM imagery in support of an approved series.

Considerations for the Employment of COMMSTRAT. Sustaining the trust and confidence of the US population, allies, partners, and internal audiences is a key COMMSTRAT objective. While COMMSTRAT communicates to competitors and adversaries to deter and dissuade malign behavior, its focus is on US citizens, allies, partners, and internal audiences, whose support is critical to mission success.

COMMSTRAT Competencies. Communication strategy and operations provide commanders increased flexibility, responsiveness, and utility when fully leveraged and synchronized with other information capabilities. The framework by which COMMSTRAT executes public affairs and COMCAM activities is described in the following core competencies:

- *Communication Counsel*. Advises the commander and staff regarding public communications and the impact of proposed COAs and policy decisions on relevant populations.
- *Research and Analysis*. Quantitative and qualitative research to better understand and define problems and opportunities, segment internal and external audiences into stakeholders and publics, and understand the cultural landscape surrounding the inherent informational aspects of Marine Corps operations. Research is used to anticipate and identify changes in the information environment, to include misinformation and disinformation, enabling leaders to adjust and respond, as needed, to ensure mission success.
- *Planning and Integration*. Ensures strategy and policy development at all levels includes communication considerations, to include responsibilities for communicating truthful, accurate information in support of transparency. The COMMSTRAT planners use the results of research to build communication strategies, plans, and campaigns; nest visual information requirements within operational plans; and provide the assigned COMMSTRAT manpower and equipment capabilities inputs into formal planning processes, through staff estimates and concepts of support.
- *Assessment and Evaluation*. Conducts real-time assessment of the information environment to include in-stride evaluation of the communication plan.
- *Engagement*. Proactively engages audiences through the social process of conversation and relationships, enabled by technical expertise in message and product creation, marketing, and dissemination.
- *Issue Management and Crisis Communication*. Assists in analyzing, prioritizing, and recommending policies and actions to solve or mitigate issue before they become a crisis. When crisis is unavoidable, COMMSTRAT advise son best COA to mitigate damage to reputation and maintain Marine Corps' institutional credibility.
- *Concept Development*. Develops specifically tailored products that support the commander’s intent which includes, but is not limited to, visualizing the final product desired and creating storyboards, written scripts, photo lists, conceptual graphics, layout and design, and social media promotion.
- *Imagery Acquisition*. Captures still and motion media to support the common operating picture, public communication, intelligence collection, investigative and evidential documentation, and historical documentation depending on the supported command or activity.
- *Product Creation and Dissemination*. Processes visual information into internal and external communication products. Products include the written word and visual information optimized

for intended publics, distribution channels, and ease of sharing by the publics to their networks through various media.

- Product Management. Manages releasable, non-releasable, and classified imagery and communication products from acquisition to archive.

COMMSTRAT Units of Action. Communication strategy and operations activities between the supporting establishment and FMF are inextricably linked. For example, a Marine supporting marketing and communication at a Marine Corps recruiting station can inject messages that may affect deployed Marines in the Indo-Pacific.

Within the FMF, COMMSTRAT personnel reside within the Marine Corps component commands, Marine expeditionary force (MEF) command elements, MEF major subordinate commands (MSCs), and major subordinate elements (MSEs). Communication strategy and operations personnel within the supporting establishment reside at joint commands, Headquarters, United States Marine Corps (HQMC), bases, posts, and stations, training and education commands, and Marine Corps Recruiting Command.

While all COMMSTRAT units and sections from the MEF and below can be task-organized to provide full-scale core competencies, the primary COMMSTRAT elements are operational support teams (also referred to as OSTs). These teams provide all COMMSTRAT core competencies and are task organized depending on the mission. The Marine Corps' primary source for these units are the Marine divisions and the three COMMSTRAT companies within the MIG. Operational support teams are typically composed of a single company grade officer, a staff noncommissioned officer, and a combination of combat photographers, videographers, and graphic specialists. Depending on the mission, operational support teams can include field grade officers, planners, and visual information officers. Operational support teams embed directly with the commands they support and include but are not limited to the following:

- Augmentation of JTFs.
- Augmentation of MEU and Marine expeditionary brigades (MEBs).
- Tactical employment within any Marine air-ground task force (MAGTF) element.
- Assignment with an expeditionary PSYOP detachment or team.

Influence Activities Considerations for COMMSTRAT. Influence is a natural by-product of all inform activities. Commanders and staff must be cognizant of the nuances between inform-based influence (e.g., public affairs activities, civil affairs) and exploitation-based influence (e.g., MISO). Marine Corps influence activities, including planning efforts, must avoid targeting the US Congress, US public, US news media, and other US entities. COMMSTRAT activities should be coordinated with information activities and civil military operations to optimize effects and the achievement of DoD goals.

Additional Visual Information Considerations. Communication strategy and operations provide a directed visual information capability; however, there are other sources of derivative visual information. Other sources include—

- Sensors on manned, unmanned, and remotely piloted platforms that collect imagery and consists of imagery obtained and processed from intelligence collection platforms, weapons system video, and optical systems.
- Camera systems integrated into land- and ship-based military equipment; security cameras; helmet cameras worn by personnel who are not performing COMMSTRAT functions.
- Imagery seized, captured, or confiscated by DoD personnel during or after military operations (captured enemy imagery can be a useful source of information once it has been exploited and declassified by proper authority).
- Imagery acquired by the DoD through contract, donation, or transfer.
- Derivative source visual information repurposed to support COMMSTRAT or other information capabilities (civil affairs, MISO, MILDEC)—including weapons system video showing the destruction of a target can be declassified and then released by COMMSTRAT to project a message of resolve for allies, reinforce prevailing narratives, and degrade an enemy's will.

COMMSTRAT Opportunities. Although high connectivity in the information environment presents numerous challenges, it also provides opportunities to engage publics that otherwise would not be exposed to information about Marine Corps forces and operations. These opportunities highlight COMMSTRAT's increased relevancy and enable the commander to gain a military advantage. Communication strategy and operations contribute to the generation, preservation, and projection of information. It is important for COMMSTRAT to be involved in managing perceptions alongside OPSEC planners, so that COMMSTRAT, and the supported commanders and units do not inadvertently reveal critical information. Communication strategy activities provide an important function in counterpropaganda by accurately documenting operations (to dispute false claims), and in the public release of statements and imagery (showing propaganda to be false).

Balancing COMMSTRAT and OPSEC. Communication strategy and operations activities present a unique knowledge and perspective of higher, adjacent, and subordinate public communication efforts, which make these activities vital to any OPSEC planning and execution. Communication strategy and operations ensure public communication considerations are addressed and that critical information is safeguarded. Operations security must be considered before, during, and after all COMMSTRAT activities to ensure public information does not create vulnerabilities or expose critical or sensitive information to enemies and adversaries. The balance between the need for OPSEC and the need to provide non-critical information to internal and external audiences must be addressed during planning and continue through mission execution.

Influence Capabilities and Activities

Power is the capacity or ability to direct or influence the behavior of others or the course of events. The relationship between informational power and physical combat power is such that the commander combines both forms of power to influence relevant actors (enemy, friendly, adversary, neutral), shape the environment, gain advantage, or defeat enemies in battle. The commander uses all available means to implement influencing behavior. This section narrows the broader discussion of influence (i.e., something all military forces do through their presence and actions) to discuss specific influence activities, which involve any activity conducted for the purpose of affecting the decisions and behaviors of a foreign target audience as a first-order effect. Influence capabilities are employed by specialized personnel with training in specific influence activities (e.g., civil affairs, MISO). At a minimum, the following factors must be considered for influence activities to be successful:

- Planners must have a sufficient understanding of the information environment and adapt their thinking about the actors who reside within it.
- Influence activities must be embedded into a command's planning effort up front.
- Influence activities are executed and assessed via a whole-of-staff and whole-of-command approach through the employment of multiple methods through one or more domains and in conjunction with other warfighting functions' activities.
- Planners must consider both offensive and defensive actions as a possible means of influence.

All four elements mentioned above are linked to influencing a foreign target audience. Marine Corps organizations and personnel conducting influence activities must avoid seeking to influence US audiences and journalists. Foreign persons or groups that a command needs to influence to shape decisions or behaviors in support of objectives become a command's target audience. The commander and staff precisely define the target audience and employ capabilities through one or more domains to create effects that drive the target audience to think and act in ways advantageous to friendly force objectives.

It is impractical to believe a commander can influence all relevant actors within the battlespace. Before identifying a target audience, the commander and staff must assess whether authorities or permissions to engage that target audience have been granted; the command has access to that target audience; and if there is a willingness to devote command resources to support influence activities on the target audience.

The foundation of all influence activities is a thorough target audience analysis (TAA). This analysis is supported by and conducted in concert with the overall intelligence preparation of the battlespace (IPB) and civil preparation of the battlespace during each step of the Marine Corps Planning Process (MCPP). The following sections identify and describe specific influence activities available to commanders.

Military Information Support Operations. Military information support operations convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of governments, organizations, groups, and individuals. The purpose of MISO is to induce and reinforce foreign attitudes and behaviors favorable to the originator's objectives. Military information support operations influence foreign attitudes and beliefs about US diplomatic, informational, military, economic, financial, intelligence, and law-enforcement power and resolve. They are also conducted to degrade the enemy's combat power and will to fight; or to reduce civilian interference, minimize collateral damage, and increase a foreign population's support for operations.

As politically sensitive activities MISO are conducted in accordance with applicable US law, regulations, DoD policy, and applicable international agreements and customary international law. The Marines in PSYOP units are specifically trained to execute MISO. Marines that execute MISO follow a seven-phase process to develop and deliver influence messages and coordinate the execution of other unit actions to affect the behavior of selected target audiences. The following sections describe the seven MISO phases.

Military Information Support Operations Planning. Military information support operations planning occurs continuously as part of the supported unit's planning process, which includes determining primary and supporting MISO objectives, identifying potential target audiences, and developing initial assessment criteria. Throughout the planning process, MISO planners must maintain situational awareness and an understanding of the effects that relevant individuals and groups have in the operational environment and on the unit's mission. Planners evaluate the psychological effects of military actions and provide advice to commanders on how to minimize adverse impacts and unintended consequences. It is essential that MISO planners include MISO assessment planning. Military information support operations assessment planning must start at the beginning the unit's planning cycle. Planners must include assessment criteria, assumptions, and other considerations (e.g., measures of effectiveness [MOEs]) and share these planning artifacts with the staff and appropriate working groups (e.g., collections or targeting working groups).

Target Audience Analysis. Through TAA, foreign groups or individuals are examined carefully for their ability to be influenced and affect objectives. This analysis provides insights on how best to influence the target audience to change its behavior to one that is more favorable to friendly force objectives. Military information support operations require cultural understanding to develop the most effective methods of persuasion for each target audience. Culture and narratives are the key lenses through which a target audience filters everything they perceive and understand. The results of TAA provide the foundation for the remaining process phases.

Series Development. In developing a series, Marine planners design multiple actions and messages, determine the appropriate mix of media, and develop an execution plan. Each series focuses on a single supporting MISO objective and target audience combination. Series are reviewed for their suitability, length or duration, potential to affect the target audience, accuracy of persuasive arguments or techniques to influence behavior change, and the resources available to execute them.

Product Development and Design. Product development and design is the process of incorporating the MISO argument into a series and making the specific products executable. Products refer to all individual artifacts (visual, audio, audiovisual) and associated actions derived from a series. The type and mix of products are outlined in the series and based on research conducted during the TAA. During this stage, pre-testing and post-testing methodologies are determined, supporting testing instruments (e.g., surveys, questionnaires, criteria, and instructions) are developed, and pre-testing of prototypes is conducted. The work completed during the planning, analysis, and series development phases is vital for designing individual products. Specific areas of operation or target audiences may be limited to certain products based on guidance from the approving authority.

Approval. By default, MISO series are approved at the combatant command (CCMD) level unless specifically delegated. Subordinate units can request the delegation of authority for specific approvals to streamline the approval process. Planners should not assume that their supported unit has been delegated any authorities unless the delegation has been explicitly spelled out. Approval is required before media production or the execution of actions for influence activities can begin.

Production, Distribution, and Dissemination. Production is the actual creation and generation of influence products (e.g., radio broadcast script, printed material). Marine Corps units can deploy with limited organic deployable production capability. Most large-scale production is accomplished through reachback support, theater-level assets, or local contracting. Communication strategy's visual information capabilities can be leveraged to support production.

Distribution is the movement of products from the producer to the disseminator. Depending on the type of product, this step may be very quick and low cost (e.g., the use of social media) or long and expensive (e.g., the transportation of mass-produced print products from the US to local foreign outlets). The time and cost associated with distribution needs are planned for in the development of series and products.

Dissemination is the act of getting the product to the target audience. Products are disseminated (information projection) over the air, on the ground, through the EMS and cyberspace, or stored for future use. Each means of dissemination has its own coordination requirements and requires a different approval depending on the area of operation.

Assessment. Assessing the effects of messages and actions on target audiences relies on intelligence collection and analysis of impact indicators produced in earlier phases. Assessment criteria supports the commander's MOEs and measures of performance (MOPs) and helps determine the effectiveness of an operation. Planners establish procedures to assess the effectiveness of influence efforts and continuously assess the effectiveness of MISO towards achieving the commander's objectives. Refer to Chapter 5 for more information about MOEs and MOPs.

Units of Action and Authority Considerations for the Employment of MISO. Military information support operations are conducted as a primary means of directly influencing an opponent to create mutually reinforcing and compounding effects, achieve objectives, and ultimately to impose one's will on another. The Marine Corps' MISO capability resides in the PSYOP companies and influence cells within the MIG and Marine Corps Information Operations Center (MCIOC). Tactical psychological operations detachments (also referred to as TPD) and tactical psychological operations teams (also referred to as TPT) are maneuver elements that perform MISO for the FMF. These detachments and teams support both conventional and special operations forces and are trained to account for statutory, policy, budgetary, and execution authority considerations in planning and conducting MISO. Authority considerations include the following:

- Statutory authority refers to the powers and duties assigned to a government official or agency through a law passed by Congress. Only certain elements are authorized by law to conduct MISO and all MISO activities require legal review prior to approval. This legal review is generally conducted by the approving authority (i.e., the geographic or functional CCMD).
- Policy authority is derived from DoD issuances and existing MISO programs, which are top-level guidance for the planning, conduct, and assessment of MISO. Marine Corps planners can leverage existing programs and affiliated series already in place at the global, regional,

and operational levels, or can initiate the development of a new MISO program following a rigorous process coordinated at the Joint Staff or Office of the Secretary of Defense level. Programs exist for global campaign objectives, CCMD theater responsibilities, all named operations, and various mission-specific requirements.

- Budgetary authority is required for MISO because they are congressional special interest items and are budgeted for and controlled by the joint staff. All aspects of MISO planning, conduct, and assessment must be funded through the approved funding lines. Funding is typically disbursed to the CCMDs with subordinate units including budgetary requests with their MISO products.
- Execution authority is required for an approved program to be conducted. Execution authority comes from an execute order (EXORD), either for a specific MISO activity or as part of the EXORD for an operation. Certain deployment orders constitute execute authority depending on the level and type of deployment authorized in the deployment order. All operation plans (OPLANs) and contingency plans include a MISO annex that outlines the execute authority as well. Execution is initiated through a MISO-specific EXORD or in support of an EXORD for an operation.

Key Leader Engagement

In the area of operations, physical proximity to civilians means that personnel will inevitably encounter local influencers and leaders. A KLE is a method for building relationships with people and groups that have influence. These interactions provide an opportunity to strengthen relationships, trust, and security Marines conduct KLEs to engage in critical dialogue and better understand and more effectively operate within a given cultural, social, and political environment. These engagements can help build alliances, encourage cooperation and noninterference, and boost support for US objectives. Engaging in dialogue with key leaders provides new information, resolves problems with civilian populations, and forges new partnerships within the battlespace. Senior-level KLEs help Marine Corps forces secure and maintain needed access, basing, and overflight rights.

At echelon, Marine unit leaders can organically conduct KLEs as an inherent informational aspect of military operations. Key leader engagements involving more senior leaders can be requested and coordinated through staff channels. Support for planning KLEs often involves personnel trained in civil affairs, MISO, or COMMSTRAT who may have important cultural, relevant behavioral, or social insights that can help with KLE planning, as well as suggestions for connecting the KLE with broader communication or influence themes and messages. Like all operations, KLE can benefit from intelligence input (knowing the identity and things about the organizational role of engagement subjects) and debriefs from KLE can be important feeders to intelligence collection. Marines conducting COMMSTRAT, MISO, or civil affairs activities can improve KLEs through cultural or linguistic contextual information, reviewing or providing talking points, and through discussions of how engagements might contribute to inform or influence objectives. When conducting KLEs, leaders and planners must consider several factors to maximize the opportunity and impact:

- Marines should consider the rank and position of the key local leader. As a show of respect and cultural awareness, the Marine leader attending the KLE should be equivalent in rank and responsibility.

- The Marine leader attending the KLE must respect and follow appropriate cultural norms and behavioral practices. Failing to abide by cultural norms risks turning a potentially beneficial KLE into a harmful event for the mission, and risks loss of advantages related to the prevailing narrative.
- The Marine leader in attendance should communicate in a way that demonstrates sincerity. The desired effect of any KLE is to build relationships, rapport, and trust between the Marine Corps, joint and multinational forces, and the local host nation. A lack of sincerity will undermine these efforts. Building trust through sincerity extends beyond the KLE event itself and can contribute to enduring information advantages.
- The KLE should be conducted with a competition mindset and with a focus on campaigning. The unit's actions must also be deliberately planned and aligned to support and demonstrate the message communicated through the KLE.

Civil-Military Operations

Civil-military operations are commander activities performed by designated military forces to establish, maintain, influence, or utilize relationships between military forces and local populations and institutions. Civil-military operations may include military forces performing activities and functions typically performed by the local, regional, or national government. These activities may occur before, during, or after other military actions. If directed, they may also occur in the absence of other military operations. Civil-military operations may be performed by designated civil affairs Marines, by other military forces, or by a combination of civil affairs and other forces. Civil-military operations are a commander's responsibility to meet the legal and moral obligation to protect the civilian population within their operational environment.

Commanders conduct CMO to achieve unified action between military and civilian counterparts during operations. Unified action synchronizes, coordinates, and integrates Marine Corps, joint, and multinational operations with the activities of other USG departments and agencies, nongovernmental organizations (NGOs), international organizations (e.g., the United Nations), and the private sector to achieve unity of effort. Unified action is achieved when all partners are integrated into planning and all actions are coordinated and synchronized to achieve common objectives. These operations can enhance situational understanding, mitigate threats to civil society, and capitalize on gains from military operations. Engagements with civil networks include opportunities for generating new information and collecting information, as well as sharing and projecting information and US perspectives. As possible contributors to a competition mindset, CMO planners should be included for their contribution to broader campaign objectives, as well as immediate mission objectives.

Distinguishing Civil-Military Operations and Civil Affairs Operations. Civil-military operations and civil affairs operations (CAO) are two distinct activities. Civil-military operations are conducted by any military unit or personnel in coordination with the civil population. Civil affairs operations, as a form of CMO, are those actions planned, coordinated, executed, and assessed to enhance awareness of, and manage the interaction with, the civil component of the operational environment. Additionally, CAO identify and mitigate underlying causes of instability within civil society; and can involve the application of functional specialty skills that are typically the civil government's responsibility. Any formation or unit can conduct CMO; however, CAO can only be conducted by personnel trained in civil affairs. Regardless of who is conducting these operations, they are about increasing operational effectiveness and achieving military objectives.

Electromagnetic Spectrum Operations

Electromagnetic spectrum operations (EMSO) are "coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment" *(DoD Dictionary)*. Electromagnetic spectrum enabled activities describe activities or actions that either utilize or rely on an EMS-dependent system or capability (e.g., radio, missile seeker, or radar). Examples of EMS-enabled activities include signals intelligence (SIGINT), space operations, cyberspace operations, MISO, and fires. Therefore, EMSO must be integrated and synchronized across domains.

The Electromagnetic Spectrum. The EMS is a contested maneuver space where military advantages can be gained or lost. The most common way to refer to the EMS is the portion most suitable for communications—the radio frequency spectrum (3 hertz [Hz] to 3 terahertz [THz] frequencies). However, maneuver across the entire EMS (3 Hz up to 30 exahertz [EHz]) is conceivable, particularly as developing technologies emerge and expand into portions of the EMS outside of radio frequencies (e.g., microwave weapons, lasers, optical communications). Figure 2-1 depicts the electromagnetic spectrum.

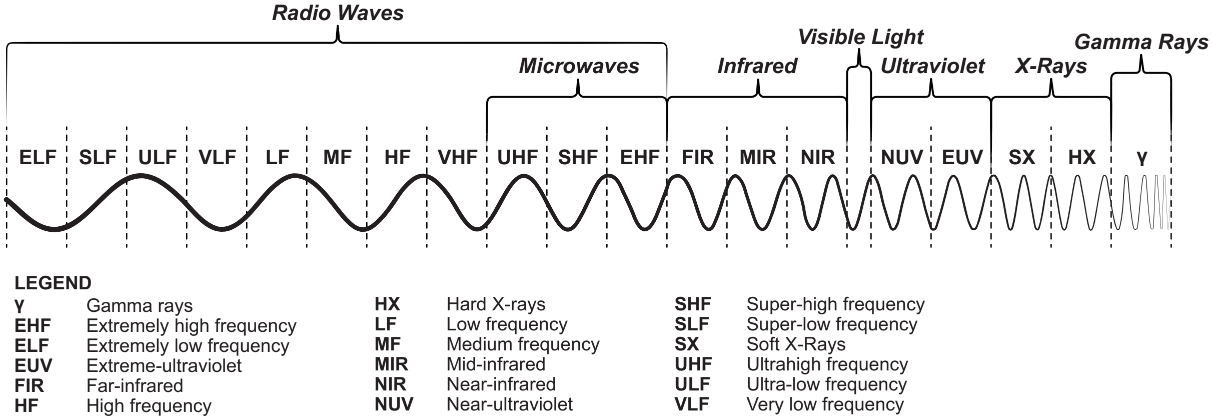


Figure 2-1. Electromagnetic Spectrum.

Electromagnetic Warfare. Gaining and maintaining freedom of action within the EMS is vital to achieving success in every domain across the operational environment. Just as in the physical domains and in cyberspace, Marine Corps forces maneuver and conduct operations within the EMS to achieve tactical, operational, and strategic advantage (JP 3-85, *Joint Electromagnetic Spectrum Operations*). This means that effectiveness in the EMS hinges upon integrated and synchronized planning and execution of electromagnetic warfare, across the MAGTF and joint force, to deconflict actions and efficiently leverage scarce EMS resources. Electromagnetic warfare is military action involving the use of electromagnetic and directed energy to control the EMS or to attack an enemy. Traditionally, electromagnetic warfare is divided into three separate areas: electromagnetic support, electromagnetic attack, and electromagnetic protection.

Electromagnetic Support. Electromagnetic support is the division of electromagnetic warfare involving actions tasked by or under direct control of an operational commander to search, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conducting of future operations. Electromagnetic support systems provide immediate threat recognition and are a source of information for immediate decisions involving electromagnetic attack, electromagnetic protection, avoidance, targeting, and other tactical employments of forces. Electromagnetic support systems collect data and produce information or intelligence that can be used to—

- Corroborate other sources of information or intelligence.
- Support SIGINT production.
- Enable cyberspace operations.
- Support target identification and location.
- Initiate self-protection measures.
- Task weapon systems for physical destruction.
- Support electromagnetic protection efforts.
- Create or modify electromagnetic warfare databases.
- Produce measurement and signature intelligence.
- Support other information activities.
- Conduct electromagnetic reconnaissance.

Electromagnetic Attack. Electromagnetic attack is the division of electromagnetic warfare involving the use of electromagnetic energy, including directed energy or anti-radiation 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. Typical electromagnetic attack capabilities include electromagnetic jamming (i.e., denial) and intrusion (e.g., spoofing or injecting false targets). Electromagnetic attacks can be destructive or non-destructive and either active (e.g., radiating, such as jamming) or passive (e.g., non-radiating and reradiating, such as chaff or spectral flares). Planning for electromagnetic attack follows the existing planning processes to include the MCPP, joint and Marine Corps targeting cycles, and the fires planning process (see Chapter 3 for more details on planning). Examples of electromagnetic attack include the following:

- Radio frequency jamming.
- High-power microwave weapons.
- Laser/dazzler.
- Spoofing (i.e., navigation warfare).
- Electromagnetic pulse.
- Radiating decoys.
- Antiradiation weapons.
- Chaff.
- Corner reflectors.
- Cyberspace enabling operations.

Electromagnetic Protection. Electromagnetic protection is the division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability. Electromagnetic protection focuses on system or process attributes or capabilities that eliminate or mitigate the impact of electromagnetic interference (EMI). Electromagnetic interference can be caused by friendly or enemy action or natural phenomena, and is defined as any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of EMS-dependent systems and electrical equipment. These inherent hardware features; processes; and dedicated TTP combine to enable friendly capabilities to continue to function as intended. Examples of electromagnetic protection include the following:

- Electromagnetic hardening.
- Technical signatures.
- Frequency agility.
- Spread-spectrum technology.
- Emissions control.

Electromagnetic Spectrum Management Operations. Electromagnetic spectrum management operations comprise those interrelated functions of frequency management, host nation coordination, and interference resolution mechanisms. Together, these functions enable the planning, managing, and execution of operations across the EMS during all phases of military operations. As Marine Corps forces operate in the EMS, operations must be managed to facilitate unity of effort in executing the mission and supporting functions. Electromagnetic spectrum management operations' objective is to enable EMS-dependent capabilities and systems to perform their functions as designed, without causing or suffering unacceptable EMI. Electromagnetic spectrum management tasks include the following:

- Electromagnetic battle management (also referred to as EMBM) includes actions to monitor, assess, plan, and direct operations in the EMS in support of the commander's objectives. Electromagnetic battle management provides EMS awareness, decision support, and C2 support.
- EMS certification ensures EMS-dependent systems are compliant with international, national, DoD, joint and Service level statutory and regulatory policy, and guidelines for effective and efficient use of the EMS.
- Frequency management encompasses interference analysis and requesting, nominating, coordinating, assigning, and promulgating frequencies for EMS-dependent capabilities and systems.
- Host nation coordination includes the coordination with nation states for authorization to operate EMS-dependent systems within national borders (includes use of systems that emanate across the border from other areas of interest).
- Interference resolution is the activity for identifying, reporting, analyzing, and mitigating or resolving incidents of EMI. The Marine Corps leverages the joint spectrum interference resolution process for EMI events within the Marine Corps. Joint spectrum interference resolution activity is a continuous action that uses a systematic process to report and diagnose the cause or source of EMI and is not solely a part of the planning process.

Cyberspace Operations

Cyberspace, while part of the information environment, is dependent on the physical domains as much as operations in the physical domains rely on human-made infrastructure and naturally occurring features. Operations in cyberspace rely on networked, stand-alone, and platform-embedded information technology infrastructure, in addition to the data that resides on and is transmitted through these components.

Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. A cyberspace capability is a device or any combination of computer software, firmware, hardware, or TTP designed to create an effect in or through cyberspace. Cyberspace operations can be offensive or defensive, with potential effects across all domains. They use computer hardware, software, code, or devices to target enemy

and hostile adversary activities and capabilities or to protect data, networks, net-centric capabilities, and other designated systems. As a component of operational planning, these operations are used to detect, identify, and respond to attacks against friendly networks (JP 3-12, *Joint Cyberspace Operations*).

Cyberspace Missions. All actions in cyberspace that are not cyberspace-enabled activities are taken as part of one of three cyberspace missions: Department of Defense information network (DoDIN) operations, DCO, or OCO. These three mission types, conducted under various sources of authority, comprehensively cover the activities of the cyberspace forces. The successful execution of cyberspace operations requires integration, synchronization, and simultaneity of these missions.

Department of Defense Information Network Operations. The DoDIN operations mission is to secure, configure, operate, extend, maintain, and sustain DoD cyberspace to create and preserve the confidentiality, availability, and integrity of the DoDIN. The mission includes cyberspace security actions that address vulnerabilities of the DoDIN or specific segments of the DoDIN to prevent exploitation and operation of red teams and other forms of security evaluation and testing. Also, DoDIN operations include various cyberspace system operation actions like the set-up of tactical networks by expeditionary forces to extend existing networks, maintenance actions, and other non-security actions necessary for the sustainment of the DoDIN.

Defensive Cyberspace Operations. Defensive cyberspace operations are executed to defend friendly cyberspace from imminent or active threats in cyberspace. Specifically, they are missions intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, cyberspace enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity (MCA). This distinguishes DCO missions, which defeat specific threats that have bypassed, breached, or are threatening to breach security measures from DoDIN operations, which endeavor to secure DoD cyberspace from all threats in advance of any specific threat activity. Defensive cyberspace operations missions are conducted in response to specific threats of attack or exploitation and leverage information from maneuver, intelligence collection, counterintelligence, law enforcement, and other sources as required to enable mission assurance.

Defensive cyberspace operations include countermeasures, outmaneuvering or interdicting adversaries taking, or about to take, actions against defended cyberspace, or otherwise responding to imminent internal and external cyberspace threats. The purpose of DCO is to defeat the threat of a specific enemy or adversary or to return a compromised network to a secure and functional state. Defensive cyberspace operations protect cyberspace capabilities and services, including data, networks, cyberspace-enabled devices, public interest technology, and other designated systems. Defensive cyberspace operations include maneuver to gain or retain an advantageous position, as well as fires when authorized, against cyberspace threats emanating from outside the protected cyberspace. Defensive cyberspace operations halt a threat's offensive initiative, sustain, or regain friendly initiative, and if required, creates conditions for a counteroffensive. The two types of DCO missions are defensive cyberspace operations-internal defensive measures (DCO-IDM) and defensive cyberspace operations-response actions (DCO-RA).

Defensive Cyberspace Operations-Internal Defensive Measures. Defensive cyberspace operations-internal defensive measures are a DCO mission where authorized cyberspace defensive actions occur within the defended area of operations. The DCO-IDM mission includes risk and intelligence-driven internal threat hunting for advanced and persistent threats, as well as the active internal countermeasures and responses to eliminate and mitigate these threats. Additionally, the DCO-IDM mission includes active and passive internal countermeasures to defeat and mitigate the MCA. Cyberspace protection team (CPT) operations on mission-relevant terrain in cyberspace (MRT-C) in response to indications of MCA, or before specific indicators of compromise exist, are an example of DCO-IDM. The Joint Force Headquarters-Department of Defense Information Network directs and synchronizes DCO-IDM of the DoDIN using a framework of DoDIN areas of operations and sectors established by United States Cyber Command (USCYBERCOM).

Defensive Cyberspace Operations-Response Actions. Defensive cyberspace operations-response actions are DCO missions where actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. Some DCO-RA missions may rise to the level of use of force to physically damage or destroy enemy systems. The specific effects created depend on the broader operational context, such as the existence or imminence of open hostilities, the degree of certainty in attribution of the threat, the damage the threat has caused or is expected to cause, and national policy considerations. Defensive cyberspace operations-response actions missions, especially when they occur before an imminent threat has a chance to act, are "defending forward" in support of the persistent engagement strategic approach. As a self-defense mission, the authorizing official determines whether the exigence of the threat and other circumstances justify use of cyberspace exploitation or cyberspace attack.

Offensive Cyberspace Operations. Offensive cyberspace operations are missions intended to project power in and through cyberspace. These missions support the CCDR or national objectives. Through target development and coordinated deconfliction with national mission elements, commanders can align objectives to facilitate the use of OCO effects. Marine Corps units can request and support the planning from OCO; however, OCO missions are typically executed by the combat mission teams (referred to as CMTs) and national mission teams (referred to as NMTs) assigned to USCYBERCOM. Combatant commanders employ OCO by requesting authority to execute through assigned capable forces, or by direct support from OCO authorized JTFs. Offensive cyberspace operations may exclusively target enemy cyberspace functions or create first-order effects to initiate carefully controlled cascading denial effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, and other high-value targets. Offensive cyberspace operations missions are conducted outside friendly cyberspace and align to a commander's intent.

Depending upon the circumstances, OCO may be conducted under the same or similar external mission authorities as DCO-RA but are not directed at imminent threats in cyberspace, although OCO can include missions to defend against non-cyberspace threats. Like DCO-RA missions, some OCO missions may include cyberspace attack actions, to include "using force" to physically damage or destroy enemy systems. Specific effects created depend on the broader operational context, such as the existence or imminence of open hostilities and national policy considerations. All external missions require a properly coordinated military order and careful consideration of scope, rules of engagement, measurable objectives, and risks (particularly potential collateral effects). The fundamental cyberspace actions of an OCO mission are cyberspace exploitation and cyberspace attack.

Cyberspace Operations Employment Considerations. Execution of any DoDIN operations, DCO, or OCO mission requires completion of specific actions that employ cyberspace capabilities to create effects in cyberspace. The pace of cyberspace operations requires significant pre-operational collaboration and constant vigilance after initiation for effective coordination and deconfliction throughout the operational environment. Keys to this synchronization are maintaining cyberspace situational awareness and assessing the potential joint force impacts of any planned cyberspace operations, including the protection posture of the DoDIN, changes from normal network configuration, or observed indications of MCA. Cyberspace mission objectives are achieved by the combination of one or more cyberspace actions, which are defined exclusively by the types of effects they create. As with the cyberspace operations missions, the actions described in the following sub-sections are only the primary categories of cyberspace operations actions. Cyberspace operations planners and operators establish and use multiple subordinate activities under each of these four categories: security, defense, exploitation, and attack.

Cyberspace Security. Cyberspace security actions are a form of information discipline in which all Marines have a role. It is part of the DoDIN operations mission exercised within protected cyberspace to reduce its vulnerability to MCA. Cyberspace security actions include preventing unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and public interest technology. These actions also secure the information within these systems to ensure availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyberspace Defense. Cyberspace defense actions are taken during DCO-IDM missions, within protected cyberspace, to discover and defeat specific threats that breach, threaten to breach, or are suspected to have breached the cyberspace security measures. Actions include detecting, characterizing, fixing, containing, clearing, and recovering or restoring after MCA, (which includes malware or the unauthorized activities of authorized users). The CCMD, Service, or DoD agency that provides or operates the network is authorized to take these defensive actions except in cases when they would negatively impact networks or systems outside the responsibility of the respective CCMD, Service, or agency.

Cyberspace Exploitation. Cyberspace exploitation actions are a primary component of OCO and DCO-RA missions and include many types of subordinate actions outside friendly cyberspace that do not create cyberspace attack effects. Cyberspace exploitation actions include access creation, military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation includes actions taken to gain and maintain cyberspace superiority and to support operational preparation of the environment for current and future operations. Actions include gaining and maintaining unauthorized access to adversary networks, systems, and nodes of military value, maneuvering to positions of advantage, and positioning cyberspace capabilities to facilitate follow-on actions. Cyberspace exploitation actions with no explanation or purpose other than to enable a follow-on cyberspace attack are considered attack-specific preparations. Cyberspace exploitation supports current and future operations through information collection and includes—

- Mapping cyberspace to support situational awareness.
- Discovering vulnerabilities.
- Enabling joint intelligence preparation of the operational environment (JIPOE).
- Warning.
- Developing Joint targets.
- Supporting the planning, execution, and assessment of military operations throughout the operational environment.

Cyberspace exploitation actions are deconflicted with those of other USG departments and agencies in accordance with national policy.

Cyberspace Attack. Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or use manipulation that leads to denial effects in the physical domains. Cyberspace attacks are coordinated and deconflicted with other USG departments and agencies, carefully synchronized with planned fires in the physical domains and—except when specifically intended to result in physically destructive denial effects—do not rise to the level of armed attack or use of force under current international law.

