Space Doctrine Publication 3-102

OPERATIONS IN THE INFORMATION ENVIRONMENT

DOCTRINE FOR SPACE FORCES

UNITED STATES

SPACE FORCE

Space Doctrine Publication (SDP) 3-102, *Operations in the Information Environment*
Space Training and Readiness Command (STARCOM)
OPR: STARCOM Delta 10
21 July 2025

Foreword

United States Space Force (USSF) doctrine guides the proper use of military spacepower in support of the Service's cornerstone responsibilities. It establishes a common frame of reference on the best way to plan and employ Space Force Guardians as part of a broader joint force. This doctrine provides official advice to execute and leverage spacepower. It is not directive—rather, it provides Guardians an informed starting point for decision making and strategy development.

SDP 3-102, *Operations in the Information Environment*, as operational doctrine for the Space Force, describes leveraging information to gain and exploit a position of advantage in the space domain, and in support of joint operations in all other domains.

Operations in the information environment (OIE) allow the joint force to shape the operational environment in all domains. These operations affect drivers of behavior by informing audiences; influencing foreign actors; and attacking and exploiting relevant actor information, information networks, and information systems. Every interaction in space between military, government, civil, and commercial entities creates a pattern of behavior to which relevant actors attribute meaning and intent. Space Force OIE intentionally shapes these perceptions to support joint force objectives and to establish and reinforce desired norms for actions in, from, and to the space domain.

I encourage you to study and learn from the information of our Service compiled in this volume. Semper Supra!

TIMOTHY A. SEJBA
Major General, USSF
Commander, Space Training and Readiness Command

Table of Contents

Figures

Space Force Doctrine

Space Force doctrine guides the proper use of spacepower and space forces in support of the Service's core functions. It establishes a common framework for employing Guardians as part of a broader joint force. Doctrine provides fundamental principles and authoritative guidance as an informed starting point for decision-making and strategy development. Since it is impossible to predict the timing, location, and conditions of the next fight, commanders should be flexible in the implementation of this guidance as circumstances or mission dictate.

The Space Force doctrine hierarchy includes four levels of doctrine and a glossary. Each level builds on the one above it, reflecting the role of Guardians in every specialty area. At the pinnacle is capstone doctrine, supported by six keystone doctrine publications. Below the keystone level, the Space Force is developing multiple operational level doctrine publications, each expanding on a specific area. Tactical doctrine provides details at the level of specific systems and tactics, techniques, and procedures, documented in a suite of tactical space operations procedures. As the mission evolves, the Space Force will add to the doctrine hierarchy.

Space Doctrine Publication (SDP) 3-102, *Operations in the Information Environment*, falls under the keystone doctrine publication SDP 3-0, *Operations*. It introduces a framework for Guardians to conduct and coordinate OIE. It emphasizes daily activities applicable to all Guardians. Additionally, it highlights how leveraging information activities in other domains supports and enhances space operations. This publication underscores the pivotal role of information in the Space Force's operational effectiveness.

- Chapter 1 presents foundational concepts and key terms for information as it relates to space operations, and their importance in shaping perceptions and behaviors. It also introduces the relationship between information and space operations.
- Chapter 2 captures the application of information forces in space and the contributions of information forces to attaining operational objectives.
- Chapter 3 discusses OIE in the planning process for space operations and how Guardians are integral to that process.
- Chapter 4 addresses the roles and responsibilities of commanders, staff, and every Guardian regarding information supporting space operations. It underscores the collaborative effort required to effectively manage and employ information as a strategic asset for space.

Chapter 1 – Introduction to Information for Space Operations

As described in Joint Publication 3-04, *Information in Joint Operations*, information is data in context to which a receiver assigns meaning. Humans use information to understand their environment, communicate, and make decisions. Information, and the meaning assigned to information, can affect the perceptions and behaviors of allies, partners, and adversaries. Understanding the factors that drive these perceptions and behaviors is essential to effective use of information for space operations. For space operations, this includes understanding how the adversary perceives action in, from, and to the space domain.

Information, one of the seven joint functions established in Joint Publication 3-0, *Joint Campaigns and Operations*, encompasses the management and application of information, and its deliberate integration with other joint functions across the competition continuum to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making. Therefore, the purpose of OIE is to shape perceptions and behaviors in ways to aid friendly objectives.

