



Handbook for Tactical Operations in the Information Environment

MICHAEL SCHWILLE, JONATHAN WELCH, SCOTT FISHER,
THOMAS M. WHITTAKER, CHRISTOPHER PAUL

For more information on this publication, visit www.rand.org/t/TLA732-1.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

© 2021 RAND Corporation

RAND® is a registered trademark.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0759-7

Cover: Marine Corps Cpl. Seth Rosenberg/U.S. Dept of Defense.

Cover design: Kristen Meadows

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.

About This Handbook

This handbook focuses on the conduct of operations in the information environment (OIE) at the tactical level of war. It is designed as a practical reference for (1) maneuver formation commanders and staffs at that echelon and (2) information-related capability personnel who integrate and support those forces. The joint force—and, specifically, the U.S. Army and U.S. Marine Corps—are continually seeking ways to leverage internal and external capabilities to achieve effects in and through the information environment. This handbook provides readers with an understanding of various OIE-related capabilities to improve collaboration and maximize operational effectiveness.

The research reported here was completed in April 2021 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Irregular Warfare Technical Support Directorate and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Acknowledgments

This research was funded by the Irregular Warfare Technical Support Directorate, and we are particularly grateful for the support of Drew Lomax, Bryan Taylor, and Lauren Neiberg. This handbook was built

on the shoulders of previous documents that address various aspects of the information environment.

We are grateful for the contributions of the Center for Army Lessons Learned, the Marine Corps Center for Lessons Learned, and the Defense Technical Information Center for their compilation and archiving of relevant experiences, observations, and lessons. We are also grateful to our RAND quality assurance reviewers, MAJ Braxton Canfield and LTC Dave Acosta, for their review and assistance with the document. Pat Scribner, Jim McNeive, MAJ Jason Romanello, and COL Marlene Markatan all provided early guidance and input to the shape of this research effort and valuable stakeholder perspectives from both the Army and Marine Corps. Other members of the information operations (IO) community, including the IO proponent, Joint Operations Security Element, Vermont National Guard IO schoolhouse, and CPT Nick Lang, SFC Christopher Page, and SFC Ian Kangas of the 151st Theater Information Operations Group, and MAJ Jack Gaines all provided critical and substantive comments that improved this handbook.

Countless others have contributed their time and energy to this handbook by providing subject-matter expert input and advice; the terms of our interviews prevent us from listing you all by name, but you know who you are, and we value your contributions. Finally, we thank the U.S. Army's Maneuver Center of Excellence for providing feedback on draft sections of this handbook and helping us ensure this handbook is useful to the junior officers at whom it is aimed. Errors and omissions remain the sole responsibility of the authors.

Summary

How does a company commander or first sergeant in a maneuver unit prepare for operations in the information environment (OIE)? What schools and courses cover this topic area? Unfortunately, there isn't much guidance out there. Early-career officers learn about combined arms warfare, the use of fires and maneuver, and how they are intertwined, but most are not taught the importance of information. There are no programs of instruction for applying information (like fires) to generate effects and help maneuver forces accomplish a mission. Across the joint force, junior officers know how to call for fires or make 9-line MEDEVAC requests. These skills are taught and are part of the way the force fights. Where is the analogous process for using information or, as one soldier put it during a workshop we held while developing this handbook, "Where is my information call for fire?"

The information environment is nebulous and confusing, but it is also a contested battlespace. U.S. adversaries are employing increasingly sophisticated capabilities across domains to achieve effects greater than the sum of their independent parts. As a leader, you will be required to understand and operate in this complex environment. A junior maneuver formation commander might be asked to raid a warehouse that higher headquarters knows is empty as part of a military deception (MILDEC) operation. Imagery or accounts of that "failed" operation might be posted to social media—where they could be retweeted thousands of times—as an intentionally false signal to adversaries. It might look like a failure, but that assumption couldn't be further from the truth.

Who is this handbook for?

This handbook will be particularly useful to the following types of practitioners:

1. Commanders and NCOs of tactical formations (platoons, companies, battalions, and regiments)
2. Battalion or regimental staff
3. External capability area personnel who might support OIE for these forces.

This handbook describes OIE-related capabilities and activities and identifies relevant tactics, techniques, and procedures that can be used as part of, and in support of, tactical-level maneuver-focused operations. It is built with practitioners in mind, leverages existing doctrine and documentation, and includes example use cases for each capability. It is intended to facilitate tactical problem-solving and increase awareness of tactical opportunities, but it is illustrative rather than exhaustive. Fictional vignettes featuring a young captain in his first company command supplement the capability-focused discussions. Murphy's experiences highlight successful—and unsuccessful—attempts to leverage various capabilities show how the handbook's lessons might translate to a real-world situation.¹

Bottom Line: Applying This Handbook

Each capability section in this handbook concludes with a roundup of what your unit can do to harness the capability and how to obtain the resources you need, which might involve sending a request to higher echelons. For quick reference, Table S.1 provides abbreviated answers to these two questions; full responses can be found in the individual sections. This list is not exhaustive but does represent the primary capability areas.

