USMC

MCTP 3-30C

Rear Operations

U.S. Marine Corps

Limited Dissemination Control: None. Approved for Public Release

PCN 147 000102 00

USMC

A no-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 to the Doctrine Branch at:

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

or by email to: usmc_doctrine@usmc.mil

Please include the following information in your correspondence:

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

Copyright Information

UNITED STATES MARINE CORPS

21 May 2026

FOREWORD

Marine Corps Tactical Publication 3-30C, *Rear Operations*, captures best practices for integrating Marine forces into joint security operations. It outlines critical frameworks for establishing command and control, organizing joint security areas, and categorizing threat levels specific to rear area security. It addresses both the evolving nature of threats and the need for coordinated operations with joint and host-nation forces. This publication also provides assessment tools Marines can use to ensure effective, adaptable security measures that align with joint force objectives.

This publication is intended for Marine air-ground task force commanders and staff responsible for executing rear operations. It is a foundational document that assists in planning, executing, and assessing rear operations.

Reviewed and approved this date.

B. K. Grayson
Colonel, U.S. Marine Corps
Commanding Officer
Marine Corps Tactics and Operations Group

Publication Control Number: 147 000102 00

Limited Dissemination Control: None. Approved for Public Release.

This publication does not implement any allied standardization agreements.

Table of Contents

CHAPTER 1. JOINT SECURITY OPERATIONS

CHAPTER 2. COMMAND AND CONTROL

CHAPTER 3. REAR OPERATIONS

CHAPTER 4. REAR AREA THREAT

CHAPTER 5. ASSESSMENT

Glossary

References

CHAPTER 1.
JOINT SECURITY OPERATIONS

The Marine Corps serves a vital role in joint security operations (JSO), leveraging its rapid-response capabilities and its experience in diverse environments to protect joint forces, bases, and critical infrastructure. These operations involve coordination with other Services, multinational or coalition forces, and host-nation elements to ensure secure movement and functionality of personnel, equipment, and logistics networks.

Joint security operations encompass a range of activities from base defense and convoy security, to countering threats from individual actors to large-scale enemy forces. The Marine Corps' proficiency in amphibious operations, rapid deployment, and sustained operations make it a key component of these efforts, ensuring a comprehensive approach to security.

FUNDAMENTAL SECURITY MISSIONS

Joint security operations are coordinated efforts conducted by multiple military branches and international partners to protect military units, bases, and strategic locations (e.g., airfields and supply routes) from various threats. Marines conducting these operations ensure that the joint force can effectively and safely carry out its missions by safeguarding personnel, equipment, and facilities from attacks or disruptions.

Joint security operations can involve the participation of US military forces, multinational forces, third-country national forces, and host nation security forces. For more information on JSO, see Joint Publication (JP) 3-10, *Joint Security Operations in Theater.*

Joint Security Area

A joint security area (JSA) is a designated zone, typically outside the United States, where military forces work together to protect critical locations and lines of communication. These areas can include bases, supply routes, airfields, and seaports. The main purpose of a JSA is to provide a secure environment for military operations by coordinating defense efforts among Services and, often, international partners. A JSA is established based on the nature of the threat, type and scope of the mission, and the size of the operational area it supports. See Figure 1-1 for a notional structure of a JSA.

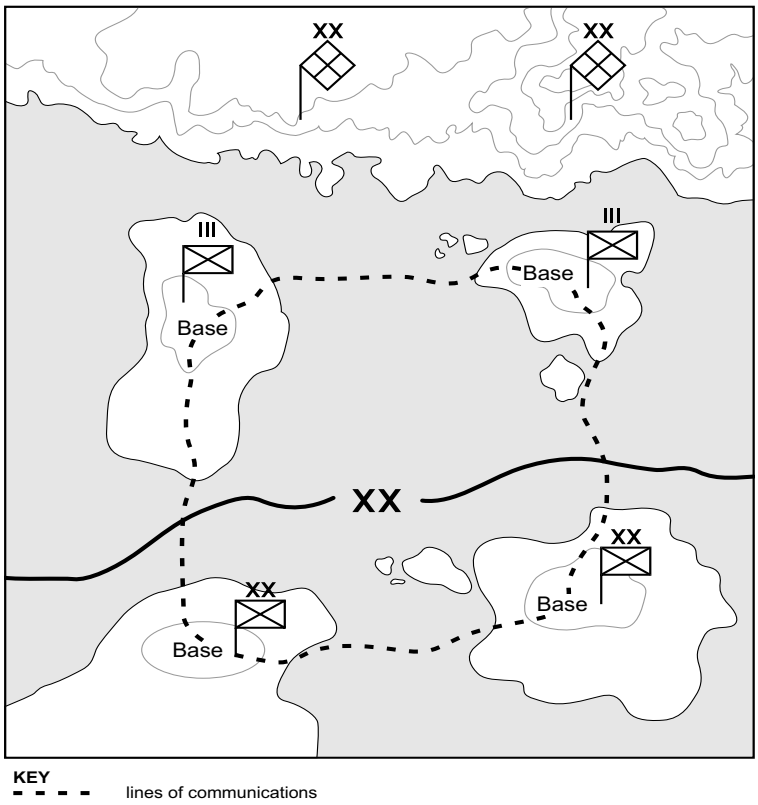


Figure 1-1. Notional Structure of a Joint Security Area.

Locations. A JSA can include enduring locations, contingency locations, lines of communication, or other designated areas outside the US and its territories. These locations are delineated as follows:

- Enduring Locations. Long-term military bases or facilities established in strategic areas to support ongoing operations and missions, providing stability and sustained presence in a region.
- Contingency Locations. Temporary military bases set up to support specific missions or operations, often in response to immediate needs or emergencies.
- Lines of Communications. Routes (e.g., roads, railways, airways, and waterways) used to transport troops, equipment, and supplies necessary for military operations.

For more information on joint contingency locations, see JP 4-04, *Contingency Basing*.

Command and Control for Joint Security Operations

Command and control (C2) for JSO involves establishing a structured system in which commanders coordinate and direct security efforts across different units within the JSA. The joint force commander (JFC) designates specific areas for security, delegates authority to subordinate commanders, and ensures effective communication and collaboration among all participating forces. This system includes setting up command centers, defining roles and responsibilities, and integrating efforts to respond quickly and efficiently to any threats. The goal of command and

control is to maintain a secure operational environment through organized and unified command. A JFC may delegate certain authorities to a joint security coordinator (JSC). A JSC establishes a joint security coordination center (JSCC).

Joint Security Coordination Center

A JSCC is a command facility established to manage and coordinate all JSO within a designated area. It serves as the hub for planning, directing, and overseeing joint security efforts, ensuring effective communication and cooperation among military units and allied forces. The JSCC integrates intelligence, monitors threats, allocates resources to maintain security, responds swiftly to incidents, and adapts to changing conditions to protect personnel, bases, and lines of communication.

Command Relationships

Within a JSCC, command relationships are structured to ensure clear lines of authority and efficient coordination among military units. The JFC delegates security responsibilities to subordinate commanders, who then manage JSO within their designated areas. The JSC oversees these operations, ensuring all participating forces, including base and tenant unit commanders, work together seamlessly. This structure allows for effective C2 and facilitates unified efforts to maintain security and respond to threats promptly. See Figure 1-2.