Cyber National Mission Force. Cyber National Mission Force (CNMF) conducts cyberspace operations to defeat cyberspace threats to the DoDIN and the Nation. The CNMF comprises various numbered national mission teams, associated national support teams, and national CPTs focused on defense of non-DoDIN cyberspace. The CNMF is one part of the DoD's effort to defend cybersecurity as national security, and it partners with the Department of Homeland Security, the Federal Bureau of Investigation, and other agencies, as well as industry, academic, and international partners. The Marine Corps contributes to the CNMF through various units assigned USCYBERCOM).

Cyber Combat Mission Force. The Cyber Combat Mission Force (CCMF) conducts cyberspace operations to support the missions, plans, and priorities of the CCDRs. The CCMF comprises various numbered combat mission teams and associated combat support teams (referred to as CSTs). The Marine Corps contributes to the CCMF through various units that operate under Marine Forces Cyber Command (MARFOR CYBERCOM).

Marine Corps Cyberspace Operations Units. Marine Corps cyberspace operations forces and formations possesses a wide range of personnel and capabilities to plan, conduct, and coordinate cyberspace operations across the three mission areas: DODIN operations, OCO, and DCO. These formations and capabilities exist across FMF, the CNMF, and the CCMF. Specific cyberspace operation missions that Marines plan and conduct vary depending on the type of unit to which they are assigned. For example, Marines assigned to MARFOR CYBERCOM support national and CCDR objectives through the CNMF by planning and executing the full range of cyberspace operations, including OCO. Within the FMF, there are organic DCO forces belonging to the DCO-IDM companies. There are also DCO personnel within the supporting establishment.

Marine Forces Cyber Command. Marine Corps Forces Cyber Command is the Marine Corps Service component to USCYBERCOM. The command enables full spectrum cyberspace operations, which include the planning and direction for the Marine Corps Enterprise Network (MCEN) operations and DCO in support of Marine Corps, joint, and multinational forces, as well as planning and directing OCO in support of CCMD requirements. Marine Forces Cyber Command's cyberspace operations are conducted to enable freedom of action across all domains and deny the same to adversarial forces.

Under MARFOR CYBERCOM, DCO forces include a CPT and forces assigned under the Marine Corps Cyberspace Operations Group (MCCOG). The CPTs support and execute missions under the authority of USCYBERCOM. However, CPTs are under the administrative and some specified operational control of the Marine Corps Cyberspace Operations Battalion (also referred to as MCCOB). The battalion is a subordinate organization to the Marine Corps Cyberspace Warfare Group that organizes, trains, and equips these forces. The MCCOG supports the Marine Corps' warfighting network, the MCEN, and has regional commands and detachments distributed globally.

Cyberspace Protection Team. A CPT's personnel make up three mission elements and a support element. The CPT mission elements execute identical functions and provide the identical capabilities across the Cyber Mission Force when provided adequate enabling support. The CPT mission element focuses on movement and maneuver to dynamically target MCA. The CPT support element contains the CPT leadership and sustains operations by providing analytic, technical, and training support. Depending on operational requirements, mission elements can operate independently or in mutually supporting roles. The mission element is the primary CPT maneuver element and is responsible for conducting the CPT core functions by—

- Conducting intelligence-enabled operations on specified MRT-C.
- Countering and clearing adversary activity on specified MRT-C in coordination with the supported commander.
- Enabling the hardening of specified MRT-C from threat-specific MCA by reducing attack threat surfaces to increase difficulty of access and system exploitation.
- Assessing the effectiveness of response actions against current and future risks to specified MRT-C.

FMF Cyberspace Operations Units. Within the FMF, Marines and units capable of performing DoDIN operations, DCO, and OCO missions reside in the MIG. The FMF units and planners plan, request, and coordinate missions to support Marine Corps objectives. Planners coordinate with the CNMF and relevant cyberspace operations-integrated planning elements, as required, to position

Marine Corps forces and enable CNMF OCO missions when required. The FMF units involved in DoDIN operations and DCO include communication battalions and the defensive cyberspace operations-internal defensive measure company.

The *communication battalions* within the MIGs perform DoDIN operations on the MCEN under the cognizance of the MCCOG. The specific mission of the communication battalion is to establish, maintain, and defend communication networks in support of MAGTF (MEB or larger), Marine Corps component headquarters, or JTF headquarters to facilitate effective command and control of assigned forces. The battalions provide communication detachments and teams, as required, to install, operate, and maintain beyond-line-of-sight wideband transmission systems, tactical network services, cyberspace security, and telephone services in support of designated battalion direct-support communication detachments and MEUs.

The *DCO-IDM company* conducts DCO in support of the commander to defend critical capabilities that facilitate a commander's ability to employ, and command and control forces. The DCO-IDM company is tasked with providing deployable units, typically in squad or platoon-sized teams that can be employed to support various Marine Corps or joint force organizations. Their mission includes conducting reconnaissance and defense operations in cyberspace to enable the operation of resilient, reliable information networks, computer processor-driven devices, and weapon systems. The company provides the supported unit with recommendations to reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised local networks, computer processor driven devices, and weapon systems in response to attack, exploitation, intrusion, or effects of malware. The DCO-IDM company performs the following tasks:

- *Conduct Hunt*. A proactive and iterative process of searching through networks and cyberspace-enabled devices to detect indicators of compromise and to identify and isolate advanced or persistent threats that evade existing security solutions.
- *Counter and Clear Adversary Activity*. Counter is the detection, illumination, and defeat of discovered or previously unknown threats within a defended network or system. Clear is an operation to eliminate or neutralize threats from a defended network or system.
- *Enable Hardening of Specified MRT-C*. A function of battlespace shaping wherein DCO forces coordinate actions with DoDIN operations forces to reduce attack surfaces on defended networks or systems to increase difficulty of systems exploitation. The MRT-C includes critical infrastructure, assets, capabilities, and weapon systems with embedded processors.
- *Assess Response Action Effectiveness against Current and Future Risk to Specified MRT-C*. Assessments are actions taken to determine whether a subject network or system and its assigned DoDIN security forces can detect and respond to a specific set of advanced threats. When authorized, cyberspace threat emulation capabilities are employed in concert with hardening efforts.

There are three DCO-IDM companies—one within each of the three MIGs. The DCO-IDM companies also support MEUs by providing detachments that deploy in support of naval operations and CCMD objectives. Additionally, there are DCO integrators at all echelons of the companies' HHQ (i.e., MIGs, MEFs, and Marine Corps component commands).

Space Operations

Space is of vital interest and integral to national security. Space superiority enables the Marine Corps, as part of the joint force, to rapidly transition from competition to conflict and prevail in a global, all-domain fight. Space-based capabilities provide a combat advantage by effectively extending the line of sight from a ground-based user to sensor or communication payload. Space operations seek to achieve superiority in the space domain and its corresponding environment. Space-based capabilities are critical for successful land, air, and maritime domain operations. Both the FMF and joint force are highly reliant on space-based communications, navigation and ISR capabilities.

Military and commercial satellites placed in different orbit types provide terrestrial forces with global satellite communications (SATCOM); positioning, navigation, and timing (PNT); and ISR. This enables freedom of maneuver and IPB, reliable communication, and accurate targeting, fires, and navigation. Military space capabilities are a product of partnerships across the DoD and among USG mission partners that provide space-derived data for military use and integration.

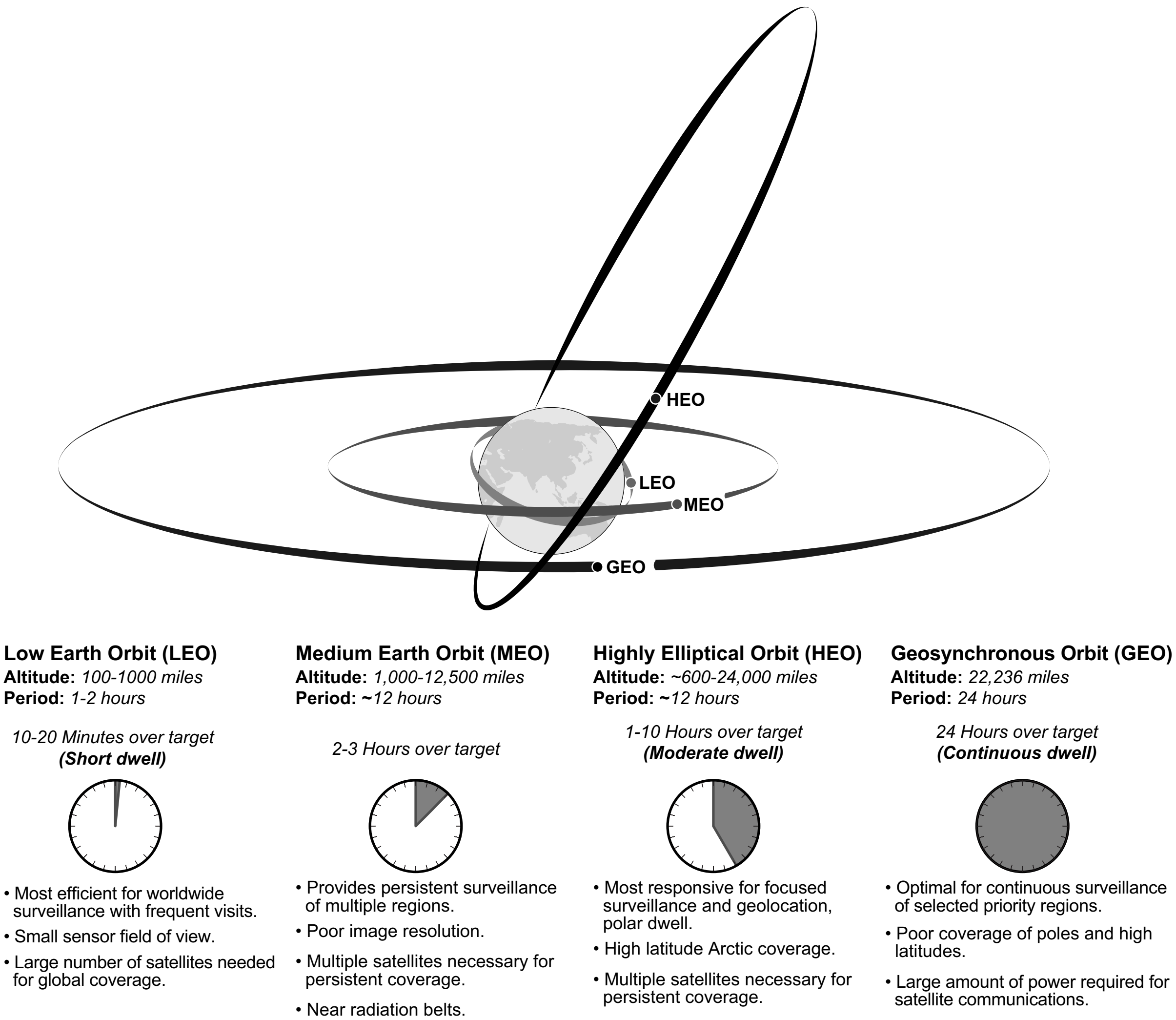
Common Satellite Orbit Types

Orbit types and parameters are generally selected to provide the greatest benefit for the least cost, based on the purpose and capabilities of the satellite. The four most common orbit types used by the military are: low Earth orbit, medium Earth orbit, highly elliptical orbit, and geosynchronous Earth orbit (see Figure 2-2). Planners should learn each orbit type’s characteristics, capabilities, and limitations to leverage a diverse mix of military, national, and commercial SATCOM capabilities in support of mission requirements.

Space Operations Missions and Capabilities

Space operations comprise a common set of capabilities applicable to all joint force components. The following sections discuss space capabilities to provide Marines with a baseline understanding of this increasingly important domain.

Space Domain Awareness. Space domain awareness is the requisite foundational, current, and predictive knowledge and characterization of space objects and the operational environment upon which space operations depend (JP 3-14, *Space Operations*). Space domain awareness includes physical, information, and human aspects, as well as all factors, activities, and events of all entities conducting, or preparing to conduct, space operations. Space surveillance is an activity that requires numerous capabilities, many of which include a mix of space-based and ground-based sensors. Space situational awareness encompasses integrating space surveillance, collection, and processing; environmental monitoring; status of US and cooperative satellite systems; understanding of US and multinational space readiness; and analysis of the space domain. Space situational awareness must incorporate an understanding of the capabilities and intent of those who pose a threat to space operations and capabilities. A main output of joint space domain awareness capabilities is a two-line element set: the data that provides orbit information essential for situational awareness on adversary space control satellites and planning for effects against adversary ISR satellites.



Low Earth Orbit (LEO)
Altitude: *100-1000 miles*
Period: *1-2 hours*

10-20 Minutes over target
(Short dwell)

- Most efficient for worldwide surveillance with frequent visits.
- Small sensor field of view.
- Large number of satellites needed for global coverage.

Medium Earth Orbit (MEO)
Altitude: *1,000-12,500 miles*
Period: ~*12 hours*

2-3 Hours over target

- Provides persistent surveillance of multiple regions.
- Poor image resolution.
- Multiple satellites necessary for persistent coverage.
- Near radiation belts.

Highly Elliptical Orbit (HEO)
Altitude: *~600-24,000 miles*
Period: ~*12 hours*

1-10 Hours over target
(Moderate dwell)

- Most responsive for focused surveillance and geolocation, polar dwell.
- High latitude Arctic coverage.
- Multiple satellites necessary for persistent coverage.

Geosynchronous Orbit (GEO)
Altitude: *22,236 miles*
Period: *24 hours*

24 Hours over target
(Continuous dwell)

- Optimal for continuous surveillance of selected priority regions.
- Poor coverage of poles and high latitudes.
- Large amount of power required for satellite communications.

Figure 2-2. Common Satellite Orbit Types.

Space Control. Space control includes offensive and defensive space control operations conducted to ensure freedom of action in space and, when directed, defeat efforts to interfere with or attack US or allied space systems. Space control uses a range of response options to provide continued, sustainable use of space. Offensive space control operations are conducted for space negation, or measures taken to deceive, disrupt, deny, degrade, or destroy space systems or services. Defensive space control operations consist of all active and passive measures taken to protect friendly space capabilities from attack, interference, or hazards. Defensive space control safeguards assets from hazards such as direct or indirect attack, space debris, radio frequency interference, and naturally occurring phenomenon such as radiation. Space control also involves navigation warfare offensive and defensive actions to ensure friendly use and prevent adversary use of PNT information through coordinated employment of space, cyberspace, and electromagnetic warfare capabilities. Navigation warfare is further enabled by supporting activities such as ISR and EMS management. All Marines must be aware of adversary capabilities and limitations pertaining to space control and navigation warfare. Marines must understand organic equipment vulnerabilities and methods to mitigate adversary space control activities. For additional information about navigation warfare, see JP 3-85, JP 3-14, and JP 3-12.

Intelligence, Surveillance, and Reconnaissance. Space-based intelligence collection synchronizes and integrates sensors, assets, and systems for gathering data and information on an object or in an area of interest on a persistent, event-driven, or scheduled basis. Space-based ISR is conducted by the national intelligence community to fulfill requirements established by CCDRs through the processes, in which the intelligence collection manager participates.

Positioning, Navigation, and Timing. Marines depend on assured PNT systems for precise and accurate geolocation, navigation, and time reference services. Whether from space-based global navigation satellite systems, such as Global Positioning System, or non-global navigation satellite systems sources, PNT information is considered mission-essential for every modern weapons system. Marines must be proactive end users of Global Positioning System services.

Satellite Communications. Satellite communications provide critical connectivity for FMF maneuver forces and disadvantaged users who, because of rapid movement and geographically dispersed deployments, lack direct access to terrestrial communications infrastructures. Satellite communications systems provide voice and data connectivity that facilitates command and control, survivable communications for presidential support, nuclear command and control, and intelligence.

Environmental Monitoring. Terrestrial environmental monitoring provides information on meteorological and oceanographic factors that affect military operations. Space-based environmental sensing supports the development of meteorological and oceanographic forecasts and assessments of environmental impacts on both friendly and threat military systems and operations. Space environmental monitoring provides data that supports forecasts, alerts, and warnings for the space environment that may affect space capabilities, space operations, and their terrestrial users. Space-based monitoring provides the ability to detect and mitigate the impacts of space weather on satellites, manned spaceflight, and communications to, from, and through space.

Missile Warning and other Space Operations Missions and Capabilities. The missile warning mission uses a mix of space- and ground-based radar systems. The missile warning mission notifies national leaders, CCMDs, multinational partners, and forward-deployed personnel of impending missile attacks and assesses missile attacks if the applicable CCMD or multinational partner is unable to do so. Collectively, space-based sensors provide persistent coverage of all areas of responsibility. In addition to the above, other space operations missions and capabilities that Marines should be aware of include nuclear detonation detection, space lift, and satellite operations.

Marine Corps Space Operations and Capabilities. Space capabilities are integral to the Marine Corps information warfighting function, contributing directly to the generation, preservation, denial, and projection of information. They are an important part of the reconnaissance and counter-reconnaissance fight, with multiple forms of space-based intelligence collection serving as an important method of observation. Marines conducting reconnaissance missions use SATCOM as an important route for passing information captured by forward sensors back for integration. The US space-based capabilities provide numerous information advantages when they are available, and if unavailable, Marines are relegated to use other means that can lead to delays or reduced effectiveness.

The Marine Corps supports previously mentioned space missions and leverages space-based capabilities. All space-based capabilities that Marines leverage are owned and operated by other military Services and USG agencies. The Marine Corps employs cross-functional specialties that rely on space-based capabilities. Marine Corps space cadre comprises personnel with required security clearance, training, and occupational specialties to plan, coordinate, and integrate space capabilities in support of operations.

United States Space Command and Marine Forces Space Command. United States Space Command (USSPACECOM) is the functional CCMD that employs forces from all five Services to accomplish missions in space. The command is responsible for collaborating with allies and partners to plan, execute, and integrate military space power into multi-domain global operations to deter aggression, defend national interests, and when necessary, defeat threats. Marine Forces Space Command (MARFOR SPACECOM) is the Marine Corps component command to USSPACECOM, and it provides space operational support to the FMF.

Operations Security and Signature Management

Operations Security. Operations security is a capability that helps to ensure mission success by preventing an enemy or adversary from observing and exploiting critical information and friendly force indicators. Operations security involves a systematic process to identify, control, and protect critical information. By identifying what the adversary can observe, OPSEC planners can alert commanders of potential unit vulnerabilities. Once a vulnerability is identified, OPSEC planners can assist in developing measures and countermeasures, including support for deception activities.

Practicing OPSEC and Physical Security. While there are professional OPSEC planners, all Marines should practice information discipline in support of OPSEC. This includes keeping critical information off social media feeds, disabling location data in the metadata of personal photos, respecting the classification markings of digital and physical documents, remembering to remove security badges when exiting secure facilities, confining discussions of sensitive material to appropriate venues, and physical security at bases and operating locations.

Physical security is also an aspect of OPSEC by preventing enemy and adversary reconnaissance assets or spies from coming close to or entering Marine Corps facilities, bases, or positions and observing or otherwise gathering critical information. Maintaining fences, barriers, and perimeters, keeping doors and hatches that are intended to be closed secure, and following badging procedures are all elements of the physical security aspect of OPSEC, intended to deny enemies and adversaries access to information.

Signature Management. Signature management is a pillar of deliberate and mission-focused OPSEC. Marines use SIGMAN to understand own-force signatures and indicators; identify adversarial methods and capabilities to collect and analyze those signatures; develop and implement countermeasures to mask those signatures; and when necessary, develop and implement methods to project false signatures which protect friendly forces from adversarial exploitation; or to draw the enemy or adversary toward a specific COA or position of disadvantage. Signature management is an operational fusion of aspects that combines traditional methods of intelligence (e.g., adversary conduit and friendly force signature), counterintelligence, OPSEC, MILDEC and fires (e.g., lethal, non-lethal, counter-reconnaissance) into a single process that enables a commander to achieve surprise and outmaneuver the enemy or adversary at the decisive moment. Figure 2-3 provides a conceptual model for SIGMAN.

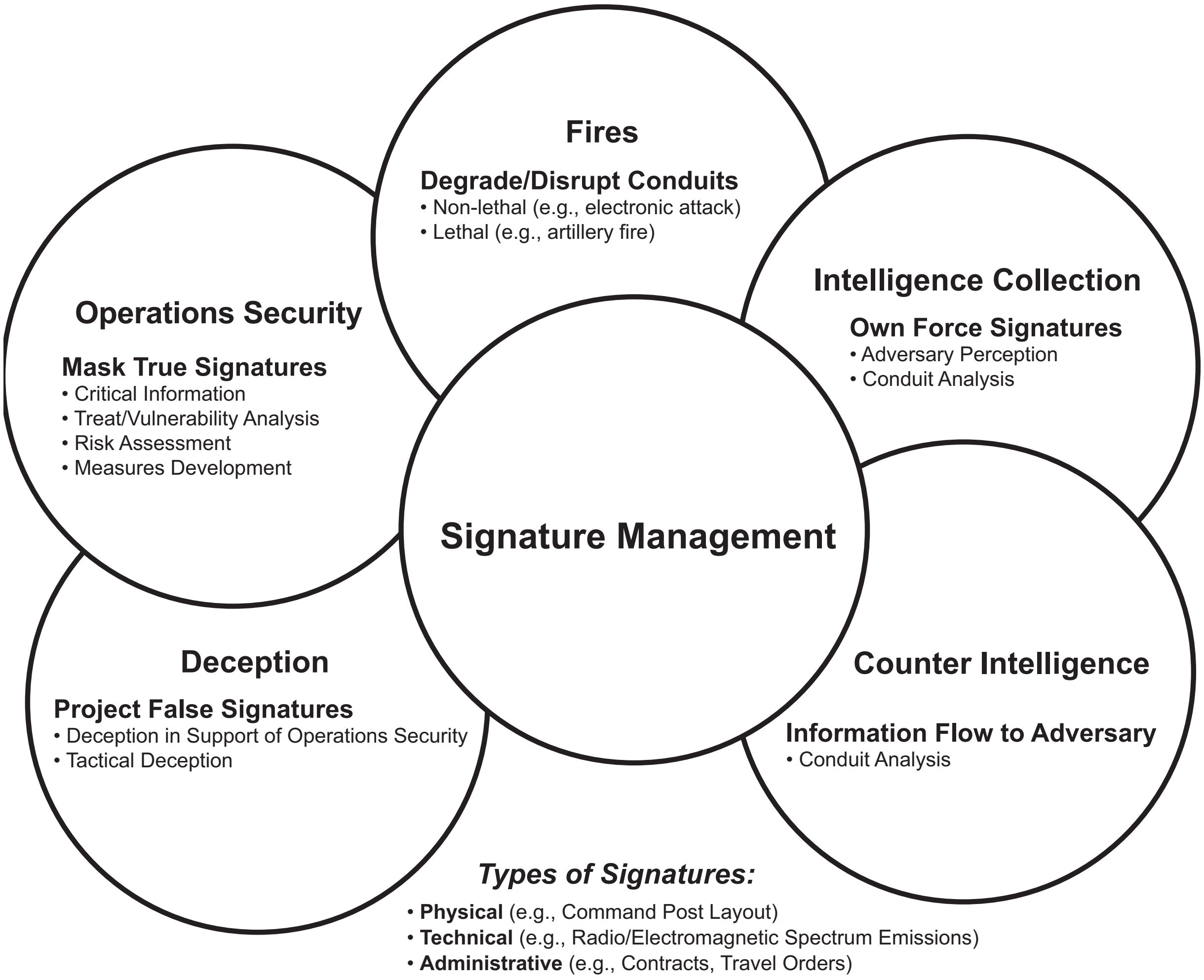


Figure 2-3. Signature Management Conceptual Model.

<u>Physical, Technical, and Administrative Signatures</u>. Signatures are grouped into physical, technical, and administrative categories that relate to their characteristics. These are separate categories based upon adversarial ISR collection capabilities but are not distinct from a friendly activity standpoint. Every Marine Corps activity (planning, operations, intelligence collection, mobilization, training, research, development, testing and evaluation, or acquisitions) has physical, technical, and administrative signatures that can provide critical insight as to who, how, when, where, and why a MAGTF will fight. When collected and analyzed by adversarial intelligence processes in conjunction with a specific friendly activity, the combination of these signatures can result in intelligence that allows an enemy or adversary to classify targets or activities.

<u>Physical Signature</u>. Physical signatures are those that can be collected by adversarial geospatial-intelligence assets or through direct observation. They include physical objects, such as an F-18 parked on an apron, which can be imaged by electro-optical, infrared, or synthetic aperture radar assets. These assets could be space-based, aerial, ground, or human-source operated. Physical signatures also include heat signatures left on the runway after the F-18 takes off, tracks in the mud from vehicular or personnel movement near a runway, and other physical traces that could be identified by coherent change detection collection techniques.

Technical Signature. Technical signatures are those that can be collected by adversarial electromagnetic warfare and SIGINT assets. They include but are not limited to radio frequency emissions from communications, C2 systems, and guidance systems; radar emissions; and unintended emissions from motorized items such as generators or vehicle engines. Technical signatures also include the specific features of acoustic, scent-based, chemical, or radiation emissions outside the radio frequency EMS that could be collected by adversarial measurement and signature intelligence assets.

Administrative Signature. Administrative signatures are created by an individual or unit when conducting planning, movement, contracting, or other administrative actions that can be collected by adversarial open-source intelligence, SIGINT, or human intelligence. Examples include planning documents, Defense Travel System orders, country-clearance submissions, passport requests, individual or unit social media posts, official media releases, sustainment contract documents, logistic parts orders, or capability research and development documents.

Whether the challenge is managing physical signatures through camouflage, concealment, and deception; or technical signatures in the EMS; or administrative signatures within a contracting office; managing signatures contributes to protecting Marines from detection or preventing detectable signatures from revealing Marine's intentions. Every Marine and unit has a responsibility to support SIGMAN, from the assistant G-6 monitoring of own force electromagnetic emissions; to the enforcement of light discipline in defensive positions; to the G-4 managing administrative signatures of unclassified logistics requests; to the commander establishing enforcement policies.

Deception

Deception includes actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization (VEO) decision makers, thereby causing the adversary decision-maker to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Deception is considered an information activity because Marines endeavor to change what adversary sensors (human or machine) see or perceive, to affect what adversary decision-makers think or understand, with the ultimate objective being to affect what the adversary does (or does not do). There are three categories of deception: joint MILDEC, TAC-D, and DISO.

Joint Military DeceptionJoint MILDEC is conducted at the operational level and is designed to support major campaigns and operations. It typically requires detailed intelligence about the beliefs, activity patterns, and training of the adversary decision maker, high-level approval, and lengthy planning timelines. It uses a wide range of resources, some of which are scarce.

Marines may contribute to a joint MILDEC operation but may be among a select few in the formation who realize what is being executed. One of the most famous historical examples of joint MILDEC was the demonstration conducted by the 5th MEB during Operation DESERT STORM, which convinced Iraqi military leadership to keep their forces close to Kuwait's border with Saudi Arabia, leaving their flank exposed for the famous "left hook" by the multinational force. Another famous example of joint MILDEC occurred in WWII in support of the allied invasion of Europe. Operation FORTITUDE SOUTH ran from July 1943 to June 1944. It succeeded in convincing the Germans that the Allied landing would occur at the Pas-de-Calais, instead of the actual intended landing site at Normandy.

As illustrated, Marines support joint MILDEC to limit the enemy's ability to apply accurately focused combat power. Joint MILDEC activities will always be conducted within approved authorities and permissions and must balance the mission's objectives with potential second- and third-order effects to Marine Corps and US credibility.

Tactical Deception. Tactical deception is an activity planned and executed by, and in support of, tactical-level commanders to cause the enemy and adversaries to take actions or inactions favorable to the tactical commanders' objectives. Tactical deception is most often planned and executed as an integral part of the unit's operations or movement. Tactical deception is conducted to enable military operations to gain a tactical advantage over an enemy or adversary, mask vulnerabilities in friendly forces, or to enhance the defensive capabilities of friendly forces. It is unique to the tactical requirements of the local commander and not necessarily linked or subordinate to a greater joint MILDEC plan.

Tactical deception is the type of deception most accessible to Marines. It must be deliberately planned and executed while maintaining essential secrecy. Tactical deception creates disproportionate advantages based on how much time and resources an enemy or adversary diverts toward the MAGTF's actions. Generally, the greater the surprise, the smaller the force required to accomplish the mission, and the fewer the casualties the force sustains.

In addition to using camouflage and decoys to frustrate an enemy's or adversary's sensing and decision-making activities, Marines conduct a range of TAC-D operations, including feints, demonstrations, ruses, and displays to draw enemy and adversary attention away from the main effort. At the smallest unit level, Marines employ deception to maximize stealth, concealment, and surprise. Similarly, Marine Corps forces at any echelon could employ deception techniques to bait an ambush. The main point is that TAC-D, at any scale, is worth the cost (time and personnel) in almost all situations.

Deception in Support of Operations Security. In support of an approved OPSEC plan, DISO conveys or denies selected information or signatures to foreign intelligence entities and limits their overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets. Where DISO differs from joint MILDEC and TAC-D plans, DISO only targets foreign intelligence entities and is not focused on generating a specific enemy or adversary action or inaction. The intent of DISO is to create multiple false, confusing, or misleading indicators to make friendly force intentions harder to interpret by the foreign intelligence entity.

CHAPTER 3.
INFORMATION PLANNING

"A good plan, violently executed now, is better than a perfect plan next week."

—General George S. Patton, United States Army

Planning is the art and science of envisioning a desired future state and laying out effective ways to attain it. Information planning encompasses the continuous process of coordinating, synchronizing, and integrating information capabilities and activities into the commander's overall concept of operations (CONOPS) or campaign plan. Planning belongs to the commander, as does the responsibility for including information considerations in every applicable plan. Including information considerations into planning early maximizes the opportunity to create and exploit information advantages and information-based effects.

INFORMATION PLANNING OVERVIEW

Two categories of information planning occur simultaneously and are integrated into a unit's overall planning effort. The first category is general information planning, which applies to all Marines, units, and organizations at every echelon. This category describes how unit operations and activities (e.g., posture, presence, profile, maneuver) are used gain information advantage or create informational effects, influence audiences, and achieve objectives. The second category is specialized information planning, which applies to units specifically organized, trained, equipped, and tasked with executing specialized information activities. General and specialized information planning are both nested within the unit's overall planning effort and are described in the unit's concept of information. Table 3-1 describes the two categories of information planning.

Table 3-1. General and Specialized Information Planning

Information Planning	
General	**Specialized**
All units and personnel	Specific information capabilities and activities
All capabilities, operations, and activities	

By conducting general and specialized information planning, Marines develop practical schemes to leverage the functions of information to create and exploit information advantages. General and specialized information planning activities work together and materialize through the planning process, doctrinal frameworks, and products, including the following:

- Combined information overlay.
- Concept of information.
- OPORD Annex I (Information).
- Information directive.
- Target list and relevant actor engagement lists. (*NOTE: Relevant actor engagement lists do not include those individuals, groups, populations, or automated systems classified as targets*).
- List of available information capabilities and authorities.
- Information Tasking and Coordination Order (ITCO).

General and specialized information planning span the planning hierarchy. General information planning relates the general means and methods of information conducted through unit operations. Specialized information planning integrates specialized information activities through unit fires and effects. Table 3-2 provides general and specialized information planning considerations.

Table 3-2. General and Specialized Information Planning.

General Information Planning	Specialized Information Planning
Applicable to all units, operations, and unit activities.	Applicable to information force, including intelligence and communications specialties, resulting in "2-3-6" integration.
Integrates the information warfighting function into operations and activities.	Compatible with the fires and effects integration methodology.
Considers how all unit operations and activities apply the four functions of information: • Generate. • Preserve. • Deny. • Project.	Planned through the information tasking and coordination cycle.
Considers how all unit operations and activities create and exploit information advantages: • Systems overmatch. • Prevailing narrative. • Force resiliency.	Integrates information support and enabling activities.
	Used to conduct functional and detailed planning and tasking of specific information activities.
	Nested within the MCPP and integrated with all other unit planning activities through the battle staff and battle rhythm events.
Example: Concept for narrative campaigning that leverages unit posture, presence, profile, and repetitious freedom of navigation operations.	Examples: Concept for MISO series to amplify repetitious freedom of navigation operations; concept for cyberspace operations to support freedom of navigation operations.

Both general and specialized information planning must be mutually supporting and coordinated in execution. For example, Table 3-2 discusses the repetitious use of freedom of navigation operations—a maneuver activity—to gain narrative advantage and achieve deterrence. Table 3-2 also uses specialized information activities (MISO series and cyberspace operations) to amplify the messages sent by the repetitious freedom of navigation operations. The main point is that the plan for the freedom of navigation operations should include the MISO component as an integral element from the beginning of the planning process, making them both an integral part of the concept of information and the overall CONOPs.

Information Planning and the Marine Corps Planning Process

Table 3-3 identifies various general and specialized information planning actions as they fit into the overall MCPP.

Table 3-3. General and Specialized Information Planning.

MCPP Step	Information Planning Actions	
	General	Specialized
1. Problem Framing	• Identify and describe the problem(s) to be solved or opportunities to be pursued. • Provide IPB and general intelligence and initiate the combined information overlay. • Develop initial staff estimates, to include a list of unit operations or activities that can be used for informational purposes	• Identify and describe the problem(s) to be solved or opportunities to be pursued. • Provide IPB and general intelligence and initiate the combined information overlay. • Develop initial staff estimates, to include a list of available specialized information capabilities and authorities available.
2. COA Development	• Identify desired information-advantages, conditions and actions that support the CONOPS for each COA. • Develop concept of information for each COA. • Develop MOEs and MOPs.	• Identify supporting actions, tasks, and effects that support the concept of information for each COA. • Develop or update the target and relevant actor list.(*NOTE: Relevant actor engagement lists do not include those individuals, groups, populations, or automated systems classified as targets*). • Develop MOEs and MOPs.
3.COA War Game	• Ensure appropriate consideration of general information considerations during wargaming, especially regarding measurement and assessment. • Refine all planning products.	• Ensure appropriate consideration of specialized information considerations during wargaming, especially regarding measurement and assessment. • Refine all planning products.
4.COA Comparison and Decision	Ensure appropriate representation of general information considerations and desired outcomes in the COA brief.	Ensure appropriate representation of specialized information considerations and desired effects in the COA brief.
5.Orders Development	• Ensure all tasks appropriately consider the information warfighting function in Annex C (Operation). • Finalize Annex I (Information).	• Develop tasks for execution. • ITCO, and other information-related orders and products. • Direct coordination with external entities and HHQ for support, authorities, etc.
6.Transition	• Ensure forces have a clear understanding of their role in the plan. • Ensure forces have the resources and authorities, permissions, and support required to fulfill their tasks.	• Execute specialized information activity planning processes. • Begin measurement and assessment to inform adjustments to the operational approach and future planning.

Problem Framing. Problem framing is the most important step of MCPP (step 1) as it requires planners to clearly identify the problem, what the command must accomplish, when and where it must be done and, most importantly, why. The operational approach and mission statement are developed during problem framing, as well as the commander's intent. The following general and specialized information planning actions occur during problem framing:

- Characterize the problem(s) to be solved.
- Develop and present IPB products and general intelligence.
- Develop initial information staff estimates, including consideration of available units, capabilities, and authorities.

There are also products that are started in problem framing and that are outputs of the MCPP in later steps. These include the following:

- Combined information overlay.
- Annex I (Information).
- Information directive (specialized information planning only).
- ITCO (specialized information planning only).