¹ Instructional fiction can be an effective teaching tool. A well-known example targeting military audiences was Ernest Dunlop Swinton's 1904 *The Defence of Duffer's Drift*, in which, through a series of dreams, the protagonist progressively learns lessons to successfully hold a defensive position against the backdrop of the Boer War. Two RAND volumes adapted this formula for U.S. Army and U.S. Marine Corps information operations contexts: Christopher Paul and William Marcellino, *Dominating Duffer's Domain: Lessons for the 21st-Century U.S. Army Information Operations Practitioner*, Santa Monica, Calif.: RAND Corporation, RR-1166/1-A, 2017, and Christopher Paul and William Marcellino, *Dominating Duffer's Domain: Lessons for the 21st-Century U.S. Marine Corps Information Operations Practitioner*, Santa Monica, Calif.: RAND Corporation, RR-1166-1-OSD, 2016.

TABLE S.1

Acquiring and Using Information-Related Capabilities Covered in This Handbook

Capability	What can my unit do now?	Where do I go for this capability?
Inherent informational aspects of military operations • Presence, posture, and profile (PPP) • Physical attack	A lot! Many decisions can be made at the tactical level in terms of PPP. And as a fighting element of the U.S. military, your unit brings physical attack capability to any operation. As always, consider the effects of these decisions.	More than almost any other capability, there are opportunities for your unit to play a role.
Key leader engagement (KLE)	You need to understand local leaders and culture and prepare for all types of engagements.	For guidance, you can consult with your commander, public affairs, and PSYOP. The S2 can provide helpful intelligence (remember to share what you learn as well).
Civil-military operations (CMO) and civil affairs operations (CAO)	Many CMO activities do not require special authorities, but you should coordinate with higher for materials and supplies, if needed. Keep in mind that these activities build rapport and send a message. U.S. forces don't dig wells and hand out supplies without a purpose.	Consult with your command's CMO planner for a better understanding of civil considerations in the area of operations.
Public affairs (PA) and combat camera (COMCAM)/service member camera	There isn't much that you can do at the tactical level. PA is handled by PA professionals. For COMCAM, even if you don't have personnel assigned to your unit, you can use a smartphone camera. But be mindful of authorized uses and restrictions.	If your unit does not have a PA detachment, consult with your commander before making a request for PA support. PA can also provide guidance and arrange for COMCAM capabilities.
Operations security (OPSEC) and signature management	You should certainly be concerned about OPSEC and signature management at the tactical level, including controlling the signals your unit emits.	Work through the command channels and your S2 and S3 for OPSEC support.
Military deception (MILDEC)	You can conduct tactical deception (TAC-D) and deception in support of OPSEC (DISO) at your level; it requires a little coordination, but it can be quite effective.	Build it into your plan, and your commander can approve TAC-D. Talk with your S2 and S3 for more deception-focused capabilities.
Electronic warfare (EW)	This is one of the capabilities that you generally can't employ without the appropriate equipment or personnel attached to your unit (or airborne support).	Work through the command channels, which will vary depending on where these capabilities are housed.

TABLE S.1—Continued

Capability	What can my unit do now?	Where do I go for this capability?
Cyber operations	There isn't much that you can do at the tactical level.	Have a clear idea of what kind of capability you need so you can be specific in your request for cyber support.
Military information support operations (MISO)/psychological operations (PSYOP)	MISO requires specially trained forces (PSYOP personnel), who can help you craft messages and design talking points for KLEs. Messaging campaigns are carefully coordinated, and there is a risk of doing more harm than good.	Coordinate through your battalion S3, who will be able to request tactical PSYOP support.
Space	You have what you have in terms of GPS-enabled and satellite communication equipment. Other than that, space-based capabilities are largely out of the realm of tactical operations. Be sure to have a backup communication plan in case of outages.	You can request imagery through your S2, and your S6 can help keep your communications up and running.
Technical effects	There's not much that can be discussed at an unclassified level.	In requesting support, be very clear about what effects you are seeking. You might not be involved in the decision about whether and how to deploy these capabilities.
Social media and open-source intelligence (OSINT)	You can use social media for situational awareness, to identify influencers, and to gauge public opinion, but there are restrictions on data collection and use.	Your battalion S2 will have some form of OSINT capability. You can also talk with PA or PSYOP, which monitor social media.