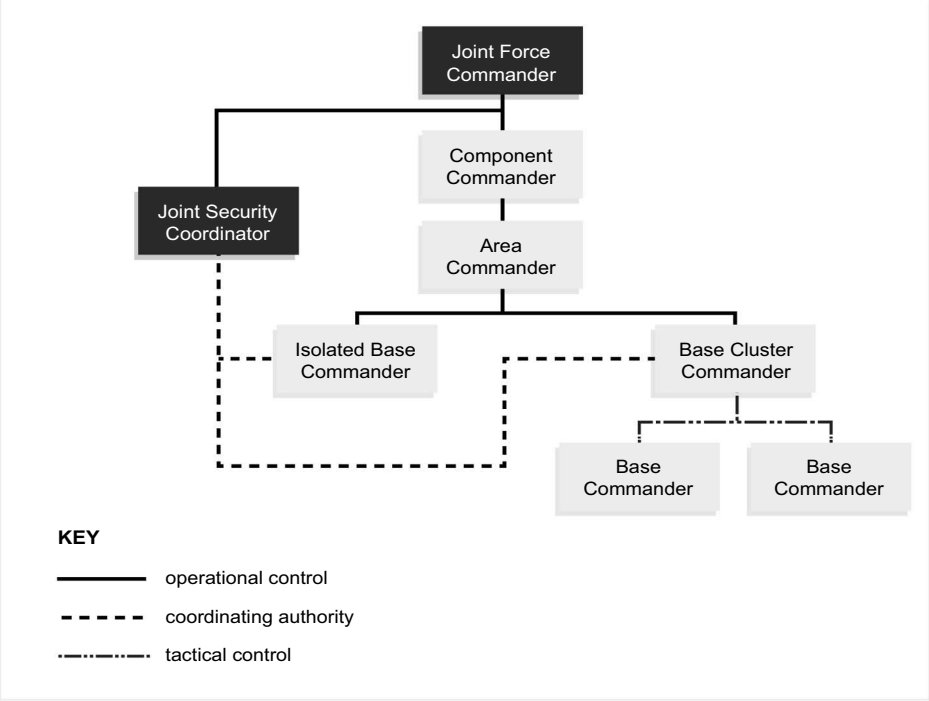


Figure 1-2. Notional Joint Security Coordinator Relationships.

Operation Centers

Operation centers are command facilities where military leaders monitor, coordinate, and direct ongoing operations. These centers serve as the central hubs for managing various aspects of

military activities, including security, logistics, and communications. Key types of operation centers for JSO include the following:

- Joint Security Coordination Center. Manages and coordinates all security operations within a designated area.
- Base Defense Operations Center. Focuses on security and defense within a specific base.
- Base Cluster Operations Center. Oversees the security of a group of geographically close bases, integrating their defense plans.

These centers ensure effective communication, resource allocation, and rapid response to emerging threats or operational changes.

Threat Levels for Joint Security Operations

Threat levels for JSO are categorized into three distinct levels to guide appropriate security responses:

- Level I Threats. These include activities such as espionage, sabotage, subversion, assassination, and bombing attacks typically conducted by foreign intelligence entities and terrorists. They often involve individual actors or small groups using improvised weapons or tactics.
- Level II Threats. These involve small-scale, well-coordinated attacks from forces that can cause significant disruptions. Examples include hit-and-run attacks, roadside or vehicle-borne improvised explosive devices (IEDs), weaponized unmanned aircraft system (UAS), and ambushes using standoff weapons, such as mortars and rockets.
- Level III Threats. These are large-scale threats where enemy forces can project significant combat power, such as airborne, air assault, or amphibious operations. A substantial military response is required for level three threats, often involving tactical combat forces (TCFs) to counter these advanced threats.

Key Personnel Responsibilities When Conducting Joint Security Operations

The effectiveness of JSO relies on the coordinated efforts of key personnel who manage and execute security measures across various levels and areas. These individuals are responsible for overseeing security within the JSA, coordinating with multiple military units and agencies, and responding to different threat levels. Their roles ensure comprehensive protection for military personnel, bases, and critical infrastructure. Key personnel include the JFC, JSC, base commander, base cluster commander, tenant unit commanders, TCF commander, operations officer, intelligence officer, and force protection officer, each with specific duties that contribute to the overall security mission.

The JFC—

- Designates JSAs.
- Establishes C2 relationships.
- Delegates authority to subordinate commanders to ensure effective security operations.

- Coordinates overall security efforts within the operational area.
- Ensures the security posture supports broader mission objectives.

The JSC—

- Oversees security within the JSA and is usually a flag officer.
- Establishes and operates the JSCC.
- Coordinates with various forces and agencies to maintain a secure environment.
- Integrates security efforts across different components, as authorized by the JFC.
- Ensures comprehensive protection measures are in place.

The base cluster commander—

- Coordinates security for a group of bases within a specific area.
- Ensures defense plans are integrated and complementary.
- Oversees the base cluster operations center.
- Collaborates with higher command and adjacent units to maintain security.

The base commander—

- Manages security operations within the base boundary.
- Coordinates with other commanders and security forces.
- Has tactical control over forces conducting base defense missions.
- Ensures all security measures are effectively implemented within their area of responsibility.

The tenant unit commanders—

- Ensure the internal security of their units.
- Participate in overall base defense plans.
- Provide necessary personnel, equipment, and facilities to support base defense operations.
- Advise the base commander on defense matters specific to their units.

The TCF commander—

- When designated, leads rapidly deployable combat units to counter Level III threats within the JSA.
- Coordinates with other commanders and security elements to respond to significant threats exceeding the capabilities of standard security forces.
- Is operational control (OPCON) to the commander designated by the JFC–typically the area or base commander–to ensure unity of command and the effective employment of forces.

The operations officer—

- Serves as the principal advisor to the TCF commander on operational matters.
- Directs operations within the operations center.
- Develops security force training and exercise plans.
- Monitors current operations.
- Ensures synchronization of efforts in line with the commander's intent.

The intelligence officer—

- Supervises the TCF intelligence section personnel.
- Provides intelligence updates and input on situation reports.
- Coordinates with higher-level intelligence organizations.
- Conducts threat analysis to inform security operations.

The force protection officer—

- Advises the TCF commander on all force protection, antiterrorism, and emergency services matters.
- Integrates signature management principles into force protection planning and operations.
- Conducts vulnerability assessments to enhance the base's security posture.

CHAPTER 2.
COMMAND AND CONTROL

MARINE CORPS COMMAND OF JOINT SECURITY OPERATIONS

Command Structure

The Marine Corps does not maintain a permanently task-organized unit specifically for JSO. Instead, when tasked by a JFC to conduct JSO, the Marine Corps creates a purpose-built task force tailored to the mission's requirements. The JSO's command structure is designed to ensure cohesive and effective control of these tasks. This structure is centered around several key elements, including, the JSC, the Marine air-ground task force (MAGTF), and its subordinate command elements, all working in unison to achieve mission objectives. For more information on command structure, see Marine Corps Tactical Publication (MCTP) 3-30A, *MAGTF Command and Staff Action.*

Joint Security Coordinator. Upon receiving a directive from the JFC, the Marine Corps Service component commander appoints a flag officer to serve as the JSC. This officer is responsible for overseeing the integration and coordination of security operations across various units and Services, ensuring a unified and effective approach to mission execution.

For example, during major combat operations for OPERATION INHERENT RESOLVE (OIR) in Iraq from 2014 to 2021, the commander of Al Asad Airbase executed the function of the JSC for that JSA. Acting as the area commander, he used the base defense operations center (BDOC) to synchronize the security efforts of all tenant forces, which included US Army base defense units, Marine Corps elements from the Special Purpose MAGTF, and US Air Force airfield security personnel. The commander, acting as the JSC, actively deconflicted patrol routes, integrated intelligence feeds, and established unified rules of engagement. When the base was attacked, the JSC directed a coordinated response, synchronizing counter-rocket systems and dispatching a designated quick reaction force to ensure the security of the entire installation and all personnel within it.