Key Terms for Information in Space Force Operations

a. **information**. Information is data in context to which a receiver assigns meaning. (Joint Publication 3-04, *Information in Joint Operations*)

b. **information advantage**. The operational advantage gained through the joint force's use of information for decision making and its ability to create effects on the information environment. (Joint Publication 3-04, *Information in Joint Operations*)

c. **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. (*Department of Defense (DoD) Dictionary of Military and Associated Terms* / Joint Publication 3-04, *Information in Joint Operations*)

d. **information forces.** Information forces are those Active Component and Reserve Component forces of the Services specifically organized, trained, and equipped to create effects in the information environment. These forces provide expertise and specialized capabilities that leverage information and can be aggregated as components of an OIE unit to conduct OIE. Information forces are available to the joint force through the request for forces process. (Joint Publication 3-04, *Information in Joint Operations*)

e. **operations in the information environment.** Military actions involving the integrated employment of multiple information forces to affect drivers of behavior. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-04, *Information in Joint Operations*)

Information in the Space Operations Across the Competition Continuum

The Space Force organizes, trains, equips, and presents Guardians as part of the joint force to conduct operations and protect the interests of the United States (US) and its allies in the space domain. Every Space Force activity, from spacecraft launches to maneuvering a spacecraft on orbit, conveys an intent that can support strategic national security activities and the objectives of the joint force. Adversaries may perceive the purpose of those same actions differently depending on the strategic context, to include current political tensions and other factors in the operational environment. The Space Force contributes to understanding and shaping the information environment across the competition continuum by exploiting information to enable, conceal, reveal, or protect space operations. Guardians, regardless of their mission or specialty, plan, resource, and apply informational power to enable integrated deterrence, build enduring advantages, compete against adversaries, and support allies and partners in the space domain. As part of joint all-domain operations, Guardians leverage a range of capabilities within the information environment to support space operations by:

a. Informing, engaging, and/or involving allies and partners.

b. Influencing key audiences.

c. Attacking, exploiting, and denying adversary information, information networks, and information systems.

d. Expanding, refining, and protecting friendly information, information networks, and information systems.

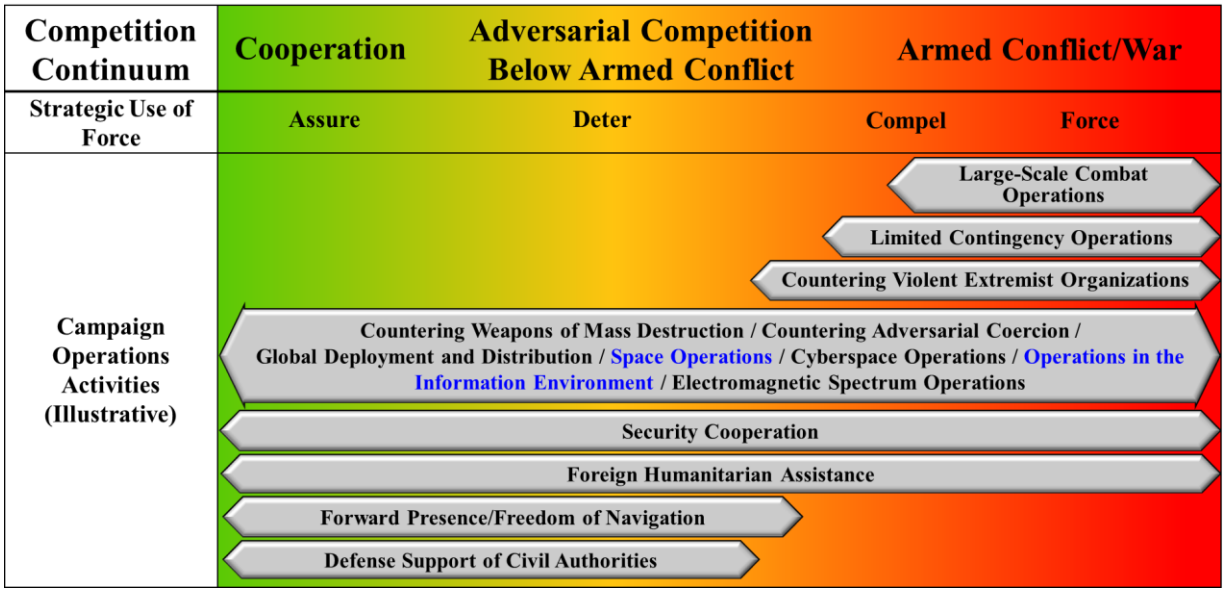

Figure 1. The competition continuum

The Space Force plays a crucial role in the dynamic landscape of warfare, where information is a potent asset across the competition continuum as depicted in figure 1. In a rapidly evolving

landscape, the ability to control and exploit the information environment enables effective operations in, from, and to the space domain. Space-based and terrestrial sensors offer the joint force a significant information advantage, to include unique access, range, and persistence. Space-enabled communication networks facilitate rapid and penetrative information transport across the physical domains, complementing terrestrial capabilities. Safeguarding advantages such as these is essential for the joint force to maintain information advantage.

Across all domains, the information environment directly affects joint operations. The collection, analysis, and dissemination (intentional or unintentional) of information to obtain desired outcomes is increasingly complex. While information environment scenarios in, from, and to the space domain can pose significantly different challenges from those encountered in other domains, the Space Force contributes to achieving an information advantage for the joint force and enables a relative advantage in decision-making in terms of:

a. Rapid and responsive collection and delivery of information in, from, and to the space domain to enhance the quality and timeliness of friendly decisions at all echelons and in all domains.

b. Conducting space operations to degrade adversary information systems or access.

c. Protecting and shaping delivery of friendly information to enable accurate decision making and shape the perspective of key audiences.

d. Disrupting or degrading adversary targeting processes.