Contents

About This Handbook..... iii
Summary..... v
Figures and Tables..... xi

How to Use This Handbook 1

Capabilities

1. Inherent Informational Aspects of Military Operations..... 9
2. Key Leader Engagement 15
3. Civil-Military Operations and Civil Affairs Operations 19
4. Public Affairs and Combat Camera/Service Member Camera..... 27
5. Operations Security and Signature Management 33
6. Military Deception 39
7. Electronic Warfare 45
8. Cyber Operations 51
9. Military Information Support Operations/Psychological Operations ... 53
10. Space Operations 59
11. Technical Effects..... 63
12. Social Media and Open-Source Intelligence 65

Conclusion 69

Appendix. Stakeholder Organizations..... 73

Abbreviations..... 77

References..... 79

Two appendixes providing an overview of force development tasks for OIE and listing joint and service-specific tasks accompany this handbook online at www.rand.org/t/TLA732-1.

Figures and Tables

Figures

1.	Notional Civil-Military Operations Center	22
2.	The Electromagnetic Spectrum.....	47

Tables

S.1.	Acquiring and Using Information-Related Capabilities Covered in This Handbook	vii
1.	Information-Related Capabilities Covered in This Handbook	4
2.	Intrinsic and Extrinsic Capabilities.....	5
3.	Use Cases: Inherent Informational Aspects of Military Operations.....	12
4.	Use Cases: Key Leader Engagement.....	17
5.	Use Cases: Civil-Military Operations and Civil Affairs Operations.....	23
6.	Use Cases: Public Affairs and Combat Camera/Service Member Camera.....	31
7.	Use Cases: OPSEC and Signature Management.....	38
8.	Use Cases: Electronic Warfare	50
9.	Use Cases: MISO/PSYOP	55
10.	Use Cases: Space Operations.....	61
11.	Example Employment Matrix for an Infantry Company Attack	71

How to Use This Handbook

The **information environment** (IE) connects and spans the spatial domains of warfare, where all operations depend on information. Actions in the IE have effects and consequences on the physical battlefield, and physical conflicts can spill over into the IE. Today's complex, interconnected operational environment (OE) requires commanders at every echelon that are prepared to fight on both fronts—and at the same time.

The U.S. Department of Defense (DoD) has been increasingly focused on **operations in the information environment** (OIE) at the operational and strategic levels of war. But, to date, there has been relatively little attention paid to OIE at the tactical level. This handbook helps close that gap while providing useful guidance to tactical-level practitioners.

The lexicon related to information is currently in flux, with **information operations** (IO) disappearing, **OIE** in use at the joint level and by the U.S. Marine Corps, and **information advantage** currently ascendant in the U.S. Army. The services are not in alignment and use terms differently. Generally speaking, IO is a staff function used to coordinate information-related capabilities (IRCs). OIE are activities conducted with the express intent of achieving effects in the IE. Information advantage consists of ways to gain credible advantage over an adversary through the continuous use of information and information systems. Regardless of what terms are used, this handbook is designed to help you better accomplish your mission. To do that, you plan and conduct missions in the physical environment, but you can also achieve effects in the IE.¹

¹ We learned in our interviews that nascent thinking challenges the term **IE** itself, arguing instead that information is inseparable from the operating environment and thus should be considered a dimension or aspect of every operating environment. Others have argued that information should be acknowledged as its own domain (with the attendant level of resources received by domain component forces). We are agnostic as to whether information be considered a dimension, an environment, or a domain. As long as readers recognize that

Two Key Terms Used in This Handbook

Information-Related Capabilities

This handbook uses the term **information-related capabilities** (IRCs) because it is used in joint doctrine and its definition is expansive. Joint Publication (JP) 3-13 defines IRCs as follows:

A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.²

Because information plays a role across the range of military activities, all forces and capability areas could be IRCs. Yet capabilities focused on generating effects in and through the IE have frequently been treated as an afterthought, sprinkled intermittently onto existing concepts of operations (CONOPS) rather than baked in as an integral part of a plan.

Information Environment

The operating environment—where operations are conducted—has defined physical borders.³ The **information environment** (IE) often does not. The IE is potentially global and comprises the social, cultural, cognitive, technical, and physical attributes that influence how people think, understand, and create their worldview. The IE consists of both technical systems and the use of data.⁴ Although it *is* global in its interconnectedness, localized portions of the IE will be the primary focus in any given area of operations (AO). However, some factors—

information is important to mission accomplishment and that important possible effects rely on thoughtful employment of information and IRCs, this handbook should be useful.

² JP 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014, p. GL-3. Note that JP 3-0, *Joint Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, 2018, promulgates a new way of referring to such capabilities: “joint force capabilities, operations, and activities for leveraging information” (p. III-22).

³ Also known as an **area of operations** or **area of responsibility**.

⁴ JP 3-0, 2018, pp. IV-1–IV-2.

such as broadcasts, phone calls, or social media influence originating outside the AO—could expand the focus of plans and operations.