COA Development. Course of action development (MCPP step 2) leads to one or more options for accomplishing the mission in accordance with the commander's operational approach. Driven primarily by the commander's COA development guidance, along with the planning products created in problem framing, information planners begin developing the concept of information for each COA that incorporates both general and specialized information activities. During COA development, information planners focus on identifying desired conditions and actions that support the CONOPS for each COA. General and specialized information planners then develop detailed actions, tasks, and effects that support the concept of information for each COA. These planners consider other supporting concepts for each COA (concept of maneuver, concept of fires, intelligence collection plan, force protection requirements, etc.). The following general and specialized information planning actions occur during COA development:

- Develop a concept of information to include available authorities and permissions.
- Develop objectives, desired effects, and transition criteria for each COA.
- Support target and relevant actor development and prioritization to identify entities to be subject to effects and determining military importance, priority, and capabilities required to create desired effects.
- Support fires and effects planners in developing specific tasks required to create desired effects; develop the fires portion of the COA development brief.
- Develop or refine assessment measures (e.g., MOEs and MOPs), and indicators to assess effects and objectives accomplishment.

COA War Game and COA Comparison and Decision. The COA war game (MCPP step 3) enables commanders and planners to improve the plan by testing each COA against a competitor or enemy with an independent will. Planners are responsible for integrating each COA's concept of information into the war game. This can be challenging because the effects of information are sometimes hard to directly measure and assess. The more experienced the information staff, the more likely reliable insights can emerge from the war game.

If the concepts of information are successfully integrated in the COA war game, the same kinds of considerations will support its inclusion in COA comparison and decision (MCPP step 4). In addition to the above, information planners typically perform the following actions during COA wargaming and COA comparison and decision:

- Refine objectives and desired effects.
- Refine high-priority targets and entities and determine the sequence of action and the information capabilities required to create desired effects to achieve objectives.
- Validate and refine tasks.
- Begin development of collection (target areas of interest, assessment, etc.) and decision point requirements.
- Refine information staff estimates for each COA, including consideration of available capabilities and authorities.
- Refine the fires portion of the COA development brief. Assist in the briefing if required.

In these two MCPP steps, all information planning products continue to mature. Each step provides strong opportunities for the further development of the target and relevant actor engagement lists (*NOTE: Relevant actor engagement lists do not include those individuals, groups, populations, or automated systems classified as targets*), and the list of available information capabilities and authorities. These lists should be used in the comparison of COAs. A single concept of information should also mature and be refined as multiple possible COAs give way to the selected COA.

Orders Development and TransitionThe purpose of orders development (MCPP step 5) is to translate the commander’s decision into oral, written, and/or graphic communication to guide execution and promote initiative by subordinates. Transition (MCPP step 6) enables the commander to personally brief, discuss, and rehearse the completed plan with the staff and subordinate commanders prior to execution. Successful transition enhances the situational understanding for individuals who will execute the order, reinforce the intent of the commander, promote unity of effort, and generate tempo. Information planners perform the following actions during orders development and transition:

- Draft general and specialized information tasks for paragraph 3 of the base order for subordinate units and agencies.
- Complete information conceptual, functional, and detailed plans (Annex I [Information] and ITCO).
- Incorporate information-based objectives and effects in the base order or plan and Annex C (Operations).
- Ensure accurate and consistent terminology when drafting objectives and tasks.
- Confirm information activities conform to battlespace geometry and coordination requirements.
- Complete information-related planning and execution tools required for use by other agencies.
- Support the development of all other relevant annexes and tabs to the OPORD.
- Ensure information activities in the OPORD are coordinated.

During MCPP step 6, the information planning products that produce planning processes outputs, Annex I, and the ITCO should be completed.

GENERAL INFORMATION PLANNING CONSIDERATIONS

General information planning considers all operations and activities that have inherent informational aspects; meaning, everything a Marine Corps unit or organization does or does not do that is potentially observable. Commanders must recognize and seize the opportunity to intentionally craft and orchestrate their unit's operations and activities to support the broader narrative, contribute to an influence campaign or a deception plan, and create and exploit other information-based advantages to achieve objectives. For example, logistics operations should be planned and executed with deliberate consideration for their visibility and the subsequent indications or messages they send to a potential adversary, as well as to allies and partners. Such messages can impact the prevailing narrative and contribute to advantages.

General Information Planning Products. The development of general information planning products requires the contributions of planners from across staff sections and warfighting functions. The following sub-sections describe the general information planning products.

Combined Information Overlay. The combined information overlay is a holistic depiction of the components and aspects of the information environment. It is a visualization product that depicts the presence and impact of information, flow of information, technologies and capabilities of information, local population, prevailing narrative, and any other relevant information about the information environment as it pertains to the unit's mission. Fundamentally, the combined information overlay visualizes the information environment from all perspectives (enemy, friendly, neutral) relevant to the mission.

The combined information overlay is developed through a whole-of-staff approach and by involving working groups during the planning process. An initial combined information overlay is compiled from basic studies and made available in and refined during problem framing (MCPP step 1) as part of the effort to describe the current state of the operational environment. The combined information overlay may be further refined in later steps in the planning process as part of staff estimates, estimates of supportability, the information running estimate, updated intelligence estimates, priority intelligence requirements (PIRs), or mission-specific intelligence products.

For additional information on the combined information overlay, refer to the Joint Guide for Joint Intelligence Preparation of the Operational Environment.

Concept of Information. Marines plan information activities to support the overall operational approach. As such, in an OPLAN or OPORD, a concept of information is used to illustrate the informational aspects of the plan or CONOPS. It must be developed in a collaborative manner with all other supporting concepts. Much like a CONOPS, a concept of information is a written statement with a supporting graphic that together clearly and concisely conveys what the commander intends to accomplish and how it will be accomplished using available information means and methods.

Depending on the nature of the planning, information planners in an operational planning team or the information working group (IWG) develop an initial concept of information during COA development (MCPP step 2). The concept of information is refined in COA war game and COA comparison and decision (MCPP steps 3 and 4), which and can be included in the OPLAN or

OPORD as part of Annex I (Information)during orders development (MCPP step 5). The concept of information also serves as a central input to the information tasking and coordination cycle (ITCC) and the development of the ITCO.

For additional information on the concept of information, refer to Appendix A.

Annex I. Annex I is a planning artifact that integrates the information warfighting function in all domains and with other functions. All base plans or orders should have an Annex I based on the concept of information. Annex I lists the major tasks stemming from the CONOPS and the concept of information that correspond to general and specialized information activities. Many of these capabilities possess unique detailed planning processes. For activities that are part of the concept of information, Annex I should include appendices describing the actions and outcomes for each detailed planning process by capability, as well as how the various activities are intended to work together.

For additional information about templates for Annex I, refer to MCWP 5-10, *Marine Corps Planning Process*.

The Role of Commanders in General Information Planning

Information, like all warfighting functions, is the commander's business. Every action a unit takes and every word or image that a Marine communicates is potentially visible and exploitable by adversaries in any part of the world. In a near-real-time global information environment, the role of commanders is to set conditions for unit success by maximizing information opportunities, protecting against information vulnerabilities, and encouraging information discipline. To support the planning process, commanders of units at every echelon must ensure information is considered. As part of hierarchical and lateral planning integration, commanders must make sure that information planning is integrated with other aspects of the planning process. This is accomplished, principally, through the following four actions:

- Emphasize information in unit planning.
- Include information in top-down planning guidance, intent, and narrative.
- Consider information in the single battle.
- Assess information activities to provide a feedback loop to further planning.

Emphasize Information in Unit Planning. Emphasizing information means that commanders should prioritize the pursuit of information advantages and information-based effects as they would with any other type of advantage or effect. To emphasize information in planning, commanders at a minimum must—

- Ensure planners with information expertise are present and contributing to each step of the planning process.
- Issue effective planning guidance (i.e., the information directive, discussed later in this chapter) related to information activities.
- Drive intelligence support to the planning processes (including IPB, JIPOE, civil preparation of the battlespace, or intelligence preparation of the information environment) to complete a combined information overlay, characterize the information environment, and identify and understand operationally relevant actors and what drives their behavior.

- Communicate and promulgate the command narrative developed by the planning staff and ensure consistency with higher-level narratives.
- Establish and describe objectives with inherent informational characteristics.
- Ensure the concept of information is included and integrated with the overall CONOPS, and all other supporting concepts.

Include Information in Top-down Planning Guidance, Intent, and Narrative. The commander's personal involvement is critical to successful planning. The commander must not merely participate in planning but must drive the process from the top-down to ensure the published plan is a clear manifestation of the commander's decision regarding how to best accomplish the mission (MCWP 5-10). The top-down approach also applies to information planning. The commander is responsible for including information in planning guidance, intent, and the command narrative.

Consider Information in the Single Battle. Commanders must always view the battlespace as an indivisible entity—a single battle. This tenet of the MCPP directs planners and commanders to maximize opportunities for success as they arrange forces in time, space, event, and purpose. This includes phasing, designation of main and supporting efforts, and the relationship among shaping, decisive, and sustaining forces and activities. Because information spans and connects all domains of the operational environment, commanders must guide staff planners in recognizing the potential of information activities to contribute to or amplify the convergence of effects across domains. The 21st century single battle includes acting in and through the information environment to create effects in any or all domains of the operational environment.

Assess Information Activities . Assessment is the overall continuous process that feeds planning cycles and decision making. It works by providing MOEs of the outcomes produced by a unit's efforts and MOPs of the execution of planned activities. Assessment cycles feed the overall determination of a unit's progress made toward accomplishing a task, creating a condition, or achieving an objective. Assessment applies to information activities and supports information planning in the same way. Assessing information activities helps answer basic questions such as:

- Are we performing the right information activities with the right capabilities?
- Are we executing the planned information activities as intended?
- Are we measuring the right things?
- Are we creating the intended effects?

The first question addresses the level at which the commander's desired effects are being observed across the operational environment. It prompts examination of the links between performance and effects. The second question addresses the performance of planned information activities by assessing the completion of tasks. The third question addresses the process of assessment itself and the importance of understanding how Marines choose to measure the links between performance, cause, and effect. The final question addresses the extent to which progress is being made toward objectives. When complete, the answers to the above questions provide the commander with feedback, from which the next planning iteration can benefit. For more on the design and execution of assessments of information activities, refer to Chapter 5.

Role of the Information Staff

The information staff is responsible for developing the overall concept of information, Annex I, and the commander's information directive for specialized information activities. Information staff planners must ensure that these products clearly state the primary tasks associated with the functions of information. The Annex I should provide enough guidance to ensure that information tasks and supporting lines of effort (to include those of specialized information activities) are all working toward the same objectives. It must also provide sufficiently detailed instructions to aid in the detailed planning of subsequent tabs to the Annex I.

Further, Annex I must be nested with the HHQ plan. This is important for three primary reasons:

- The effects of information activities can reach far across the assigned area of operations and affect the missions of higher, adjacent, and supporting units.
- Many of the information capabilities contributing to a Marine Corps unit's mission, and their associated authorities, will likely reside with the JFC, the CCDR, or other higher-level agency.
- A Marine Corps unit, based on its placement and access, can serve as the JFC's primary mechanism or platform for delivering a JFC (or higher) desired effect.

General Information Planning Considerations Across the Marine Corps

The information warfighting function is applicable to the entire Marine Corps, not just the FMF. This is because every activity performed by any unit or organization in the Marine Corps is potentially observable and can thus be used to send a message or create an effect in support of an objective. For example, the Service headquarters' Title 10 functions involve numerous activities focused on organizing, training, and equipping the force. These activities are of significant interest to potential adversaries as well as allies and partners. These activities can and should be coordinated and communicated in ways that benefit and support DoD and national strategic objectives. The following sections discuss general information planning considerations applicable to HQMC, FMF, and the supporting establishment.

Headquarters, United States Marine Corps. Headquarters, United States Marine Corps consists of the Commandant of the Marine Corps (CMC), the Assistant Commandant of the Marine Corps, deputy commandants, Staff Judge Advocate to the CMC, directors, other members of the Navy and Marine Corps assigned or detailed to HQMC, and civilian employees in the DON assigned or detailed to HQMC. The following are information planning considerations and key tasks applicable to all HQMC organizations and supporting activities:

- Develop and communicate policy, strategy, and official communication in alignment with national, strategic, and DON objectives and narratives.
- Monitor and assess the information environment.
- Assess the potential informational impacts of new policies or strategies prior to release.
- Practice OPSEC and encourage information discipline across the workforce.
- Assess the potential informational impacts of revealing new capabilities prior to revelation.
- Develop and synchronize communication activities to support the revelation of new capabilities and CMC priorities.

- Coordinate senior leader speaking engagements to ensure narrative consistency and effective timing.
- Monitor and assess relevant actor perceptions and reactions to Marine Corps Service-level initiatives.

Fleet Marine Forces: Marine Corps Component Commands. The Marine Corps component commander functions at the operational level of warfare and is responsible for accomplishing the assigned mission, providing forces, and accomplishing operational-level administrative and logistic tasks to assigned or attached Marine Corps forces. The following identifies general planning considerations and key tasks applicable to Marine Corps component commands:

- Develop and communicate component command narrative.
- Development and implement component command OPSEC policy and practices.
- Monitor and assess the information environment.
- Develop and implement information discipline procedures.
- Monitor and assess physical, technical, and administrative signatures across the component.
- Determine whether to include DoD deception activities in supported events (see Chapter 2).
- Ensure planning, coordination, and execution of information activities support CCMD objectives.

Fleet Marine Forces: Marine Air Ground Task Forces. The following are general information planning considerations and key tasks applicable to MAGTFs:

- Plan and conduct MAGTF operations to support and reinforce higher level narratives (from HHQ all the way up to national/strategic level narratives).
- Provide OPSEC and SIGMAN guidance to MAGTF elements (see Chapter 2).
- Establish presence, posture, and profile guidance to MAGTF elements (see Chapter 2).
- Develop and communicate the MAGTF’s command narrative.
- Plan and conduct operations deliberately to create or exploit information advantages.
- Develop and implement information discipline procedures.
- Monitor and assess physical, technical, and administrative signatures across the MAGTF.
- Determine whether to include DoD deception activities in supported events (see Chapter 2).
- Weigh actions intended to influence relevant actors as part of shaping activities.
- Synchronize official communication with operations and other command activities to support commander’s objectives.

Supporting Establishment. The Marine Corps supporting establishment consists of personnel, bases, and activities that support the FMF. Marine Corps installations are critical national defense assets that are the force generation and projection platforms supporting FMF basing, training, sustainment, mobilization, deployment, embarkation, redeployment, reconstitution, and force protection. The primary supported commands are the MEFs. The following identifies general information planning considerations and key tasks applicable to the supporting establishment:

- Determine and assess foreign observation and intelligence collection methods and timing of installation operations and tenant activities.
- Develop and implement installation wide OPSEC policy and practices applicable to supporting establishment personnel and tenet organizations.
- Develop and implement installation-wide information discipline practices.
- Coordinate and synchronize installation official communication activities with FMF tenant command official communication activities to ensure alignment with CCDR, Service, DON, and national strategic narratives.
- Consider and coordinate what is indicated by administrative signatures of logistics activities.
- Tenant commands assess the potential impacts of revealing new capabilities during exercises and coordinates with the installation commander to use facilities and spaces in ways to reduce foreign collection.

SPECIALIZED INFORMATION PLANNING CONSIDERATIONS

Specialized information planning considerations are implemented through the ITCC by specialized units and personnel trained and equipped to employ specialized information activities (e.g., MIG). All specialized information activities must be part of the ITCC and appear on the ITCO. The ITCC is an integral part of the commander's decision cycle along with other primary planning cycles that support mission planning and execution. Figure 3-1 illustrates the ITCC as an integral part of the commander's decision cycle.

The commander's decision cycle is a process in which command and staff elements determine required actions, which are then codified in directives, executed, and the results monitored. Four interrelated planning efforts or cycles include: the intelligence cycle, the air tasking cycle, the targeting cycle, and the ITCC. These planning efforts are inextricably linked and conducted collectively with the inputs and outputs of each cycle, interacting with the other cycles on a continuous basis. The MCPP provides the MAGTF mission detail and focus for these planning efforts, all of which support the commander's decision cycle.

Information Activities and the Fires and Effects Integration Methodology

The MAGTF fires and effects integration methodology embraces the single-battle concept by promoting unity of effort across the commander's decision cycle and its interrelated planning efforts. For specialized information activities that directly support fires and effects objectives and tasks (e.g., MISO, OCO, DCO-RA), coordination with the MAGTF fires and effects coordination center (FECC) is required. Coordination between information and fires and effects planners ensures unity of effort and avoids creating conflicting effects (e.g., contradictory messaging, or electromagnetic interference). This is accomplished by using the ITCC as the primary mechanism for planning and executing information activities as a part of the MAGTF fires and effects integration methodology.

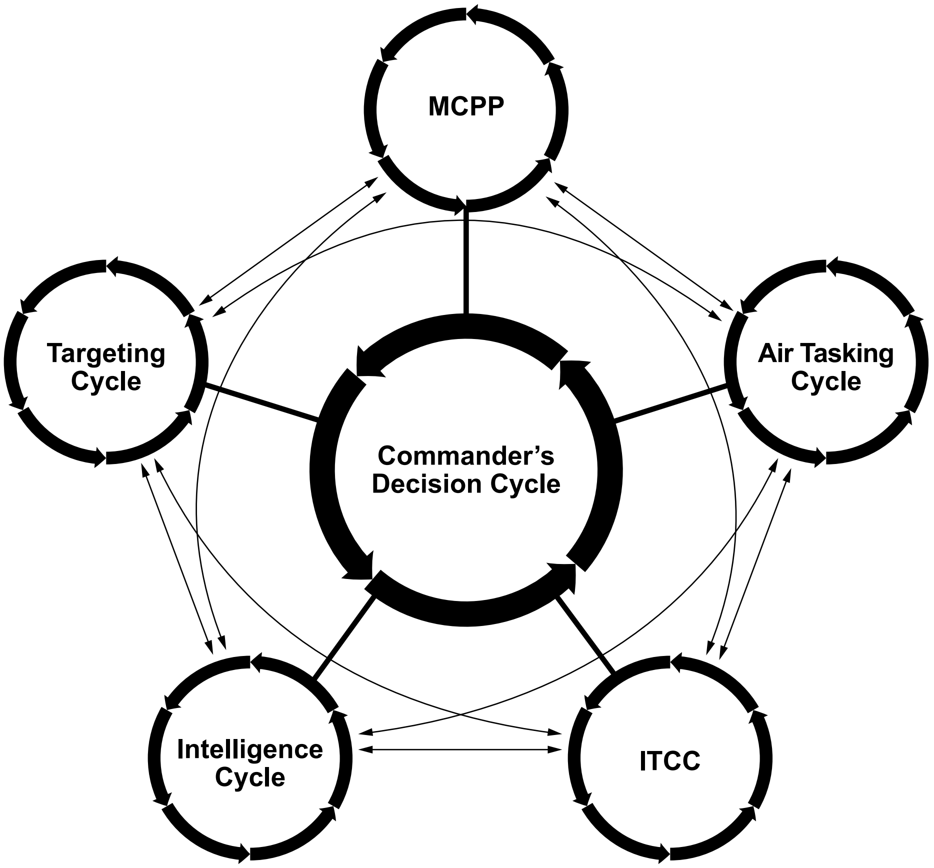


Figure 3-1. Planning Cycle Alignments to Achieve Unity of Effort.

Information Activities and Other Coordination Requirements

Specialized information activities that do not contribute directly to fires and effects objectives do not need to be coordinated with the fires and effects coordination center. However, these specialized information activities must still be planned, tasked, and coordinated with appropriate staff sections and centers through the ITCC, and appear on the ITCO. For example, cybersecurity activities do not generate fires and effects directly, but they are critical and need to be coordinated with the appropriate MAGTF staff sections, communications centers, MAGTF elements and subordinate/supporting units. The ITCC is applicable to all specialized information activities—whether they contribute directly to fires and effects objectives or not. All specialized information activities must be planned and executed through the ITCC and appear on the ITCO.

Information Tasking and Coordination Cycle Phases

The ITCC is the process for the integrated employment and coordination of organic and externally provided specialized information activities and capabilities. It is a methodical, iterative, and responsive process that translates strategic guidance into tactical-level plans and operations. The ITCC is primarily a MEF-level process but can be scaled for use at any echelon. Figure 3-2 illustrates the ITCC with six phases.

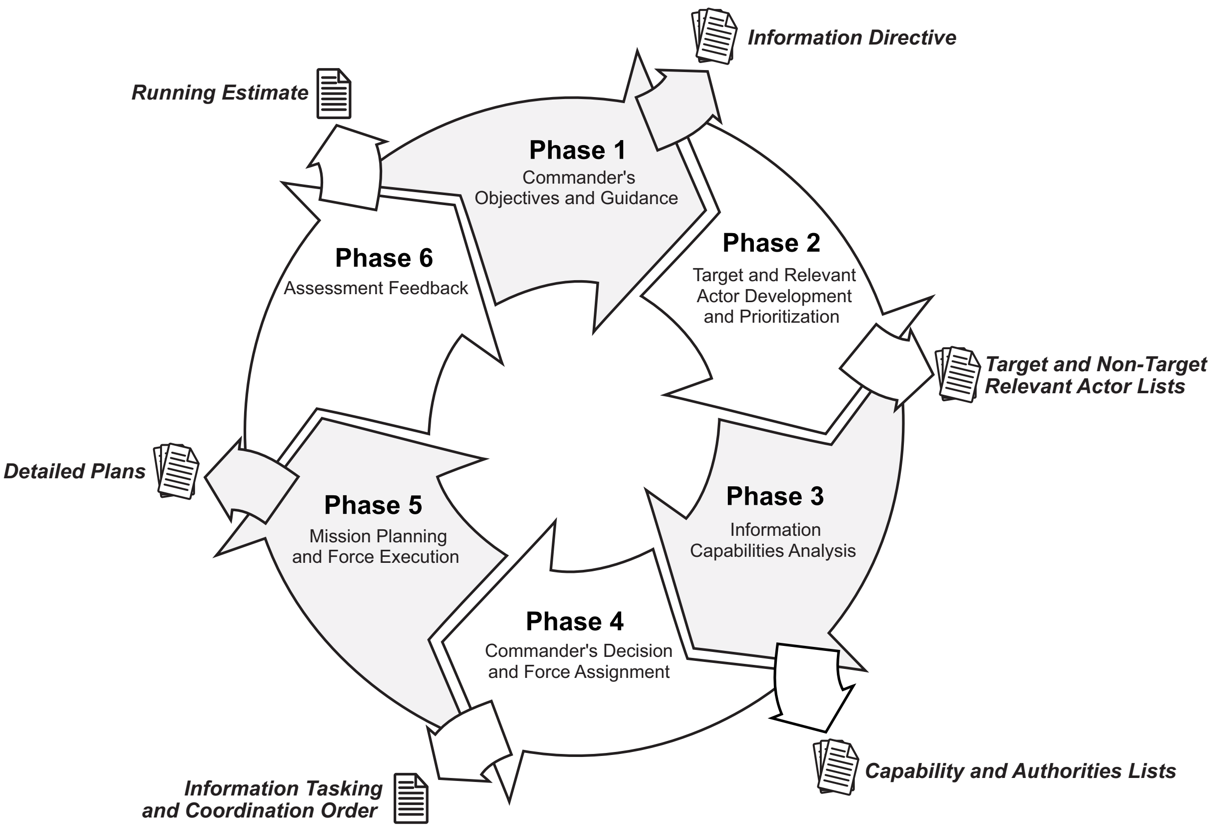

Information Directive
Running Estimate
Phase 1
Commander's Objectives and Guidance
Phase 2
Target and Relevant Actor Development and Prioritization
Phase 6
Assessment Feedback
Target and Non-Target Relevant Actor Lists
Detailed Plans
Phase 3
Information Capabilities Analysis
Phase 5
Mission Planning and Force Execution
Phase 4
Commander's Decision and Force Assignment
Capability and Authorities Lists
Information Tasking and Coordination Order

Figure 3-2. Six ITCC Phases.

A typical ITCC period is 24-72 hours. Multiple cycles can be in various concurrent stages of planning and development. The following sections discuss each phase of the ITCC in more detail.

Phase 1: Commander's Objectives, Guidance, and Intent. The information directive is the primary output of phase 1.

Phase one of the ITCC begins with developing objectives and guidance (the information directive), includes capabilities planning, culminates with the commander's decision (ITCO), and ends with assessment feedback to inform the next cycle of specialized information planning. During phase 1, commanders provide specific guidance that focuses planning and enables the information staff and working groups to develop and refine functional COAs for the employment of specialized information activities.

Objective-to-Task Approach. The ITCC involves an objective-to-task approach that directly links operational design elements to objectives, desired effects and outcomes, and tasks. The objective-to-task approach is a continuous, iterative process applicable across the planning horizons. Planners ensure the objective-to-task approach is nested with and supports the HHQ approach. The approach begins with identifying objectives and the desired future state. Once the desired future state and overall objectives are identified, planners can begin to plan specific information activities, effects, outcomes, and tasks.

Determining Desired Effects and Outcomes. Many specialized information activities are planned to create effects in support of fires and effects objectives. An effect is a change in the physical or behavioral state of an entity that results from an action, a set of actions, or another effect. Planners must be mindful that the effects created by specialized information activities can accumulate or compound, such that the result of several direct or indirect effects produce greater outcomes than the sum of their individual impacts. Thus, the effects of specialized information activities can cascade or ripple through a system, often influencing other systems, typically through nodes and links that are critical to related systems. These effects can create unintended consequences, which may be counterproductive, or they might create new and unforeseen opportunities. For specialized information activities that do not directly support fires and effects objectives, information planners still seek specific outcomes, to include new or altered states or conditions. For example, implementing new cybersecurity measures changes the state of critical systems to help assure command and control.

Information Directive. The information directive is the starting point for each iteration of the ITCC. It provides the task and purpose for specialized information activities to be planned and coordinated across the commander's decision cycle. Analogous to the air operations directive, the information directive specifies prioritized effects and coordination requirements for the conduct of specialized information activities. It captures commander's guidance over a specified period (typically 24–72-hour period), creating unity of purpose and effort. The information directive is an opportunity for the commander to prioritize or reprioritize specialized information activities, direct coordination with other aspects of operations, or adjust the emphasis toward new objectives as the situation unfolds.

All specialized information tasks are developed concurrently, in a collaborative manner with input from subordinate commands and subjects matter experts from multiple functional areas. The G-3, in coordination with the FECC, information coordination center (ICC), and MIG, is responsible to ensure objectives and tasking associated with the fires and effects integration methodology and information directive/ITCO are properly coordinated and disseminated.

See Appendix A for a sample format of the information directive.

MOEs and MOPs for Specialized Information Activities. During phase 1, planners determine MOEs and MOPs for specialized information activities. An MOE gauges the achievement of a future state or outcome, while MOPs gauge the successful completion of a well-defined task or progress within a well-structured process. Appropriate and effective MOEs and MOPs require a framework for organizing thinking and setting objectives, beginning with a precise definition of what is being measured.

Refer to Chapter 5 for additional information on MOEs and MOPs for information activities.

Phase 2: Target and Relevant Actor Development and Prioritization. Target list and relevant actors (other than targets) lists are the primary outputs of phase 2.

The methods used to list targets and relevant actors (*NOTE: Relevant actor engagement lists do not include those individuals, groups, populations, or automated systems classified as targets*). will vary based on entity type (target or neutral and friendly entity). Targets are listed, prioritized, and tracked on appropriate target lists (e.g., joint target list, restricted target list, joint integrated prioritized target list, MATF integrated target list). Neutral and friendly entities not validated and classified as valid military targets are listed, prioritized, and tracked on a separate list. These lists are developed during the MCPP, refined during the battle rhythm, and approved by the MAGTF commander. The fires and effects coordinator (also referred to as FEC) or FECC is responsible to coordinate overall list management to ensure both targets and neutral and friendly entities are identified, analyzed, and listed.

Refer to MCWP 3-31 for additional information on lists and related integrating processes. Refer to Appendix A for additional information about the other relevant actor engagement lists, to include a sample format.

Phase 3: Capabilities Analysis. The list of available capabilities and authorities for the execution period is the primary output of phase 3.

Phase 3 of the ITCC involves evaluating all organic and external information capabilities available to generate effects. Information, intelligence, fires, and effects planners collaborate in this phase to identify which capabilities will be used to create effects or achieve other desired outcomes. The focus of capabilities analysis is to maximize the effectiveness of scarce information capabilities. Capabilities analysis is constrained or restrained by the existing authorities and permissions associated with certain capabilities. A capability's physical availability does not always mean it is authorized for use. However, some capabilities may have existing programs in place that make them readily available to generate effects (e.g., an established MISO program).

Integration and Coordination. During capabilities analysis, planners integrate specialized information capabilities across all domains and the EMS. Multiple capabilities should be used when appropriate to create combined effects. Planners consider that certain information capabilities could take time to produce effects, and that such tasks might need to be executed over time to be effective. Planners finalize integration and synchronization requirements at the targeting or other working groups.

Sequence, Timing, and Adaptability. Planners carefully synchronize and sequence (spatially and temporally) specialized information activities to optimize effects and outcomes. For example, MAGTF planners may determine a desired effect is to neutralize an enemy unit's combat capabilities at a determined objective location. As the maneuver unit moves towards the objective, planners determine that specific information activities used to isolate (e.g., cyberspace operations, EMSO) and influence (e.g., MISO's "retreat" messaging) the enemy unit, synchronized with fires targeting tasks (e.g., destroying or disrupting enemy C2 and sustainment capabilities) could create the desired effect in a synergistic manner.

List of Available Capabilities and Authorities. The list of available information capabilities and authorities is started in step 1 of the MCPP but is finalized in phase 3 of the ITCC, capabilities analysis. The list is confirmed and updated as part of that stage by the information staff based on updated staff estimates, notification of assignment or availability of new capabilities, and updated readiness reporting from the capabilities themselves. The completed list of available information capabilities and authorities is a critical input to ITCC phase 3, where the prioritized relevant actors and effects are matched to specific capabilities and sequenced in time and space for delivery. The completed list of available information capabilities and authorities is a critical input to ITCC phase 4, commander's decision and force assignment.

See Appendix A for more information about and a sample format of the list of available capabilities and authorities.

Phase 4: Commanders' Decision and Force Assignment. The Marine Corps ITCO is the primary output of phase 4, commander's decision and force assignment.

The ITCO is the output of phase 4 of the ITCC. It is the ITCO that issues specialized information tasks assigned to specific information units and organizations. It is analogous to an air tasking order (ATO). The ITCO includes coordination requirements with higher, adjacent, or supporting units. All specialized information activities are planned and coordinated as part of the ITCO, which is concerned primarily with effects, sequencing, coordination, and deconfliction. Essentially, it encompasses numerous sub-processes, such as the detailed planning processes associated with different specialized information capabilities.

The ITCC is effectively a macro-process that composites and integrates multiple subordinate planning processes. The ITCO lists units, targets or non-target entities, capabilities, tasks, locations, time, and the effects and outcomes desired. It also lists authorities and coordination requirements. The ITCO can also include a synchronization matrix and any resulting special instructions for coordination to help maximize synergy and minimize cross-capability interference. These might include, for example, explicit notes about the intended layering of effects; perhaps for "surrender" broadcasts to begin almost immediately after physical fires destroy a command post, or deconfliction of precision messaging with cyberspace and EMI with enemy and who to contact for final deconfliction.

By combining the commander's guidance and priority effects from the information directive with the lists of priority targets, relevant actors (*NOTE: Relevant actor engagement lists do not include those individuals, groups, populations, or automated systems classified as targets*), and available capabilities, planners complete the ITCO and submit it for approval. The ITCO is intended primarily as a MEF commander-signed product; but the ITCC and ITCO can be scaled to apply at any echelon. At a minimum, the ITCO includes the following:

- Commander's guidance, objectives, and intent, summarized as the information directive.
- Prioritized desired effects and their association to objectives.
- Prioritized target and relevant actor engagement lists. (*NOTE: Relevant actor engagement lists do not include those individuals, groups, populations, or automated systems classified as targets*).
- Tasking of specific units and capabilities.
- MOPs and MOEs to be collected for feedback.

Refer to Appendix A for additional information about the ITCO, including a sample format.

Phase 5: Mission Planning and Force Execution. Information forces conduct detailed planning and execute assigned tasks in phase 5.

During phase 5 of the ITCC, units or agencies conduct detailed planning and execute assigned tasking. The tasking orders (e.g., ITCO, ATO) provide requisite information to facilitate detailed tactical-level planning. For example, the ITCO is published to allow information forces and agencies adequate time to coordinate specialized information activities and conduct detailed mission planning. During execution, the battlespace changes because of actions from friendly forces, adversaries, and other actors. During this phase, planners monitor changes and use capabilities to seize and maintain the initiative. Planners collaborate with current operations personnel across various centers to validate planned actions and adjust required actions.

Phase 6: Assessment. An assessment of information activities effectiveness is the primary output of phase 6.

The last phase of the ITCC is assessment. Planners participate in assessing the effectiveness of information activities as discussed previously. Given the scarcity of information capabilities, assessment serves an important role in determining whether previous information capabilities and activities successfully contributed toward achieving objectives. While considered the last step in the ITCC, assessment provides input into the continuous planning process, returning ITCC back to phase 1.

For more information about MOPs and MOEs, refer to Chapter 5.

INFORMATION PLANNING IN PRACTICE

Planning and executing general and specialized information activities must be nested with HHQ plans and support the CONOPS and overarching objectives. Day-to-day planning and execution of information activities is managed through a series of boards, centers, cells and working groups, which are composed of cross-functional teams of planners and decision makers from across the staff. The battle rhythm, or how boards, centers, cells, and working groups fit together in time, enables the commander's decision making. Thoughtfully managing the battle rhythm can itself create an information advantage by increasing efficiency and effectiveness of commander's decision making relative to an enemy or adversary. Information planners participate in numerous battle rhythm events, which vary among staffs; however, the most salient of these information planners is the IWG.

Information Working Group

The IWG is composed of information planners and pertinent representatives from different functional areas. Its primary role is to synthesize guidance related to information (concept of information, Annex I, previous information directive(s), list of available information capabilities and authorities, etc.) and execute the ITCC. The IWG, unlike its legacy predecessor the information operations working group, conducts comprehensive planning to address all four functions of information (generation, preservation, denial, and projection), resulting in the creation or exploitation of information advantages.

The IWG serves as a command's focal point for planning, coordinating, and synchronizing the employment of specialized information activities and capabilities. This includes both information activities that generate effects directly and those that enable them. For those that generate effects, close coordination with the FECC, or comparable organization, is critical to ensure they are appropriately accounted for in the fires and effects integration methodology. Key functions of the IWG include the following:

- Creating and revising the information directive in support of or in coordination with the information staff.
- Developing and assessing MOPs and MOEs.
- Nominating targets for inclusion on the FECC's target list.
- Determining relevant actors. (*NOTE: Relevant actor engagement lists do not include those individuals, groups, populations, or automated systems classified as targets*).
- Conducting capability analysis, in collaboration with intelligence, and fires and effects planners, to maximize impact of effects through deconfliction, synchronization, coordination, and integration.
- Assigning tasks to information capabilities or forces.
- Developing or revising the ITCO for MEF commander approval.

Other Battle Rhythm Events

While the IWG is the main effort for information planners, there are other battle rhythm events that affect the information warfighting function. Just as the IWG relies on inputs from planners across the staff, information planner's inputs are required in other working groups and boards. Every staff functions differently, but some of the most common and critical places for information planner inputs are the following working groups (and their parent boards):

- *Targeting Working Group*. Led by the FECC, it executes the fires and effects integration methodology integrating fires and information activities to create effects in support of the commander's objectives.
- *Collections Working Group*. Led by the intelligence section, it develops and coordinates the collection plan to satisfy intelligence requirements.

CHAPTER 4. COMMAND AND CONTROL OF INFORMATION ACTIVITIES

"We need to make sure in the context of transregional, multi-domain, multifunctional conflicts that we have the right command-and-control construct in place to integrate joint capabilities and support rapid decision-making by national command authorities."