The Space Force strives to develop every Guardian to enable information capabilities in, from, and to the space domain in support of joint all-domain operations by ensuring Guardians:

a. Recognize the informational qualities and observables (behaviors) inherent to space operations and how they can positively or negatively impact the overall operational environment.

b. Identify misinformation or manipulation of information that may result in errant actions by the Space Force in a joint operational environment.

c. Understand how actions in, from, and to space have strategic implications that shape allied, partner, commercial, civil, and adversary behavior.

d. Coordinate and deconflict operations in the information environment with other Services, the joint force, other DoD organizations and agencies, allies, and partners.

Guardians and Information

Every Guardian relies on information to accomplish their mission. As representatives of the Space Force and the United States, Guardians understand that their presence, posture, and actions always convey a message open to interpretation. Guardians, regardless of rank or organization, understand that every action or statement communicates a message to allies, partners, neutral parties, and adversaries. Each Guardian's approach to information should reflect this reality

every day, through practicing disciplined communication whether in an official capacity or personal exchanges, while employed in place, deployed, or on personal time.

The Space Force provides Guardians trained for positions supporting OIE. The Air Force provides additional support in the development and execution of activities in support of space operations. The Space Force is actively integrating OIE and knowledge of information forces into its culture. Part of this is the recognition that information or information sources can influence the capabilities at a commander's disposal.

Information Across the Competition Continuum

Instead of a binary world divided strictly between peace and war, the competition continuum (figure 1) portrays a reality characterized by ongoing competition, manifested through a blend of cooperation, competition below armed conflict, and armed conflict or war. These terms delineate the dynamic relationship between the United States and other strategically significant actors—be they states or non-state entities—in pursuit of specific policy objectives.

Information activities are inherent across the competition continuum and are critical in decision making. These activities allow commanders to monitor foreign states, volatile regions, and transnational issues to identify threats to US interests in time for senior leaders to respond effectively. Strategic messaging (figure 2) to our allies, partners, and adversaries is also a value tool in the mix of information activities.

Deterrence also applies across the competition continuum. Deterrence can create a human psychological effect and cognitive outcome that occurs within the minds of relevant actors, especially the key leaders and decision makers. OIE are key to deterring malign activities, disincentivizing adversaries from conducting operations, activities, and investments counter to US interests, and the identification, characterization, attribution, and countering of those activities and organizations.