Special Purpose MAGTF. The JSC establishes a purpose-built MAGTF tailored specifically for the JSO's mission. The size and composition of the MAGTF are determined by the assessed threat level. For Level I or II threats, a MAGTF might not be required. A Level III threat, however, necessitates a fully integrated MAGTF, comprising the following elements:

- Command Element. Provides overall command and control of JSO, including headquarters, communications, intelligence assets, and specialized information capabilities.
- Ground Combat Element. Executes ground operations, delivering the primary combat power through infantry, artillery, and specialized assets tailored to JSO.

- Aviation Combat Element. Provides air support, including close air support, reconnaissance, and air defense, using aircraft, equipment, and associated personnel.
- Logistics Combat Element. Ensures logistical support, including transportation, supply, maintenance, general engineering, services, and health services necessary to sustain JSO.

Subordinate Elements. Within the MAGTF, there are several subordinate elements that have crucial roles in JSO. These elements ensure that the MAGTF functions efficiently and effectively:

- Security Forces. These units provide a range of ground security operations, including static security for key infrastructure and personnel, mobile patrols to deter threats and maintain visibility, and response forces to address developing incidents. These forces conduct security assessments, implement access control measures, and enforce security regulations within the JSA.
- Aviation Units. These units provide aviation capabilities that are crucial for JSO. This includes aerial patrols for surveillance and reconnaissance, providing real-time situational awareness to ground forces. Aviation assets also offer rapid-response capabilities that facilitate quick reaction to emerging threats and evacuations.
- Logistics Units. These units ensure the continuous flow of essential resources to sustain all aspects of JSO. This encompasses transportation of personnel and equipment, supply chain management for food, water, fuel, and ammunition, maintenance services to keep equipment operational, and comprehensive health support ranging from routine care to emergency treatment and evacuation.
- Specialized Units. These can include intelligence, explosive ordnance disposal, civil affairs and other support units tailored to specific security tasks. These units enhance the MAGTF's capability to address diverse security challenges.
- Liaison Officers. Liaison officers are embedded within host-nation forces and other allied units to facilitate coordination and communication, ensuring JSOs are synchronized, and all relevant parties are informed and engaged.

Employing this structured approach, the Marine Corps ensures that JSOs are managed effectively, with clear lines of authority and communication, enabling a unified and coordinated effort in maintaining security and accomplishing the mission objectives.

Operations Centers

Joint Security Coordination Center. The Marine Corps designated JSC establishes a JSCC. The JSCC is responsible for executing JSOs per the JFCs guidance. The JSC organizes subordinate operations centers that can include a MAGTF combat operations center (COC) and a rear area operations center (RAOC).

MAGTF Command Operations Center. The MAGTF COC serves as the central hub for units to conduct command and control for all joint security operations within the JSC’s area of responsibility. Key functions of the COC include the following:

- Centralized Command and Control. The COC provides a centralized location for the MAGTF command element to monitor, direct, and coordinate security operations.
- Intelligence and Communications. The COC facilitates real-time intelligence gathering, analysis, and dissemination to ensure situational awareness and informed decision making.

- Operational Planning and Execution. The COC is responsible for developing and executing operational plans, integrating efforts across different MAGTF elements to achieve mission objectives.
- Crisis Response Coordination. The COC manages crisis-response activities, coordinating the deployment of rapid reaction forces and other resources to address security incidents and emerging threats.

Rear Area Operations Center. The RAOC is tasked to oversee security and support operations in the rear areas of the operational theater. Key responsibilities of the RAOC include:

- Rear Area Security Management. The RAOC coordinates all aspects of rear area security, including base defense, convoy security, and protection of critical infrastructure.
- Coordination with Support Units. The RAOC coordinates with logistical, medical, and engineering units to ensure the seamless integration of support operations with security efforts.
- Threat Monitoring and Response. The RAOC continuously monitors threats to the rear area and coordinates appropriate response actions to mitigate risks and ensure the safety of personnel and assets.
- Support to Forward Operations. The RAOC provides essential support to forward operations by securing lines of communication and supply routes, enabling sustained operations.

ARMY COMMAND OF JOINT SECURITY OPERATIONS

Command Structure

The command structure for the Army's execution of JSO is designed to ensure comprehensive and effective management of security tasks. This structure leverages the capabilities of the JSC, the Army's Maneuver Enhancement Brigade, and various subordinate command elements to maintain order and achieve mission objectives. See Field Manual (FM) 3-81, *Maneuver Enhancement Brigade,* for more information.

Joint Security Coordinator. Similar to the Marine Corps, the Army appoints a flag officer as the JSC upon receiving a directive from the JFC. This officer is responsible for the integration and coordination of security operations across various units and Services, ensuring a unified approach to mission execution.

Maneuver Enhancement Brigade. The maneuver enhancement brigade is a critical component of the Army's structure for conducting JSO. It is designed to provide the necessary support and security functions to enhance the maneuverability and operational effectiveness of joint forces. Key aspects of the unit include the following:

- Command and Control. The headquarters element provides robust C2 capabilities, enabling effective management of subordinate units and coordination with higher headquarters.
- Support Functions. The brigade headquarters integrates various support functions, including engineering, military police, chemical defense, and civil affairs, to ensure comprehensive security and support operations.

- Operational Flexibility. The brigade's modular structure allows it to be tailored to the specific needs of the mission, providing flexibility in task organization and resource allocation.
- Integration with Joint Forces. The maneuver enhancement brigade coordinates closely with other joint and coalition forces, ensuring interoperability and cohesive execution of JSO.

Subordinate Elements. The subordinate elements within the brigade play vital roles in executing the broader security mission. These elements ensure that the brigade operates effectively and efficiently across its various responsibilities:

- Battalion and Company Headquarters. These units provide command and control for their respective subordinate units, ensuring that tactical operations are carried out in accordance with the JSC's directives.
- Liaison Officers. Embedded within host nation forces and allied units, liaison officers facilitate communication and coordination, ensuring JSO are well-integrated and that all relevant parties are informed and engaged.
- Support Units. These include logistics, medical, and maintenance units that provide critical support to ensure the sustainability and effectiveness of security operations.

Operations Centers

Joint Security Coordination Center. The Army designated JSC will establish a JSCC. The JSCC is responsible for executing JSO per the JFC's guidance. The JSC organizes subordinate operations centers that can include a tactical operations center (TOC) and a RAOC.

Tactical Operations Center. The TOC is the primary command and control for the maneuver enhancement brigade. It serves as the focal point for planning, directing, and coordinating operations. Key responsibilities of the TOC include the following:

- Command and Control. The TOC provides a centralized location for the maneuver enhancement brigade commander and staff to conduct mission planning, monitor operations, and make critical decisions.
- Operational Planning. The TOC is responsible for developing operational plans, orders, and directives, ensuring all units understand and effectively execute their tasks.
- Situational Awareness. The TOC maintains real-time situational awareness through constant communication with subordinate units, higher headquarters, and adjacent units, ensuring a comprehensive understanding of the operational environment.
- Coordination and Communication. The TOC facilitates coordination with other Services, host-nation forces, and interagency partners, ensuring operations are unified and synchronized.

Rear Area Operations Center. The RAOC is crucial for managing and coordinating security and support operations in the rear areas. Its primary functions include the following:

- Rear Area Security. The RAOC oversees the security of critical infrastructure, supply routes, and bases in the rear area, coordinating with military police and other security forces to prevent and respond to threats.
- Logistical Support. The RAOC manages logistical operations, ensuring the timely and efficient movement of supplies, equipment, and personnel to support forward-deployed units.
- Emergency Response. The RAOC coordinates emergency response efforts, including medical evacuations, fire support, and disaster relief operations, ensuring quick and effective action during crises.
- Liaison and Coordination. The RAOC acts as a liaison with host-nation authorities, civilian organizations, and other military units, ensuring integrated and cooperative rear operations.