—General Joseph Dunford, 19th Chairman of the Joint Chiefs of Staff

Command and control is the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. It encompasses all military functions and operations, giving them purpose and harmonizing them into a meaningful whole. The commander commands by deciding what needs to be done and directing or influencing the conduct of others. Control takes the form of feedback—the continuous flow of information about the situation returning to the commander. Feedback may come from any direction and in any form (e.g., intelligence about how the enemy is reacting, information about the status of subordinate or adjacent units, or revised guidance from higher authority based on developments). Feedback is the mechanism that allows commanders to adapt to changing circumstances (e.g., to exploit fleeting opportunities, respond to developing problems, modify schemes, or redirect efforts). In this way, feedback "controls" subsequent command action.

MULTI-DOMAIN AND ALL-DOMAIN COMMAND AND CONTROL

Multi-domain command and control is the command and control of forces, operations, and activities across more than one, but not all, domains within the operational environment—including the EMS and information environment. All-domain command and control is the command and control of forces, operations, and activities across all domains, the EMS, and the information environment. Marines should not mistake multi-domain or all-domain command and control as anything other than command and control. The Marine Corps' long standing, and well proven C2 theory and practices still apply. Adding the "multi-domain" or "all-domain" descriptor is meant for effect by indicating there are additional factors and requirements associated with harmonizing actions across a broader range of capabilities and contested spaces than have been traditionally taught or practiced.

The key characteristic of multi-domain or all-domain command and control is the dynamic, resilient, and scalable architecture that fuses data, organizations, systems, and people together to allow for the convergence of intelligence, fires, maneuver, and information throughout the operational environment. The objective of multi-domain and all-domain command and control is to enable combined arms effects throughout the competition continuum in the 21st century *single battle*.

Commanding and controlling information activities as part of multi-domain or all-domain operations is fundamentally about combining informational and physical power across relevant portions of the operational environment to create advantages and effects. To fulfill this fundamental purpose, a commander needs to leverage a C2 support system made up of the optimal mix of data, organizations, systems, and people. Because the information environment spans all domains, the C2 support system must work across multiple or all domains simultaneously in a specific, relevant operational area. The following sub-sections discuss key characteristics of multi-domain or all-domain command and control and its respective support system.

The Challenge of Multi-Domain and All-Domain Command and Control

The desire to replace detailed directive actions and tight control with spontaneous low-level cooperation is the crux of the multi-domain and all-domain command and control challenge. There is an inherent tension between achieving speed, flexibility, and low-level initiative versus the complexity of integrating an ever-increasing number of information and other capabilities across multiple domains that are required by today's commanders.

Resolving this tension requires at least four factors to be in place:

- Sufficient situational awareness in relevant domains.
- Extensive planning and preparation.
- Queued authorities and conditional permissions.
- Extensive trust-based relationships and communication patterns that span echelons.

Multi-Domain and All-Domain Situational Awareness. Multi-domain or all-domain situational awareness is knowledge and understanding of the current situation across all contested relevant spaces such that it promotes timely, relevant, and accurate assessment of friendly, enemy, environment, and other operations within the battlespace to facilitate decision making. Multi-domain or all-domain situational awareness fosters an ability to quickly determine the context and relevance of events that are unfolding in all relevant portions of the operational environment. Further, multi-domain or all-domain situational awareness involves a continuous process that fuses intelligence with all other relevant information from any source and any domain to facilitate decision making regarding threats, vulnerabilities, and opportunities. The tools and tradecraft of multi-domain or all-domain situational awareness are tailored to meet the requirements of the specific mission.

Extensive Planning and Preparation. Planning and preparation enhance the commander's ability to make sound and timely decisions. This is particularly important in complex operations, where many specialized information activities involve extensive planning, complex authorities and permissions, and robust coordination requirements. Information planners should become familiar with authorities and permissions that already exist and are available. Additionally, information planners should anticipate to the extent possible, new requirements that may not be covered by existing CONOPS or EXORDs. In these situations, it is vital that information planners know how to plan and submit new CONOPS for approval and how to obtain necessary authorities and permissions to execute the CONOPS.

Queued Authorities and Conditional Permissions. Effective multi-domain or all-domain command and control requires the ability to direct and coordinate activities simultaneously throughout the competition continuum and across domains as an inherent part of joint warfighting. Commanders must understand their authority to act at a designated time and location, which is often characterized as a permission. To execute an action, Marines must have both the authority and permission to do so. To increase the range of options available, commanders task their staffs to conduct planning and preparation to build a queue of available authorities under which they can act. These authorities are often tied to specific approved CONOPS or EXORDS that already exist, and that can be submitted up the chain of command for approval. Ideally, information planners develop and gain approval of plans that include conditions that when met, accelerate the permission to execute. Authorities and permissions are discussed again later in this chapter.

Trusted Relationships and Communication Across Echelons. Command and control demand mutual trust among all commanders, staffs, and Marines, and confidence in the abilities and judgment of subordinates, peers, and seniors. Trust is the cornerstone of cooperation, which is the bedrock of multi-domain or all-domain command and control. Because many of the information capabilities employed through multi-domain or all-domain operations exist outside of the Marine Corps commander's sole authority to execute, establishing strong trusted relationships with the JFC, CCDR, or other external agencies with the needed capability and authority is essential.

INFORMATION DIRECTION AND CONTROL

Information Direction

The parts of any mission include the task(s) to be accomplished, the purpose, and the reason for the mission. Information direction is the authority to task the employment of information organizations to perform specialized information activities and tasks. Information direction must always be accompanied by the commander's intent; both are typically communicated through the information directive as discussed in Chapter 3. The purpose of information direction is to achieve balance between finite information capability resources and mission accomplishment. Information direction is exercised by any commander with the authority to task a unit that employs information capabilities and activities.

Information Control

Information control is the authority to direct the maneuver, timing, or reassignment of information capabilities during mission execution. It is the process of synchronizing, deconflicting, and coordinating the information activities that appear on the ITCO. It is important during the planning process to clearly identify who has control authority of specific information capabilities and activities once the mission is underway. This can be complicated if the specific capability is being employed by an external agency or by another joint force component. Information control is exercised on behalf of the commander through the designated center or staff section.

MARINE CORPS INFORMATION UNITS AND ORGANIZATIONS

Deputy Commandant for Information

The Deputy Commandant for Information develops and supervises plans, policies, and strategy for all information, intelligence, and communications activities and identifies requirements for doctrine, manpower, training, education, and equipment in support of the Marine Corps. In support of the CMC, Title 10 responsibilities as a Service chief, the Deputy Commandant for Information serves as the principal advisor on all information-related matters and as the principal spokesperson on related Marine Corps programs, requirements, and strategy throughout the DON and the DoD.

Communication Directorate

The Communication Directorate —

- Enables the Service to communicate with precision and consistency by providing communication counsel to the Secretary of the Navy, CMC, and HQMC staffs.
- Develops, integrates, and assesses Service-level communication plans, guidance, and music programs.
- Produces communication products.
- Informs and educates relevant audiences to set conditions to achieve organizational objectives.

The director of communication serves as the doctrinal proponent for COMMSTRAT comprising the sub-functions of public affairs and COMCAM. The Communication Directorate prioritizes requirements at the HQMC-level to provide support to HQMC and Service-wide entities, as appropriate. This is achieved through developing and updating the Marine Corps Service Communication Strategy, which establishes the Marine Corps' master narrative and provides general communication guidance to help shape FMF and supporting establishment communication campaigning.

Marine Corps Information Command

The Marine Corps Information Command (MCIC) integrates, synchronizes, and enables information capabilities and Service activities to support the conduct of naval, joint, and combined campaigning to deter adversaries in competition and warfare. The MCIC supports information planning and operations across all domains. The MCIC is a Service-retained command whose Commanding General is the same general officer serving as Commander, MARFORCYBER. As a separate and distinct command, MCIC's Service-retained status means that CCMD planning and execution authorities cannot be delegated to the MCIC. As such, the MCIC's primary mission is to execute the Service's man, train, and equip functions in ways that support the integration and synchronization of assigned force information activities and Service intelligence activities. It can also support assigned forces through individual augmentation via the Global Force Management process. The commanding general of the MCIC is also Commander, MARFOR CYBERCOM and Commander, MARFOR SPACECOM. The MCIC leverages MARFOR CYBERCOM's operations center to provide a persistent situational awareness of the information environment.

Marine Corps Information Command Relationships. The MCIC is a separate and distinct command from both MARFOR CYBERCOM and MARFOR SPACECOM. As noted above, all three commands are commanded by the same general officer. While serving in the capacity of Commanding General, MCIC, this general officer also serves as a subordinate commander to Commander, Marine Forces Command. When serving in the capacity of Commander, MARFOR CYBERCOM or MARFORSPACECOM, this general officer serves as a subordinate Service component commander to Commander, USCYBERCOM or Commander, USSPACECOM, respectively. The MCIC includes the MCIOC, Marine Cryptologic Office, Marine Corps Cryptologic Support Battalion, and the responsibilities of the Service Cryptologic Component (SCC).

Marine Corps Information Command Roles and Responsibilities. The MCIC serves as a link across adjacent commands that conduct operational level planning. It plays a crucial role in multi-domain operations by providing task organized detachments in support of CCDR objectives. The MCIC is strategically placed and designed with interior organizational lines of communication to coordinate action with partner organizations and agencies. The MCIC supports FMF multi-domain command and control by providing reach back guidance to FMF units. Specifically, the MCIC is organized to provide or support—

- Globally focused capabilities that mutually support FMF, joint, Service, and interagency requirements.
- Globally integrated information forces and synchronized strategies.
- Training support to assist planners in developing space, cyberspace, and information CONOPS and authorities by leveraging proximal relationships with MARFOR CYBERCOM, MARFOR SPACECOM, USCYBERCOM, and USSPACECOM.
- Tracking of global information forces disposition, activities, and effects in support of Marine Corps interests.
- Providing input on Marine Corps capabilities to support operational units in their planning and incorporation of information activities into OPLANs and concept plans as required.

The MCIC supports all five Service commands by planning, synchronizing, and coordinating pairing task-organized detachments and capabilities with authority to execute missions. This serves an important role in forecasting requirements, apportionment, and force offering initiatives thereby ensuring force provisions and force generation initiatives are conducted in concert with each of the respective commands. The commands collectively possess the expertise and capabilities to support space, full spectrum cyberspace, and the full range of information activities.

Marine Corps Component Commands

Marine Forces Cyber Command. Marine Forces Cyber Command enables full-spectrum cyberspace operations, to include the planning and direction of MCEN operations and OCO in support of Marine Corps, joint, and multinational forces, to enable freedom of action across all domains and deny the same to adversarial forces.

Commander, MARFOR CYBERCOM is the Service component commander that represents Marine Corps capabilities and interests in support of cyberspace operations. The command is delegated directive authorities for cyberspace operations by USCYBERCOM, enabling the exercise of both Title 10 and Title 50 authorities. As such, MARFOR CYBERCOM uses a range of tools to conduct surveillance and reconnaissance, collect and analyze data, improve situational awareness, execute the targeting cycle, and assure command and control throughout the competition continuum. Further, it enables the warfighter through protecting and hardening friendly force networks.

Marine Forces Space Command. As the Marine Corps component to USSPACECOM, MARFOR SPACECOM supports USSPACECOM space superiority mission and enables the FMF by providing space support to operations and integrating, coordinating, and employing multi-domain capabilities to create competitive advantages that increase lethality, maneuverability, and survivability. Marine Corps Forces Space Command represents the Marine Corps' capabilities and interests and advises USSPACECOM on integration with and support to Marine Corps operations.

Marine Forces Special Operations Command. Marine Forces Special Operations Command (MARFORSOC) uniquely enables its deploying Marine special operations companies with key support personnel, to include intelligence, logistics, communications, explosive ordnance disposal, and information forces. Given MARFORSOC's lack of organic information capabilities, a relationship between MARFORSOC and the MCIOC has been established using the global force management process. The MARFORSOC G-39 is primarily focused on ensuring all deploying units are manned, trained, and equipped with the appropriate information forces and that all MARFORSOC's information-related requirements are managed and fulfilled.

Marine Expeditionary Force Information Group

The MIG assures command and control; conducts ISR and counter ISR operations; and integrates effects to create and exploit information advantage; enable combined, joint, and naval maneuver; and prevent adversary freedom of action. The MIG is organized with a headquarters and subordinate units to provide and integrate communications, intelligence, EMSO, inform and influence operations, cyberspace operations, space operations, supporting arms liaison, administrative, security, infrastructure, and sustainment support to a MAGTF, or assigned units.

The MIG headquarters provides the MIG commander the means to exercise command and control over elements of the MIG to conduct ISR and counter-ISR, and generate effects for the supported commander, while preventing adversary freedom of action. The MIG HQ provides capabilities at echelon.

Based on the MEF or MEB CONOPS, task organization, or mission requirements, the MIG commander directs and coordinates subordinate command relationships. The MIG commander can direct subordinate units to support the MEF or MEB command element, supporting MSCs operational requirements, or providing capabilities to MSCs. The MIG typically retains operational control or administrative control of subordinate units depending on the mission and environment. Any tasking for support to the command element or another MAGTF is accomplished via standard tasking channels during planning and execution.

COMMAND AND CONTROL CENTERS, AGENCIES, AND UNITS

Command Element

The command element is the MAGTF headquarters. As with all other MAGTF elements, the command element task-organizes to provide the C2 capabilities necessary for effective planning, execution, and assessment of operations in all domains, the EMS, and the broader information environment. Additionally, the command element can exercise command and control within a joint force and act as a JTF headquarters core element with significant personnel augmentation. The following sub-sections describe organizations and agencies typically established in a MEF to provide C2 capabilities. The MEUs and special purpose MAGTFs typically possess the same organization but on a smaller scale.

Combat Operations Center. The MAGTF combat operations center (COC) provides the MAGTF commander with a means to command and control forces. The G-3 directs all activities and functions within the COC and is responsible for synchronizing the warfighting functions (including the information warfighting function) to accomplish the MAGTF commander's intent during the current battle and to set the conditions for the next battle. From an information warfighting function perspective, the COC personnel—

- Supervise and execution of the concept of information as part of the current MAGTF CONOPS or fragmentary order (FRAGO).
- Monitor the effects of general information activities.
- Monitor the effects of specialized information activities.
- Monitor friendly, enemy, and adversary information activities that impact the situation and current battle.
- Analyze the current battle; and recommend to the MAGTF commander adherence to or changes in the current order, priority of effort, and targeting priorities.
- Advise the MAGTF commander in assessing whether conditions for phasing of an operation have been met or whether the end-state has been achieved.

Fires and Effects Coordination Center. The FECC serves as the MAGTF commander's principal agency responsible for overall fires and effects integration, which includes ensuring the effects from specialized information activities support the overall operational scheme of maneuver. The G-3 fires and effects coordinator serves as the MEF commander's principal fires and effects integrator. The MEF FECC is responsible for the planning, integration, synchronization, and execution of fires and effects throughout the MEF battlespace. The MEF FECC is staffed with subject matter experts from fires, aviation, and information disciplines, and is task-organized into cells appropriate for a given MEF's battlespace and battle rhythm. These cells may correspond to disciplines, planning horizons, or another such suitable distinguishing characteristic.

The FECC responsibilities include the following:

- Planning for fires and effects as an integral element of the MAGTF's overall CONOPS, in conjunction with the other warfighting functions, to promote a single battle and provide fires and effects direction to the MSCs or major subordinate elements.

- Coordinating the integration and synchronization of MAGTF fires and effects and specialized information activities to achieve objectives.
- Planning, coordinating, and directing the MAGTF fires and effects integration methodology and counterfire activities.
- Assessing the effectiveness and performance of MAGTF fires and effects and specialized information activities, and coordinating adjustments required to achieve objectives.
- Sponsoring and hosting targeting boards, working groups, and other forums to plan and coordinate MAGTF fires and effects and specialized information activities as required during the battle rhythm.
- Coordinating with higher, adjacent, subordinate, and supporting agencies/entities to integrate MAGTF fires and effects and specialized information activities.
- Coordinating requests for external fires and effects and specialized information activities support to address MAGTF shortfalls.
- Coordinating fires C2 systems planning and monitoring system status during execution.
- Monitoring and supporting MSC fires and effects and specialized information activities within their assigned boundaries.
- Resolving fires and effects and specialized information activities issues requiring MAGTF-level decisions.

The size, scope, and organization of an FECC varies with MAGTF type and mission requirements. To facilitate synergy of fires and effects, MAGTFs may tailor the FECC organization and MAGTF COC layout based on battlespace considerations and mission requirements.

Air Center. The MAGTF air center provides the MAGTF commander with aviation expertise and an essential interface between the MAGTF commander, the aviation combat element (ACE), the joint force air component commander or airspace control authority, and other air-capable commands as required. The air center coordinates with appropriate agencies across the three planning horizons to integrate and synchronize the six functions of Marine aviation with the MAGTF CONOPS. The MAGTF air center, ACE, and Marine liaison element coordinate and liaise with higher and adjacent aviation coordination agencies to facilitate MAGTF aviation integration with joint and combined air operations. The air center is supervised by the MAGTF air officer. The MAGTF air center may require augmentation and additional personnel during operations to successfully accomplish all required functions to include electromagnetic warfare, cyberspace operations, and space operations.

Information Coordination Center. The ICC plans, coordinates, integrates, and employs information activities to ensure the commander’s ability to facilitate friendly forces fires and maneuver and deny the enemy freedom of action in the information environment. The MIG commander determines how to organize and employ the ICC based on mission requirements, available resources, and established command relationships. The ICC includes personnel from the MIG headquarters and subordinate battalions, and it supports and is supported by cells and centers in the MEF (primarily the FECC), its MSCs, and external entities. Depending on mission requirements, the ICC can grow, divide, or flex to meet the demands of the specific situation. The ICC’s structure is based on a flexible and scalable grouping of interlinked functional cells that support planning, execution, and assessment. The cells are crewed by functional experts either organic to the MIG, or available to support the MIG ICC as augments. Cells support the operation of the ICC watch floor to assist in near-real-time information activity coordination and deconfliction. The MIGs consider the following areas when establishing cells:

- Intelligence.
- Cyberspace operations.
- EMSO.
- Space operations.
- SIGMAN.
- OPSEC.
- Deception.
- MISO.
- Civil affairs.
- COMMSTRAT.

Through the MIG headquarters and ICC, the MEF commander or information coordinator maintains a current in-depth multi-domain understanding of the information battle to include the unfolding situation; location and status of friendly maneuver forces; location, status and availability of organic and external information capabilities and formations; pending FRAGOs; and the commander's mission priorities. The ICC also supports the commander's or information coordinator's responsibility for nominating targets for deliberate or dynamic targeting, and for coordinating the timing and tempo of externally provided information capabilities and activities applied against targets when authorized.

For operations conducted during campaigning or below the threshold of armed conflict, the MIG commander coordinates with the MAGTF G-3 and FECC to develop an integrated plan and coordinate information activities to support the CONOPS. The MIG supports the MAGTF fires and effects integration methodology, battle rhythm events, and fires plans by providing planners, technical subject matter experts, and authorities required to effectively employ information-related tasks.

Intelligence Centers. At the MEF command element level, the intelligence operations center is the primary MAGTF intelligence node that is established at the direction of the MIG commander to support the MEF G-2. The intelligence operations center works to fulfill intelligence requirements of the MEF commander, as identified by the G-2. The intelligence operations center plans, directs, collects, produces, and disseminates intelligence and provides counterintelligence support to the MEF, MSCs, subordinate MAGTFs and other commands as directed.

The intelligence operations center is collocated with the MAGTF's main command post and includes both the operations control and analysis center and surveillance and reconnaissance coordination center, along with other intelligence capabilities. Radio battalion plans and coordinates ground-based SIGINT, electromagnetic warfare, and special intelligence communications through the operations control and analysis center.

The force reconnaissance company conducts pre-assault and deep post-assault reconnaissance and surveillance in support of MAGTF operations. The reconnaissance operations center is the principal operations, information, and C2 center for ground reconnaissance units. The reconnaissance for COMCAM imagery to be shared publicly in support of public communication objectives must be reviewed and cleared for public release. This imagery release is done through public affairs authorities.

Release of COMCAM imagery can also occur under authorities granted to other information activities. For example, influence Marines conducting MISO activities can release COMCAM imagery in support of an approved series. If the unit deploys with a HHQ command group, the reconnaissance operations center will either provide liaison to or integrate with the surveillance and reconnaissance coordination center. For additional information, refer to MCWP 2-10, *Intelligence Operations* and MCRP 2-10A.6, *Ground Reconnaissance Operations*.

Communications Centers. The MIG establishes all MEF level communications centers. The G-6 exercises technical direction and overall control over the communications networks and information systems from the MAGTF communications control center. The communications battalion or communications squadron assists the G-6 in these responsibilities. The MAGTF communications control center coordinates external communications control with the JTF or CCDR J-6 through the joint communications control center and may also provide communications control support to the MAGTF communications control center. Separate MEF and MAGTF communications control centers may require augmentation from other communications battalions. Communications control occurs at all echelons of the command down to battalion level with the assistance of organic and supporting communications units or detachments. The MAGTF communications control center directs subordinate MSC communications control centers. For additional information, refer to MCRP 1-10.1, *Organization of the United States Marine Corps*, and MCRP 3-30B.2, *MAGTF Communications System*.

Ground Combat Element

The ground combat element (GCE) main headquarters echelon provides the principal headquarters for the commander, and supplies all the resources necessary for sustained operations. Resources include planning, executing, and assessing operations across all warfighting and staff functions. The main headquarters echelon possesses the ability to plan for future operations and includes a COC that provides command and control of current operations. In support of the commander and the staff, the GCE COC fuses information to provide situational awareness across multiple domains, the EMS, and the broader information environment. An intelligence operations center provides command and control of the intelligence effort if it is required. From an information warfighting function perspective, GCE personnel—

- Supervise and execute information activities as part of the current GCE CONOPS or FRAGO.
- Monitor the effects of general information activities.
- Monitor the effects of specialized information activities.
- Monitor friendly, enemy, and adversary information activities that impact the situation and current battle.
- Monitor logistics combat element (LCE) signatures across domains.

The GCE employs a fires support coordination center, which provides a single agency that has centralized communications facilities and personnel to coordinate of all forms of fire support for the GCE. From an information warfighting function perspective, the fires support coordination center provides the location where specialized information activities are planned and integrated into fires and effects to support the scheme of maneuver.

Logistics Combat Element

The LCE is the agency the commander uses for the control and coordination of logistics and sustainment operations. The LCE establishes an LCE COC that controls and coordinates the day-to-day operations and focuses on meeting the needs of supported units. From an information warfighting function perspective, the LCE provides opportunity for conducting general or specialized information activities. The presence and movement of LCE units can be used not only to send a message to adversaries, allies, and partners, but also for providing placement and access for the employment of specialized information activities. The LCE planners and information planners must coordinate during the MCPP to maximize opportunities for creating and exploiting information advantages by leveraging all available capabilities, including LCE capabilities. From an information warfighting function perspective, LCE personnel—

- Supervise and execute information activities as part of the current LCE CONOPS or FRAGO.
- Monitor the effects of general information activities.
- Monitor the effects of specialized information activities.
- Monitor friendly, enemy, and adversary information activities that impact the situation and current mission.
- Monitor LCE signatures across domains.

Aviation Combat Element

The ACE provides the MAGTF tremendous capability due to its operational reach, speed, and flexibility in tasking sorties. The ACE can shape the deep battle through deep air support, extend the MAGTF's all-domain collection ability with its reconnaissance assets, serve as an extension of the MAGTF's C2 capability, and conduct combined arms with the GCE. Like the other MAGTF elements, all warfighting functions apply to and can be leveraged to gain advantages or achieve objectives. From an information warfighting function perspective, ACE personnel—

- Supervise and execute information activities as part of the current CONOPS or FRAGO.
- Monitor the effects of general information activities.
- Monitor the effects of specialized information activities.
- Monitor friendly, enemy, and adversary information activities that impact the situation and current mission.
- Monitor ACE signatures across domains.

CHAPTER 5. ASSESSMENT: MEASURING INFORMATION EFFECTIVENESS AND PERFORMANCE

> *"Not everything that can be counted counts, and not everything that counts can be counted."*
>
> — William Bruce Cameron, Sociologist, 1963

As described in Chapter 3, assessment is an essential element of the iterative cycles of operational planning the fires and effects integration methodology and the ITCC. Assessment provides a method for determining whether the desired effects are being generated. However, assessing the efficacy of information activities is often much more challenging than conducting a battle damage assessment of effects generated through the application of traditional fires.

CORNERSTONES OF ASSESSMENT

Effective assessment has several prerequisites and is made easier by adherence to certain principles. This section discusses those principles and offers advice for mobilizing them in pursuit of measuring the performance and effectiveness of information efforts.

Evaluating Change Requires a Baseline

To see a change, an observer needs a starting point—a baseline with which to compare and measure change. It is best to measure the baseline before activities begin. While the need for a baseline (against which to evaluate change), and the importance of taking a baseline measurement (before change-causing activities begin) seem self-evident, these principles are often not adhered to in practice. Without a baseline it is difficult to determine whether an information activity has had its desired impact—or any impact at all. Marines cannot evaluate change without a starting point. Always seek an initial measure or validate initial assumptions about the starting state using data. A baseline should help identify the starting system state, the typical behavior of the relevant entity, or the initial extent or degree of relevant information advantages. A baseline evaluation should include the following:

- *Systems analysis*. To establish the initial condition of the system, its performance, and its relationships and nodes. If the intent is to make the system function differently (or function less well) then a system's baseline will suggest possible avenues of effect and provide an initial state against which to compare.
- *Behavioral or pattern of life analysis*. To develop a description of the routine, typical, or intended actions or behaviors of entities of interest that might be intentionally affected through operations.

- *Media analysis*. To examine the media landscape to identify outlets, conduits, preferred sources, outlet biases, key influencers, etc.
- *Friendly narrative prevalence and perceptions analysis*. To determine the prevalence and perceptions of friendly objectives, narratives, and operations, activities, and investments.
- *Adversary narrative prevalence and perceptions analysis*. To determine the prevalence and perceptions of adversary objectives, narratives, and operations, activities, and investments.

Baseline measures should ideally emerge during the IPB and drive problem framing (MCPP step 1). If specific measurements for baselines of behaviors, characteristics, or other factors that operations are intended to change are not available (or are insufficiently detailed) in the initial IPB and other available estimates, they should then become requests for information, PIRs, or commander's critical information requirements, and they need to be tasked for collection. Intelligence capabilities and organizations will be critical to establishing baselines.

Effective Assessment Starts in the Planning Phase

Objective refinement and specification are important parts of the planning process. The need to articulate assessable goals and objectives starts in planning. If poorly specified or ambiguous objectives survive the planning process, both assessment and mission accomplishment will be in jeopardy. This applies in both general and specialized information planning.

In addition to specifying objectives in an assessable way during planning, assessments should be designed and planned alongside the planning of activities so that the data needed to support assessment, including a baseline measurement, can be collected before, during, and after the related activities. Knowing what needs to be measured and assessed at the outset clarifies what success should look like at the end and enables collection of sufficient information to observe that success or lack thereof. Because of the criticality of intelligence capabilities and organizations in these observations and measurements, a unit's intelligence section should also be involved in early planning for assessment.

Effective Assessment Requires Clear, Realistic, and Measurable Goals

Making the connection between indirect observations and the actions that may have caused them requires effort and expertise in novel areas. How can one determine whether an effort has achieved its desired outcomes if the desired outcomes are not clear? How can one develop and design activities to accomplish desired goals if the desired goals have not yet been articulated? How can one evaluate a process if it is not clear what the process is supposed to accomplish? While the importance of setting clear goals may appear self-evident, often this requirement is not met. Good assessment demands specific, measurable, achievable, relevant, and time-bound [known as SMART] objectives that can be incorporated in the initial planning process. Table 5-1 elaborates on SMART objectives.

Table 5-1. Characteristics of SMART Objectives

An Objective is…	If…
Specific	It is well defined and unambiguous and describes exactly what is expected.
Measurable	One can measure the degree to which the objectives is being met.
Achievable	It is realistic and attainable.
Relevant	The achievement of the objective contributes to progress toward high-level strategic and policy goals.
Time-Bound	It has deadlines or is grounded within a deadline.

Marines charged with assessment should demand SMART objectives. If SMART objectives fail to emerge from the planning process, Marines should cycle through another iteration of planning and push to get it right. If the overall process has moved past that point, assessment practitioners should attempt to respecify the objectives to align as closely with SMART criteria as possible and present them to leaders or senior planners for approval. When effective, refined objectives are pushed back to the originator, one of three things will likely happen:

- The originator of the objective will agree with the refinement and adopt it (good).
- The originator will see that the refinement is a little off mark but correct it (good).
- The originator will strongly prefer their original objective and insist that it remain unchanged (not good).

When objectives cannot be changed, another option is to develop subordinate, supporting, or intermediate SMART objectives (one level down from the immovable objectives), and then assess to them.

The SMART objectives should emerge from phase 1 (objectives and guidance) of the ITCC. Objectives should become more specific in phase 2 (target and relevant actor development and prioritization). Should the objectives emerging from phase 1 and phase 2 in the ITCC be insufficiently specified for measurement, that will likely become evident in phase 3 (information capabilities analysis) when planners attempt to match capabilities to objectives. Since planning and the ITCC are iterative processes, proposed refinements can be provided as feedback for the next iteration or cycle.

Planning for MOPs and MOEs should begin concurrently defining and refining the objectives in phase 1 of the ITCC. Final planning for MOPs should accompany the determination of which capabilities will be used to pursue which effects in ITCC phase 3 (capabilities analysis). Along with the tasking and assignment of capabilities, collection of MOPs and MOEs should be explicitly assigned in phase 4 (commander's decision and force assignment). Phase 4 of the ITCC needs to include an interface with other capabilities' planning and tasking processes because collecting measurement data will likely rely on capabilities other than the executing forces, such as intelligence capabilities. A unit's intelligence section will likely be an important contributor to assessment data and should be involved early in the design of objectives, MOPs, MOEs, and proposed (and possible) measurement.

Theory of Change or Logic of the Effort Connecting Activities to Objectives

Implicit in many examples of effective assessment and explicit in much of the work by scholars of evaluation is the importance of a theory of change. A theory of change, or logic of the effort, is the underlying logic for how planners think elements of an activity, line of effort, or operation will lead to desired results. Simply put, it is a statement of how a planner believes the things they are planning to have Marines do will lead to the objectives sought. When an effort does not produce the expected outcomes and one wants to determine why, having a clear logic of the effort helps.

Marines planning (or planning assessment for) information activities should be explicit about the logic of the effort or the theory of change. Marines should spell out the logic by writing it down to help determine what strategy works, or to support a conclusion that no strategy is working at all. This helps make assumptions and untested hypotheses explicit and helps reveal which hypotheses may be tenuous and in need of confirmation through measurement. This also can help clarify whether the desired objectives are not achieved and whether the cause for failure is poor execution, program failure (the activity was not properly completed), or a theory failure (the properly completed activity did not work). Figure 5-1 depicts the difference between theory failure vs program (or activity) failure.

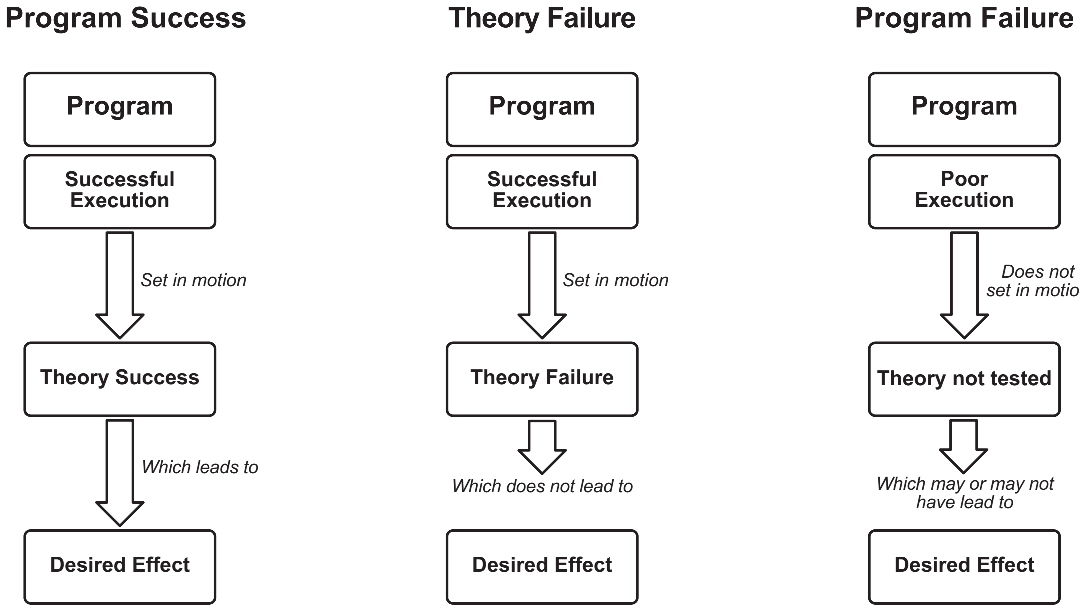


Figure 5-1. Program Failure Versus Theory Failure.

A clear theory of change is more important for some information activities than for others. For example, an influence activity or an effort to deceive an enemy commander needs to be as explicit as possible about the logic of the effort. A theory of change should include the following:

- How information will be projected.
- Who will receive it.
- How it will be conveyed to ensure receipt.
- How many times and in what way the message needs to be received before it is accepted.
- How the receiver's perceptions will change.
- How that perception change will affect target audience's behavior.
- When the friendly force should be able to begin to observe the behavior change.

In contrast, the logic of the effort for an electromagnetic warfare jamming effort is much simpler. For example, directed emissions on a targeted frequency will suppress communications on that frequency and perhaps herd users to other frequencies or systems. However, even for an example such as this it can be beneficial to write down the logic, particularly to enable the understanding of those less experienced in the capability. A theory of change could include the following:

- How long it will take those communicating on the jammed frequency to switch to a different frequency.
- How long it will take jamming to follow those communicating on the new frequency.
- How many frequencies the enemy will try before switching to a different mode.
- What mode is the enemy expected to go to next.
- Whether the next mode can be jammed, collected against, or subjected to other effects.
- How long it will take for the enemy to identify the source of the electromagnetic attack.
- What impact the jamming might have on own force protection.

Using specific details in the theory of change can improve planning. This can help make assessment better by pointing out specific things that might be worth measuring (or possible to measure). Being able to distinguish theory failure from program failure is the first step toward ascertaining and fixing an effort that is not working.

The logic of the effort should be clearly stated in the ITCC phase 3, where specific capabilities are matched to specific effects. A clear theory of change is particularly important when campaigning as part of a competition mindset; if an objective has a lengthy time horizon, it needs to be very clear exactly how proposed activities are intended to contribute progress toward that objective.

Assessment is Iterative

Assessment must be an iterative process, not something planned and executed once. First, efforts to track trends over time or to track incremental progress toward an objective require repeated, iterative measurement. Second, assessment needs to be planned and conducted iteratively, as things change over time; objectives can change, available data (or the ease of collecting those data) can change, and other factors can change—thus, assessment must change with them. Third, various information efforts can involve numerous dynamic processes and require dynamic evaluation. Context, understanding of the contexts, theories of change—all *change*, and activities are modified based on revisions to theories of change. Assessments need to adapt to reflect these changes. As information activities change, measures must be recalibrated and corrected, iteratively, along the way.

Learning from Failure

Related to the iterative nature of assessment is the importance of learning from failure. Marines assess information activities in part for accountability purposes, but also to support a host of critical planning, resourcing, and process requirements. Consequently, it is important to determine as early as possible whether certain activities are failing or have failed. Something must be acknowledged to be not working before it can be fixed. Ultimately though, it is the commander's prerogative to determine when something has failed and when to adjust an operational approach or objective.