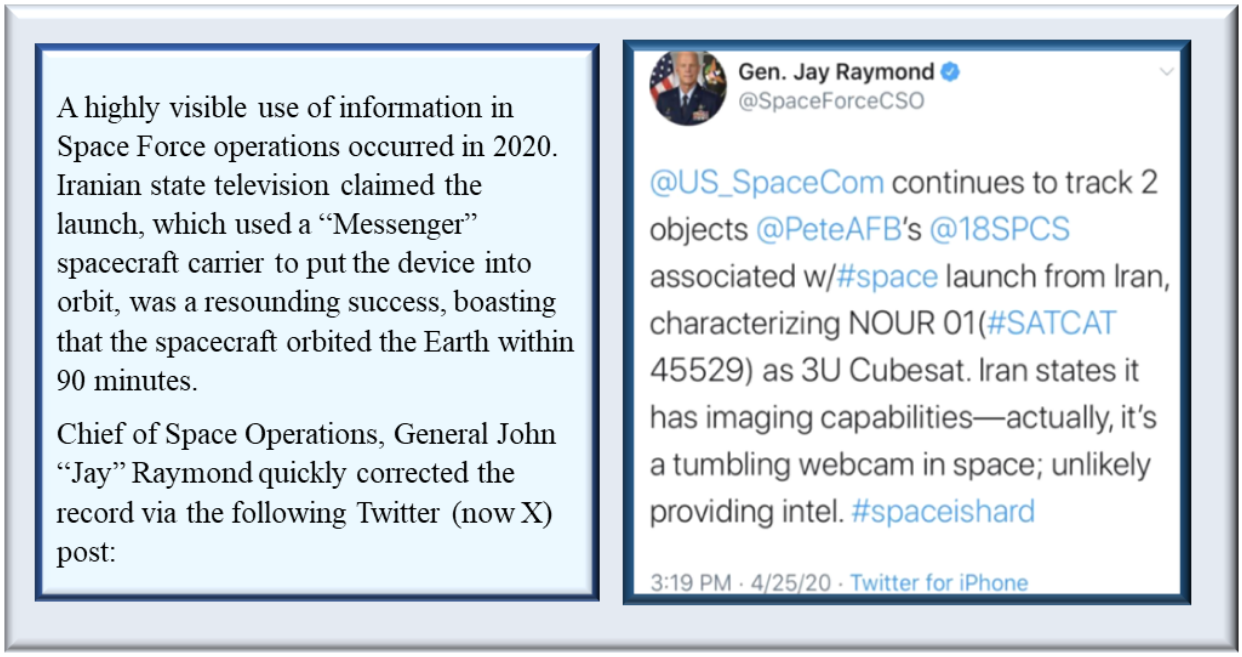

Figure 2. Information activities – strategic messaging

Integration with Allies and Partners

Allies and partners are crucial in the realm of information in Space Force operations. Their contributions extend operations beyond what the United States alone can achieve. These nations provide unique information and intelligence that might otherwise remain inaccessible or unknown. Additionally, some allies and partner units possess specialized information capabilities, which complement and enhance US capabilities. Synchronizing messaging with allies and partners demonstrates strength of cooperative security agreements and related activities. By collaborating closely with our allies and partners, Guardians strengthen the collective ability to effectively shape the information environment.

Legal Considerations

The United States conducts all military operations in accordance with applicable international and domestic laws, regulations, and policies, to include the law of war and rules of engagement. Operations in, to, and from space, or otherwise related to space, can have serious legal implications. As such, commanders must work closely with their servicing legal office to ensure they comply with laws and regulations when planning and executing any operations, including OIE. Executive orders can impose restrictions and may establish an organization other than the DoD as the lead. DoD policy may introduce restrictions for military operations. Specific rules of engagement for the operating environment or area of responsibility are also applicable. These vary from domain to domain.

Many decisions and actions in the space domain can have serious legal implications. The commander can only consider an information operation when sufficient intelligence or information exists to support the operational and legal requirements and provide awareness of how allies, partners, and adversaries will perceive our actions. Guardians should prepare to provide more comprehensive support for OIE relevant to operations in, from, and to the space domain. To facilitate the coordination and deconfliction of inform-and-influence tasks, commanders and staff members should remain cognizant of all treaties, laws, and policies related to information use across the competition continuum—whether employed in place or deployed.

Chapter 2 – Information Forces and Enablers

The application of information in the conduct of space operations to affect drivers of behavior strategically combines information forces at specific times and in a coherent manner to generate effects within the information environment that support achievement of operational objectives. While individual information forces create distinct effects, they may also aggregate and synchronize those effects with other information forces to attain operational objectives. Guardians conducting planning and assessment leverage these sources as part of integrating OIE into space operations.

Operations Security

> An activity that identifies and controls critical information and indicators of friendly force actions.
>
> Joint Publication 3-55, *Joint Operations Security*

The operations security (OPSEC) cycle is a systematic method used to identify, control, and protect critical information and indicators, and subsequently analyze friendly actions associated with military operations and other activities. OPSEC is a force multiplier that can maximize operational effectiveness by saving lives and resources when integrated into operations, activities, plans, exercises, training, and capabilities.

Integrating OPSEC considerations early in mission planning significantly contributes to its effectiveness and reduces the possibility of gaps or failures in OPSEC measures and countermeasures. OPSEC planning and execution occur as part of the command or organization's operations, protection, and OIE planning and execution which prevent enemies and adversaries from gaining critical information concerning friendly operation. The commander's objectives are the basis for OPSEC planning. OPSEC planning is an important part of achieving the commander's objectives. Threat assessments identify risks to friendly operations, including the capability, intent, and methods an adversary would use to threaten, collect, and exploit friendly forces and operations. Threat assessments allow OPSEC planners to prioritize the risks to plan against within the limited information resources.

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.
> Joint Publication 3-53, *Joint Military Information Support Operations*

Military Information Support Operations (MISO) convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. MISO is a principal information force activity. MISO may involve discrediting adversary propaganda to delegitimize an adversary, thereby reinforcing, or oppositely, inducing change in foreign attitudes and behavior.

Deception Activities

> 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.
> Joint Publication 3-13.4, *Military Deception*

Properly planned and executed military deception (MILDEC) is one of the most effective activities available to the joint force commander. It can directly influence, corrupt, disrupt, and usurp the adversary's military decision-making process and the subsequent direction of their forces. MILDEC targets the informational and cognitive processes of the adversary military decision maker by using means and information to lead them to incorrect conclusions about friendly capabilities and intentions. This can in turn causes the adversary to respond to a faulty construct of the operational environment and order the action or inaction of critical capabilities that, when misallocated, generate a friendly advantage, and substantially reduce risk to the friendly mission and forces. Successful MILDEC also requires a holistic and seamless integration with OPSEC to conceal or protect vulnerable physical, technical, and administrative indicators of our true capabilities and intent.

a. **Deception in Support of Operations Security.**

> Conveys or denies selected information or signatures to a foreign intelligence entity and limits the foreign intelligence entity's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets.
> Joint Publication 3-13.4, *Military Deception*

Deception in Support of Operations Security (DISO) is a MILDEC activity that protects friendly operations, personnel, programs, equipment, and other assets against foreign intelligence and security services collection. The intent of a DISO is to create multiple false indicators to confuse or make friendly force intentions harder to interpret by foreign intelligence, limiting the ability of an adversary to collect accurate intelligence on friendly forces. DISO activities are general in nature; they do not specifically target a particular adversary but instead mislead foreign intelligence entities by obfuscating friendly capabilities, intent, or vulnerabilities.