MARINE CORPS OR ARMY KEY RESPONSIBILITIES

Security

When tasked to command a JSO, the Marine Corps or Army is responsible for ensuring comprehensive security within the JSA. Specific responsibilities are as follows:

- Establishing Security Protocols. Developing and implementing detailed security plans, standing operating procedures, and protocols tailored to the specific operational environment.
- Assessing and Mitigating the Threat. Conducting continuous threat assessments to identify, evaluate, and mitigate potential risks and vulnerabilities, adapting security measures as necessary.
- Providing Force Protection. Ensuring that all personnel, equipment, and facilities are protected through active and passive security measures, including surveillance, patrols, and fortifications.
- Providing Incident Response. Organizing and deploying rapid-reaction forces to respond to security incidents, to neutralize threats, and to restore order.
- Establishing Signature Management. Implementing measures to minimize detectable signatures (e.g., visual, electronic, acoustic) that could compromise the security of personnel, equipment, and operations within the JSA.

Coordination with the Joint Force Commander

Effective coordination with the JFC is essential for the successful execution of JSO. Each Service's responsibilities include the following:

- Communication. Maintaining open and continuous communication with the JFC to ensure overarching mission objectives and directives are aligned.
- Reporting. Providing regular situation reports and intelligence updates to the JFC, keeping them informed of the security status and any significant developments.

- Resource Allocation. Requesting additional resources and support from the JFC as needed, ensuring that all units have the necessary assets to maintain security and respond to threats.
- Operational Synchronization. Ensuring that Marine Corps or Army security operations are fully integrated with the broader joint force efforts, supporting the overall strategy and mission goals.

Integration with Host-Nation Forces

Integrating with host-nation forces is crucial for enhancing the effectiveness of JSO. The Marine Corps or Army's responsibilities in this area include the following:

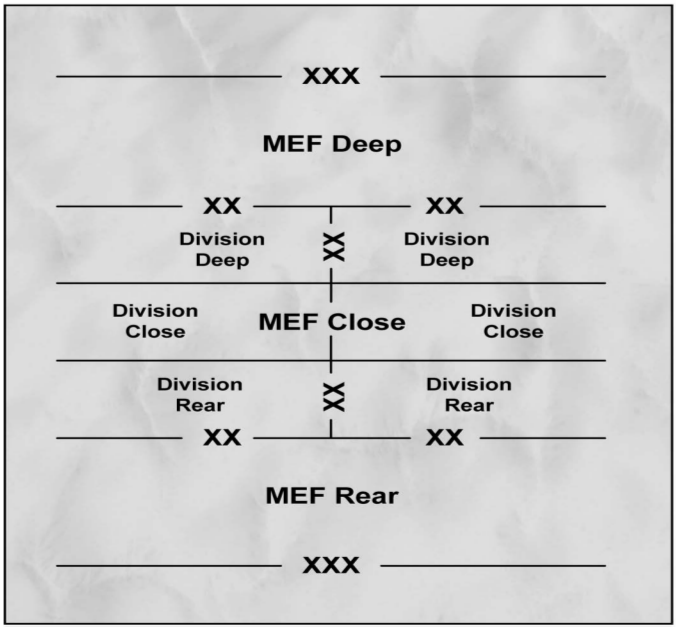
- Liaison and Coordination. Deploying liaison officers to work with host-nation military and security forces, facilitating communication and cooperation.
- Support and Assistance. Providing logistical, intelligence, and operational support to host-nation forces, including equipment, training, and advisory services to bolster security efforts.
- Cultural Awareness. Conducting operations with an understanding of and respect for the host nation’s cultural norms and practices, fostering positive relationships and mutual trust.

CHAPTER 3.
REAR OPERATIONS

Rear operations are essential to support and sustain combat forces engaged in deep and close battles. These operations, encompassing military actions conducted to enable force sustainment and provide security for those actions, focus on the rear area—the space extending from the command's rear boundary forward to the rear of its subordinate units' areas, primarily used for combat service support. Protecting this area, a critical function known as rear area security, involves preemptive, concurrent, and post-event measures to mitigate threats, such as airborne attacks, sabotage, infiltration, guerrilla activity, and psychological or propaganda warfare. By securing critical assets and facilitating logistical and operational activities within this protected rear area, rear operations enhance the force's operational reach and freedom of action, ultimately supporting the overall mission. For more information on rear area security, see Marine Corps reference publication, MCRP 3-30C.1, *MAGTF Rear Area Security.*

BATTLESPACE FRAMEWORK

The battlespace framework consists of three interconnected areas: deep, close, and rear. Each area serves a distinct purpose within a commander’s design plan, contributing to a cohesive and comprehensive approach to military operations. Understanding the purposes of deep, close, and rear operations is critical for effective planning and execution. These areas are interrelated and support one another. See Figure 3-1.



Legend
MEF Marine expeditionary force

Figure 3-1. Battlespace Framework.

Deep Operations

Deep operations are critical for shaping the battlespace because they strike at the enemy's key assets far from friendly forces. These operations aim to weaken the enemy's ability to sustain their combat efforts, create favorable conditions for subsequent operations, and disrupt their overall strategy. Actions Marines take during deep operations include the following:

- Disrupting enemy capabilities by targeting the enemy's critical assets such as command and control, reconnaissance assets, air defense systems, radar, and aviation assets.
- Degrading the enemy's combat power and creating opportunities for exploitation.
- Preventing enemy reinforcements by engaging forces and infrastructure deep in the battlespace to delay or prevent resupply.
- Coordinating long-range fires and strikes to achieve maximum impact on the enemy's depth of operations.
- Leveraging intelligence and reconnaissance to identify and prioritize high-value targets for strikes.
- Synchronizing close and rear operations to maintain a unified approach throughout the battlespace.

Close Operations

Close operations involve direct engagement with the enemy in the immediate area of operations. These operations are crucial for achieving tactical objectives and maintaining the momentum of the overall mission. When conducting close operations, Marines should consider—

- Seizing and holding key terrain to gain tactical and operational advantages.
- Destroying enemy forces by engaging and neutralizing enemy combat units to reduce their fighting capability.
- Protecting friendly forces by ensuring the safety and effectiveness of units through coordinated attacks and defensive actions.
- Maintaining momentum by sustaining offensive actions, preventing the enemy from regrouping and counterattacking.
- Coordinating with deep and rear operations to ensure unified efforts across the battlespace.
- Employing combined arms tactics to maximize the effectiveness of close engagements and destroy the enemy.

Rear Operations

Rear operations focus on maintaining the security and functionality of the rear area, which is essential for supporting deep and close operations. These operations ensure that the broader mission remains sustained and resilient. Actions Marines take during rear operations include the following:

- Providing continuous support by ensuring the steady flow of logistics, supplies, and reinforcements to engaged units.
- Securing critical infrastructure, including sustainment nodes, and other vital facilities, from enemy action.

- Facilitating operational mobility by managing transportation and movement within the rear area to enhance flexibility and responsiveness.
- Safeguarding troops and infrastructure against threats within the rear area.
- Coordinating with deep and close operation forces to maintain alignment and effective execution.
- Implementing robust communication networks to ensure reliable command and control throughout the battlespace.

REAR AREA FUNCTIONS

Rear operations encompass a broad range of essential functions that support the MAGTF's overall mission. These functions are crucial for maintaining operational effectiveness, ensuring the security and sustainment of forces, and enabling the smooth coordination and management of activities within the rear area. The eight functions of rear operations are security, communications, intelligence, sustainment, area management, movements, infrastructure development, and host-nation support. For more information on logistics functions that support the rear area, see MCTP 3-40B, *Tactical Logistics*.