Assessment can directly support learning from failure, mid-course correction, and planning improvements. An after-action review is a familiar and widely used form of evaluation that is dedicated to learning from both success and failure. The principles of good assessment articulated above can help prevent program failure, but they can also help detect imminent failure early on, saving precious time and resources. When information activities involve unvalidated assumptions or other uncertainties, planners should structure the efforts and assessments to fail fast, and then learn, iterate, and improve.

In planning and assessing information activities, Marines should take an experimental mindset. Try something, see how well it works, and adjust to improve before scaling up. For example, bracketing with indirect fires before firing for effect. As with physical fires, information activities require that there is sufficient observation, intelligence collection, or other measurement in place to note the extent of effect on the relevant entity.

MEASUREMENT

Existing joint and Service doctrine divides assessment measures into MOPs and MOEs. While appreciating the conceptual differences between measure types can be valuable, Marines should avoid being overly concerned with the difference between MOPs and MOEs. There is a spectrum of measure types, and the MOE-MOP dichotomy can mislead evaluators into thinking that there are only two relevant measures. At worst, premature conclusions made based on a single MOE can lead to the termination of an otherwise promising effort. In principle, MOPs measure the successful completion of a well-defined task or progress within a well-structured process, while MOEs measure the achievement of an end state or outcome. One source of possible confusion is at the boundary between MOPs and MOEs; when are measures about performance, and when are they about effectiveness?

Measures of Performance

All the tasks that are completed as inputs to an activity are clearly MOPs. For example, the following are clear and typical MOPs for a MISO product:

- Time required for planning.
- Whether or not the planning and approval process for the product was completed.
- Whether the product went to production and was recorded or printed.
- Number of printed copies (if print material) produced.
- Number of copies delivered (mailed, posted, dropped etc.).
- Number of broadcasts that took place and over what proportion of the targeted area.
- Frequency of broadcast or other delivery.

Where it starts to become less clear whether a measure is an MOP or MOE, is at the transition between the actions Marines will take to perform the activity and the events that happen with the target audience. For example, receipt of message or measurements of exposure (e.g., how many people heard the broadcast, saw a digital advertisement, or were near a drop of leaflets) and measurements (estimates) of reach are probably still MOP. However, what about measures of audience awareness of the message? One might make a distinction between hearing a message and listening to the message; both are key steps in the process, but attentive listening, and then actually gaining knowledge of what is trying to be conveyed, begins to spill over into the intended effects rather than the performance.

Measures of Effectiveness

At the end of the logic chain, the "real" MOEs are likely more clear: actual changes in target audience behavior, actual effects on relevant actors, and actual accomplishment of specified objectives. But the incremental estimates and measures of how many people received (heard and listened to or read, and maybe started to think about) a message is a critical step in the process; it does not matter if that is labeled as an MOP or an early MOE, provided it is not the only MOE. It is well known that MOEs can lead to confusion or dysfunction if they do not include measures that get past the superficial and loop back to the core objective. This is another place where a clear theory of change can help if it notes all the steps necessary to achieve an objective.

For example, if a significant fraction of a target audience is shown to change their behavior based on receipt of a MISO product (a good MOE), does that mean that the overall objective has been achieved? What if there is an incorrect assumption that changing the behavior of the target audience will complete some objective? Consider a historical battle damage assessment example. In World War II, the Allies conducted a massive bombing raid over Schweinfurt, Germany to destroy the production of ball bearings. While the Allies demonstrated great effect (i.e., MOE) against the target of that raid, post-war surveys (a different MOE) concluded that ball bearing production and distribution was not significantly disrupted by a single raid but would have been if raids had been repeated over time.

In another example, this one of counterterrorism context: if a high-value target is neutralized that is a successful MOE, but it does not capture whether the actual performance of the enemy network is degraded (a second and arguably more important MOE). Marines should seek measures across the range of tasks that need to happen to complete an activity (MOP), and across the range of effects desired from the activities (i.e., MOE) to include immediate outputs, the near-term outcomes, and the wider-ranging impacts and actual progress contributed to objectives.

The development of measures can be thought of in the following two parts:

- Deciding what constructs, elements, or steps are essential to measure.
- Operationally defining the measures.

Each part is discussed in the following sections.

Choosing What to Try to Measure

The importance of measuring something, or the information value of a measure, is a function of uncertainty about its value and the costs of being wrong. When identifying constructs worth measuring, give priority to "loadbearing" and vulnerable cause-and-effect relationships in the chain of logic. These can be identified by drawing on scientific theory, empirical research, expert elicitation, or rigorous evaluations of similar programs implemented in the past. Marines should not discount the value of past assessments as possible future templates.

If there is well laid-out logic of the effort, assessors should seek at least one measure at each node or step in the chain of logic. Table 5-2 shows twelve steps in a chain of logic for message-based influence, beginning with a target audience member's exposure to the message and walking through all the steps necessary for that audience member to adopt and sustain the desired behavior. The rightmost column shows the cumulative probability of success under an assumption of a 75 percent probability that any given individual successfully moves from one step in the process to the next.

Even under this optimistic assumption about conversion rate, a single individual in an area where they had a 50 percent chance of being exposed to the message, has about a 2 percent chance of transiting through all steps and adopting an enduring behavior change. This is why it is important to broadcast messages repeatedly, in multiple media, and to as many members of the target audience as possible. This is also why it is important to measure each step in the chain of logic, as if any steps have very low or zero conversation rates the cumulative probability of success is going to quickly plunge close to zero, and without some improvement in the effort, it is likely to fail to meet its goals.

Table 5-2. Constructs to Measure from McGuire's Hierarchy of Effects Model

Category	Construct to Measure	Notional Cumulative Success Rate (75%)
Exposure	1. Exposed to a message.	50%
	2. Recalls the message.	38%
Knowledge	3. Comprehends the message.	28%
	4. Knows how to change behavior.	21%
Attitudes and Behavioral Intention	5. Likes the message.	16%
	6. Considers the message important (saliency).	12%
	7. Recognizes the positive impact of behavior.	9%
	8. Believes they can change behavior (self-efficacy).	7%
	9. Intends to practice behavior.	5%
Behavior	10. Begins to practice behavior.	4%
	11. Experiences benefits of behavioral change	3%
	12. Sustains behavior/proselytizes to others.	2%

Developing Measures

Sometimes, constructs that represent a step in a chain of logic are easy to tie to a specific measure. For instance, anything that includes a numerical count of instances, such as number of broadcasts, number of products produced, number of products disseminated, etc., should connect to something that can be measured. Other times, steps in a chain of logic make sense, but are hard to directly observe or count. It may be possible to identify a target measurement but collecting that measure may be impractical. Consider, for example, step 9 in Table 5-2, in which the target intends to practice the behavior. Behavioral intent can be measured by asking the target about their plans in a survey or interview; however, in many kinds of operations initiating that kind of engagement with the target audience may not be possible.

Instead, sometimes assessors need to develop indicators for the element they wish to measure. Or, sometimes no direct or indirect measurement of a step is possible, and it becomes necessary to measure something related to the next step in the chain of logic and then infer that for that step to be measured as successful, both it and the prior step must have been successful. So, for example, again returning to Table 5-2, if one measures members of the target audience beginning to practice the behavior (step 10) perhaps through surveillance or some other form of observation, that is an indicator that all audience members who engage in step 10 activities must have also completed step 9 (the intent to practice the behavior).

Measure What is Possible to Observe. Assessors should tie each element of their logic model, particularly the outcomes and objectives, to several specific measures. The more important to the overall process the element is, the more measures or indicators should be sought. "Important" of course means the outcome or desired effect, but it should also include any steps in the chain of logic that involve an untested assertion or hypothesis. If the assertion or hypothesis is uncertain, can it be tested, and shown to be valid or invalid with data? How might it be observed and measured? Additionally, some measures will have insufficient or unreliable data and need as much support as possible. If it looks like it cannot be measured, the objective is likely incorrectly specified.

Develop a Measures Repository. Marines conducting assessments should keep a record of validated and potential measures and indicators related to their programs and capabilities. Ideally, there would be a central repository of successful and unsuccessful information-related metrics. Until such a repository is established, practitioners should keep records on where measures have been used before, how well they worked, and the evidence that supports them. It also might be useful to keep records of invalid measures and indicators to avoid using them again.

Manage Measures. Marines should avoid "metric bloat," meaning, too many measures per objective can complicate analysis and the interpretation of results. If the number of measures is becoming unmanageable, discard the lower-performing ones. Assessment is an iterative process; therefore, assessment planners should always be on the lookout for underperforming or un-needed metrics to cut. When assessment is working as expected, some measures may seem like a waste of effort. Certain measures will only be useful when things are not going well, but they may be essential to diagnosing and correcting a problem. Assessment is at its best when it allows the commander to adjust an effort that is not working as well as expected and get it working. As a rule, discard metrics that are not measuring what they are intended to, keep measuring things that have the potential to identify problems if an effort begins to struggle.

Measure for Indications of Success and Failure. Marines should avoid the temptation to collect data only on indicators of success. Measures or indicators should be defined or scaled to capture failure or regression as well as success. The measurement system should also be flexible enough to capture unintended consequences. When things are going well, it may be tempting to only measure outcomes, but assessment is at its best when things are not going well. Measuring intermediate nodes in a theory of change can help determine why things are failing.

Avoiding Negative Incentives and Measures that are Easily Manipulated. Designing measures should avoid negative incentives. A negative incentive is an incentive (usually an unintended one) that rewards an undesirable result. Measures of exposure are particularly susceptible to negative incentives. For example, a Department of State (DOS) Inspector General's report accused the

Bureau of International Information Programs of “buying likes” on Facebook to improve the perceived reach of one of their programs. Such a strategy may increase awareness, but it will not tell practitioners anything about a program’s impact. Marines should also avoid measures that are easily manipulated. Past examples of manipulated or “captured” metrics in previous operations have included exaggerated reports of the operational readiness of host-nation forces or of enemy casualties and reduced reporting of civilian casualties.

Develop Varied Measures. Different capabilities require different measures. If the chain of logic that connects activities is different for two different capabilities, then the constructs that need to be measured and the actual measures developed are also going to differ. For example, the chain of logic that connects an electromagnetic warfare effort to jam enemy communications and herd them to a specific alternative mode requires both technical measures about the frequencies jammed and the match of the jamming footprint to the desired area of affect. It also requires measures of the behavior of enemy communications operators in terms of their observable response to the jamming, whether they end up communicating in the modes intended by the herding, and how long it takes them to get there. In contrast, measuring the influence of a campaign seeking to promote acceptance of Marine forward basing in a partner nation will need to measure different things, will focus on a much wider time horizon, and will need to measure a much broader swath of the population. In the same vein, identifying measures for some capabilities will just be easier. For example, if the data and access available are sufficient to conduct targeting in the offensive cyberspace realm, the data are likely sufficient to assess the impact of operations.

Employ Quantitative and Qualitative Measures. Measures can be either qualitative or quantitative. Quantitative measures are preferred because they are typically less subjective. However, Marines should not assume that a numerical measure is better if it just quantifies something subjective. While some measures are potentially quantitative, sometimes a binary version (yes/no) based on a rough threshold is sufficient. For example, if Marines wish to keep the population in an area pacified, they may wish to know how many individuals participated in a demonstration (number of people). However, the real measures of interest may be less about the actual numbers and more about a threshold.

For example: Was the demonstration large enough to block traffic in the square (Y/N)? Was the level of participation in the demonstration noticeably larger than participation in the prior demonstration (Y/N)? While both measures could be inferred from tracking actual participation counts, getting such counts may be difficult from a data-collection perspective (discussed later in this chapter) and the raw counts are likely to be less useful than the binary threshold measures. Some of the best MOEs capture changes in an observable behavior over time. Measuring change over time enables a trend chart, which can be a useful form of assessment.

Identifying constructs and matching and designing measures is as much art as it is science. Experience, even the experiences of others, can provide useful insights for this challenging process. Table 5-3 provides a checklist of desired attributes for MOPs and MOEs from the North Atlantic Treaty Organization (NATO) assessment handbook.

Table 5-3. Necessary and Desired Attributes of MOPs and MOE

Necessary and Desired Attributes of MOPs and MOEs (NATO Assessment Handbook)
MOPs Must…
MOPs only: Align to one or more own-force actions
Describe the system element or relationship of interest that must be observed
Be observable in a manner that produces consistent data over time
Describe as specifically as possible how the action is to be executed (MOP) or how the element is expected to change (MOE)
Be sensitive to change in a period of time meaningful to the operation
Have an associated acceptable condition
MOPs only: Have a known deterministic relationship to the action
MOEs only: Be culturally and locally relevant
Measures Should…
Be reducible to a quantity (as a number, percentage, etc.)
Be objective
Be defined in sufficient detail that assessments are produced consistently over time
Have an associated rate of change
MOEs only: Have appropriate threshold(s) of success and failure

Obtaining Measurement Data. Once planners have preliminarily identified desired MOP and MOE, they should consider how to collect measurement data and observations. These two steps of necessity, should be considered in a cyclic process. Assessment planners should—

- Identify what they want to measure.
- Consider how those measures might be collected (recognizing that collection of some will be impossible, impractical, or too costly).
- Revise measures based on what is available or feasible to collect.
- Verify that what can be collected still meets measurement goals.
- Determine new measures or indicators that will support goals.
- Determine if those new measures can be collected.

Measurement data can come from a range of sources such as the intelligence enterprise (particularly through the collection plan), Marines executing information activities (or other Marines operating in the area), other Services, Allies or partners, other government agencies, NGOs, or contractors. Specific types of measurement data might include the following:

- Human intelligence.
- SIGNINT.
- Other intelligence reports and products.
- Open-source information.
- Observations from MISO civil affairs teams.
- Maneuver unit observations.
- Direct contact with the public.
- Press inquiries or commentary.

- DOS polling, reports, or surveys.
- Contracted or commercial polls or surveys.
- Observations from NGOs or private organizations.

Marines attempting to obtain data or information from outside their unit must ask permission. This may be in the form of requests for information through intelligence channels, or liaison of other government agencies, engagement with NGOs, or hiring (or leveraging) contractors. It is always better to ask early rather than late: some entities will have a process to answer requests that may take time (and approval), and for any observer, it is much easier for them to collect information if they know ahead of time to monitor and track events rather than trying to reconstruct what they observed after the fact.

Needs for external measurement (i.e., measurement or data collection from elements other than the executing capability) should be identified in ITCC stage 1 (objectives, guidance, and information effects) or stage 3 (information capabilities analysis), and can become requests for information, commander's critical information requirements, PIRs, or friendly force information requirements, as appropriate. For external measurement from non-intelligence source or forces, different request processes may be necessary, and it will be incumbent on information planners to figure out who is going to collect or measure, how, and how they can be asked or tasked.

Sample Metrics for Performance and Effectiveness of Various Information Capabilities

A useful archive of successful and unsuccessful metrics for activities of the Marine Corps information warfighting function is not currently available. This section contains example measures drawn from training materials and assessment studies. Marines are encouraged to develop their own measures that match their operational environment and mission. For example, consider a JTF operation, in which Marines participate. Sample objectives that might be supported by the Marine Corps information warfighting function include:

- Disrupting enemy ground force commander's synchronization of Marine Corps and Army-level operations.
- Influencing local civilian leaders and population groups to not interfere with JTF forces and operations.

To assess the effectiveness of JTF efforts to achieve these objectives, one might seek to measure the following MOEs (phrased as objectives, but SMART):

- Ninety percent or more of enemy early warning sites and air defense sector control centers suppressed.
- No JTF air assets are effectively engaged by radar-guided surface-to-air missiles.
- No JTF high-value assets are attacked by surface-to-surface fires, air strikes, or special purpose forces' direct action.

- Enemy first- and second-echelon ground forces are unable to synchronize fires and maneuver above division level.
- Enemy strategic reserve forces are not committed against the JTF's main ground attack before penetrating the second operational echelon.
- No JTF main supply routes are blocked by the civilian populace.
- No instances of local leaders inciting the populace to interfere with JTF operations.

Tables 5-4 through 5-10 provide samples of some different possible metrics (mostly MOPs, but some MOEs) across a range of different information capabilities.

Table 5-4. Sample Cyberspace Defense Metrics.

Percent of Systems Compliant	The percent of systems that are compliant with specified security requirements.
Vulnerabilities per Node	The number of known vulnerabilities that have not been patched.
Probability of Detection	The probability that network security measures will identify an adversary cyberspace attack or intrusion.
Time to Detect	The time required before an enemy or adversary attack or intrusion is identified.
Time to Recover	The time required to restore compromised systems or network after an enemy or adversary cyberspace attack or intrusion.
Message Completion Rate	The percent of data that reaches the intended destination.
Message Latency	The time it takes for data to get from its source to the intended destination.
Mission Delay	The time delay (e.g., hours, days) in executing a mission due to an enemy or adversary cyberspace attack.

Table 5-5. Sample Offensive Cyberspace Metrics.

Covertness	The ability of an asset to evade detection.
Attribution	The likelihood an enemy or adversary can attribute the asset to the developer or author.
Forensic Discovery	The number of artifacts left behind by an asset that could be discovered by a security audit.
Target Recoverability	The ability of a target to recover from intended or unintended environmental changes.
Co-optability	The ability of an enemy or adversary to co-opt an asset for their own means.
Intelligence Gain and Loss	The degree to which intelligence collection increases or improves relative to sources now being closed off due to employing an asset.
Capability Gain and Loss	The extent to which a capability cannot be used again after employment.
Exposure of Friendly Vulnerabilities	The degree to which the employment of an asset allows the enemy or adversary to identify friendly force vulnerabilities.

Table 5-6. Sample Electromagnetic Warfare Metrics.

Received Power	The power of the transmitted signal at the receiving target.
Beamwidth	The aperture angle from where most of an antenna’s power is radiated.
Effective Isotropic Radiated Power	Measure (in decibels) of power emanating from an antenna when compared to a theoretical omni directional antenna. Equivalent isotropic radiated power measures antenna gain.
Bandwidth	The actual operational frequency range of a receiver when it is tuned to a certain frequency.
Effectiveness Range	The distance an antenna’s signal is transmitted, predicated on jammer to signal noise ratio, or Joint Staff. Joint Staff is a ratio that assists the EMSO planner determine the effectiveness range of intended effects.
Target Fidelity	The degree to which a target is susceptible to electromagnetic attack.
Power Spectral Density	The power of a transmitted signal as a function of frequency, per unit frequency.
Preventing or reducing an enemy’s or adversary’s effective use of EMS	The number of EMS jammers available for use by the US or multinational forces.
	The percentage of EMS jammed and for what durations by the US or multinational forces.
	The number of enemy or adversary EMS reliant capabilities destroyed, degraded, or disrupted.
Projection to the enemy or adversary the appearance of objects that do not exist or appear to be something else	The number of enemy or adversary systems targeted.
	Difference in projected objects and real objects.
	The number of false objects created and projected to enemy or adversary systems

Table 5-7. Sample Influence or Deceive Metrics.

Sample Influence or Deceive Output or Performance Metrics	
Production	The time it takes to make a product and the extent to which products are made to specification
Distribution	The type and numbers of products and messages produced.
Dissemination	The volume, means, and schedule (timing and frequency) of products released.
Sample Influence or Deceive Penetration or Receipt Metrics	
Target Audience or Adversary Decision-maker Reception	The extent to which the product reached the target audience (influence) or enemy or adversary decision-maker (deception).
Credibility	How believable or reasonable the message content is to the target audience or enemy or adversary decision-maker, and how credible the messenger or means of dissemination is.
Sample Influence or Deceive Penetration Effects Metrics	
Awareness	The extent to which the target audience or enemy or adversary decision-maker understands the intended behavior.
Knowledge	The extent to which the target audience or enemy or adversary decision-maker knows how to perform the intended behavior.
Attitudes	The extent to which the message or product resonates with the target audience or enemy or adversary decision-maker.
Intentions	The extent to which the target audience or enemy or adversary decision-maker wants or plans to perform the intended behavior.
Behavior	The extent to which the target audience or enemy or adversary decision-maker performs the intended behavior.

Table 5-8. Sample Inform Metrics

Sample Inform Performance Metrics	
Product Development	The total type and number of visual information products produced in support of a given command objective (public affairs, MISO, intelligence, space support element, etc.).
Transmission	The time it takes to transmit visual information from the acquisition source to the receiving entity (release authority, intelligence, etc.).
Dissemination and Distribution	The total type and number of written and visual information products publicly released, and the way they were released (accessioning to official web sites, posts on social media, etc.).
	The total number of visual information products directly distributed to media.
	The total number of visual information products downloaded from official sites by external media.
Sample Inform Effectiveness Indicators	
Knowledge	Number of released written or visual information products repurposed and used by the media segmented by type, size or reach, and location of media outlet.
	Number or interactions with social media posts (comments, shares, likes, etc.)
	The extent to which desired messages are included in media reporting (official quotes, message paraphrasing, etc.).
	The extent to which an audience or key public responds to a message or communication activity.
	The total number of media engagements conducted segmented by type, size or reach, and location of media outlet.
Attitude	How a key public responds to a message or communication activity, and the extent to which that public indicates their perception. The sentiment, by which media reports on military actions.
	Public opinion polls of attitudes toward military actions.
Behavior	The extent to which a key public or stakeholder speaks positively about military actions and operations or the military in general.
	The extent to which a key public or stakeholder acts in support of military actions and operations or the military in general.

Table 5-9. Sample Command and Control Metrics

Time Required for Planning	The time required to execute the operational planning process.
Time to Develop Course of Action	The time required to develop one or more options for how the mission and commander's intent might be accomplished.
Speed of Decision	The time required to decide in an operation (observe, orient, decide, act).
Operational Tempo	The maximum frequency with which operations are performed.
Agility	The ability of an organization to sense and respond quickly to advancement opportunities to stay ahead and competitive on a battlespace.
Clarity of Command	The degree to which an order is understood without ambiguity.
Risk Identification	The extent to which operational risks are identified and mitigated.

Table 5-10. Sample Targeting Metrics

Probability of Target Engagement	Probability that the weapon or asset can be employed against a target.
Number of Targets Held at Risk	Number of targets a weapon or asset can engage.
Time to Engage Targets	Time it takes to engage a target after target identification.
Lethality and Probability of Successful Deployment	Probability that employing the weapon or asset will result in the intended effect on the target.
Persistence and Time Out of Action	Time it takes the target to operate at restored capacity after intended effect is achieved.
Collateral Damage	The unintended degradation or destruction of friendly or neutral capabilities.

APPENDIX A. INFORMATION ENVIRONMENT CHARACTERIZATION AND PLANNING TEMPLATES

This appendix is divided into two parts. The first offers insights on how to characterize and analyze the information environment and the second provides overviews and examples of sample products for information planning addressed earlier in this publication, principally in Chapter 3. Products include but are not limited to the following:

- Combined information overlay (see the Joint Guide for Joint Intelligence Preparation of the Operational Environment).
- Concept of information, established in MCWP 8-10.
- Annex I (Information), from MCWP 5-10.
- Information directives, established in MCWP 8-10.
- Relevant actor (other than target) engagement list, established in MCWP 8-10.
- List of available information capabilities and authorities, established in MCWP 8-10.
- ITCO, established in MCWP 8-10.

KEY TERMS AND THEMES

Joint doctrine defines the operational environment "the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities that bear on the decisions of the commander" (JP 3-0*, Joint Campaigns and Operations*). The operational environment includes land, maritime, air, space, and cyberspace domains; the information environment; and electromagnetic operational environment. The Marine Corps uses a similar definition but prefers the term battlespace, which it defines as "the environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, and/or accomplish the mission. It includes the air, land, maritime, and space domains; the information environment and cyberspace domain; the electromagnetic spectrum; and other factors to include friendly, enemy, adversary, and neutral entities contained within or having an effect on the operational areas, areas of interest, and areas of influence" (*Marine Corps Supplement to the DoD Dictionary of Military and Associated Terms,* hereafter referred to as the *USMC Dictionary*). Understanding these definitions is helpful for understanding the framing and expectation of commanders for Marines seeking to generate and exploit information advantages through the planning and execution of information activities.

The information environment is a complex and pervasive element of everyday life. The behaviors of political leaders, populations, computers or machines, or opposing military organizations can be understood by the way they process information. The Marine Corps uses the term information environment to refer to the global competitive space spanning the domains. It includes information itself and all relevant social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information—including the individuals, organizations, and systems that collect, process, disseminate, or use information (JP 3-04). The information environment is an always live and often contested space where military advantages can be gained or lost. It is essential that Marine Corps units and organizations understand and estimate relevant portions of the information environment as it pertains to their operations, activities, and the authorities required to perform specific information activities. Achieving this requires planners to characterize and categorize threats, vulnerabilities, and opportunities in all relevant domains and the EMS.

This includes characterizing the totality of all relevant networks, actors, influences, and actions that are constantly evolving with the generation and dissemination of data, narratives, attitudes, values, and beliefs that affect commander's decision making. Compression of the levels of warfare and the blurring of battlespace boundaries, combined with complex rules of engagement, necessitates the identification of current conditions and desired future states. Understanding the information environment requires critical and systematic thinking, pattern recognition, anomaly detection, and must be nested within the unit's whole-of-staff IPB process. This appendix addresses the above by providing fundamental considerations and planning templates used to characterize the information environment, and to support the planning process.

INFORMATION AND INTELLIGENCE

Intelligence staff and personnel have primary responsibility for maintaining a body of knowledge from which decision makers can draw to better understand the enemy and the environment. However, the intelligence enterprise represents a set of finite resources that must be allocated and prioritized and cannot possibly cover all potentially relevant aspects of the operational environment. Collaboration, cooperation, and mutual support between the intelligence enterprise and other information capabilities and specialties are essential to building a comprehensive and relevant understanding of emergent conditions in the information environment. Intelligence information must be combined with all other available and relevant forms of information to build the commander's situational awareness.

The collaboration and synchronization of information and intelligence capabilities and activities provides mutually supporting personnel and practices that are necessary for sufficiently characterizing the information environment. For example, Marines employ complementary analytic processes and models, such as PMESII [political, military, economic, social, information, and infrastructure] and ASCOPE [areas, structures, capabilities, organizations, people, events], cyberspace network characterization, or electromagnetic survey and signal identification to characterize components of the information environment. Further, planners and analysts trained in the use of information capabilities and technologies contribute their specific expertise to support the IPB process to—

- Understand how information moves in and through the operational environment. This includes identifying how information is received, processed, and employed, by whom or what, and for what purposes.
- Establish a baseline of the information environment to create a reference point of relevant actor perceptions, beliefs, attitudes, and behavior, while assessing changes to the baseline over time.

- Distinguish what information in the information environment is relevant and characterize its sources and methods of movement or transmission.
- Identify misinformation, disinformation, and credible information from noncredible sources.
- Understand the information networks and systems being used by relevant actors.
- Identify which activities are observable and by whom. This includes understanding the inherent information aspects of those activities that are most likely to be used by relevant actors to derive meaning.
- Produce a running estimate of relevant factors and features within the information environment.

ASPECTS OF THE INFORMATION ENVIRONMENT

According to JP 3-04, there are three distinct aspects of the information environment that must be characterized and understood by commander: informational, physical, and the human aspects of the information environment. Understanding these aspects requires fusing formal intelligence analysis with all other forms of data collection and analysis that stem from non-intelligence functional areas and disciplines (COMMSTRAT, spectrum management planning, civil information management, etc.). All aspects of the operational environment overlap and interact with each other.

Informational Aspects

Informational aspects reflect the way that individuals, information systems, and groups communicate and exchange information. Informational aspects are the sensory inputs (e.g., content, medium, format, and context) of activities that a receiver interprets and uses to assign meaning. The content of communication can be verbal and nonverbal. If nonverbal cues do not align with the verbal message, ambiguity is introduced, and uncertainty is increased. Medium refers to the system used to communicate (e.g., radio, television, print, Internet, telephone, fax, and billboard). The details of the medium can be described in as little or much detail as necessary. Format is how the information is encoded, such as what language is used, style of delivery (e.g., poetry, songs, imagery), tone, and volume. Context refers to the environment, in which the communication happens (e.g., face-to-face, over the phone). Format and context can affect the content of a communication. For example, a text message may contain different content than the same communication delivered face-to-face. Actions are a form of nonverbal communication that have inherent informational aspects and are generally more impactful.

Physical Aspects

Physical aspects are the material characteristics, both natural and manufactured, of the environment that may inhibit or enhance communication. Physical aspects may create constraints and freedoms on the people and information systems that operate in it. Physical aspects are critical elements of group identity and impact how groups form, behave, or might be disrupted or cease to exist. For example, groups may be formed by the people inhabiting an island or an isolated jungle habitat. Similarly, a community might be disrupted by the building of a highway that divides a neighborhood and causes the creation of new, separate, and distinct communities. How information is exchanged is where the interplay between the informational and physical aspects is most apparent. As an example of this interplay, an isolated community without access to modern communications technology will likely have a stronger group identity and be more likely to communicate face-to-face compared to residents of a large modern city.

Human Aspects

Human aspects are the interactions among and between people and the environment that shape human behavior and decision making. Those interactions are based upon the linguistic, social, cultural, psychological, and physical elements. Human aspects influence how people perceive, process, and act upon information by impacting how the human mind applies meaning to the information it has received. Individuals have distinct patterns of analyzing a situation, exercising judgment, and applying reasoning skills impacted by their beliefs and perceptions. Character and tradition are aspects that suggest how humans perceive a situation and how they might behave under particular circumstances in the future. For example, individual and group identity is often closely related to a geographical area, which can impact how individuals and groups in that region relate to one another and communicate along with the forms that communication may take. Describing these inextricably linked aspects will provide insight into relevant actors' worldviews that frame the perceptions, attitudes, and other elements that drive behaviors.

For more information on each of the above aspects, refer to JP 3-04.

Characterizing Information Networks

As planners identify and analyze aspects of the information environment, there is a need to develop models that depict how friendly, enemy, adversary, and neutral forces observe, orient, decide, and act on information. Analyses and depictions of information networks enable the staff to plan activities to exploit opportunities and protect vulnerabilities. Information networks analyses can be used by the information staff to support the MCPP and focus the information staff's use of other information environment characterization techniques. Conduit analysis, network engagement, and information environment advanced analysis (IEAA) are three examples of analytical frameworks that can be used to characterize the information environment in support of planning.

Conduit Analysis

As the three information-related aspects of the operational environment are characterized, certain networks may emerge that require rapid analysis to determine their suitability for exploitation or influence. These networks and their information pathways can be simple or complex. During problem framing, conduit analysis diagrams are conceptual and primarily serve to map information networks to aid the planner's visualization of information flows within the relevant portions of the information environment. During COA development, these diagrams are expanded and validated to ensure that planners can generate effects against the appropriate decision maker. Conduits are pathways to a decision maker and can be constructed to model enemy or adversary decision-making. Identifying the conduits that connect the physical aspects of the information environment and a decision maker is central to understanding how to create or exploit information advantages by applying means and methods to affect systems or behavior. Conduit analysis is captured in the combined information overlay.

The primary components of a conduit are the sensor, links, node, filter, and decision maker. Upon the detection of an indicator, the sensor reports information to a node. Ideally this is a closed-system and is developed systematically.

Sensors are any object or entity capable of gathering, obtaining, or collecting information when signatures and indicators are observed. These can be extremely complex and calibrated technical systems (e.g., IADS radar) or rudimentary methods (e.g., fisherman with binoculars). Examples of sensors are intelligence collection platforms, and individuals capable of relaying information to a decision maker.

Links are the pathway, in which data flows from a sensor to a node. This is akin to the information aspect mentioned above. Links are activated when a sensor translates and transmits the report through means such as keying a handset, transmitting on a cell phone, or an automated report from a radar to a fusion center which relays data to their assigned node.

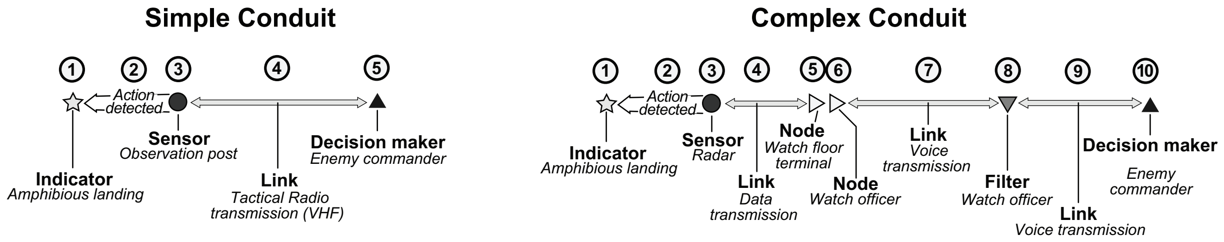
Nodes are "an element of a system or network that represents a person, place, or physical thing" (Marine Corps Tactical Publication [MCTP] 3-02A, *Network Engagement: Targeting and Engaging Networks*). Nodes receive information from a sensor or another node, transpose it for passing via a new link, and retransmit the information to additional nodes and filters or directly to the decision maker.

Filters are nodes within this line of communication that determine if the information being provided is legitimate, verifiable, consistent, and worthy of the attention of the decision maker. There are multiple reasons why a filter may choose not to pass along information such as a personal bias or a decentralized system that allows them to decide based on the observable. While most planners focus on disrupting links and degrading sensors, filters as a target for influence should not be overlooked.

Decision makers are the final authority in determining an action or inaction based on the situation presented. Every decision maker has their own bias, perceptions, beliefs, and attitudes that manifest, regardless of their commitment and adherence to doctrinally described processes.

Not every conduit will have filters and nodes. For example, a simple conduit might be an observation post reporting directly to the local area commander capable of deciding. If an observation post (sensor) observes an amphibious landing, they may make a single, very high frequency radio transmission (link) to the enemy commander (decision maker). See Figure A-1 for an example of such a conduit.

A complex conduit could be modeled as: a radar (sensor) detects a signature associated with a MEU afloat and provides a track sent via data (link) to the watch floor terminal (node). The individual operating the terminal on the watch floor (node) will call their watch officer (filter) or send it straight to the naval base commander (decision maker) based on previously determined reporting criteria.


Simple Conduit

Complex Conduit

Figure A-1. Conduit Example.

For more examples regarding the use of conduits, refer to JP 3-13.4, *Military Deception*.

Network Engagement

Network engagement uses existing human or functional networks to help shape the operational environment. Examples of human networks might include social, professional, religious, or fraternal networks. Examples of functional networks might include logistics, communications, financial, or criminal networks. Networks are two or more nodes connected via a link that shares a common purpose. Today's complex environments highlight the need for detailed understanding of the characteristics, components, behaviors, and relationship of friendly, neutral, and threat networks.

Network engagement expands the decide, detect, deliver and assess (also referred to as D3A) methodology, which has traditionally been threat focused, to consider the friendly and neutral networks. This methodology is used to systematically analyze and prioritize entities for possible engagement, match the appropriate capabilities to those entities to generate specific effects, and deliberately assess the effects created. The decide, detect, deliver and assess methodology helps the staff organize key engagement requirements. The planning products are inputs to the unit's engagement working group, which synchronizes the unit's engagement efforts across the relevant friendly and neutral networks.

For a comprehensive analysis of network engagement and supporting products, see MCTP 3-02A.

Information Environment Advanced Analysis

As a method to augment the COG analysis and ensure a holistic understanding of systems inside the information environment, Marines can employ IEAA as a technique. The IEAA is based on systems theory, utilizing a methodology of decomposing and analyzing the elements and links of a system to determine avenues for exploitation or effect. This methodology results in enhanced understanding and increased interactions among intelligence, planning, and operations personnel at both the strategic and tactical levels.

The six-step process of IEAA is:

1. Identify systems in the information environment for decomposition.
2. Decompose systems and sub-systems.
3. Determine elements of system.
4. Determine interconnections.
5. Define attributes of system elements.
6. Determine system function and purpose.

The links are the conduits through which communications and actions flow and are directly targetable to weaken or strengthen a system. An example of this relationship is depicted in Figure A-2.