b. **Tactical Deception.**

> A deception activity planned and executed by, and in support of, tactical-level commanders to cause adversaries to take actions or inactions favorable to the tactical commanders' objectives.
>
> Joint Publication 3-13.4, *Military Deception*

The joint force conducts tactical deception (TAC-D) activities to influence military operations in order to gain a tactical advantage over an adversary, mask vulnerabilities of friendly forces, or to enhance the defensive capabilities of friendly forces. TAC-D is unique to the tactical requirements of the local commander and not necessarily linked or subordinate to a greater MILDEC plan.

Public Affairs

> Communication activities with external and internal audiences.
>
> Joint Publication 3-61, *Public Affairs*

Public affairs personnel focus on informing domestic, international, and internal audiences via overt, public communication, command information, media operations, and community and key leader engagement activities. Public affairs personnel at all levels contribute to research, planning, assessment, and execution, providing counsel to leaders and key staff members on the possible outcomes of military activities, lead development of the mission narrative, and identify the potential impact on domestic and international perceptions. Public affairs personnel provide commanders with an understanding of how information impacts the perceptions, attitudes, and decision-making process of friendly, neutral, and adversary audiences in support of friendly mission objectives.

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.
>
> Joint Publication 2-0, *Joint Intelligence*

Information forces require prioritized intelligence support. Intelligence directly contributes to developing situational understanding and informs decision making. Intelligence as part of information in Space Force operations provides context, contributing to understanding the human, information, and physical dimensions of the operational environment to include identifying relevant actors, their relationships, and patterns of thinking. Informational functions require timely coordination of intelligence to establish baseline characterizations of the information environment, develop detailed targeting packages for information effects, conduct effects assessments, and aid in relevant actor/target audience analysis.

Counterintelligence

> Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.
>
> Joint Publication 2-0, *Joint Intelligence*

The principal objective of counterintelligence is to assist with protecting friendly forces. Counterintelligence enhances command security by identifying foreign intelligence entities targeting friendly forces and provides protection by identifying and neutralizing espionage, sabotage, subversion, or terrorist organization efforts. Counterintelligence provides critical intelligence support to command force protection efforts by helping identify potential threats, adversary capabilities, and planned intentions to friendly operations. The Department of the Air Force Office of Special Investigations is the sole authorized executor of the counterintelligence mission for the Department of the Air Force.

Cyberspace Operations

> The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.
>
> Joint Publication 3-0, *Joint Campaigns and Operations*

Cyberspace consists of myriad different and often overlapping elements, including networks, data centers, nodes, links, interrelated applications, user data, and system data. Cyberspace, while part of the information environment, is dependent on each of the physical domains. When employed in support of OIE, cyberspace operations enable the flow of information to desired users, allow the joint force to gain intelligence, maneuver, collect information, or perform other enabling actions, and conduct offensive and defensive operation. Cyberspace operations may be employed independently or in conjunction with other capabilities to create effects in the adversary's battle space and ensure freedom of maneuver in the information environment.

As part of joint cyberspace operations, Guardians conduct offensive and defensive cyberspace warfare to protect and control the space domain. Offensive cyberspace warfare negates an adversary's ability to use space or counterspace systems. Guardians conduct defensive cyberspace warfare to protect against the adversary's ability to attack friendly systems.

Electromagnetic Spectrum Operations

> Coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment.
>
> Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations*

Electromagnetic spectrum operations contribute to the success of OIE by enabling the flow of information and using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the electromagnetic spectrum (EMS) while protecting friendly freedom of action. The specialties of electromagnetic spectrum warfare and management both fall under EMS operations.

For the Space Force, electromagnetic spectrum operations include electromagnetic warfare and theater electromagnetic warfare. Electromagnetic warfare includes offensive and defensive combat operations on the link segment through electromagnetic spectrum fires to control the space domain. Theater electromagnetic warfare includes actions taken in the electromagnetic spectrum (EMS) to protect or prevent the ability to communicate using space-based platforms. Electromagnetic attack, electromagnetic protection, and electromagnetic surveillance (referred to as electromagnetic support in joint doctrine) all enable theater electromagnetic warfare as part of space operations.

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.
>
> Joint Publication 3-57, *Civil-Military Operations*

As part of civil-military operations, military personnel often perform functions placing them in direct contact with civilian populations. Engagement with target audiences or key leaders are an important contributor to OIE, aiding accomplishment of military objectives by conveying key messages. Forces involved in engagement opportunities such as medical, engineering, or security assistance can provide key information environment opportunities in a civil military operations capacity. Throughout all operations planners should consider the impact of any information operations on the civilian population, civil-military engagement to reduce potential impacts, and other options mitigate potential harm.

Chapter 3 – Operations in the Information Environment for Space

Operations in the information environment are military actions involving the integrated employment of multiple information forces and contributing capabilities 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.