Security

Rear area security is crucial for safeguarding personnel, materials, and facilities against potential threats. This function requires a comprehensive approach that integrates multiple layers of defense, proactive measures, and coordinated efforts to maintain a secure environment. Actions Marines might take when establishing rear area security include the following:

- Establishing and maintaining perimeter defense around critical facilities and installations through physical barriers, surveillance systems, and strategically positioned security forces to detect and deter unauthorized access.
- Implementing signature management measures to minimize electronic, visual, infrared, and acoustic signatures and reduce the risk of detection and targeting by adversary forces.
- Conducting active patrolling and surveillance activities to detect and respond to security breaches or suspicious activities.
- Maintaining security forces to respond swiftly to security incidents or attacks, ensuring rapid and effective responses to various threats, including direct assaults, sabotage, and infiltration attempts.
- Operating an RAOC as a centralized command center to coordinate all security activities, manage incident responses, and maintain communication with higher command echelons.
- Ensuring clearance of fires within the rear area to coordinate the use of firepower, preventing friendly fire incidents, and optimizing defensive operations safely and effectively.
- Managing airspace in the rear area to support defensive and operational needs, ensuring safe coordination, and preventing conflicts.

- Conducting personnel recovery operations to recover isolated, missing, detained, or captured personnel, including search and rescue missions and coordination with recovery forces.
- Implementing air defense measures to detect, track, and intercept incoming threats, protecting personnel and critical infrastructure from aerial attacks.

Communications

Effective communication is critical for the coordination and control of rear operations. This function includes establishing reliable communication networks, maintaining secure lines of communication, and ensuring interoperability among various units and command elements. Actions communications Marines might take in the rear area include the following:

- Establishing communication networks that are robust, that can withstand potential disruptions and include both wired and wireless communication systems.
- Implementing secure communications through encryption and other security measures to protect sensitive information from interception and cyberspace threats.
- Ensuring interoperability of communication systems across different units, branches, and allied forces to facilitate seamless coordination and information sharing.
- Maintaining alternative communication methods to ensure continuity in case primary systems fail.
- Coordinating with intelligence and security teams to monitor and counter any communication-related threats, including jamming and cyberspace attacks.

Intelligence

The intelligence function is vital for understanding the operational environment and anticipating potential threats to rear operations. This function includes the collection, analysis, and dissemination of intelligence to support decision making and enhance situational awareness. Actions intelligence Marines might take in the rear area include the following:

- Establishing intelligence networks that gather information from various sources, including human intelligence, signals intelligence, and imagery intelligence.
- Analyzing and processing intelligence to produce actionable insights that can inform tactical decisions.
- Disseminating intelligence to relevant command elements and units in a timely and secure manner, ensuring that information is accessible to those who need it.
- Implementing counterintelligence measures to identify and neutralize enemy intelligence activities, protecting sensitive information and operations.
- Coordinating intelligence efforts with allied and host-nation intelligence agencies to enhance the overall intelligence picture and support joint operations.

Sustainment

Sustainment activities ensure that the logistical support necessary to maintain operational effectiveness is continuously available in the rear area. This function includes managing resources, maintaining equipment, and providing essential services to support ongoing operations. Sustainment actions Marines might take in the rear area include the following:

- Managing the sustainment network to ensure efficient procurement, storage, and distribution of supplies, equipment, and materials required for operations.
- Conducting regular maintenance and repair of equipment and vehicles to ensure they remain operational and ready for use.
- Providing comprehensive health services to maintain the physical and mental well-being of personnel, including medical treatment, preventive care, and evacuation procedures.
- Coordinating transportation to move personnel, equipment, and supplies efficiently and securely to their destinations, ensuring timely support for all operational needs.
- Managing logistics-related communications to ensure that all sustainment activities are effectively coordinated and aligned with operational priorities.

Area Management

Area management involves the organization and utilization of space and resources in the rear area to support mission objectives. This function includes planning the layout of facilities, managing resources, and coordinating activities to ensure Marines can conduct efficient and effective operations. Actions Marines might take in area management include the following:

- Planning facility layouts to optimize space, enhance operational efficiency, and support the security and functionality of critical areas.
- Allocating resources and space according to operational priorities, ensuring that key functions have the necessary infrastructure and support to succeed.
- Coordinating activities across different units and functions within the rear area to prevent conflicts, reduce congestion, and ensure seamless operations.
- Implementing land use controls to manage the deployment of forces, equipment, and services, while maintaining flexibility for future adjustments.
- Monitoring and adjusting the area management plan as operational needs evolve, so that personnel conducting rear area operations can respond to changing requirements.

Movement

Movement involves the coordinated control and oversight of transporting forces, equipment, and supplies within and through the rear area. This function is critical when supporting operational objectives and ensuring the continuous flow of logistics. Actions Marines might take to support movement include the following:

- Managing movement control to ensure that personnel, equipment, and supplies are transported efficiently, safely, and in accordance with operational priorities.
- Planning and executing convoy operations with a focus on security measures, route planning, and coordination to protect convoys from potential threats and ensure timely delivery.
- Implementing traffic management strategies to regulate and direct traffic within the rear area, prevent congestion and facilitate smooth and orderly movement.
- Coordinating with security and intelligence elements to assess and mitigate movement risks.
- Maintaining flexibility in movement plans to adapt to changing operational needs or unexpected disruptions, ensuring that personnel and critical supplies reach their destinations without delay.

Infrastructure Development

Infrastructure development involves constructing, maintaining, and improving facilities in the rear area to support operational requirements. This function ensures that all necessary physical assets are in place to facilitate ongoing and future operations. Actions Marines might take to support infrastructure development include the following:

- Planning and constructing essential infrastructure, such as roads, airfields, storage facilities, and command centers, to support operational efficiency and logistical needs.
- Maintaining existing infrastructure to ensure its continued functionality, addressing wear and tear, and making necessary repairs or upgrades as needed.
- Implementing force protection measures during construction.
- Coordinating with engineering units and host-nation resources to leverage additional capabilities and expedite infrastructure projects.
- Ensuring flexibility in infrastructure development to adapt to changing operational requirements, including the ability to expand or reconfigure facilities as needed.

Host-Nation Support

Host-nation support involves leveraging host-nation resources, facilities, and services to enhance operational effectiveness and reduce the logistical burden on deployed forces. Actions Marines might take when conducting host-nation support include the following:

- Using host-nation resources such as supplies, transportation, and facilities to supplement operational needs and reduce the strain on military logistics.
- Establishing and maintaining effective coordination and liaison with host-nation authorities to facilitate smooth cooperation and timely support for ongoing operations.
- Integrating host-nation cultural and linguistic expertise to facilitate communication, foster positive relationships with local populations, and improve cooperation with local authorities.
- Fostering mutual understanding of legal and regulatory frameworks to avoid conflict and promote compliance with host-nation laws and policies.
- Developing contingency plans for varying levels of host-nation support to maintain operational continuity should the availability or reliability status of these resources change.
- Collaborating with civilian agencies and organizations through civil-military operations to enhance host-nation support and achieve mutual objectives.

For more information on civil-military operations, see MCRP 3-03A.2, *MAGTF Civil-Military Operations Planning.*

CHAPTER 4.
REAR AREA THREAT

In modern military operations, rear area security is critical to maintaining the effectiveness of the force. The threats Marine encounter while conducting rear area operation can vary in scale and complexity, requiring tailored responses from Marine units and the MAGTF. However, the MAGTF alone does not have the capability to address every type of threat. In many cases, coordination with joint and multinational forces is essential, particularly for multi-domain threats such as those in the space and cyberspace domains.