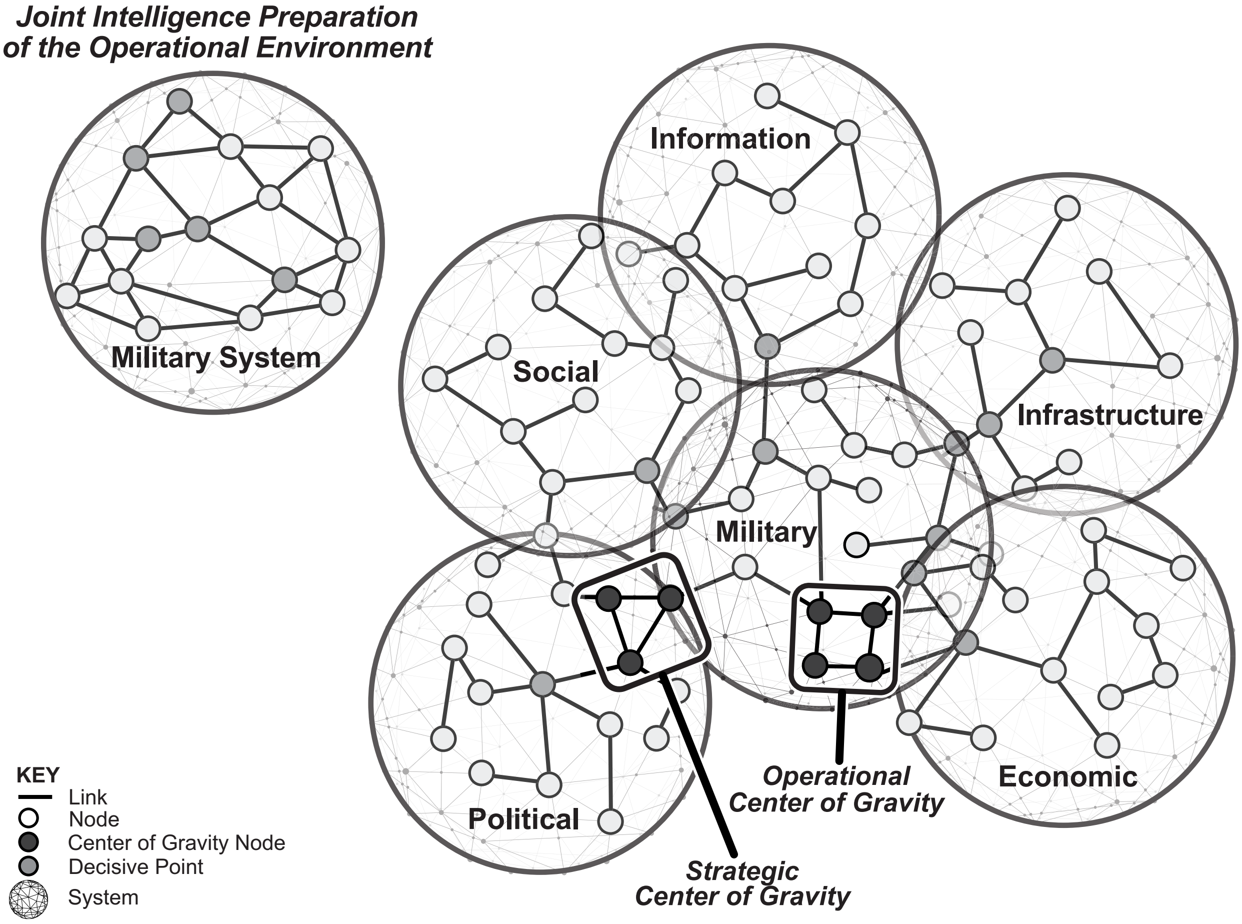


Figure A-2. Link Analysis Example.

This detailed look at a singular system amplifies the conceptual techniques utilized in the combined information overlay and conduit analysis, which allows planners to generate a functional approach to targeting and engagement.

PRODUCT DESCRIPTIONS, SAMPLE FORMATS, AND TEMPLATES

The previous section explored several approaches to characterizing, analyzing, and understanding the information environment. The following sections provide more detailed descriptions of the planning products discussed in Chapter 3 and templates for their presentation. Note that all templates presented here are notional examples and when employed should be tailored to fit the specific operational context and the preferences of the commander.

Combined Information Overlay

The combined information overlay is the result of analysis of the potential impact of the information environment on military operations. The joint guide on JPIOE provides a detailed description of the process and an example. Doctrinally, this is not currently part of Marine Corps' IPB, but that is not to say that it cannot be conducted at levels below a joint force command to graphically depict strengths and/or vulnerabilities in the information environment that might be turned into information advantages by Marine Corps, enemy or adversary forces. The combined information overlay might also depict various information advantages held by Marine Corps forces as well as enemy and adversary forces, or even a relative estimate of the extent and nature of comparative advantages held by each.

The combined information overlay is an input to planning, an effort to convey relevant aspects of the characterization of the information environment to support problem framing, COA development, and COA comparison and decision, as well as detailed capability planning. As such, there is not necessarily a final combined information overlay included in a final plan, instead it is likely to feed into the development of the concept of information. As a JPIOE or IPB product, the intelligence staff has the primary responsibility for the combined information overlay, but its completion and refinement will require input from and collaboration with the information planners, information forces, and possibly other staff elements.

For more on the combined information overlay, see the relevant discussion in the *Joint Guide for Joint Intelligence Preparation of the Operational Environment*.

Concept of Information

Information activities support the overall operational approach. As such, a concept of information in an OPLAN or OPORD is used to illustrate the informational aspects of the CONOPS, akin to a concept of maneuver, fires, or support. Much like a CONOPS, a concept of information is a written statement and graphic that clearly and concisely express what the commander intends to accomplish and how it will be done using available resources.

Depending on the nature of the planning, information planners in an operational planning team or the collective IWG develop a preliminary concept of information during problem framing, and then refine it during COA development. The concept of information may be further refined during COA wargaming and may then be included in the OPLAN or OPORD as part of Annex I during orders development. The concept of information also serves as a central input to the ITCC and the development of the ITCO.

Figure A-3 provides a sample summary graphic for a mature concept of information. A concept of information that is earlier in its life cycle might be summarized with a more notional graphic, or in a short summary statement. To capture the contribution of information, elements of the concept of information narrative and graphic summary should appear in each proposed COA during MCPP step 2. Upon COA approval, the selected COA graphic and narrative should also include key elements of the concept of information as it moves through MCPP steps 5 and 6.

Date/Time/ATO Day

Concept of Information

- **Mission Statement**
- **Objective(s)**
- **Commanders Intent**

Operational Lines of Efforts (LOE)

1. LOE 1 title and objective alignment.
2. LOE 2 title and objective alignment.
3. LOE 3 title and objective alignment.

Information Tasks

1. Unit "A" task title, description, and LOE alignment.
2. Unit "B" task title, description, and LOE alignment.
3. Unit "C" task title, description, and LOE alignment.

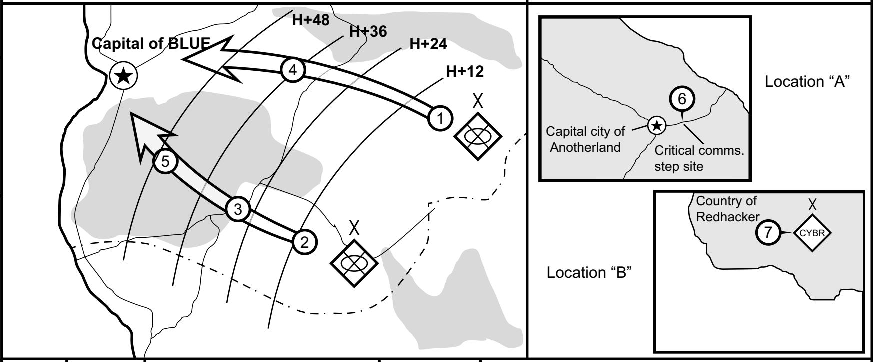
Narrative Statement

Written description of the information COA support as it support the overall mission, objective, and commander's intent. Provides a description of the desired future state.

LEGEND

ENY	enemy	**RF**	radio frequency
LOE	line of effort	**Ops**	operations

Area of Operations Map | **External Areas**



Task #	Authority	Activity	Effect	
①	Source #	e.g., MISO Series	Dissuade ENY	H+6 – H+12
②	Source #	e.g., Electromagnetic Attack	Disrupt ENY	H+10 – H+36
③	Source #	e.g., RF-Delivered Cyberspace Attack	Degrade ENY	H+26 – H+28
④	Source #	e.g., MISO Series	Disrupt ENY	H+36 – H+48
⑤	Source #	e.g., COMMSTRAT	Inform locals	H+44 – H+60
⑥	Source #	e.g., Offensive Cyberspace Ops	Deny ENY	H+8 – H+14
⑦	Source #	e.g., Offensive Cyberspace Ops	Deceive ENY	H+6 – H+30

Figure A-3. Example of a Mature Concept of Information Summary Graphic.

Figure A-3 illustrates the key elements that belong in a depiction of a concept of information. On the left, the figure briefly summarizes the overall mission and CONOPS and how information activities align to and support the CONOPS, detailing general information tasks and providing a short narrative summary. The graphic also offers a map chip or area of operations graphic, noting key locations for information tasks or activities, or effects. The specific tasks are then listed below the map along with the executing capability, the needed authorities, the desired effect(s), and notes on the sequence and timing. If available and complete, this summary could be drawn from the ITCO (described in Chapter 3 and in greater detail below). Where a concept of information precedes the beginning of ITCC cycles producing an ITCO (e.g., as part of prior planning), the capabilities and sequencing connected to the tasks can be more provisional, drawing from staff estimates and initial understandings about available forces and capabilities. Such a provisional task list might then feed the ITCC in its first cycle. The elements described in this paragraph are all optional elements of a concept of information summary graphic, and if included can be positioned or repositioned as desired.

Information Directive

Copy no.___of___copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

APPENDIX 1 TO ANNEX I TO OPERATION ORDER OR PLAN (NUMBER) (Operation CODE WORD) (U)

INFORMATION DIRECTIVE (U)

(U) REFERENCES

(a) Relevant plans or orders
(b) Required maps and charts
(c) Other relevant documents

1. (U) Situation.
a. (U) General. See base order or plan.
b. (U) Enemy/Adversary. See base order or plan.
c. (U) Friendly. See base order or plan.
d. (U) Assumptions. List any assumptions of friendly, enemy, adversary, or third-party.

2. (U) Mission. See base order or plan.

3. (U) Execution.

a. (U) Commander's objectives.
(1) (U) Commander's key objectives
(2) (U) Information specific objectives linked to key objectives
b. (U) Commander's guidance.
(1) (U) Guidance for achieving information objectives
(2) (U) Limitations
(a) (U) Constraints
(b) (U) Restraints
c. (U) Commander's desired effects.
(1) (U) Link between information objectives and desired effects

Table A-1. Information Directive Effects Matrix.

	Generate	Preserve	Deny	Project
Effect 1	Unit (X), Action	Unit (X), Action	N/A	Unit (X), Action
Effect 2	Unit (X), Action	N/A	Unit (X), Action	N/A
Effect 3	N/A	Unit (X), Action	N/A	N/A
Effect 4	N/A	N/A	Unit (X), Action	N/A

d. (U) Coordinating Instructions. Address mutual support issues relating to information.

4. (U) Administration and Logistics. Address any information environment administrative or logistic requirements.

5. (U) Command and Control. List information environment command and control instructions.

ACKNOWLEDGE RECIEPT

Name
Rank and Service
Title

EXHIBITS:

1-
2-
3-

OFFICIAL:

S/Name
Rank and Service
Title

Relevant Actors (Other than Target List

Per DoD policy (Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 3370.01D, *Target Development Standards*), entities or objects not assessed as valid military targets are not placed on target lists. As such, MAGTFs develop and maintain a separate list of relevant actors that are selected for engagement but are not classified as targets. The format of this list should include the relevant actor name, location, desired effect(s), engagement capability, assessment metrics, etc. (See Figure A-4 below). Development of this list is a collaborative effort during the MCPP, and the list is further refined in the IWG and the target development working group. In coordination with the ICC, intelligence operations center, and MAGTF G-3, the FECC assumes responsibility for maintaining this list and ensures relevant actor engagements are integrated and synchronized with target engagements and other MAGTF operations.

#	Name	Location	Desired Effects	Engagement Capability	MOP	MOE

Figure A-4. Example Relevant Actor (Other than Target) List.

Information Tasking and Coordination (ITCO)

Copy no.___of___copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

APPENDIX 2 TO ANNEX I TO OPERATION ORDER OR PLAN (NUMBER) (Operation CODE WORD) (U)

INFORMATION TASKING AND COORDINATION ORDER (U)

(U) REFERENCES

(a) Relevant plans or orders
(b) Required maps and charts
(c) Other relevant documents

1. (U) Situation.

a. (U) General. See base order or plan.
b. (U) Enemy/Adversary. See base order or plan.
c. (U) Friendly. See base order or plan.
d.(U) Assumptions. List assumptions made of friendly, enemy, adversary, or third-party.

2. (U) Mission. See base order or plan.

3. (U) Execution.

a. (U) Concept of Information.
b. (U) Information Tasks. Provide specific tasks for information forces to conduct by capability and/or activity. Identify the commander's priorities for information activities.

1.(U) Task Number
2.(U) Task Reference (Information Directive Reference)
3.(U) Target or relevant actor number or reference
4.(U) Time of intended effect
5.(U) Location of intended effect
6.(U) Information capability category
7.(U) Unit of action name assigned the task
8.(U) Desired effect(s) description
9.(U) Authority reference associated with the task
10.(U) List other orders products this task also appears on (e.g., ATO ref #.)
11.(U) Assessment assets assigned

c. (U) Coordinating Instructions. Address mutual support issues relating to Information. This could include a synchronization matrix.

4. (U) Administration and Logistics. Address information environment administrative or logistic requirements.

5. (U) Command and Control. List information environment command and control instructions.

ACKNOWLEDGE RECIEPT

Name
Rank and Service
Title

EXHIBITS:

1-
2-
3-

OFFICIAL:

S/Name
Rank and Service
Title

APPENDIX B.
THE STATUS OF INFORMATION IN JOINT DOCTRINE AND THINKING

This appendix provides a brief overview of JP 3-04 and discusses points of similarity between current joint information concepts and the ideas and thinking embodied in MCDP 8 and MCWP 8-10, and briefly describes the status of information in the conceptual thinking of the other services.

INFORMATION IN JOINT OPERATIONS

Joint Publication 3-04 was published in September of 2022. This capstone doctrinal publication describes how the joint force is intended to approach information as a joint function. This is particularly relevant here, because the Marine Corps information warfighting function must nest within the broader joint approach to information.

Joint Publication 3-04 notes that the information joint function is the intellectual organization of the tasks required to use information during all operations. Joint Publication 1, Volume 1, Joint Warfighting, formally describes the function, noting "*The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant-actor perceptions, behavior, action or inaction, and support human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides [joint force commanders] the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of all military activities to achieve the commander's objectives and attain the end state.*"

Joint Publication 3-04 defines the information environment as "the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information." The Marine Corps' description presented in MCDP 8 and this MCWP align to this definition by including its essential elements.

Essential Elements of Joint Publication 3-04

Joint Publication 3-04 includes several points of emphasis for all members of the joint force. This includes the recognition, and the call to leverage, the inherent informational aspects of all military operations. "[A]ll activities have inherent informational aspects that impact the operational environment and can generate effects that may contribute to or hinder achieving commanders' objectives." (JP 3-04) Another point of emphasis is JP 3-04's focus on the use of information to influence behavior and the course of events. This invokes a broadening of the scope of those who might need to be influenced in pursuit of joint force objectives to "relevant actors," with relevance depending on the context and operation. This includes individuals, groups, populations, or automated systems whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action. Relevant actors include adversaries and competitors, but might also include noncombatants, civilians, and civilian infrastructure.

The information joint function includes three tasks that are applicable to all joint force components:

- Understand how information impacts the operational environment.
- Support human and automated decision making.
- Leverage information to affect behavior.

Each joint function tasks is supported by a range of subtasks. To "understand how information impacts the operational environment" task, subtasks include: analyzing informational, physical, and human aspects of the environment; identifying and describing relevant actors; determining likely behaviors of relevant actors. To "support decision making" task, subtasks include facilitating shared understanding across the joint force; protecting friendly information, information networks, and information systems; protecting joint force morale and will. To "leverage information" task, subtasks include informing domestic and international audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems. While sometimes described using slightly different language, these tasks and subtasks are predominantly consistent with the tasks and functions described in MCWP 8-10.

Aspects of the Joint Approach to Information are Consistent with Information in Marine Corps Operations

Much of the material in JP 3-04 and the description of information as a joint function is consistent with how the Marine Corps describes information as a Marine Corps warfighting function in MCDP 8 and in MCWP 8-10. For example, both joint doctrine and Marine Corps doctrine embrace the same definition and understanding of the information environment. Similarly, assessment and measurement are central in and essential to both information as a joint function and information as a Marine Corps warfighting function. Further, both JP 3-04 and MCWP 8-10 call for the use of a synchronization matrix that contains the phasing of the operation and enables planners to graphically display the activities, linked to the scheme of maneuver, that leverage information.

The joint force contributes to the informational instrument of national power by using information to impact the way, in which humans and systems behave or function, and it does so throughout the competition continuum to assure, deter, compel, and force relevant actor behaviors that support US interests. In keeping with this approach, the Marine Corps information warfighting function is a contributor to the informational instrument of national power, used in concert with other instruments to influence strategic outcomes, achieve policy goals, and impose the Nation's will.

Joint Publication 3-04 notes that, "Defeat of an enemy, by whatever mechanism, is usually a psychological outcome. The enemy is not really defeated until they believe they are defeated." It describes informational power as the ability to use information to support achievement of objectives and gain an information advantage, noting that the essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of objectives. This is consistent with the Marine Corps view of war as a contest of wills and resembles the same four functions emphasized in MCWP 8-10 and in MCDP 8.

Joint Publication 3-04 recognizes information as data in context to which receivers assign meaning; notes that humans use information to understand, make decisions, and communicate; and notes that information can affect the behavior of both humans and automated systems. MCWP 8-10 acknowledges information's use for similar purposes and includes both humans and automated systems when seeking systems overmatch and other forms of information advantages. As described in JP 3-04, narratives are an integral part of campaigns, operations, and missions. The joint force strives to provide a compelling narrative that is integrated into OPLANs and resonates with relevant actors by fitting their frame of reference. The Marine Corps also asserts the importance of narratives. Joint publication 3-04 provides details that Marines may find useful for the development of narratives in Appendix A.

Differences Between the Joint Approach and the Marine Corps Perspective

Marine Corps doctrine contributes to and supports related joint concepts and requirements, but there are some differences between how joint doctrine (i.e., JP 3-04) and Marine Corps doctrine (i.e., MCDP 8 and MCWP 8-10) approach information. Marines must be aware of and understand these differences, as Marines will participate in and contribute to joint operations.

The biggest difference is that JP 3-04 uses the term operations in the information environment, describing them as "military actions involving the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and protecting friendly information, information networks, and information systems." Joint usage separates the actions of information forces as OIE, and the information contribution of other forces as leveraging the inherent informational aspects of activities (separate from OIE). Joint usage considers both categories part of the information joint function. Marine Corps doctrine does not use this term nor make this distinction. In a joint context, Marines need to understand that the information activities of information forces may be referred to as OIE. Note that the purposes to which OIE are put in joint doctrine (informing or influencing relevant actors, attacking/exploiting relevant actor systems, and protecting friendly information and systems) correspond closely with the three main types of information advantages described in MCPW 8-10 and in MCDP 8 (i.e., prevailing narrative, systems overmatch, and force resiliency).

Considering information advantages, JP 3-04 describes information advantage as the operational advantage gained through the joint force's use of information for decision making and its ability to leverage information to create effects on the information environment. This is consistent with how information advantages are described in MCDP 8 and in MCWP 8-10, except that Marine doctrine explicitly allows for a wide range of simultaneous information advantages and disadvantages. For Marines, there are many possible information advantages. At the joint level, JP 3-04 sometimes refers to a singular state of information advantage and sometimes refers to a range of possible information advantages.

Another term distinct to JP 3-04 is the *information staff estimate*. “The information staff estimate is a continual evaluation of how factors related to the information environment impact the planning and execution of operations. The purpose of the information staff estimate is to inform the commander, staff, and subordinate commands on how information can be used to support mission accomplishment.” Many of the products and outputs described in this warfighting publication could feed into a joint information staff estimate, but Marine Corps processes do not themselves explicitly require such a product.

Marine Corps information planners will be well prepared to participate as information planners in a JFC staff. Planning at the joint level follows the joint planning process (see JP 5-0, *Joint Planning*), a process like the MCPP that is fundamentally grounded in operational design but has slightly different steps and processes. And, because of slight differences between the joint and Marine Corps approach to information, Marines in joint billets should familiarize themselves with and know the differences in JP 3-04, MCDP 8, and MCWP 8-10.

APPENDIX C.
VIGNETTES OF
INFORMATION IN MARINE CORPS OPERATIONS

This appendix presents the abstract concepts and processes described throughout this warfighting publication using vignettes. These vignettes not only illustrate the principles of MCDP 8 and the practices and processes promoted here, but are included to help Marines recognize how they contribute to the fight for, and with, information. Marines from across the FMF and supporting establishment should be able to identify with one or more of these examples.

VIGNETTE 1: OPERATION THUNDER HAMMER AND OPERATION MALEVOLENT WRENCH

Operation THUNDER HAMMER captures a snapshot of how Marines might have fought before information became a Marine Corps warfighting function. Operation MALEVOLENT WRENCH shows how Marines might approach the same mission while employing information as a Marine Corps warfighting function.

Operation THUNDER HAMMER

A US adversary's manipulation of the commodities market sparks an economic crisis inone of its neighboring countries. Much of the neighbor's population suffers in the downturn, but citizens in the western part of the country who share the adversary's ethnicity are particularly hard hit. Demonstrations in the region turn violent (possibly due to adversary provocateurs), and adversary propagandists paint the local security forces' dispersion of mobs as an atrocity. Under the pretext of defending their ethnic brethren from injustice and persecution, three brigades of adversary forces surge across the border in a land grab. Neighbor forces attempt to fight back but are unprepared and badly overmatched by adversary regulars. The neighbor appeals to the world for help, and the United Nations' condemnation of the invasion is swift. The United States is granted authority and designated as the multinational force lead by a United Nations Security Council resolution. Fearing ethnic cleansing and further entrenchment by the adversary, the US President launches a rapid countermove supported by responsive international allies.

As a part of Operation THUNDER HAMMER, the Commanding General, II MEF is designated as the JFC of the combined joint task force (CJTF) and ordered to dislodge and push back the adversary nation aggressors and restore the integrity of the border. Forces include 2d MEB, an available MEU, a carrier battle group, as well as a United Kingdom task force built around a Royal Marine commando battalion and a French task force built around a battalion from their 9th Light Armored Marine Brigade.

continued...

Operation THUNDER HAMMER (Continued)

The CJTF's commander and staff quickly refine their plans while they steam toward the area of operations. The COA that emerges from planning is to engage and fix all three adversary brigades simultaneously, with a heavy, high-tempo drive at the brigade in the center as the main effort, supported by air-inserted forces. This effort will leave an isolated brigade on either side. Penetrating CJTF forces would then turn into the flanks of their foes, hitting them hard, breaking them, and hounding them all the way to the border. The commander's end state includes the defeat of all adversary forces and their capture or withdrawal to beyond the borders.

As the operation begins, joint aviation quickly achieves air superiority, though not outright air dominance, as near the border a surprisingly sophisticated IADS remains a threat. Joint aviation, naval guns, and Marine and multinational artillery engage all three enemy brigades. Using forces previously concealed from the enemy and forces that appeared to be in reserve, the CJTF uses ship-to-shore movement and air mobility to place a substantial force to the rear of the center brigade. Before that brigade can reorient, it is pressed hard from both the front and the rear. A fourth brigade of enemy forces held in reserve on the other side of the border seeks to advance but joint aviation brings them under fire, fixing them and closing their main line of advance. Despite the success of the GCE, persistent enemy IADS continues to attrite MAGTF air assets, greatly reducing the JFC’s ability to project combat power via air assault or maintain persistent overhead ISR.

After two days of hard fighting, the surrounded enemy brigade disintegrates, having suffered heavy casualties, massive loss of equipment, and loss of command and control. Pressing the tempo and following the plan, the CJTF forces that destroyed the first brigade press the flanks of the remaining two. The brigade to the south recognizes its position as untenable and makes a fighting withdrawal toward the border under cover of IADS and artillery positioned inside enemy territory. The enemy brigade to the north finds itself partially enveloped with its line of retreat cut off. The tempo of the CJTF advance caught them by surprise, and they did not recognize their deteriorating position soon enough to change it. They fight hard in their defensive positions. As the pressure on this northern brigade mounts and they begin to disintegrate, remnant elements withdraw into the nearby regional capital. This leads to bloody urban fighting as Marine Corps forces root out the isolated holdouts, some of whom have escaped; these escapees will subsequently form the cadre for a separatist guerrilla movement, blending in with sympathetic local co-ethnics.

The CJTF prevails, having destroyed two enemy brigades and driven the third back across the border. However, the cost is high. The stiff fighting left multinational ground forces severely depleted and Joint air has been significantly attrited by IADS. Already economically depressed, the western region (around the capital) of the neighbor nation is now similarly war-torn after experiencing high numbers of civilian casualties and much collateral damage. The neighbor-nation government is grateful for the assistance provided by the multinational forces, but feelings are decidedly mixed among the populace. The adversary nation moves three fresh brigades to the border region, claiming a need to protect themselves against aggression from the neighbor and its “mercenary allies.” Intelligence suggests that the adversary intends to sustain economic pressure on the neighbor and pursue unconventional warfare options to promote discord and sap international will. They will bide their time until another opportunity arises to make a bid for annexation of the western region.

The fictitious vignette above (Operation THUNDER HAMMER) illustrates the traditional use of combined arms (fires and maneuver) as the principal means for defeating the enemy. The timeframe for the vignette could be any time since the mid-20th century. In the 21st century, the combined-arms concept remains fundamental and valid in warfighting. However, the characteristics of the global information environment and the widespread proliferation and use of information and communications technologies creates opportunity to apply combined arms in new and novel ways. To illustrate, the fictitious vignette below (Operation MALEVOLENT WRENCH) replays the first scenario but incorporates an expanded concept that includes the Marine Corps information warfighting function (fires and maneuver and information) to accomplish the mission.

Operation MALEVOLENT WRENCH

The CJTF's commander and staff work to update their understanding of the situation and revise plans while they steam toward the areas of operations. The commander believes the force is sufficient to destroy the three adversary brigades, but not without a heavy cost. Before asking the staff to develop and evaluate COAs, the commander carefully considers the desired end state and how it might relate to enduring strategic outcomes. First, the mission dictates the eviction of adversary forces, but does not necessarily require their destruction. Second, whether adversary forces are defeated and withdraw or just withdraw intact, the commander wants to mitigate the chance of future adversary aggression. Third, the commander wants to protect the reputation of the United States and the Marine Corps, and to preserve (to the extent possible) the combat power with which the commander has been entrusted. Fourth, the commander intends to preserve the support of neighboring nations and favorable global opinions. With this broader set of objectives in mind, the commander directs the staff to frame the problem broadly, and to gather information about the proclivities and motives of the adversary dictator and the adversary brigade commanders, as well as their intelligence and C2 processes.

The COA that ultimately emerges from the planning process emphasizes creating perceptions among adversary commanders that they are isolated and their positions are untenable, forcing them to withdraw. This will also demonstrate international resolve to the adversary dictator. The operation will unfold in a carefully planned sequence, first driving the commander of the northernmost adversary brigade to withdraw adversary forces, then pressing on the center brigade until it withdraws, and then threatening to cut off the southern adversary brigade’s ground line of communications (GLOC) back to the adversary nation.

Joint aviation quickly achieves air superiority but not outright air dominance. The CJTF brings all three enemy brigades under fire and closes with all three. Simultaneously, the CJTF, supported by various Joint assets, works hard to degrade enemy communications, and otherwise isolate the three formations. They rely heavily on SIGINT, cyberspace operations, and electromagnetic warfare to physically destroy selected communications nodes.

The CJTF does not press the enemy positions too closely. Using forces previously concealed from the enemy and forces that appeared to be in reserve, the CJTF uses ship-to-shore movement and air mobility to place a substantial force to the flank and rear of the northern enemy brigade, intentionally leaving a line of retreat open toward the border, but in a blocking position between the brigade and the western region’s capital city. The CJTF commander does not want to risk elements of the enemy brigade entering the city and creating the opportunity for significant collateral damage or bloody urban fighting.

continued...

Operation MALEVOLENT WRENCH (Continued)

The CJTF chooses to press the northernmost enemy brigade because a detailed analysis of available intelligence suggests that their commander was likely the most vulnerable to unwitting direction. A thorough estimate, conducted in collaboration with host-nation analysts and the US intelligence community, concluded that when facing sufficient attrition from indirect fire, lack of communication with HHQ, and in a disadvantageous position, the enemy commander would likely withdraw to a less detrimental position.

The CJTF commander approves this assumption as the basis for the scheme of maneuver and designates its validation as a PIR. After an intensive and focused intelligence collection and analytical effort, the J-2 is able to confirm the assessment.

While maintaining a stranglehold on the northern brigade's ability to communicate with the other brigades and with their HHQ, the CJTF leaves the brigade's internal communications untouched, monitoring them closely. After a short while, the J-2 is able to confirm that the organic ISR assets of the enemy brigade got a good look at the formations massing to their front and flank, and that their commander and key staff members are beginning to panic. These formations then move to demonstrate an advance (an advance that would become real if the enemy brigade does not shift), which creates an excuse to suspend indirect fires. Willfully resisting their Marine inclinations, the CJTF purposefully and intentionally slows its tempo, allowing time for the commander of the targeted enemy brigade to observe, orient, and decide what to do. Seeing the two forces closing in, and knowing the road back across the border is open, and fearing that the communications silence with higher and adjacent unit means that the other two enemy brigades are similarly beset, the commander of the northern brigade leaves a small rear guard and hastily begins to withdraw the balance of the brigade toward the border. Once they are clearly committed to their withdrawal, joint air and CJTF artillery begin a pursuit by fire, ensuring that many of the enemy brigade's vehicles are lost in transit along with all the equipment they abandoned in their initial positions.

With the bulk of the northern brigade fleeing, the CJTF picks up the tempo again, rapidly encircling and capturing the rear guard and preparing to advance on the center brigade. The disruption of enemy communications is modified and re-engineered in support of information warfighting function activities. First, the citizens of the enemy nation (and all enemy forces currently within their neighbor nation) can see news broadcasts of the prisoners from northernmost enemy brigade, their heavy equipment abandoned in their defenses, and the celebrations of the crowds in the western region's capital. Friendly SIGINT assets can now exploit the enemy's attempts to coordinate their defense to refine the CJTF's targeting, scheme of maneuver, and combat assessment efforts.

The release of multinational visual information footage is selective, including no imagery of the highway littered with the burned-out hulks of the destroyed vehicles, as it is not in the interest of the CJTF for enemy forces to have any misgivings about the safety of retreating.

After all-source analysis reveals a seam in the enemy's defenses, the still relatively fresh multinational ground forces, led by British Royal Marines, crashes into the front and rear of the center brigade, again carefully leaving a GLOC open for a possible retreat. The enemy forces fight tenaciously and are pushed back only slowly. However, the scene changes when patchy enemy C2 networks begin pick up partial messages of panic and fragmented orders to withdraw. Though these withdrawal orders are false and were manufactured by the MIG, they are sufficient to make the demoralized and desperate troops of the central enemy brigade race toward the border.

continued...

Operation MALEVOLENT WRENCH (Continued)

With two of the three enemy brigades out of the fight, the CJTF again intentionally moderates its tempo, demonstrating a partial regrouping and a partial (and intentionally slow) advance toward cutting off the remaining enemy's GLOC to its superiors across the border. Again, the CJTF intentionally allows the enemy's ISR to observe this movement and allows the enemy commander time to decide whether to withdraw. The typically reliable commander of the remaining brigade, abandoned by the other two brigades, knows the brigade is now in danger of being cut off. The brigade commander sends an aggressive blocking force to prevent the CJTF flanking force from cutting off the GLOC, and then uses that route to conduct a well-organized withdrawal. Once the staff's combat assessment efforts determine all friendly objectives have been met, the CJTF commander directs forces to break off the pursuit and stand down.

The enemy dictator is humiliated; two of three enemy brigades suffered grave losses, while multinational casualties were non-negligible but modest. The CJTF has imposed its will on the enemy forces, using physical and informational power as part of combined arms maneuver to drive enemies toward actions that were ultimately consistent with the CJTF commander's end state, including the withdrawal of enemy forces, deterrence of future adversary aggression, and preservation of US reputation and forces.

Discussion

What makes these two vignettes noteworthy is what is not different between them: The Marine Corps ethos to fight and win does not change. In fact, Marines use the same ethos to integrate the Marine Corps information warfighting function through the informational, physical, and human aspects of military operations to generate, preserve, deny, and project information to create and exploit information advantages, imposing their will on the enemy and achieving mission objectives. Marines still need to integrate intelligence, command and control, logistics, and force protection functions with traditional fires, maneuver, and information capabilities.

During Operation MALEVOLENT WRENCH, as part of the fight for information, Marine intelligence investigates (generates) the dispositions and proclivities of the enemy commanders so Marines can then fight with this information to create an advantage that can be leveraged to achieve desired outcomes. The overall concept of maneuver for the operation, or the sequence in which the three enemy formations are attacked, is based on information considerations and is driven in part, by which enemy commander is assessed to be most likely to lose the will to fight and withdraw when pressed, leaving the most psychologically resilient commander's formation until last, when those forces have already been abandoned by the other brigades.

The use of selective and heavy interference with enemy sensors and communication equipment to deny the enemy good situational awareness and awareness of specific events is a key component of the operational plan. This is accomplished through combined arms, including cyberspace operations, electromagnetic warfare, and lethal fires; and physical and informational maneuver (by attacking one enemy brigade at a time through physical and electronic isolation).

Although Marines are accustomed to adopting the most rapid possible tempo, as part of information as a form of maneuver when trying to induce a specific behavior from the commander of the northernmost enemy brigade the Marine Corps force intentionally slows its tempo to allow the enemy time to misperceive the situation and act accordingly; had Marines kept the tempo high, the enemy might not have had time to begin a withdrawal and might have ended up fighting a defensive battle much more desperate and physically costly to both forces.

The Marine Corps plan was quite conscious of possible narrative and second-order effects, making sure to prevent enemy withdrawal into the partner's regional capital, and denying the central enemy brigade the opportunity to fully understand what has happened to the first brigade so that they did not end up fearing that same fate; winning the reconnaissance/counter-reconnaissance fight and the fight for information allows the Marine Corps force to gain a narrative advantage and influence the sensing and making sense of the remaining enemy forces so that they cannot avoid an outcome similar to what happened to the first force.

When assaulting the central enemy brigade, the Marine Corps force leveraged a set of systems overmatch advantages to weaken enemy ability to communicate, project information to briefly usurp enemy command and control, and issue false withdrawal orders. To accomplish this required the Marine Corps force to first realize this as a possibility. Second, the fight for information provided sufficient detail on enemy C2 frequencies and order formats to be able to spoof the enemy. Third, they needed the capability to penetrate enemy communications networks at least briefly and partially. This third requirement might have been supported by communications herding, using jamming and other technical capabilities to deny the enemy the use of those communications systems the Marines were unable to spoof, and driving them onto communications systems the Marines could penetrate.