While OIE expand a commanders' range of options for action across the competition continuum, they do not do so without risk. Throughout the entire planning and execution process, OPSEC remains a vital component, ensuring intentional or unintentional disclosures or actions do not compromise mission success or security. Some information activities such as whether to conceal or reveal a capability or action require early planning and operational considerations. In some cases, OIE may be the primary option available to a joint force commander during long-duration cooperation and competition short of armed conflict, where the use of physical force is inappropriate or restricted.

Information Planning for Space Force Operations

Planning for space operations includes addressing how space operations employ and support OIE as part of joint all-domain operations. The space planning process (SDP 5-0, *Planning*) aligned to the joint planning process enables Guardians to integrate space operations, including requirements for information or support to information operations into combatant command planning. The role of information as it relates to space operations should be addressed at each phase of the planning process, through an OIE working group or information planning cell that incorporates the expertise across information forces. Public affairs personnel aid senior leaders and Guardians at all levels to ensure their activities in the public domain incorporate consistent messaging aligned across the Space Force enterprise, and to identify potential impacts on domestic and international perceptions.

Guardians engaged in the initial phases of planning, including mission analysis and red teaming, developing assessment measures, and course of action development and approval, should consider each the orbital, terrestrial, and link segments of space systems to understand information dependencies, and how information forces can help shape the perceptions of key audiences about space operations and space capabilities. Guardians also need to present potential vulnerabilities and avenues of attack against space systems from the information environment. They also need to identify complementary space operations to protect and enable OIE and be able to explain to the joint force how the adversary may perceive action in the space domain.

Information Environment Considerations Throughout Planning

For all aspects of space operations, it is important to understand how OIE can contribute to desired effects, may result in undesired effects, and how those operations may have cumulative

or cascading effects that could produce undesired or unintended consequences. Public affairs personnel support in planning aids Guardians in the development of constraints and restraints, identification of the identification of potential desired and undesired consequences of planned actions.

Guardians should be ready to advise the joint force planning team on risks from or to information related to operations in, from, or to the space domain.

a. **Desired Effects.** Desired effects are conditions that directly support achieving the commander's objectives. Desired effects are first-order consequences of a military action. Non-lethal direct effects, such as in the information environment, may not be immediate or easily recognizable.

b. **Unintended Effects.** Unplanned or unexpected results of an operation may spill over to create unintended or undesired consequences. Unintended effects may have delayed results or second-, or third-order consequences to include unintentional harm to civilians. These outcomes may be physical or behavioral in nature. Unintended effects may be difficult to recognize due to subtle changes in system behavior. While these may be counterproductive or hinder progress toward an objective, they may also create opportunities. Planners should consider potential second-, and third-order effects that could require mitigation during planning and assessment.

Desired or unintended effects often combine to produce greater outcomes, positive or negative, than the sum of their individual impacts. Effects can ripple through an operational environment influencing other conditions or capabilities. This most typically occurs through nodes and links that are common and critical to related systems. The cascading of desired or unintended effects may have a variety of consequences.

Clear communication of desired and undesired effects is crucial. Everyone involved, from planners to operators, needs to understand them. As the staff develops the desired effects, objectives, and end states during planning, they should concurrently identify the specific pieces of information they need to infer changes in the operating environment supporting them. Public affairs personnel can assist in the identification of relevant overt and covert communication channels, audiences, messengers, adversarial information approaches, and tactics to support achieving desired effects. In addition, public affairs personnel can assist planners by formulating and delivering timely and culturally attuned messages to shape foreign actor perceptions to support the commander's intent and concept of operations.

Chapter 4 – Roles and Responsibilities

To achieve information advantage for space operations, the commander, supported by the staff, integrates information activities throughout operations. This process—comprising planning, preparation, execution, and assessment—stands as the central command and control activity during operations. Given that most military capabilities and actions can contribute to gaining or exploiting information advantages, the staff collaborates with the commander to integrate information tasks across the planning, preparation, execution, and assessment phases.

Commanders

At every level, commanders rely on information to seize, retain, and exploit the initiative to achieve the desired results. Space Force commanders need to understand the information forces available to them, and how to integrate them as part of space operations to support the combatant commander's objectives. Information is essential for establishing shared understanding, the primary means of command and control, and the inputs and outputs of every decision-making process. Information plays a pivotal role in operational success at all levels, regardless of whether a unit has an assigned information-related function. Commanders ensure staff and subordinate units conduct OIE through tasks and mission-type orders to achieve information advantage.

The decision to conceal or reveal information involves a delicate balance between advantages and disadvantages, informed by risk assessment. DoD Directive 5122.05, *Assistant to the Secretary of Defense for Public Affairs,* requires DoD commanders abide by the principles of information to make available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy. Throughout operations, commanders carefully evaluate the pros and cons of disclosing or withholding information. A commander only withholds information when the disclosure would adversely affect national security, threaten the safety or privacy of Service members, or if otherwise authorized by statute or regulation. For instance, revealing information about friendly forces as part of deterrence may inadvertently provide valuable intelligence to the adversary on how to counter joint operations.