THREAT LEVELS

Chapter 1 introduced the three categories of threat levels: Level I, Level II, and Level III. To accurately assess and categorize these threats within the rear area, staff elements must conduct a thorough intelligence preparation of the battlespace. This process helps element staff determine the appropriate threat level. For more information on the intelligence preparation of the battlespace, see MCRP 2-10B.1, *Intelligence Preparation of the Battlespace*.

Level I Threats

Level I threats are typically low intensity, involving individual actors or small groups attempting to disrupt operations through acts such as espionage, sabotage, or small-scale terrorist attacks. These threats often remain covert, requiring keen situational awareness and effective counterintelligence measures. The clandestine nature of Level I threats makes detection difficult, but they often can be countered by local security forces and internal MAGTF resources. However, for more sophisticated espionage activities, joint force counterintelligence or other specialized support may be needed.

Level II Threats

Level II threats involve more coordinated and organized attacks that exceed the capacity of local forces to handle alone. These can include hit-and-run attacks, weaponized UAS, and vehicle borne IEDs targeting critical infrastructure or supply lines.

Although the MAGTF has capabilities to deal with many Level II threats, such as deploying TCFs or using counter-UAS technology, these operations might still require external support. Joint assets, such as air or cyberspace capabilities, can augment the MAGTF's response to standoff attacks and emerging UAS threats, particularly in situations where enemy forces operate across multiple domains.

Level III Threats

Level III threats pose a serious risk, involving large, organized enemy forces that could conduct mechanized assaults, airborne operations, or multi-domain attacks. These threats directly target rear operations, aiming to disrupt the overall operational effectiveness of the MAGTF.

A coordinated response involving the entire MAGTF—supported by artillery, air assets, and quick reaction forces—is often necessary to repel Level III threats. However, large-scale mechanized or multi-domain attacks may overwhelm organic MAGTF capabilities, requiring assistance from joint or coalition forces to maintain the operational integrity of the rear area. In particular, responding to space threats or extensive cyber-attacks will necessitate direct support from the joint force.

Domain and Environment Threats

Threats in the rear area emerge across various domains: land, maritime, air, space, cyberspace, and the electromagnetic spectrum environment. Each presents unique challenges, and the MAGTF must be able to address these threats through a combination of its organic capabilities and external support when necessary.

Land Domain

Land domain threats such as large-scale ground assaults, long-range artillery, surface-to-surface missile systems, insurgent activities, and ambushes, pose complex challenges. The enemy can use terrain to their advantage, using ambush tactics against convoys or sabotage against rear installations. Actions Marines might take to mitigate land threats include the following:

- Establish layered defenses with checkpoints, obstacles, surveillance, and sensors to secure key infrastructure.
- Conduct active ground and aerial reconnaissance patrols to detect enemy movements.
- Maintain security forces ready to respond to attacks on convoys or facilities.
- Employ camouflage, concealment, and light and noise discipline to minimize visual and acoustic signatures.
- Coordinate with the JFC for additional support in Level III threat environments when the scale of enemy attacks are likely to exceed the MAGTF's capability to defend.

Maritime Domain

Maritime threats focus on coastal installations, sea lanes, and logistics networks. These threats can include piracy, swarming boat attacks, and amphibious assaults. Ensuring maritime security is essential for maintaining logistical flow and defending critical naval assets. Actions Marines might take to mitigate maritime threats include the following:

- Use naval patrols, coastal radar, sensors, and barriers to detect and deter approaching maritime domain threats.
- Coordinate with naval units and joint force maritime assets to counter amphibious threats, such as enemy landing craft, unmanned surface vessels, or naval fires.

- Implement rapid response capabilities to intercept swarming boats or amphibious forces before the threat reaches critical infrastructure.
- Minimize detectability through radar and visual signature management techniques.

Air Domain

Air threats can involve manned or unmanned aircraft, including UAS used for surveillance or strikes. Rear area installations may be targeted by air-to-ground missiles or air raids aimed at disrupting operations. Actions Marines might take to mitigate air threats include the following:

- Establish a layered air defense system that integrates assets, such as radar, anti-aircraft systems, and surface-to-air missiles to engage both manned aircraft and UAS.
- Employ counter-UAS capabilities such as jammers and interceptors to neutralize UAS threats before they reach key assets.
- Manage aircraft electronic emissions and use appropriate camouflage and concealment techniques.
- Coordinate with joint force aviation; air superiority and integrated air defense could require the use of specialized resources beyond the MAGTF's organic capabilities.

For more information on control of aircraft and missiles, see MCTP 3-20F, *Control of Aircraft and Missiles.*

Space Domain

Space threats, such as physical attacks on satellite systems, challenge the MAGTF's ability to communicate, navigate, and gather intelligence. Adversaries can use anti-satellite weapons or jamming technologies to disrupt space operations. Adversaries can also use space systems to conduct intelligence, surveillance, and reconnaissance tasks against Marines conducting operations in rear areas. These disruptions and adversary operations can severely degrade the MAGTF's situational awareness and operational effectiveness. Actions Marines might take to mitigate the space threat include the following:

- Establish redundant communication systems that do not rely solely on space assets.
- Coordinate with joint space operations to monitor for potential space threats and protect critical satellite infrastructure.
- Minimize electromagnetic emissions to reduce the risk of detection and targeting by hostile space assets.
- Review satellite vulnerability windows when conducting rear operations.

> *NOTE:* The MAGTF has limited capacity to counter space threats independently and could require immediate integration with joint force capabilities to mitigate the loss of key satellite functions.

Cyberspace Domain

Cyberspace threats in rear operations target command networks, logistics systems, and critical infrastructure. Cyberspace attacks can disrupt operations by stealing data, compromising communications, or sabotaging logistical systems. Actions Marines might take to mitigate the cyberspace threat include the following:

- Maintain robust cyberspace security protocols, including encryption and firewalls, to safeguard communications and databases.
- Implement strict emissions control and operations security measures to minimize cyberspace vulnerabilities.
- Establish a dedicated cyberspace response team that can identify and mitigate attacks in real time.
- Coordinate with higher level cyberspace commands to address high-level threats that exceed the MAGTF's cyberspace defense capabilities, to maintain operational continuity in the event of sustained cyberspace attacks.

For more information on operations security, see MCTP 3-32B, *Operations Security*.

Electromagnetic Spectrum

Electromagnetic warfare threats involve jamming, spoofing, or attacking radar and communication systems. Such disruptions can degrade the MAGTF’s ability to conduct operations effectively, particularly in high-threat environments. Actions Marines might take to mitigate the electromagnetic threat include the following:

- Deploy electromagnetic warfare units to protect critical communication and radar systems from jamming or spoofing.
- Use radios and communications that are equipped with frequency-hopping and encryption capabilities to resist enemy interference.
- Control electromagnetic emissions to minimize detection and targeting.
- Employ countermeasures to mitigate hostile electromagnetic warfare activities.

When encountering advanced electromagnetic warfare threats, request higher headquarters assistance to ensure comprehensive electromagnetic protection and to maintain the integrity of communication systems during operations.

CHAPTER 5.
ASSESSMENT

OBJECTIVES OF REAR OPERATIONS ASSESSMENT

Conducting a rear operations assessment enables MAGTF elements operating in the rear area to remain resilient and responsive. This process evaluates the effectiveness of security measures, logistical support, and the readiness of support units to adapt to changes in the operational environment. Regular performance reviews allow commanders to make informed adjustments that strengthen rear area stability. Assessments also provide critical insights that influence command decisions, ensuring operations align with mission goals and evolving conditions. In cases where the MAGTF cannot address threats or operational gaps alone, assessments highlight where coordination with joint or coalition forces is required to maintain effectiveness across all domains.