Finally, an advantage in prevailing narrative at the end of the operation served a key role in meeting the operation's future deterrence objective. Even though the enemy was not destroyed, the US and allied forces won and remained intact and in a strong position, and the adversary (and the adversary dictator) lost.

VIGNETTE 2: THE MARINE EXPEDITIONARY UNIT AND THE HIGH-VALUE INDIVIDUAL

Under the Marine Corps information warfighting function, the MEU is positioned to employ information as part of combined arms. As an example of how the MEU can perform 21st century combined arms, consider a hypothetical MEU mission to strike and eliminate a high-value individual (HVI) (e.g., key leader, technical expert, financier) within a VEO. In this vignette, the MEU creates a combined arms dilemma by using one capability to deny the HVI use of a critical asset, another to track the HVI, and another to strike and eliminate the HVI when the individual attempts to access, use, or repair the asset. The technique of "herding" individuals to a specific location to address a problem exposes them to physical harm.

The Marine Expeditionary Unit and the High-Value Individual

The MEU, working under the authority of the CCDR and in concert with applicable intelligence agencies and the DOS, is assigned the mission to disrupt a VEO's online media operations. The VEO's core leadership group is in a relatively small and geographically isolated area within the MEU's reach. However, its media operations, to include its propaganda and recruitment efforts, are highly sophisticated and effective at projecting an outsized image through a global online presence. This presence has proved effective at increasing the group's support, funding, and influence, and thus represents a growing threat.

The MEU receives intelligence on the physical locations of the VEO's media production studio, primary server, and backup server. These three assets are located in two separate buildings approximately three miles apart. At the designated time, the MEU's cyberspace planner coordinates with USCYBERCOM, through the CCDR, to initiate a pre-planned denial of service attack against the VEO's servers. At the same time, the MEU's tactical PSYOP team delivers tailored messages via cell phone to an identified HVI—the VEO's chief of media operations. Earlier, evaluators assessed the intelligence gain and loss associated with the using this conduit and determined it worthwhile. Carefully crafted, pre-approved messages are sent that are consistent with the HVI's language and culture and with current events in the local area. The HVI suspects nothing when notified of the malfunctioning servers.

As the cyberspace-attack and deceptive messaging occur, MEU reconnaissance teams occupy positions to observe and report on all relevant activity at the two locations. A cascade of rapidly unfolding events is triggered when the HVI arrives at the primary site to investigate the server issue. A reconnaissance report notifies the MEU commander of the HVI's arrival. The commander's decision to strike unleashes two orbiting F-35s waiting to deliver ordnance on both locations. The no-win situation created by this scenario is to either accept disrupted media operations or attempt repair and suffer physical harm and destruction. The strike results in eliminating the HVI and several support personnel, and destroying the buildings housing the studio and both servers.

Discussion

The success of the MEU's operation starts with an operational mindset that values information as a potential combined arms contributor and with success in the fight for information: this operation is predicated on recognizing adversary media operations as a COG, and on knowing where their servers are located, who the HVI is, and that the adversary chief of media operations was vulnerable to herding to one of the media centers when a server was taken down. Why were VEO media operations a COG? Because of comparative advantage in prevailing narrative held by the VEOs. It is hard enough to change the prevailing narrative in many audiences of interest without an adversary or competitor continuing to post narrative-reinforcing propaganda; by disrupting VEO media operations, the MEU creates some narrative space into which they or other DoD or USG entities can seize the initiative regarding narrative and perhaps gain some ground (see Appendix D for more on narrative).

With the information advantages gained by identifying both the critical targets and their relationships to VEO media operations, the operation could proceed. The operation unfolds with support from and sequenced integration of several capabilities. The denial-of-service attack is an example of information as a form of fires, while the targeted MISO messaging is an example of information maneuver. Information activities often have longer lead times than those required for physical fires and maneuver, either for the time necessary to develop access, develop information "munitions," or to align authorities and approvals. See Chapter 3 for more detail on information planning and coordination considerations.

Note that herding can be thought of as generalizable technique for information as a form of maneuver – using a combination of physical or informational power to deny an adversary access to a location, a frequency, or a capability and then setting a trap of some kind (something that allows the friendly force to gain an advantage) when they move or transition to an (anticipated) alternative means or location.

Vignette 3: Stand-In Forces and Sea Denial

Stand-in forces deter our adversaries by establishing forces that persist forward alongside allies and partners within a contested area. These forces provide the fleet, joint force, interagency, and allies and partners more options for countering an adversary's strategy. When directed, stand-in forces perform sea denial operations to support fleet maneuver and operations through the application of both organic sensors and weapons, and integration with naval and joint sensors and weapons. Achieving this requires stand-in forces that can conduct combined arms in all domains and the EMS and fully employ the Marine Corps information warfighting function. This vignette illustrates how stand-in forces can combine fires, maneuver, and information to create dilemmas in sea denial operations thorough a hypothetical scenario where conflict erupts between the United States and a competitor-turned-enemy. The combined arms dilemma created in this vignette is the enemy's inability to counter a friendly force electromagnetic attack, which renders the enemy more vulnerable to precision strike.

Stand-In Forces and Sea Denial

The Marine littoral regiment (MLR) maritime fires element occupies key maritime terrain sufficient for conducting long range precision fires in the vicinity of a critical chokepoint. The maritime fires element relies on combined arms to maneuver to and occupy the objective undetected, and to conduct fires against the enemy.

The maritime fires element can move undetected as a result of winning the counterreconnaissance fight. Prior to conflict, the stand-in forces succeeded in uncovering and mapping out the enemy's collection methods, capabilities, and techniques in and around the key maritime terrain. Knowing how the maritime fires element would be collected upon, the plan to maneuver is supported by TAC-D, astute timing to exploit known gaps in the enemy's collection windows, OCO, and physical attacks to divert the enemy's attention away from the unit's maneuver to the objective.

The MLR has plans in place to use OCO, which includes pre-approved authorities and permissions. The maritime fires element coordinates with the MLR headquarters' cyberspace operations cell (a component of regimental fires and effects), to ensure the timing of the OCO mission supports their movement. The OCO mission specifically targets the one remaining SIGINT asset the enemy had collecting in the vicinity of the objective. The cyberspace planner at the MLR headquarters facilitates the OCO mission through pre-coordinated joint fires channels and through the CCDR.

While occupying the firing position and conducting the firing mission, the maritime fires element uses passive and active SIGMAN techniques to suppress and manipulate their physical and electromagnetic signatures. Passive measures include the use of communications discipline, concealment, and camouflage. Active measures include the use of decoys to deceive enemy collection.

The firing unit executes long-range precision fires in combination with joint forces. The timing is critical to mass several different munitions from air, surface, and land-based systems against the enemy surface target. This joint combined arms operation includes airborne electromagnetic attack from close-in unmanned aerial systems and from manned stand-off jamming aircraft to reduce the enemy's defenses against the MLR's strike. The inability of the enemy ship to counter joint force electromagnetic attacks reduces the ship's defenses and makes the ship vulnerable to precision strike.

Upon completion of the fire mission, the MLR unit immediately displaces from its position using combined arms to support movement to a pre-designated hide position. Movement is facilitated by a pre-approved CONOPS that includes the use of joint electromagnetic protection and attack capabilities designed to screen the MLR's movement against known collection threats. In this scenario, the MLR unit coordinates with the MLR headquarters' EMSOC [electromagnetic spectrum operations cell] to synchronize the timing of the joint screening action with diversionary attacks to cover the MLR's movement from the firing position to the hide position.

Discussion

The ability to deny the enemy the ability to detect the maritime fires element as it moves into position is critical to success in this mission, and it is only possible due to advantages exploited and advantages gained as part of the counter reconnaissance fight. An intimate knowledge of the enemy sensor network (a significant systems overmatch advantage) allows the MLR to (in coordination with other components) either avoid sensors or disrupt them sufficiently to emplace the maritime fires element undetected.

To remain in place while waiting to execute their fires, the maritime fires element relies on SIGMAN, an example of information as a form of maneuver. By denying the adversary the opportunity to distinguish their emissions from background noise, and deploying decoys to distract enemy sensors, the maritime fires element creates and maintains a force resiliency information advantage – you cannot kill us if you cannot find us. Then, during the attack, the maritime fires element contributes to the weight of informational and physical fires directed at the target, overwhelming any possible defensive measures, and achieving full effect.

Finally, projection of decoy signals and jamming helps to screen the withdrawal of the maritime fires element, again denying the enemy the opportunity to find and fix them.

VIGNETTE 4: THE ARG/MEU IN COMPETITION

The MAGTF is an effective counter to competitors endeavoring to undermine US objectives through the area denial threat posed by large weapon engagement zones and precision strike. This is particularly true when MAGTFs coordinate their actions with a host nation, other MAGTFs, joint forces, and interagency partners like the DOS and the US Coast Guard. This vignette describes this role for the MAGTF in a hypothetical scenario, in which a MEU coordinates action with the amphibious ready group (ARG), host nation, CCDR, DOS, and the US Coast Guard to stymie a potential adversary's illegal territorial claims over a key international trade route.

The ARG/MEU in Competition

A potential adversary has been conducting a small-boat harassment campaign, targeting international cargo vessels in a narrow, but heavily trafficked, shipping lane. The potential adversary uses the cover of its long-range precision strike capability to employ a network of small boats that conduct high-speed approaches and near misses to harass transiting vessels. The objective of the harassment campaign is to slow the movement of these vessels and disrupt trade. Decision makers must choose between engaging the small boats (and risk escalation), or suffering the economic consequences of trade and supply chain disruptions. While this campaign attracts international criticism, the lack of an effective response signifies an inability to oppose the potential adversary's long-term pursuit of a territorial *fait accompli*.

The MEU is tasked to disrupt the small-boat harassment campaign for 30 days without triggering armed conflict. and thereby facilitate the free flow of trade through international waters. The goal of the MEU-led mission is to create a dilemma for the potential adversary: the more they harass, the more harmful it becomes to pursue their territorial ambitions. The mission involves the MEU planning and coordinating the effort to find, fix, track, interdict, disrupt, and then expose (through various media) the harassing swarms of small boats.

The ARG vessels with embarked MEU, a US Coast Guard cutter, and two host nation coast guard vessels position themselves in the straits to demonstrate resolve through physical presence. The coast guard vessels patrol international waters near the potential threat. The ARG vessels patrol international waters between the coast guard vessels and commercial ships transiting the straits. This highly visible presence coincides with a significantly ramped up strategic messaging campaign, wherein senior US and host- nation government leadership issue regular joint statements and hold press briefings. The messaging campaign highlights the strengthening ties between the nations to ensure freedom of navigation in international waters.

Over the 30 days, the MEU S-2 fuses intelligence from ARG sensors, US Coast Guard sensors, theater and national assets, and organic MEU aviation assets to maintain maritime domain awareness in the contested zone. Integrating these assets provides a multi-layered network of sensors that gives indications and warnings of a small-boat swarm formation on the adversary's near shores. Early warning is key to tracking and interdicting the swarm. Upon finding, fixing, and tracking the swarm, the interdiction begins with host-nation and US Coast Guard vessels moving to intercept the swarm formation before they can approach a commercial ship. As the coast guard vessels approach the swarm, a MEU unmanned aircraft flies over the small-boat swarm. The aircraft is equipped with video recording equipment and a radio frequency jamming payload.

Using a pre-approved CONOPS with authorities and permissions from the CCDR, the unmanned aircraft records the swarm and jams its radio communications, which disrupts the swarm commander's ability to direct and coordinate action. As US Coast Guard vessels arrive the harassing swarm loses cohesion and abandons its mission. This interdiction concludes with the MEU releasing video footage of the harassing swarm, along with a combined public statement from the MEU, ARG, and US and host nation-coast guard commanders, reinforced with additional US and host-nation public statements and press briefings.

To communicate additional resolve, the coast guard interdiction, disruption, and exposure operation is conducted against the backdrop of a MEU combined arms demonstration exercise with the host nation. Images and video from both the interdiction mission and the combined arms demonstration are used to illustrate resolve in a multi-media campaign.

Discussion

This operation is all about prevailing narrative—being able to promote narratives, supported by recorded visual evidence, of the potential adversary's dangerous and unneighborly behavior, and of the US-led multinational standing up to and thwarting the bullying.

The success of the operation depends on winning the fight for information and being able to maintain maritime domain awareness and detect and track the potential adversary's harassing forces while concealing the precise location of friendly forces and the range of locations where they can quickly mass. Good sensing and sense-making create a (systems overmatch) information advantage which allows the ARG/MEU and partners to create localized physical overmatch and to create an advantage in prevailing narrative.

The ability to use unmanned aircraft-based electromagnetic warfare to deny the potential adversary boat swarm their customary means of command and control is key to the success of the operation. With communications intact, the harassing swarm might be able to maneuver in such a way as to thwart the interdiction. Jamming their communications puts them at a disadvantage and forces them to cede the physical and information initiative to the ARG/MEU.

Note the importance of the presence, posture, and profile of the ARG/MEU and coast guard partners as a capability, and the supporting visual information capability, as well as the role for COMMSTRAT in dissemination of operational footage and the accompanying narrative. The operation was likely rendered even more effective by the inclusion of regional journalists on one or more of the multinational vessels as embedded press.

Finally, one of the informational challenges of this operation is the need to balance between the presence aspect of the mission, of being visibly present guarding shipping lanes, with the concealment aspect of the mission, hiding (at specific times) the location and response radius of at least part of the multinational force. This might be accomplished by the surreptitious inclusion of additional forces, using night operations to relocate and conceal elements of the multinational flotilla, decoys or SIGMAN, or effects on specifically targeted enemy sensors or sensor platforms.

APPENDIX D.
NARRATIVES

Prevailing narrative is a possible source of advantage, but also a possible source of disadvantage. In the contemporary era marked by informational competition, one of the most important activities of a Marine Corps command is the development, presentation, and support of the command's intended narrative. Communication strategy and operations personnel should take the lead in conceptualizing and planning narrative but will require support and input from elsewhere in the staff. This appendix explains what narratives are and how they are important to Marine Corps operations, and then moves on to what Marine Corps commands can and should try to accomplish with narrative: internal coordination, offering a positive or alternative explanation to external audiences, and competing with narratives at odds with mission objectives.

WHAT ARE NARRATIVES?

There are many different definitions of and views on narrative; however, there is consensus on the nature, relevance, and importance of narratives to operations. First, narratives are essentially stories and have story properties (settings, characters, plots, resolutions, beginnings, middles, and ends). Second, stories are how human beings understand and make sense of the world and their place in it. And third, the stories told or get used to make sense of the events of military operations and conflicts affect perceptions and understandings of those operations. This in turn affects the perceived legitimacy of those operations and the extent to which one side or the other receives an individual or group's support.

WHAT IS IMPORTANT ABOUT NARRATIVES?

There are three facts about narratives that are relevant to Marine Corps efforts to use narratives in support of operations:

- People use narratives to make sense of the world and their place in it.
- Compelling narratives have consistency, familiarity, and proof.
- Narratives already exist, and although they can be shaped over time, they cannot always be changed or replaced.

Each of these is three points is explained in the following sections.

People Use Narratives to Make Sense of the World

Narratives and other mental shortcuts help people make sense of the things they see and experience in the world. Research shows that people use stories to help structure memory, cue certain approaches to problem-solving, format new information, and define our identities. Narratives also often suggest or hint at how we should, or could, feel about an event based on the emotional context of the narrative or even suggest a COA, perhaps based on the moral of the story. As Mark Laity, former Chief of Strategic Communications at Supreme Headquarters Allies Command Europe has noted, “Narratives make sense of the world, put things in their place according to our experience, and then tell us what to do.”

Part of making sense of the world is making sense of our place in it. When exposed to compelling stories, we build narratives to support our interpretation of events to acknowledge the subjective and cognitive biases we carry. We consciously and subconsciously identify with the actors and struggles explained in those narratives. When we relate to the characters or their struggle, we use the outcomes in the narrative to validate our current context and give us purpose to our possible COA. For example, many Marine Corps recruiting commercials tell a story about a young person facing difficult personal challenges or defending innocents from chaos. Similarly, VEOs offer opportunities for recruits to protect the “persecuted” and be a part of an organization not afraid to act in the face of “oppression,” and in their stories they use characters, struggles, and goals chosen to resonate with their target audiences. In both cases, potential recruits can identify personally and emotionally, and see a path of action to address key events in their worldviews; thus, narratives can be both explanatory and mobilizing.

What happens when we cannot make sense of events witnessed or accounts heard? The human brain wants the information it receives to make sense. When the brain cannot make sense out of incoming information, that information is more likely to be discounted or ignored, or recombined with previous information until it does make sense. So, if something new happens (for example, the arrival of Marines to provide humanitarian aid), it is interpreted based on the existing stories or overarching narratives held by the observing audience. If the dominant existing narrative about US forces is negative, then the new facts will predominantly be interpreted in a way that is consistent with that narrative, even if this requires the omission of some of the details (e.g., mention of the humanitarian aid), leaving the audience with a negative view.

Always remember that different groups of people have different collections of stories. This is important, because different groups of people will perceive the same events differently, and make different sense of them, based on the narratives available to them. For example, the Marine Corps has several memorable and important specific narratives: Tripoli, Chesty Puller, Guadalcanal, Iwo Jima, etc. There is a Marine Corps narrative perspective, a way of seeing the world and the Marines’ role in it consistent with all those stories and is more or less shared by all Marines – but these stories and perspectives are not shared by others.

Compelling Narratives have Consistency, Familiarity, and Proof

Compelling narratives have at least three characteristics: consistency, familiarity, and proof. Consistency refers both to the internal consistency of a story (i.e., whether the outcome follows logically from the action described, whether the characters' behavior is true to type, etc.) and to the story’s consistency with other relevant narratives. Familiarity is about how well known a story or narrative is; more than just awareness of the story, familiarity also implies a level of comfort with the story, which could come from sharing themes in common with stories within a broader set of narratives. Proof is about the evidence available in support of the narrative and can vary widely. Proof can hinge on the perceived credibility of what is claimed, perceived credibility of the narrator, eyewitness accounts, or recorded pictures or video. Note that what constitutes proof varies considerably by context and medium. For example, in the United States, the facts in stories presented by television news anchors are accorded high degrees of credibility and generally accepted as strong proof. Elsewhere in the world, however, state-run television news reports are not considered much proof at all, while a story repeated from a friend of a friend might count as strong proof, despite less-compelling evidence.

Narratives Already Exist, and You Cannot Always Change or Replace Them

As mentioned earlier, audiences ascribe different levels of consistency, familiarity, and proof to different narratives, have different collections of stories and narratives available to them, and prefer to interpret new events in a way that is consistent with their existing collection of stories. Most events audiences witness, or experience immediately fit within at least one of those pre-existing narratives. This can make it very difficult to present a new or alternative narrative that will have any traction.

Narrative Opportunity

In most cases, when Marines act in foreign lands, relevant foreign audiences will already have one or more dominant narratives in place, regardless of what themes, messages, and images accompany the Marines' actions. If pre-existing narratives drive the understanding of events in most cases, when and how can Marines oppose, counter, or offer alternatives to those narratives? More briefly, when are there narrative opportunities, and what kinds of opportunities are they?

When something happens, that people notice and care about, relevant audiences and key publics will become aware of it and try to make sense of it. One of three things will happen:

1. The event fits perfectly within one existing narrative, reinforcing that narrative, and connecting to all the other content (negative or positive) from that narrative – which becomes the dominant narrative for this event.
2. The event fits reasonably well within more than one available narrative or can be viewed through the lens of more than one relevant narrative. The event will be understood through one or more of the available narrative lenses, but which one(s) will be dominant is unclear (and perhaps shape-able).
3. The event does not fit well within available narratives. The event will end up connected to one or more narratives, but which ones and how it will be interpreted is an open question.

Each of these three possibilities corresponds to a different level of narrative opportunity.

1. If the event fits within an existing mobilized narrative, there is very limited narrative opportunity, leaving few options. These include:

   A. Accept and embrace all or part of that narrative (if it is positive, or has positive or at least tolerable aspects).

   B. Adjust planned actions so that they are easily connected to that narrative (if the planned action is going to connect directly to an unfavorable narrative, consider not doing that action, or finding a way to do it that will be perceived differently).

   C. Try to emphasize aspects of the action that suggest an alternative narrative frame. Sometimes the only way to create an opportunity to change the narrative is to change the actions.

2. If events fit within one or more alternative narratives or frames, there is narrative opportunity. Marines trying to fight through and against narratives can pick the available narratives that are most favorable or beneficial to the Marine Corps and try to emphasize aspects of the action that are consistent with those narratives, or otherwise try to frame the event so it is viewed in that way. There might be an opportunity to emphasize how the event is not like what happens in an unfavorable narrative, provided there is an alternative narrative. This is not a narrative opportunity to make up a wholly new narrative but an opportunity to push toward and emphasize favorable available narratives and push away from unfavorable narratives.
3. If the event is something new or different, people are still going to try to understand it and connect it to existing narratives, but there may be greater opportunity to shape which ones or to introduce new ones. Here, narrative opportunity is greatest, as a much wider range of available narratives can potentially be mobilized to help observers understand the event. It may even be possible to promote a wholly new narrative; however, it would be easier, and would likely have more traction, to try to mobilize some dormant pre-existing narrative or lens than to create a wholly new one. A dormant narrative is more likely to be consistent and somewhat familiar, whereas a wholly new narrative, even if there is an opportunity for one, will need to build its consistency, familiarity, and proof from scratch.

When comparing competing narratives or narrative frames, audiences consider and weigh the consistency, familiarity, and proof of each. This subconscious or conscious comparison of competing narratives operates following cognitive processes not unlike those used by a jury during deliberations.

Once a given narrative has been associated with an event or series of events, it will be difficult to change that connection. However, there may be opportunities to emphasize different aspects of that narrative, to try to combine it with another salient narrative with more favorable characteristics, or otherwise shape the narrative. Again, in most situations, a wholly new narrative is unlikely to gain much traction, as, compared with other available narratives, it will lack external consistency and it will be unfamiliar, regardless how much proof is associated with it and particularly if that proof is more compelling to Western audiences than to relevant audiences.

What can Commands try to Accomplish with Narratives?

What should a command hope to accomplish with narratives in support of Marine Corps operations using command narrative? First, internal coordination. If humans make sense of events through narrative, then a clear mission narrative will be particularly useful for Marines. The narrative needs to fit with existing military and Service-specific narrative perspectives; a mission narrative makes it easier for Marines to understand and remember mission objectives, and to understand their role in the story that will lead to achievement of those objectives. A clear mission narrative can help Marines avoid the gap that often opens between actions and communications, promotes unity of effort, and diminishes the likelihood of miscommunication. A good mission narrative guides follow-on planning, targeting, and execution, and enables mission command because subordinates will be better able to judge whether an available COA is consistent with the narrative and thus preferred.

Second, commands can use command narrative to offer a positive or alternative explanation to external audiences. As discussed throughout this appendix, relevant audiences and key publics are going to find narratives that help them make sense of US operations. Left to rely solely on their own histories and experiences, many of these narratives will support views and actions that are contrary to the command's mission and intent. Countering these existing perceptions is a core challenge of narrative in operations. Marine Corps commands should seek to promote narratives of their operations that ascribe positive meanings to their actions so that they add up to something that should be supported, or at least patiently tolerated, rather than being viewed negatively. The extent to which this is possible will be constrained by the level of narrative opportunity available, as described in the previous section. Done well, command actions are the foundation of effective narratives and inherently increase understanding, tolerance, and support for Marine Corps operations. This increased tolerance can increase the likelihood of desired behaviors (e.g., non-interference, cooperation), and freedom of maneuver because Marine actions occur within the confines of a locally accepted narrative of legitimacy.

Third, the command may want to compete with or undermine narratives at odds with mission objectives, when there is sufficient narrative opportunity to do so. Many operational environments contain narratives that do not support Marine Corps force presence or objectives, or such narratives may be introduced or mobilized by adversarial groups whose interests do not align with those of the Unite States. To reap the benefits of having a broadly accepted legitimating narrative and achieve desired levels of support, Marines need to find a way to fight those alternative narratives.

Defeating hostile narratives must go hand in hand with the promotion of positive narratives. Audiences will find a narrative or narrative frame for events, and they will make sense of them, one way or another. It is impossible to defeat a narrative and just leave a narrative vacuum. There must be a better alternative narrative that replaces it.

FIGHTING AGAINST, WITH, AND THROUGH NARRATIVE

With these three objectives – internal coordination, offering a positive narrative, and competing with opposing narratives – in mind, how can Marine Corps commands do this in practice? This should involve consideration of the command's mission narrative (the internal narrative to help Marines consistently orient on the mission), the command's external narrative (the story Marines will tell others about their mission), and other narratives that are (or should be) present in the operational environment.

Develop a Command's Mission Narrative

The command's mission narrative is the simple orienting story the commander will offer to Marines to convey the objectives of the mission and their role in accomplishing them. The same process that produces the commander's intent can produce the command's mission narrative with very slight adjustment. As the planning staff concludes problem framing and prepares the commander's guidance and intent, they should also prepare the mission narrative as part of that intent. Ultimately, the mission narrative is just a restatement of the commander's desired end state as the conclusion of a story, and the role the commander expects troops to play in bringing that end state about: it captures the essence of the "why" and the "how" of the mission as envisioned by the commander and should help Marines remain oriented on the commander's approach to achieving the mission's objectives.

An example of an excellent summary phrase for a command's mission narrative is "No better friend, no worse enemy" by then-Major General James Mattis with 1st Marine Division as they began Operation IRAQI FREEDOM I in March of 2003. Before leading the 1st Marine Division into Iraq in 2003, Major General Mattis offered a succinct, yet passionate, example of a mission narrative in the letter he sent his Marines before going into the fight: "When I give you the word, together we will cross the Line of Departure, close with those forces that choose to fight, and destroy them. Our fight is not with the Iraqi people, nor is it with members of [Iraq's army] who choose to surrender. While we will move swiftly and aggressively against those who resist, we will treat all others with decency, demonstrating chivalry and soldierly compassion for people who have endured a lifetime under Saddam's oppression." In one paragraph, Major General Mattis states his intent, lays out his end state, and makes very clear how he expects his Marines to conduct themselves. From this command narrative, Major General Mattis coined a division motto that would cement his narrative and intent into the minds of every Marine under him: "No better friend, no worse enemy." This phrase captured two facets of his intent: Marines must be aggressive and flexible in taking the fight to the enemy, but that civilians and prisoners be treated with chivalry and spared unnecessary harm. It gave clear roles to his Marines and tied into the existing Marine Corps narrative perspective, with the same narratives that confirm "every Marine a rifleman" being highly consistent with the "no worse enemy" portion. When he returned to Iraq in 2004 for Operation IRAQI FREEDOM II, he kept "no better friend, no worse enemy" but also added "first, do no harm" to emphasize the relief and reconstruction emphasis of the new mission.

Not every command's mission narrative will be as straightforward and short as Major General Matti' masterpiece, but every such narrative should connect with the narratives and identities of the Marines Corps, describe the roles Marines will serve as the operation unfolds, and state the desired conclusion of the story of the operation.

Develop a Command's External Narrative

Developing a narrative for external audiences is much more challenging. Ideally, the command's mission narrative and the command's external narrative will be one in the same. It is much more effective to offer the same story of justification, explanation, and purpose to the Marines executing the mission and to the audiences witnessing their actions. Unfortunately, a quick and easy narrative that resonates with Marines may fall flat with relevant external audiences, and particularly foreign audiences, because it is inconsistent with the latter's pre-existing narratives, is unfamiliar to them, and lacks proof that they find compelling.

Developing a command's external narrative necessitates work and effort beyond current operational planning routines, though it can certainly be nested within existing processes. Preparing a command's external narrative requires a robust understanding of the relevant audiences (those people whose behavior is instrumental to the success or failure of the campaign), their narrative frames in terms of their history, worldview, and recent events, and the available narratives about the United States, its armed forces, and their operations and actions. To be able to plan effectively for a command's external narrative requires analysis related to these kinds of issues. This analysis might come from the intelligence staff, or it might come from the efforts of expert practitioners in COMMSTRAT, MISO, or civil affairs, or subject matter experts outside the Marine Corps, from among joint, interagency, or international partners. This analysis may require (or benefit from) media and social media monitoring or available behavioral, cultural, and linguistic subject matter experts who have sufficient knowledge of the operational context to meet the need. Needed background can be bolstered by seeking existing intelligence products and building collection requirements that focus on the groups and cultures in the operational environment. If available information is lacking, the kinds of information required are most closely akin to the output of a TAA.

The command's external narrative needs to be planned as a separate but integrated part of the planning process. Again, primary responsibility for planning and consideration related to both internal and external narratives falls on COMMSTRAT. If a narrative is important to the commander, needed information can be prioritized as part of commander's critical information requirements. Available information about the "narrative landscape" of any operational context is likely to be insufficient to understand it wholly and completely. Still, an earnest effort to begin to understand relevant audiences, their desires and motivations, their style of narration, their core myths, legends, and perspectives, and the existing narratives about the US and US Marines will likely provide a foundation from which to start.

Identify and Promote Desired Narratives Among Relevant Audiences

The story that Marines tell about what they are doing is important, but what is even more important are the stories relevant local groups tell each other and themselves about what Marines are doing, and about what US adversaries are doing. The biggest challenge when fighting with, against, and through narratives is getting external narrators to tell and repeat favorable stories about Marines and reducing the prevalence of narratives favorable to adversaries.

Selectively promoting or discouraging specific narratives or narrative elements within the broader relevant narrative landscape requires deep understanding and a deft touch. This requires additional understanding and capability, and if attempted, should be done in close collaboration with relevant regional joint headquarters, DOS representatives, and relevant international partners. Shaping and fighting narratives at this level requires even more extensive cultural and linguistic inputs; deeper understanding of available myths, memes, and other narrative elements; intelligence about key influencers; capabilities for persuasion and influence; and better understanding of the cultural and cognitive aspects of narrative generation and promulgation than can be included here. Further, the command may have to be willing to adjust and fine tune its operations to provide proof for the desirable stories and stop supporting undesired ones. If the commander does not like the stories being told about Marine actions, the command needs to be prepared to adjust the stories and the actions to be consistent with preferred stories.

REQUIREMENTS FOR EFFECTIVE COMMAND NARRATIVES

To achieve effectiveness in fighting with, against, and through narrative, Marines must—

- Identify available salient narratives and narrative frames already present in the operational context.
- Anticipate which of those narratives are likely to be connected to planned Marine Corps actions and undertakings.
- Identify which narratives or aspects of narratives are favorable or neutral to command objectives and which are unfavorable.
- Recognize when altering planned actions can create opportunities for more favorable narratives.
- Push on and into the information environment to promote more favorable alternatives (when available), or more positive/favorable aspects of unavoidable narratives.

Addressing narratives is difficult, but doing so will ultimately allow Marines to operate more effectively in complex modern environments. It is only by embracing the complexities of human understanding of conflict, and affecting them through narratives, that we will truly be able to fight and win in the information age.

APPENDIX E.
INFORMATION CAPABILITY AUTHORITIES

In addition to the traditional military authorities available to commanders, operating with a whole-of-government and planning of multinational operations greatly expands the authorities available and necessary. Commanders can leverage authorities that stem from various sources, including US laws, regulations, and policies.

The types of authorities can broadly be separated in the following categories: US focused intelligence; military, interagency, and USG authorities; and partner and allies authorities.

MILITARY AUTHORITIES (US CODE, TITLE 10)

Service authority and responsibility, the authority necessary to equip and train the armed forces, establish a command structure, maintain good order and discipline, along with some operational authorities, are addressed in Title 10.

- Combatant command (command authority) (referred to as COCOM) authorizes CCDRs to exercise authority based on the Goldwater-Nichols Defense Reorganization Act of 1986, which modified US Code, Title 10, Section 164. The CCDR exercises authority provided directly from Goldwater-Nichols and the Unified Command Plan, which establishes the missions and geographic responsibilities among the CCDRs.
- Combatant command (command authority) is not transferable and cannot be delegated. It authorizes a CCDR to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the assigned missions to the command.

INTELLIGENCE AUTHORITIES (US CODE, TITLE 50)

The intelligence community has its origin in the National Security Act of 1947, amended by the Intelligence Reform and Terrorism Prevention Act of 2004, and guided by Executive Order 12333, United States Intelligence Activities, as amended. It refers in the aggregate to those executive branch agencies and organizations that are listed in 50 U.S.C. section 3003(4) as members of the intelligence community. Intelligence doctrine describes the roles and relationships of intelligence organizations at the national, combat support agency, CCMD, and subordinate joint force levels.

INTERAGENCY AND US GOVERNMENT AUTHORITIES

The DoD works closely with other USG departments and agencies when planning. The supported geographic CCMDs are DoD principal planning agents and provide joint planning directives for peacetime assistance rendered by DoD within their assigned areas of responsibility. Upon issuance of an EXORD by the Chairman of the Joint Chiefs of Staff, at the direction of the President or Secretary of Defense, to initiate or conduct military operations, the supported commander implements and relays the authority of the order with their own orders directing action to subordinate commanders, supporting commanders, and directors of supporting agencies. Depending on the type of operation, the extent of military operations, and the type of agency, international organization, NGO, and private sector involvement, the focal point for operational- and tactical-level coordination with civilian departments and agencies may vary. For example:

- The DOS' principal role in its relationship with DoD is to ensure that defense activities support national foreign policy and to facilitate defense activities overseas. In performance of the first role, the DOS attends interagency meetings, responds to requests from Joint Staff and Office of the Secretary of Defense for foreign policy reviews of DoD proposed activities, and alerts DoD to defense activities of foreign policy concerns that have come to DOS's attention. In its role as facilitator of defense activities overseas, the DOS approaches foreign governments through high-level visits, diplomatic representations by US missions overseas, or contact with foreign government representatives in the United States to negotiate agreements or obtain authorization for defense activities in the foreign country. In recognition of the impact that DoD activities have on US foreign affairs, the DOS has assigned a single bureau, Bureau of Political-Military Affairs (PM), to be its primary interface with DoD. This bureau manages political-military relations throughout the world, including training and assistance for foreign militaries, and works to maintain global access for US military forces
- The Coast Guard in accordance with US Code, Title 14 must be a Service in the Department of Homeland Security, except when operating as a Service in the Navy. The Coast Guard specific mission sets and capabilities are emphasized in recently published Advantage at Sea: Prevailing with Integrated All-Domain Naval Power as part of an integrated naval forces and are uniquely suited for operations throughout the competition continuum. The Coast Guard's mission profile makes it the preferred maritime security partner for many nations vulnerable to coercion. Integrating its unique authorities—law enforcement, fisheries protection, marine safety, and maritime security—with Navy and Marine Corps capabilities expands the options provided to JFCs for cooperation and competition. Navy and Coast Guard ships conduct freedom of navigation operations globally, challenging excessive and illegal maritime claims. Coast Guard cutters and law enforcement detachments aboard Navy and allied ships exercise unique authorities to counterterrorism, weapons proliferation, transnational crime, and piracy.

PARTNER AND ALLIES AUTHORITIES

United States' allies and partners bring unique perspectives, capabilities, forces, access, and authorities to critical regions that complement US assets. For example, a particular message may not be releasable under our authorities but may be under those of our partners and allies. The

2018, National Defense Strategy highlights this unique relationship, "Our strength and integrated actions with allies will demonstrate our commitment to deterring aggression, but our dynamic force employment, military posture, and operations must introduce unpredictability to adversary decision-makers. With our allies and partners, we will challenge competitors by maneuvering them into unfavorable positions, frustrating their efforts, precluding their options while expanding our own, and forcing them to confront conflict under adverse conditions."

AUTHORITIES FOR MILITARY INFORMATION SUPPORT OPERATIONS ACTIVITIES

Due to the opportunity for myriad unintended consequences including information mishandling between US military, agencies and organizations, and US allies and partners, MISO activities require early and extensive coordination.