Recognizing the significance of optimizing the information environment, commanders include OIE planning across all phases of the competition continuum. Component field command commander's staff ensure integration of information activities into space operations through the space planning process (See SDP 5-0, *Planning*). This requires an understanding of the available information forces to create and exploit informational advantages. A commander directs information activities through orders while leading and assessing progress throughout operations, supported by an OIE working group or planning cell. Based on changes in a situation that reveal opportunities or vulnerabilities, commanders adjust information activities and related tasks as required.

It is up to each commander to establish and convey his or her priorities and take actions to ensure timely access to information to support decision-making for space operations. Commanders rely on their subordinates to assist in planning, preparation, execution, and assessment of space operations to include support required from OIE to space operations, and the role of space in OIE.

Staff

Guardians as part of any staff collectively bear the responsibility of supporting OIE to achieve information advantage. To achieve information advantage, the commander, supported by the staff, integrates information activities throughout the operations process. The staff collaborates with the commander to integrate information tasks across the planning, preparation, execution, and assessment phases. The staff fulfills this role within integration cells (current operations, future operations, and plans), working groups, boards, and other integrating processes. Staff responsibilities include:

a. Taking risk-informed initiative.

b. Protecting and managing friendly information.

c. Integrating OIE best practices into space operations.

d. Developing the information and intelligence requirements needed to support upcoming operations.

e. Responding to requests for information.

f. Informing and educating US, allied, and partner audiences.

g. Influencing adversary and other audiences.

h. Conducting OIE, including messaging, according to approved rules of engagement and commander's guidance.

i. Generating relevant information through accurate reporting.

j. Using the OPSEC cycle to identify and protect critical information and indicators.

k. Being aware of threat information manipulation methods.

l. Obscuring friendly actions and protecting sensitive capabilities from threat collection.

m. Considering the operational impact of releasing information and coordinating actions with appropriate organizations or entities.

n. Being aware of the message their actions convey.

o. Maintaining cyberspace hygiene practices to protect friendly information, maintaining OPSEC, and combating adversary social engineering tactics.

The fight for information is continuous. Whether employed-in-place or deployed, Guardians should be aware of the information the adversary can, and is likely collecting on them, and the

information which they should protect. Guardians' actions either help establish and maintain information advantage or increase the risk of losing that advantage.

Guardians should be vigilant to prevent unauthorized disclosure of critical information. Information forces, along with supporting capabilities, are essential for mission success. Each of these entities has specific responsibilities and vital relationships to establish and maintain, all aimed at achieving an advantage in the information environment.

Guardians at every level of the staff collaboratively contribute to achieving information advantage. Each member has distinct duties and responsibilities aligned with their expertise. The staff advises commanders and senior leaders on information relevant to their domains. Guardians on the combatant commander's staff bear the responsibility for conducting or coordinating information and engaging in the working groups and other information operations processes in support of space operations.

Guardians on the staff employ critical thinking to mitigate confirmation bias, groupthink, and other biases. A common error lies in assuming that adversaries perceive and use the information environment in the same manner as the United States and its allies. To avoid projecting the friendly OIE concept onto the adversary and to prevent misalignment of US capabilities and vulnerabilities, Guardians assess adversary operations within the information environment, focusing on activities related to information collection, protection, and projection. These three functions remain universally applicable to the strategic framework's ability to leverage information, regardless of organizational structure, capabilities, or mission.

Appendix A – Acronyms, Abbreviations, and Initialisms

CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
DISO	deception in support of operations security
DoD	Department of Defense
DoDD	Department of Defense Directive
EMS	electromagnetic spectrum
MISO	military information support operations
MILDEC	military deception
OIE	operations in the information environment
OPSEC	operations security
SDP	Space Doctrine Publication
STARCOM	Space Training and Readiness Command
TAC-D	tactical deception
US	United States
USSF	United States Space Force

Appendix B – Terms and Definitions

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. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-57, *Civil-Military Operations*)

counterintelligence - Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 2-0, *Joint Intelligence*)

cyberspace operations - The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-0, *Joint Campaigns and Operations*)

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 of Military and Associated Terms* / Joint Publication, 3-12, *Joint Cyberspace Operations***)**

cyberspace warfare - Combat operations conducted in the cyber domain through fires, movement, and maneuver to control the space domain. (*United States Space Force Military Space Operations Terms of Reference)*

deception in support of operations security - Conveys or denies selected information or signatures to a foreign intelligence entity and limits the foreign intelligence entity's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-13.4, *Military Deception*)

defensive cyberspace operations - Missions to preserve the ability to utilize and protect blue cyberspace capabilities and data by defeating on-going or imminent malicious cyberspace activity. (*DoD Dictionary of Military and Associated Terms* / Joint Publication, 3-12, *Joint Cyberspace Operations***)**