KEY ASSESSMENT QUESTIONS

When assessing rear operations, commanders should ask key questions that guide performance, security, and readiness evaluations. These questions help commanders align rear operations with broader mission objectives and adapt to evolving challenges. Asking questions serves as a starting point to identify areas of concern and opportunities for improvement. Questions commanders can ask include the following:

- How effectively do rear operations support the MAGTF's mission?
- What changes in the operational environment affect rear area security?
- Are current security measures sufficient to counter identified threats?
- How well are logistical operations being executed, and where are the gaps?
- What are the primary causes of operational shortcomings or successes?
- What adjustments in rear operations are necessary to enhance mission success?

ASSESSMENT FRAMEWORK

Building an effective assessment framework requires a structured approach that evaluates rear operation activities. This framework should be flexible enough to adapt to specific mission needs and the operational environment. A clear, methodical process helps commanders collect

relevant data, analyze performance, and implement necessary improvements. See MCRP 5-10.1, *Multi-Service Tactics, Techniques, and Procedures for Operation Assessment,* for more information.

It is essential for commanders to define the assessment objectives. Objectives must align with overall mission goals and identify the key areas for evaluation. The scope of the assessment, including the size of the area, number of units, and complexity of operation, should be determined early in the planning phase. Identifying stakeholders, such as command elements, support units, and external agencies, ensures all perspectives are considered.

Next, collecting relevant data is critical. Operational data—such as patrol reports, incident logs, and logistics throughput—provides a complete picture of performance. Intelligence on enemy activity and local conditions should shape the assessment. Establishing key performance indicators, such as response times, unit readiness, and logistical efficiency, enables commanders to effectively measure performance.

Once data is gathered, it is analyzed. A trend analysis identifies patterns, such as recurring security breaches or logistical delays, while a gap analysis compares current performance to mission requirements. Conducting a root-cause analysis helps determine underlying factors contributing to these gaps, whether procedural, resource-based, or external threats.

Communicating assessment findings ensures that actionable recommendations are implemented. Reporting clearly summarizes key insights, while briefings to command elements and key stakeholders facilitate decision making. Establishing a feedback loop allows assessments to evolve as operational conditions change, ensuring the assessment process remains relevant.

Finally, implementing changes based on assessment findings is vital. Detailed implementation plans assign responsibilities, timelines, and resources, ensuring that recommended improvements lead to operational gains. Continuous monitoring evaluates the impact of changes, while iterative assessments maintain alignment with mission objectives and adapt to new challenges.

EXAMPLES OF ASSESSMENT INDICATORS

Security

Security indicators evaluate rear area protection measures. Indicators focus on patrol effectiveness, incident response, and overall readiness to respond to potential threats. Some examples of indicators that inform commanders on how effective security is include the following:

- Quantitative indicators include—
  - Number of security incidents reported per week.
  - Average time it takes to respond to security breaches (minutes).
  - Percentage reduction in threat incidents following changes in patrol and surveillance procedures.
  - Patrol coverage area (square kilometers) compared to identified threat areas.

- Qualitative indicators include—
  - Evaluation of patrol routes based on their effectiveness in preventing breaches.
  - Feedback from units on the preparedness and responsiveness of security forces.
  - Assessment of how well intelligence informs security planning and patrol effectiveness.
  - Effectiveness of signature management training and implementation across units.

Communications

Communications indicators measure the reliability and functionality of communication systems. These indicators ensure that communication protocols support effective command and control. Examples of indicators that support effective communications include the following:

- Quantitative indicators include—
  - Uptime of communication systems as a percentage of operational time.
  - Time taken to restore communication after outages (hours).
  - Number of successful transmissions compared to failed or interrupted communications.
- Qualitative indicators include—
  - Feedback from units regarding the clarity and reliability of communications during operations.
  - Evaluation of communication protocols during high-stress scenarios, such as emergencies or combat situations.
  - Assessment of interoperability among MAGTF communications and joint or coalition partners.

Intelligence

Intelligence indicators assess the enemy's effectiveness against rear operations. These indicators can shape decision making and operational planning. Examples of indicators that support informed decision making include the following:

- Quantitative indicators include—
  - Number of enemy attacks against friendly forces in rear area.
  - Percentage of high-value targets that are active in the rear area.
  - Time it takes the enemy to mass a platoon-sized element against the rear area.
- Qualitative indicators include—
  - Identification and evaluation of the enemy's composition and disposition.
  - Feedback from units on enemy activity in their area of responsibility.
  - Evaluation of intelligence-sharing mechanisms with joint or host-nation forces.

Sustainment

Sustainment indicators evaluate the efficiency of logistics and supply operation. Knowing these indicators helps ensure resources are delivered in a timely manner to support the mission.

Examples of indicators that support the sustainment function include the following:

- Quantitative indicators include—
  - Average throughput of supplies (tons per day).
  - Time it took distribute critical resources (fuel, ammunition) to units (hours or days).
  - Percentage of logistics requests fulfilled within mission requirements.
- Qualitative indicators include—
  - Feedback from units on resource shortages or delays and the affect this indicator had on operations.
  - Evaluation of coordination between rear area sustainment operations and forward units.
  - Assessment of how inventory management procedures support readiness and supply needs.

Area Management

Indicators in area management assess how terrain and infrastructure are used and maintained to support rear operations. These indicators focus on operational readiness and infrastructure maintenance. Examples of indicators that help units use terrain and infrastructure to gain advantages include the following:

- Quantitative indicators include—
  - Percentage of critical infrastructure maintained in operational condition.
  - Time required to repair damaged infrastructure (hours or days).
  - Number of terrain modifications (e.g., fortifications, access roads) completed during a specific time-frame.
- Qualitative indicators include—
  - Commanders' evaluation of how well Marines use the terrain to align with operational objectives.
  - Feedback from engineering units on the efficiency of terrain modifications.
  - Assessment of how terrain management improves operational flexibility and mobility.

Movement

Movement indicators determine how effective transportation and logistics coordination is in the rear area. These indicators help commanders assess the safety, timeliness, and efficiency of personnel and resource movement. Examples of indicators that can improve movement include the following:

- Quantitative indicators include—
  - Average delay in scheduled movements (minutes or hours).
  - Number of movement-related incidents (e.g., ambushes, IED strikes) reported per month.
  - Percentage of successful convoy missions completed on time.

- Qualitative indicators include—
  - Feedback from units on the coordination and deconfliction regarding movement schedules.
  - Evaluation of alternative routes units can use if primary routes are disrupted.
  - Commander assessment of the overall effectiveness of movement control.

Infrastructure Development

Infrastructure development indicators assess progress on construction and maintenance projects in the rear area. These indicators ensure that infrastructure supports operational needs and readiness. Examples of infrastructure development indicators include the following:

- Quantitative indicators include—
  - Percentage of infrastructure projects completed on time.
  - Number of facilities constructed or repaired per operational cycle.
  - Quality ratings of new infrastructure based on post-construction evaluations.
- Qualitative indicators include—
  - Commanders' assessment of how infrastructure improvements align with operational needs.
  - Feedback from users on the functionality and durability of new or upgraded facilities.
  - Evaluation of engineering support in meeting project timelines and requirements.

Host-Nation Support

Indicators for host-nation support evaluate the level and effectiveness of assistance provided by the host nation. These indicators acknowledge that host-nation cooperation contributes to mission success and operational integration. Examples of host-nation support indicators include the following:

- Quantitative indicators include—
  - Percentage of host-nation support requests fulfilled (logistics, intelligence, security).
  - Time taken to coordinate and receive host-nation resources (days or weeks).
  - Number of operations successfully completed with host-nation forces.
- Qualitative indicators include—
  - Feedback from commanders on the effectiveness of coordination with host-nation entities.
  - Evaluation of host-nation integration into MAGTF planning and operations.
  - Assessment of cultural and operational challenges encountered in host-nation collaboration.