Authorities for Conduct of MISO Programs:

- Prior to conducting MISO, CCDRs must have their MISO programs approved in accordance with Department of Defense Instruction (DoDI) O 3607.02, *Military Information Support Operations*, CJCSI 3110.5, *Military Information Support Operations*, and Chairman of the Joint Chiefs of Staff Notice 3110.05, *Interim Guidance for the Military Information Support Operations Supplement to the Joint Strategic Capabilities Plan*.
- MAGTFs gain their authority to execute MISO from their supported CCDR. These authorities are usually found in a CCMD's theater campaign plan, contingency plan, or EXORD.
- An approved MISO program alone is not an execution authority. Authority of a program does not equal permission to execute. Execution comes in the form of an order from the CJCS, as approved by the Secretary of Defense. A program is either a stand-alone document or it becomes part of the theater campaign plan or an OPLAN. Execution also requires an EXORD and deployment order to proceed.

MISO Program Approval Requests Must Address:

- MISO objectives.
- Target audiences.
- Themes to stress and avoid.
- Means of dissemination.
- Attribution plan.
- Designated approval authority.
- CONOPS.
- Concept for assessment.
- Assessment of the potential for collateral effect and exposure to unintended audiences.
- Assessment of risk by the execution of the planned MISO.
- CCMD proposed Public affairs guidance.

AUTHORITIES FOR CIVIL MILITARY OPERATIONS AND CIVIL AFFAIRS OPERATIONS

Civil military operations are an inherent command responsibility to coordinate civil and military activities; minimize civil-military friction and reduce civil threats to maximize populace support for US operations. These operations also meet the commander's legal obligation and moral responsibility "to do no unnecessary harm" to the civilian populations within the operations area. See *Civilian Harm Mitigation and Response Action Plan* (CHMR-AP), 2022.

Both CMO and CAO occur simultaneously in the same battlespace as other military operations including defensive and offensive combat operations. Department of Defense Directive (DoDD) 2000.1, *Civil Affairs* establishes policy and assigns responsibilities for conducting DoD-wide civil affairs activities including the use of military forces to support approved humanitarian and civic assistance provided in conjunction with military operations, and disaster relief operations conducted in accordance with DoDD 5100.46, *Foreign Humanitarian Assistance,* in addition to allowing immediate humanitarian actions to prevent the loss of life, property, and unnecessary human suffering:

- Typical requirements are chief of mission (embassy) and HN permissions, which are typically granted through the coordination of the unit political advisor, or a military attaché/desk officer assigned to the embassy that can be requested through the chief of staff or G3/S3 (depending on unit level and mission).
- When possible, locally developed projects and programs should be reviewed by the political advisor or commander's legal advisor for compliance with international law.
- Civil affairs personnel often have access to the Defense Security Cooperation Agency or Overseas Humanitarian Disaster and Civic Aid funds in cooperation with United States Agency for International Development guidelines to perform their duties.

LEGAL CONSIDERATIONS

All US military information activities are subject to applicable international laws and treaties, US laws and policies, and DoD regulations and policies. Understanding how various policies and laws interact in practice with respect to the information environment is a challenging task. To overcome these challenges, commanders and staff consult with legal advisors throughout the planning process. Planners should maintain awareness of relevant international agreements and consult with legal advisors to identify associated legal obligations or constraints that must be incorporated into plans. The DoS publication Treaties in Force outlines international agreements currently binding on the United States but is not intended to be a definitive listing of all such obligations (i.e., classified agreements, implementing arrangements, and other agreements are intentionally omitted).

Many activities and operations that leverage information require specific review processes and execution authorities. Presidential executive orders and policy memorandums and DoD directives, instructions, manuals, and policy memorandums establish the authorities and permissions to plan, integrate, approve, and execute information activities. During the initial planning process, planners should coordinate information activities across the joint force, as well as with USG departments and agencies. In some cases, DoD may not be the lead agency and, therefore, may be subject to additional constraints.

Conducting information activities involves complex legal issues such as statutory, policy, and budgetary authorities that require careful review and may require national-level coordination and approval. Moreover, legal interpretations can differ because of the range of legal interests potentially affected and the challenges for laws and policies to keep pace with the complexity of, and rapid changes in, information technology. Commanders and their staffs should involve legal advisors and policy experts early in, and throughout, the planning and execution process.

Department of Defense components execute information activities in accordance with DoDD 3600.01, *Information Operations* (IO); DODD 5122.05, *Assistant to the Secretary of Defense for Public Affairs (ATSD[PA]*); US law; and other supporting policy, guidance, and directions.

Department of Defense personnel do not intentionally disseminate information to influence US domestic audiences, organizations, or individuals, to include US Service members and their families.

Department of Defense components conducting information activities that also qualify as intelligence activities comply with all law and guidance applicable to such activities including, but not limited to, Executive Order 12333, *United States Intelligence Activities* (as amended), and DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*. Refer to JP 3-84, *Legal Support*, for additional guidance on legal support to CCDRs.

GLOSSARY

Section I: Abbreviations and Acronyms

AC/S	assistant chief of staff
ACE	aviation combat element
ATO	air tasking order
C2	command and control
CAO	civil affairs operations
CCDR	combatant commander
CCMD	combatant command
CCMF	Cyber Combat Mission Force
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJTF	combined joint task force (NATO)
CMC	Commandant of the Marine Corps
CMO	civil-military operations
COA	course of action
COC	combat operations center
COG	center of gravity
COMCAM	combat camera
COMMSTRAT	communication strategy and operations
CONOPS	concept of operations
CPT	cyberspace protection team
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations-internal defensive measures
DCO-RA	defensive cyberspace operations-response actions
DISO	deception in support of operations security
DoD	Department of Defense
DoDD	Department of Defense directive
DoDI	Department of Defense instruction
DoDIN	Department of Defense information network

DON	Department of the Navy
DOS	Department of State
EMI	electromagnetic interference
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EXORD	execute order
FECC	fires and effects coordination center
FMF	Fleet Marine Forces
FRAGO	fragmentary order
G-2	assistant chief of staff, intelligence/intelligence staff section
G-3	assistant chief of staff, operations and training/operations and training staff section
G-4	assistant chief of staff, logistics/logistics staff section
G-6	assistant chief of staff, communications/communications system staff section
GCE	ground combat element
GLOC	ground line of communications
HHQ	higher headquarters
HQMC	Headquarters, United States Marine Corps
HVI	high-value individual
IADS	integrated air defense system
ICC	information coordination center
IEAA	information environment advanced analysis
IPB	intelligence preparation of the battlespace
ISR	intelligence, surveillance, and reconnaissance
ITCC	information tasking and coordination cycle
ITCO	information tasking and coordination order
IWG	information working group
J-2	intelligence directorate of a joint staff
J-6	communications systems directorate of a joint staff
JEMSO	joint electromagnetic spectrum operations
JFC	joint force commander
JIPOE	joint intelligence preparation of the operational environment

JP	joint publication
JTF	joint task force
KLE	key leader engagement
LCE	logistics combat element
MAGTF	Marine air-ground task force
MARFOR CYBERCOM	Marine Forces Cyber Command
MARFORSOC	Marine Forces Special Operations Command
MARFOR SPACECOM	Marine Forces Space Command
MCA	malicious cyberspace activity
MCCOG	Marine Corps Cyberspace Operations Group
MCDP	Marine Corps doctrinal publication
MCEN	Marine Corps Enterprise Network
MCIC	Marine Corps Information Command
MCIOC	Marine Corps Information Operations Center
MCPP	Marine Corps Planning Process
MCRP	Marine Corps reference publication
MCTP	Marine Corps tactical publication
MCWP	Marine Corps warfighting publication
MEB	Marine expeditionary brigade
MEF	Marine expeditionary force
MEU	Marine expeditionary unit
MIG	Marine expeditionary force information group
MILDEC	military deception
MISO	military information support operations
MLR	Marine littoral regiment
MOE	measure of effectiveness
MOP	measure of performance
MRT-C	mission-relevant terrain in cyberspace
MSC	major subordinate command
NATO	North Atlantic Treaty Organization
NGO	nongovernmental organization

OCO	offensive cyberspace operations
OIE	operations in the information environment
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PIR	priority intelligence requirement
PNT	positioning, navigation, and timing
PRC	People’s Republic of China
PSYOP	psychological operations (forces)
S-2	intelligence officer/office
S-3	operations and training officer/office
SATCOM	satellite communications
SIGINT	signals intelligence
SIGMAN	signature management
TAA	target audience analysis
TAC-D	tactical deception
TTP	tactics, techniques, and procedures
US	United States
USD(P)	Undersecretary of Defense for Policy
USG	United States Government
USCYBERCOM	United States Cyber Command
USSPACECOM	United States Space Command
VEO	violent extremist organization

Section II: Terms and Definitions

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (DoD Dictionary)

area of operations

An operational area defined by a commander for the land or maritime force commander to accomplish their missions and protect their forces. Also called **AO**. (DoD Dictionary)

assessment

1. A continuous process that measures the overall effectiveness of employing capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. (DoD Dictionary; parts 1 and 2 of a 4-part definition.)

attack

An offensive action characterized by coordinated movement, supported by fire, conducted to defeat, destroy, or capture the enemy and/or secure key terrain. (USMC Dictionary)

audience

In public affairs, a broadly-defined group that contains stakeholders and/or publics relevant to military operations. (DoD Dictionary)

battle damage assessment

(See DoD Dictionary for core definition. Marine Corps amplification follows.) The timely and accurate estimate of the damage resulting from the application of military force. Battle damage assessment estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. Also called **BDA**. (USMC Dictionary)

battle rhythm

A deliberate, daily schedule of command, staff, and unit activities intended to maximize use of time and synchronize staff actions. (DoD Dictionary)

battlespace

The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, and/or accomplish the mission. It includes the air, land, maritime, and space domains); the information environment and cyberspace domain; the electromagnetic spectrum; and other factors. Included within these are friendly, enemy, adversary, and neutral entities contained within or having an effect on the operational areas, areas of interest, and areas of influence. (USMC Dictionary)

campaigning

The persistent conduct of related operations, activities, and investments that align military actions with the other instruments of national power, supporting global integration across the competition continuum in pursuit of strategic objectives. (DoD Dictionary)

center of gravity

(See DoD Dictionary for core definition. Marine Corps amplification follows.) A key source of strength without which an enemy cannot function. Also called **COG**. (USMC Dictionary)

civil affairs

Designated Active Component and Reserve Component forces and units organized, trained, and equipped specifically to conduct civil affairs operations and to support civil-military operations. Also called **CA**. See also civil-military operations. (DoD Dictionary)

civil affairs operations

Actions planned, coordinated, executed, and assessed to enhance awareness of, and manage the interaction with, the civil component of the operational environment; identify and mitigate underlying causes of instability within civil society; and/or involve the application of functional specialty skills normally the responsibility of civil government. Also called **CAO**. (DoD Dictionary)

civil-military operations

Activities of a commander performed by designated military forces that establish, maintain, influence, or exploit relations between military forces and indigenous populations and institutions by directly supporting the achievement of objectives relating to the reestablishment or maintenance of stability within a region or host nation. Also called **CMO**. See also civil affairs. (DoD Dictionary)

collateral damage

A form of collateral effect that causes unintentional or incidental injury or damage to persons or objects that would not be lawful military targets in the circumstances ruling at the time. (DoD Dictionary)

collateral effect

Unintentional or incidental effect to objects that would not be lawful military targets in the circumstances ruling at the time. (DoD Dictionary)

collection

(See DoD Dictionary for core definition. Marine Corps amplification follows.) The gathering of intelligence data and information to satisfy the identified requirements. (USMC Dictionary)

collection plan

A systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements. (DoD Dictionary)

combatant command

A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Also called **CCMD**. (DoD Dictionary)

combatant command (command authority)

Nontransferable command authority, which cannot be delegated, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Also called **COCOM**. (DoD Dictionary)

combat assessment

The determination of the overall effectiveness of force employment during military operations. Also called **CA**. (DoD Dictionary)

combat camera

Specially-trained expeditionary forces from Service-designated units capable of providing high-quality directed visual information during military operations. Also called **COMCAM**. (DoD Dictionary)

combat operations center

The primary operational agency required to control the tactical operations of a command that employs ground and aviation combat, combat support, and logistics combat elements or portions thereof. The combat operations center continually monitors, records, and supervises operations in the name of the commander and includes the necessary personnel and communications to do the same. Also called **COC**. (USMC Dictionary)

combat power

The total means of destructive and disruptive force that a military unit/formation can apply against an enemy at a given time. (DoD Dictionary)

combined

A term identifying two or more forces or agencies of two or more allies operating together. See also joint. (DoD Dictionary)

combined arms

1. The full integration of combat arms in such a way that to counteract one, the enemy must become more vulnerable to another. 2. The tactics, techniques, and procedures employed by a force to integrate firepower and mobility to create a desired effect upon the enemy. (USMC Dictionary)

command

1. The authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. 2. An order given by a commander. 3. A unit or units, an organization, or an area under the authority of one individual. (DoD Dictionary)

command and control

(See DoD Dictionary for core definition. Marine Corps amplification follows.) The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. Command and control is one of the seven Marine Corps warfighting functions. Also called **C2**. (USMC Dictionary)

commander’s critical information requirement

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decision making. The two subcategories are priority intelligence requirements and friendly force information requirements. Also called **CCIR**. (USMC Dictionary)

commander’s intent

(See DoD Dictionary for core definition. Marine Corps amplification follows.) A commander’s clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement that guides the exercise of initiative in the absence of instructions. (USMC Dictionary)

command relationships

The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command.. (DoD Dictionary)

component

1. One of the Service or functional subordinate organizations that constitutes a joint force. 2. In logistics, a part or combination of parts having a specific function, which can be installed or replaced only as an entity. (DoD Dictionary)

concept of operations

A verbal or graphic statement that clearly and concisely expresses what the commander intends to accomplish and how it will be done using available resources. Also called **CONOPS**. (DoD Dictionary)

condition

1. Those variables of an operational environment or situation in which a unit, system, or individual operate and that may affect performance. 2. A physical or behavioral state of a system that is necessary for the achievement of an objective. (DoD Dictionary)

constraint

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Something that must be done that limits freedom of action. Constraints are included in the rules of engagement, commander’s guidance, or instructions from higher headquarters. See also restraint. (USMC Dictionary)

control

1. Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (DoD Dictionary, part 1 of a 4-part definition)

coordination

The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (USMC Dictionary)

counterreconnaissance

All measures taken to prevent hostile observation of a force, area, or place. (USMC Dictionary)

course of action

1. Any sequence of activities that an individual or unit may follow. 2. A scheme developed to accomplish a mission. Also called **COA**. (DoD Dictionary)

critical information

Specific facts about friendly intentions, capabilities, and activities needed by an enemy or adversary for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (DoD Dictionary)

cyberspace

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. (DoD Dictionary)

cyberspace exploitation

Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations. (DoD Dictionary)

cyberspace operations

The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Also called **CO**. (DoD Dictionary)

deceive

To manipulate an enemy into believing and acting upon something that is not true for a selected period of time and/or at a particular location to create a friendly advantage. (USMC Dictionary)

deny

(See DoD Dictionary, denial measure, for core definition. Marine Corps amplification follows.) To hinder or prevent the enemy from using terrain, space, personnel, supplies, facilities, and/or specific capabilities. (USMC Dictionary)

dissemination

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Conveyance of intelligence to users in a suitable form. (USMC Dictionary)

doctrine

Fundamental principles by which the Marine Corps forces or elements thereof guide their actions across the range of military operations in support of national objectives. It is authoritative but requires judgment in application. (USMC Dictionary)

effect

1. The physical or behavioral state of a system that results from an action, a set of actions, or another effect. 2. The result, outcome, or consequence of an action. 3. A change to a condition, behavior, or degree of freedom. (DoD Dictionary)

electromagnetic attack

Division of electronic warfare involving the use of electromagnetic 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. Also called **EA**. (DoD Dictionary)

electromagnetic hardening

Actions taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. (DoD Dictionary)

electromagnetic interference

Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. Also called **EMI**. (DoD Dictionary)

electromagnetic protection

Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Also called **EP**. (DoD Dictionary)

electromagnetic spectrum management

The operational, engineering, and administrative procedures to plan and coordinate operations within the electromagnetic operational environment. (DoD Dictionary)

electromagnetic spectrum operations

Coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment. Also called **EMSO**. (JP 3-85)

electromagnetic support

Division of electromagnetic warfare involving 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 electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Also called **ES**. (DoD Dictionary)

electromagnetic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. (DoD Dictionary)

end state

The set of required conditions that defines achievement of the commander's objectives. (DoD Dictionary)

entity

Within the context of targeting, a term used to describe facilities, individuals, virtual (nontangible) things, equipment, or organizations. (DoD Dictionary)

exploitation

(See the DoD Dictionary, part 3, for core definition. Marine Corps amplification follows.) An offensive operation, following a successful attack, designed to disorganize the enemy in depth and extend the initial success of the attack by preventing the enemy from disengaging, withdrawing, and reestablishing an effective defense. (USMC Dictionary)

external audience

In public affairs, all people who are not Untied States military members, Department of Defense civilian employees, and their immediate families. See also internal audience. (DoD Dictionary)

fires

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight. Fires is one of the seven warfighting functions. See also warfighting functions. (USMC Dictionary)

fire support coordination center

A single site in which centralized communications facilities and personnel incident to the coordination of all forms of fire support for Marine Corps forces are located. Also called **FSCC**. (DoD Dictionary)

Fleet Marine Forces

Those combined arms forces and the integral supporting elements thereof whose primary missions are to participate in combat and other operations as lawfully assigned. These forces may be task-organized as Marine air-ground task forces or as a Service component under a combatant command and include the Marine Corps Reserve, Marine Corps security forces at Navy shore activities, Marine Corps integral supporting elements, and Marine Corps combat forces not otherwise assigned. Also called **FMF**. (USMC Dictionary)

force

1. An aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof. (DoD Dictionary)

force protection

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. Force protection is one of the seven Marine Corps warfighting functions. Also called **FP**. (USMC Dictionary)

fragmentary order

(See DoD Dictionary for core definition. Marine Corps amplification follows.) An abbreviated form of an operation order, usually issued on a day-to-day basis, that eliminates the need for restating information contained in a basic operation order. It may be issued in sections. Also called **FRAGO**. (USMC Dictionary)

freedom of navigation

Actions conducted to protect United States navigation, overflight, and related interests on, under, and over the seas. (DoD Dictionary)

function

The specific responsibilities assigned by the President and Secretary of Defense to enable Services to fulfill legally established roles. (USMC Dictionary)

host nation

A nation which receives forces and/or supplies from allied nations and/or North Atlantic Treaty Organization to be located on, to operate in, or to transit through its territory. Also called **HN**. (DoD Dictionary)

imagery

A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (DoD Dictionary)

indicator

1. In intelligence usage, an item of information that reflects the intention or capability of an enemy and/or adversary to adopt or reject a course of action. 2. In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. 3. In the context of assessment, a specific piece of information that infers the condition, state, or existence of something, and provides a reliable means to ascertain performance or effectiveness. (DoD Dictionary)

influence

To cause the enemy to behave in a manner favorable to friendly forces. (USMC Dictionary)

information

The actions taken to generate, preserve, deny, or project informational power to increase and protect competitive advantage or combat power potential within all domains of the operational environment. Information is one of the seven warfighting functions. See also warfighting functions. (This term and definition are approved for use and will be included in the next edition of the USMC Dictionary.)

information environment

The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information. Also called **IE**. (DoD Dictionary)

integration

In intelligence usage, the application of the intelligence to appropriate missions, task, and functions. (DoD Dictionary)

intelligence

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Knowledge about the enemy or the surrounding environment needed to support decision-making. Intelligence is one of the seven Marine Corps warfighting functions. (USMC Dictionary)

intelligence cycle

A six-step process by which information is converted into intelligence and made available to users. The six steps are planning and direction, collection, processing and exploitation, production, dissemination, and utilization. (USMC Dictionary)

intelligence operations

The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. (DoD Dictionary)

intelligence preparation of the battlespace

The systematic, continuous process of analyzing the threat and environment in a specific geographic area. Also called **IPB**. (USMC Dictionary)

intelligence requirement

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called **IR**. (USMC Dictionary)

intelligence, surveillance, and reconnaissance

1. An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors; assets; and processing, exploitation, and dissemination systems in direct support of current and future operations. 2. The organizations or assets conducting such activities. Also called **ISR**. (DoD Dictionary)

internal audience

In public affairs, United States military members and Department of Defense civilian employees and their immediate families. See also external audience. (DoD Dictionary)

joint

Organizations, activities, or missions in which two or more significant elements Military Departments operate under a single joint commander or leader. (DoD Dictionary)

joint doctrine

Fundamental principles and standardized terminology the guide the employment of United States military forces in coordinated action toward a common objective and may include tactics, techniques, and procedures. (DoD Dictionary)

joint electromagnetic spectrum operations

Military actions undertaken by a joint force to exploit, attack, protect, and manage the electromagnetic environment. Also called **JEMSO**. (DoD Dictionary)

joint force

A force composed of significant elements, assigned or attached, of two or more Military Departments that operate under a single joint force commander. (DoD Dictionary)

joint force commander

A general term applied to a combatant commander, subunified commander, or joint task force commander. Also called **JFC**. (DoD Dictionary)

joint function

A grouping of capabilities and activities that enable joint force commanders to synchronize, integrate, and direct joint operations. (DoD Dictionary)

joint operation

(See DoD Dictionary, joint operations, for core definition. Marine Corps amplification follows.) An operation carried on by a force that is composed of significant elements of the Army, the Navy or the Marine Corps, and the Air Force, or two or more of these Services operating under a single commander authorized to exercise unified command or operational control over joint forces. *(Note: A Navy/Marine Corps operation is not a joint operation.)* (USMC Dictionary)

joint staff

1. The staff of a commander of a unified or specified command, subordinate unified command, joint task force, or subordinate functional component (when a functional component command will employ forces from more than one Military Department), that includes members from the several Services comprising the force. 2. (capitalized as Joint Staff) The staff under the Chairman of the Joint Chiefs of Staff that assists the Chairman and the other members of the Joint Chiefs of Staff in carrying out their responsibilities. Also called **JS**. (DoD Dictionary)

joint task force

A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subordinate unified commander, or an existing joint task force commander to accomplish a specific mission. Also called **JTF**. (DoD Dictionary)

leverage

(See DoD Dictionary for core definition. Marine Corps amplification follows.)Exploiting action, power, or influence from an external source to gain an advantage. (USMC Dictionary)

link

1. A behavioral, physical, or functional relationship between nodes. 2. In communications, a general term used to indicate the existence of communications facilities between two points. 3. A maritime route, other than a coastal or transit route, that connects any two or more routes. (DoD Dictionary)

maneuver

(See DoD Dictionary for core definition. Marine Corps amplification follows.) The movement of forces for the purpose of gaining an advantage over the enemy. Maneuver is one of the seven Marine Corps warfighting functions. (USMC Dictionary)

Marine Corps forces

The amalgamation of personnel, materiel, and support elements that comprises the Marine Corps. These forces (formally identified as Fleet Marine Forces in Title 10) include the Regular Marine Corps, the Fleet Marine Corps Reserve, and the Marine Corps Reserve. (MCRP 1-10.2)

Marine Corps Planning Process

A six-step methodology that helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the mission and the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of problem framing, course of action development, course of action war game, course of action comparison and decision, orders development, and transition. Also called **MCPP**. *(Note: Tenets of the MCPP include top-down planning, single-battle concept, and integrated planning.)* (USMC Dictionary)

military deception

Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called **MILDEC**. (DoD Dictionary)

military information support operations

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Also called **MISO**. (DoD Dictionary)

mission

1. The essential task or tasks, together with the purpose, that clearly indicates the action to be taken and the reason for the action. 2. The dispatching of one or more aircraft to accomplish one particular task. (DoD Dictionary)

neutral

In combat and combat support operations, an identity applied to a track whose characteristics, behavior, origin, or nationality indicate that it is neither supporting nor opposing friendly forces. (DoD Dictionary)

neutralize

1. As it pertains to military operations, to render ineffective or unusable. 2. As a tactical task, render the enemy or enemy resources ineffective or unusable. (USMC Dictionary)

node

2. In communications and computer systems, the physical location that provides terminating, switching, and teleport access services to support information exchanges. 3. An element of a network that represents a person, place, or physical object. (DoD Dictionary, parts 2 and 3 of a 3-part definition)

objective

1. The clearly defined, decisive, and attainable goal toward which an operation is directed. 2. The specific goal of the action taken which is essential to the commander's plan. (DoD Dictionary)

observable

In military deception, the detectable result of the combination of an indicator within an adversary's conduit intended to cause action or inaction by the deception target. (DoD Dictionary)

offensive cyberspace operations

Missions intended to project power in and through cyberspace. Also called **OCO**. (DoD Dictionary)

operation

1. A sequence of tactical actions with a common purpose or unifying theme. (JP 1, Vol 1) 2. A military action or the carrying out of a military mission. (DoD Dictionary)

operational approach

A broad description of the mission, operational concepts, tasks, and actions required to accomplish the mission. (DoD Dictionary)

operational area

An overarching term encompassing more descriptive terms (such as area of responsibility and joint operations area) of locations for the conduct of military operations. Also called **OA**. (DoD Dictionary)

operational control

The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Also called **OPCON**. (DoD Dictionary)

operational environment

A aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Also called **OE**. (DoD Dictionary)

operation order

A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. Also called **OPORD**. (DoD Dictionary)

operation plan

A complete and detailed plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment list. Also called **OPLAN**. (DoD Dictionary)

phase

(See DoD Dictionary for core definition. Marine Corps amplification follows.) A planning and execution tool that is used to divide an operation in duration or activity. A change in phase may involve a change in task or task organization. Phasing helps in planning and controlling and may be indicated by time, distance, terrain, or occurrence of an event. (USMC Dictionary)

priority intelligence requirement

(See DoD Dictionary for core definition. Marine Corps amplification follows.) An intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. Also called **PIR**. (USMC Dictionary)

public

In public affairs, a segment of the population with common attributes to which a military force can tailor its communication. (DoD Dictionary)

public affairs

Communication activities with external and internal audiences. Also called **PA**. (DoD Dictionary)

public affairs guidance

Constraints and restraints established by proper authority regarding public communication activities. Also called **PAG**. (DoD Dictionary)

reconnaissance

A mission undertaken to obtain information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, geographic, or other characteristics of a particular area, by visual observation or other detection methods. (DoD Dictionary)

relevant actor

Individual, group, population, or automated system whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action. (DoD Dictionary)

scheme of maneuver

The central expression of the commander's concept for operations that governs the development of supporting plans or annexes of how arrayed forces will accomplish the mission. (DoD Dictionary)

sensor

Equipment that detects, and may indicate, and/or record objects and activities by means of energy or particles emitted, reflected, or modified by objects. (USMC Dictionary)

shaping

The use of lethal and nonlethal activities to influence events in a manner that changes the general condition of war to an advantage. (USMC Dictionary)

situational awareness

Knowledge and understanding of the current situation that promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decision-making. An informational perspective and skill that fosters an ability to quickly determine the context and relevance of events that are unfolding. (NTRP 1-02)

space domain

The area above the altitude where atmospheric effects on airborne objects become negligible. (DoD Dictionary).

staff estimate

A continual evaluation of how factors in a staff section's functional area support and impact the planning and execution of the mission. (DoD Dictionary)

strategy

An idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and multinational objectives. (DoD Dictionary)

stakeholder

In public affairs, an individual or group that is directly impacted by military operations, actions, and/or outcomes, and whose interests positively or negatively motivate them toward action. (DoD Dictionary)

support

1. The action of a force that aids, protects, complements, or sustains another force in accordance with a directive requiring such action. 2. A unit that helps another unit in battle. 3. An element of a command that assists, protects, or supplies other forces in combat. (DoD Dictionary)

supported commander

1. The commander having primary responsibility for all aspects of a task assigned. 2. In the context of joint planning, the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff. 3. In the context of a support command relationship, the commander who receives assistance from another commander, and who is responsible for ensuring the supporting commander understands the assistance required. (DoD Dictionary)

surveillance

(See DoD Dictionary for core definition. Marine Corps amplification follows.) The systematic visual or aural observation of an enemy force, adversary, named area of interest, or an area and the activities within it to collect intelligence required to confirm or deny enemy and adversary courses of action or identify their critical vulnerabilities and limitations. (USMC Dictionary)

synchronization

1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In intelligence usage, application of intelligence sources and methods in concert with the operation plan to answer intelligence requirements in time to influence the decisions they support. (DoD Dictionary)

synchronization matrix

A format for the staff to record results of wargaming and synchronize the course of action across time, space, and purpose in relation to an enemy's and/or adversary's course of action. (MCRP 1-10.2)

system

A functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements that form a unified whole. (DoD Dictionary)

target

An entity or object that performs a function for the threat considered for possible engagement or other action. (DoD Dictionary)

target audience

An individual or group selected for influence. Also called **TA**. (DoD Dictionary)

target development

The systematic examination of potential target systems and their components, individual targets, and even elements of targets to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objectives. (DoD Dictionary)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (DoD Dictionary)

target list

Those targets maintained and promulgated by the senior echelon of command that are to be engaged by supporting arms, as distinguished from a “list of targets” (confirmed, suspected, or possible) maintained by any echelon for informational and planning purposes. (USMC Dictionary)

task

A clearly defined action or activity specifically assigned to an individual or organization, or derived during mission analysis, that must be accomplished. (DoD Dictionary)

tasking

The process of translating the allocation into orders and passing these orders to the units involved. Each order normally contains sufficient detailed instructions to enable the executing agency to accomplish the mission successfully. (USMC Dictionary)

techniques

1. Non-prescriptive ways or methods used to perform missions, functions, or tasks. 2. The general and detailed methods used by troops and/or commanders to perform assigned missions and functions; specifically, the methods of using equipment and personnel. (USMC Dictionary)

unit

1. Any military element whose structure is prescribed by competent authority. 2. An organization title of a subdivision of a group in a task force. (DoD Dictionary)

unity of effort

Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization that is the product of successful unified action. (DoD Dictionary)

visual information

Various visual media with or without sound that generally includes still and motion photography, audio video recording, graphic arts, and visual presentations. Also called **VI**. (DoD Dictionary)

vulnerability

1.The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system that can cause it to be degraded (incapability to perform the designated function or mission) as a result of being subjected to certain level of effects in an unnatural (man-made) hostile environment. (DoD Dictionary)

warfighting functions

The seven mutually supporting military activities integrated in the conduct of all military operations. The seven Marine Corps warfighting functions are command and control, fires, force protection, information, intelligence, logistics, and maneuver. (USMC Dictionary)

wargaming

A step-by-step process of action, reaction, and counteraction for visualizing the execution of each friendly course of action in relation to enemy and adversary courses of action and reactions. It explores the possible branches and sequels to the primary plan resulting in a final plan and decision points for critical actions. (USMC Dictionary)

weapon system

A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (DoD Dictionary)

working group

An enduring or ad hoc organization within a headquarters consisting of a core functional group and other staff and component representatives whose purpose is to provide analysis on the specific function to users. Also called **WG**. (DoD Dictionary)

REFERENCE AND RELATED PUBLICATIONS

Federal Issuances

UN Charter Article 2(4) and Article 51

1967 Outer Space TreatyExecutive Order 12333, *United States Intelligence Activities*

United States Code

Title 10 US Code Armed Forces

44 U.S.C. Public Printing and Documents

44 U.S.C. Chapter 31 Records Management by Federal Agencies

44 U.S.C. Chapter 33 Disposal of Records

USC 3093 MILDEC

Department of Defense Issuances

Department of Defense Directives

DoDD 2000.13	Civil Affairs
DoDD 5100.46	Foreign Humanitarian Assistance

Department of Defense Instructions

DoDI 3607.02	Military Information Support Operations
DoDI 5400.13	Public Affairs (PA) Operations
DoDI 5040.02	Visual Information
DoDI 5040.07	Visual Information Productions
DoDI 5330.03	Single Manager of DoD Document Services

Chairman of the Joint Chiefs of Staff

Chairman of the Joint Chiefs of Staff Instruction

CJCSI 3370.01D	Target Development Standards
CJCSI 3110.5	Military Information Support Operations
CJCSI 3205.01D	Joint Combat Camera

Chairman of the Joint Chief of Staff Manual

CJCSM 3108.01 Joint Fires Element

Joint Publications

1	Joint Personnel Support
1, Volume 1	Joint Warfighting
2-0	Joint Intelligence
3-0	Joint Campaigns and Operations
3-04	Information in Joint Operations
3-09	Joint Fires Support
3-12	Cyberspace Operations
3-13.2	Military Information Support Operations
3-13.3	Operations Security
3-13.4	Military Deception
3-14	Joint Space Operations
3-25	Joint Countering Threat Network
3-57	Civil-Military Operations
3-60	Joint Targeting
3-61	Public Affairs
3-85	Joint Electromagnetic Spectrum Operations
4-0	Joint Logistics
5-0	Joint Planning
6-0	Joint Communications

Miscellaneous

Department of Defense Dictionary of Military and Associated Terms
Joint Doctrine Note 1-19, Competition Continuum
National Defense Strategy (2018)
Joint All-Domain Command and Control (JADC2) Strategy (2021)
Joint Guide for Joint Intelligence Preparation of the Operational Environment
Civilian Harm Mitigation and Response Action Plan (CHMR-AP), 2022

Navy Publications

Naval Doctrine Publication (NDP)

1	Naval Warfare

Marine Corps Publications

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-0	Marine Corps Operations, w/change 1,2,3
1-1	Strategy
1-2	Campaigning
1-4	Competing
2	Intelligence
4	Logistics
5	Planning
6	Command and Control
8	Information

Marine Corps Warfighting Publications (MCWPs)

2-10	Intelligence Operations
3-20	Aviation Operations
3-30	Marine Air-Ground Task Force Command and Control
3-31	Marine Air-Ground Task Force Fires
5-10	Marine Corps Planning Process

Marine Corps Tactical Publications (MCTPs)

3-02A	Network Engagement: Targeting and Engaging Networks
3-03A	Marine Air-Ground Task Force Civil-Military Operations
3-20C	Antiair Warfare
3-20D	Offensive Air Support
3-20E	Assault Support
3-20F	Control of Aircraft and Missiles
3-20G	Air Reconnaissance
3-30A	Command and Staff Action
3-30F	Marine Corps Public Affairs
3-32A	Marine Air Ground Task Force Combat Camera
3-32B	Operations Security

Marine Corps Reference Publications (MCRPs)

1-10.1	Organization of the United States Marine Corps
2-10B.1	Intelligence Preparation of the Battlespace
3-20F.2	Marine Tactical Air Command Center Handbook

3-20F.5	Direct Air Support Center Handbook
3-20F.6	Tactical Air Operations Center Handbook
3-30B.2	MAGTF Communications System
3-31.6	Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower
3-32D.1	Electronic Warfare

Marine Corps Miscellaneous

Marine Corps Supplement to DoD Dictionary of Military and Associated Terms

Air Force Publications

Air Force Doctrinal Publication (AFDP)

3-99	The Department of the Air Force Role in Joint All Domain Operations

Air Force Miscellaneous Publications

US Department of the Air Force, Memorandum: USAF Operating Concept for Information Warfare, Washington, D.C.,March 30, 2022

US Air Force, Air Combat Command, COMACC Intent for Information Warfare, July 2, 2022

US Air Force Headquarters, Headquarters Air Force Operations in the Information Environment Strategic Plan 2022-2026

Miscellaneous Publications

Handbook for Tactical Operations in the Information Environment, RAND Corporation (2021)

Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art During Multi-Domain Operations, Cyber Defense Review, Fall 2021

The Causes of War (New York: The Free Press, 1973)

Marine Corps Gazette ““National Instruments and Warfighting Functions, A view of information” October, 2023, Vol. 107 No. 10. (www.mca-marines.org/gazette)