defensive cyberspace warfare - Protection against enemy ability to attack friendly systems. (*United States Space Force Military Space Operations Terms of Reference)*

defensive space control electromagnetic warfare - Protection against enemy ability to attack friendly systems. (*United States Space Force Military Space Operations Terms of Reference)*

electromagnetic attack - Transmission of energy through the EMS to disrupt or degrade a terrestrial target's ability to receive signals or deliver data. (*United States Space Force Military Space Operations Terms of Reference)*

electromagnetic protection - Protection of personnel, facilities, and equipment from intentional or inadvertent electronic interference. (*United States Space Force Military Space Operations Terms of Reference)*

electromagnetic spectrum operations - Coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations*)

electromagnetic surveillance - The search for interception, identification, location, or localization of sources of intentional or unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, or future operations. (*United States Space Force Military Space Operations Terms of Reference)*

electromagnetic warfare - Combat operations through the electromagnetic spectrum to negate space or counterspace threats. (*United States Space Force Military Space Operations Terms of Reference)*

information - Information is data in context to which a receiver assigned meaning. (Joint Publication 3-04, *Information in Joint Operations*)

information advantage - The operational advantage gained through the joint force's use of information for decision making and its ability to create effects on the information environment. (Joint Publication 3-04, *Information in Joint Operations*)

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. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-04, *Information in Joint Operations*)

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. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 2-0, *Joint Intelligence*)

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. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-13.4, *Military Deception*)

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. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-53, *Joint Military Information Support Operations*)

offensive cyberspace operations - Missions intended to project power in and through cyberspace. (*DoD Dictionary of Military and Associated Terms* / Joint Publication, 3-12, *Joint Cyberspace Operations*)

offensive cyberspace warfare - Negate enemy ability to use space or counterspace systems. (*United States Space Force Military Space Operations Terms of Reference)*

offensive space control electromagnetic warfare - Negate enemy ability to use space or counterspace systems. (*United States Space Force Military Space Operations Terms of Reference)*

operations in the information environment - Military actions involving the integrated employment of multiple information forces to affect drivers of behavior. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-04, *Information in Joint Operations*)

operations security - An activity that identifies and controls critical information and indicators of friendly force actions. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-55, *Operations Security*)

public affairs - Communication activities with external and internal audiences. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-61, *Public Affairs*)

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 of Military and Associated Terms* / Joint Publication 3-04, *Information in Joint Operations*)

tactical deception - A deception activity planned and executed by, and in support of, tactical-level commanders to cause adversaries to take actions or inactions favorable to the tactical commanders' objectives. (*DoD Dictionary of Military and Associated Terms* /Joint Publication 3-13.4, *Military Deception*)

target audience - An individual or group selected for influence. (*DoD Dictionary of Military and Associated Terms* / Joint Publication 3-04, *Information in Joint Operations*)

theater electromagnetic warfare - Actions taken in the electromagnetic spectrum to protect or prevent the ability to communicate using space-based platforms. (*United States Space Force Military Space Operations Terms of Reference)*

Appendix C – References

Department of Defense Directive (DoDD) 3600.01, *Information Operations*

DoDD 5122.05, *Assistant to the Secretary of Defense for Public Affairs,* 7 August 2017

Department of Defense Dictionary of Military and Associated Terms, February 2025

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3110.05G, *Military Information Support Operations Supplement to the Joint Campaign Plan*, 3 May 2023

CJCSI 3205.01D, *Joint Combat Camera (COMCAM)*, 20 October 2014

CJCSI 3210.01C, *Joint Information Operations Proponent*, 14 February 2014

CJCSI 3211.01F, *Joint Policy for Military Deception*, 14 May 2015

CJCSI 3213.01D, Joint Operations Security (OPSEC), 7 May 2012

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3105.01B, *Joint Risk Analysis Methodology*, 22 December 2023

Joint Publication 2-0, *Joint Intelligence*, Change 1, 5 July 2024

Joint Publication 3-0, *Joint Campaigns and Operations,* 10 June 2022

Joint Publication 3-01, *Countering Air and Missile Threats*, 6 April 2023

Joint Publication 3-04, *Information in Joint Operations*, 14 September 2022

Joint Publication 3-13.4, *Military Deception*, 14 February 2017

Joint Publication 3-14, *Joint Space Operations,* 23 August 2023

Joint Publication 3-53, *Joint Military Information Support Operations*, 11 October 2024

Joint Publication 3-55, *Joint Operations Security*, 20 February 2025

Joint Publication 3-57, *Civil-Military Operations,* 9 July 2018

Joint Publication 3-60, *Joint Targeting,* 20 September 2024

Joint Publication 3-61, *Joint Public Affairs,* Change 1*,* 8 January 2025

Joint Publication 3-84, *Legal Support,* 2 August 2016

Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations,* 22 May 2020

Joint Publication 5-0, *Joint Planning*, Change 1, 1 July 2024

Space Doctrine Publication 5-0, *Planning*, 20 December 2021

United States Space Force Military Space Operations Terms of Reference, 24 September 2024