GLOSSARY

Section I. Acronyms and Abbreviations

C2	command and control
COC	combat operations center
IED	improvised explosive device
JFC	joint force commander
JP	joint publication
JSA	joint security area
JSC	joint security coordinator
JSCC	joint security coordinator center
JSO	joint security operations
MAGTF	Marine air-ground task force
MCRP	Marine Corps reference publication
MCTP	Marine Corps tactical publication
RAOC	rear area operations center
TCF	tactical combat force
TOC	tactical operations center
UAS	unmanned aircraft system

Section II. Terms and Definitions

air domain

The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible. (DoD Dictionary)

assessment

A continuous process that measures the overall effectiveness of employing capabilities during military operations. (Part 1 of a 4-part definition.) (DoD Dictionary)

aviation combat element

The core element of a Marine air-ground task force (MAGTF) that is task-organized to conduct aviation operations. The aviation combat element (ACE) provides all or a portion of the six Marine aviation functions necessary to accomplish the MAGTF's mission. It typically comprises an aviation unit headquarters and various other aviation units or their detachments. It can vary in size from a small aviation detachment of specifically required aircraft to one or more Marine aircraft wings. In a joint or multinational environment, the ACE may contain other Service or multinational forces assigned or attached to the MAGTF. The ACE itself is not a formal command. Also called **ACE**. See also Marine air-ground task force; Marine aviation functions; special purpose Marine air-ground task force.air-ground task force. (USMC Dictionary)

base cluster operations center

A command and control facility that serves as the base cluster commander's focal point for defense and security of the base cluster. (DoD Dictionary)

base defense operations center

A command and control facility established by the base commander to serve as the focal point for defense and security of the base cluster. (DoD Dictionary)

close operations

Military actions conducted to project power decisively against enemy forces that pose an immediate or near-term threat to the success of current battles or engagements. These military actions are conducted by committed forces and their readily available tactical reserves, using maneuver and combined arms. See also deep operations; rear operations. (USMC Dictionary)

combat operations center

The primary operational agency that controls tactical operations for commands that employ ground, aviation, logistics, and aviation elements, and combat support elements. Also called the **COC**. (USMC 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 warfighting functions. Also called **C2**. (USMC Dictionary)

command element

The core element of a Marine air-ground task force (MAGTF) that is the headquarters. The command element is composed of the commander, general or executive and special staff sections, headquarters section, and requisite communications support, intelligence, and reconnaissance forces, necessary to accomplish the MAGTF's mission. The command element provides command and control, intelligence, and other support essential for effective planning and execution of operations by the other elements of the MAGTF. The command element varies in size and composition. In a joint or multinational environment, it could contain other Service or multinational forces assigned or attached to the MAGTF. See also Marine air-ground task force; special purpose Marine air-ground task force. (USMC Dictionary)

contingency location

A non-enduring location outside of the United States that supports and sustains operations during contingencies or other operations and is categorized by mission life-cycle requirements as initial, temporary, or semipermanent. (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)

deep operations

Military actions conducted against enemy capabilities that pose a potential threat to friendly forces. These military actions are designed to isolate, shape, and dominate the battlespace and influence future operations See also close operations; rear operations. (USMC Dictionary)

electromagnetic warfare

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

enduring location

A main operating base, forward operating site, or cooperative security location designated by the Department of Defense for strategic access and use to support United States security interests for the foreseeable future. Also called **EL**. (DoD Dictionary)

explosive ordnance disposal

The process to detect, locate, access, diagnose, render safe/neutralize, recover, exploit, and dispose of explosive or improvised explosive threats. Also called **EOD**. (DoD Dictionary)

ground combat element

The core element of a MAGTF that is task-organized to conduct ground operations. It is usually constructed around an infantry organization but can vary in size from a small ground unit of any type to one or more Marine divisions that can be independently maneuvered under the direction of the MAGTF commander. It includes appropriate ground combat and combat support forces, and in a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the MAGTF. The ground combat element itself is not a formal command. Also called **GCE**. See also Marine air-ground task force; Marine aviation functions; special purpose Marine air-ground task force. (USMC Dictionary)

human intelligence

A category of intelligence derived from information collected and provided by human sources. Also called **HUMINT**. (DoD Dictionary)

imagery intelligence

The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. Also called **IMINT**. See also intelligence (DoD Dictionary)

intelligence

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. (Part 1 of a 3-part definition.) (DoD Dictionary)

joint force commander

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

joint security area

A specific area to facilitate protection of joint bases and their connecting lines of communications that support joint operations. Also called **JSA**. (DoD Dictionary)

joint security coordination center

A joint operations center tailored to assist the joint security coordinator in meeting the security requirements in the joint operational area. Also called **JSCC**. (DoD Dictionary)

joint security coordinator

The officer responsible for coordinating the overall security of the operational area in accordance with joint force commander directives and priorities. Also called **JSC**. (DoD Dictionary)

land domain

The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals. (DoD Dictionary)

logistics combat element

The core element of a Marine air-ground task force (MAGTF) that is task-organized to provide the combat service support necessary to accomplish the MAGTF's mission. The logistics combat element varies in size from a small detachment to one or more Marine logistics groups. It provides supply, maintenance, transportation, general engineering, health services, and other services to the MAGTF. In a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the MAGTF. The logistics combat element itself is not a formal command. Also called LCE. See also Marine air-ground task force; special purpose Marine air-ground task force. (USMC Dictionary)

Marine air-ground task force

The Marine Corps' principal organization for all missions across the range of military operations, composed of forces task-organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the Marine air-ground task force (MAGTF) are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a logistics combat element. The four core elements are categories of forces, not formal commands. The basic structure of the MAGTF never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs to be assigned. In a joint or multinational environment, other Service or multinational forces may be assigned or attached. Also called **MAGTF**. See also aviation combat element; command element; ground combat element; logistics combat element; special purpose Marine air-ground task force. (USMC Dictionary)

maritime domain

The oceans, seas, seabed, bays, estuaries, islands, coastal areas, rivers and littorals and the airspace above and the water below. (DoD Dictionary)

rear operations

Military actions conducted to support and permit force sustainment and to provide security for such actions. (USMC Dictionary)

signals intelligence

Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT**. (Part 2 of a 2-part definition.) (DoD Dictionary)

space domain

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

sustainment

The provision of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment. (DoD Dictionary)

tactical combat force

A rapidly deployable, air-ground, mobile combat unit with appropriate combat support and combat service support assets assigned to, and capable of, defeating Level III threats, including combined arms. Also called **TCF**. (DoD Dictionary)

unmanned aircraft system

That system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft. Also called **UAS**. (DoD Dictionary)

REFERENCES

Department of Defense Publications

Department of Defense Dictionary of Military and Associated Terms

Joint Publication (JPs)

3-10	Joint Security Operations in Theater
4-04	Contingency Basing

Marine Corps Publications

Marine Corps Tactical Publications (MCTPs)

3-30A	MAGTF Command and Staff Action
3-30F	Control of Aircraft and Missiles
3-32B	Operations Security
3-40B	Tactical Logistics

Marine Corps Reference Publications (MCRPs)

2-10B.1	Intelligence Preparation of the Battlespace
3-03A.2	MAGTF Civil-Military Operations
3-30C.1	MAGTF Rear Area Security
5-10.1	Multi-Service Tactics, Techniques, and Procedures for Operation Assessment

Miscellaneous Marine Corps Publication

Marine Corps Supplement to the DoD Dictionary of Military and Associated Terms

Army Publication

Field Manual (FM)

3-81	Maneuver Enhancement Brigade