How to Use This Handbook

This handbook can be used multiple ways. You could read it straight through, cover to cover. Alternatively, you could read the introductory material and then cherry-pick the sections that are most useful to you. We urge you to retain the handbook as a reference: During a future deployment, you might need to know more about one of the capabilities described here, or you might simply have downtime to browse all the sections.

We have tried to keep the format consistent, but there are exceptions. At times, IRCs can be the main capability used to accomplish a mission. Other times, they serve as supporting capabilities. Learning what they are, what they offer, and how to employ them will give you more tools to achieve mission success.

Navigation

To help you easily find the information you need, Table 1 lists each of the capabilities covered, its abbreviation, a plain-language definition (not necessarily the doctrinal definition), and the chapter and section where you can find the full discussion in this handbook. Any discussion of military concepts can quickly become an acronym soup. Although the table lists abbreviations for these capabilities that you are likely to find in planning, doctrine, and other documents, we have attempted to keep their use to a minimum in this handbook. The need to decode acronym-heavy discussions can slow down efforts to find the information you're looking for.

Identifying Your Role

Table 2 shows capabilities that are intrinsic or extrinsic to tactical formations. This table has been adapted from a table in Army Techniques Publication (ATP) 3-13.1, *The Conduct of Information Operations*. It shows which capabilities are relatively available to tactical maneuver formations (intrinsic) and which need to be sought from and coordinated with higher echelons (extrinsic).

TABLE 1
Information-Related Capabilities Covered in This Handbook

Capability	Abbrev.	Plain-Language Definition
Inherent informational aspects of military operations	None	Every action the force takes (or does not take) sends a message. These are the features and activities that an observer interprets and uses to assign meaning to military activities. (Joint Concept for Operating in the Information Environment [JCOIE])
Presence, posture, and profile	PPP	Presence is about being physically present. Profile is the degree of presence (e.g., how many forces). Posture is an expression of attitude, which can be active or passive, menacing or welcoming. (ATP 3-13.1)
Physical attack	None	Fires and maneuver, including closing with and destroying the enemy. The application of combat power to create desired effects in the information environment. (ATP 3-13.1/MCWP 3-32)
Key leader engagement	KLE	Talking to influential people to achieve mutual understanding. KLEs are deliberate, planned engagements with foreign leaders that have defined objectives. (JP 3-13)
Civil-military operations	CMO	Activities to establish, maintain, influence, or exploit relations among military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area to achieve U.S. objectives. (JP 3-13)
Civil affairs operations	CAO	Actions conducted that address the civil component of the OE. Building a well, refurbishing a school, paving a road; address the underlying causes of instability within an AO.
Public affairs	PA	Communication activities with external and internal audiences used to convey themes and messages through the media to selected audiences. (JP 3-61)
Combat camera/service member camera	COMCAM	Supports information collection, battle damage assessment, military deception (MILDEC), and legal and historical or archival functions. COMCAM units acquire, edit, disseminate, archive, manage, and transmit imagery. (ATP 3-13.1/CJCSI 3205.01D)
Operations security	OPSEC	Information that needs to be protected for military operations to be successful or to prevent harm to U.S. forces.
Signature management	SIGMAN	Sometimes described as “offensive OPSEC,” involves managing emissions and observables that can reveal (or mislead about) force positions or intentions. Can also play a role in MILDEC.
Military deception	MILDEC	Actions executed to deliberately mislead adversary decisionmakers.
Electronic (or electromagnetic) warfare	EW	Use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack an enemy. (JP 3-85)
Cyber operations	CO	The employment of cyberspace capabilities to achieve objectives in or through cyberspace, including defensive and offensive operations, securing communications, and detecting and deterring threats. (JP 3-0/ATP 3-13.1)

TABLE 1—Continued

Capability	Abbrev.	Plain-Language Definition
Military information support operations/psychological operations	MISO/PSYOP	Influence the behavior of selected foreign audiences. MISO is sometimes used interchangeably with psychological operations (PSYOP).
Space operations	None	Space operations seek to achieve superiority in the space domain and its corresponding environment. (JP 3-14)
Technical effects	None	Classified operations or effects that utilize technical capabilities to gain a decisive advantage over an adversary.
Social media and open-source intelligence	OSINT	Relevant information derived from the systemic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. (JP 2-0)

SOURCES: Compiled largely from doctrinal definitions, which have been edited for clarity and conciseness. The publications can be found in the References section at the end of this handbook.
 NOTE: Capabilities with matching color-coding are covered in a single section of the handbook.

TABLE 2
 Intrinsic and Extrinsic Capabilities

Battalion and Below	Brigade	Echelons Above Brigade	Intrinsic/ Extrinsic
Inherent informational aspects of military operations			Intrinsic capabilities
Presence, posture, and profile (PPP)			
Physical attack			
Key leader engagement (KLE)			
Civil-military operations (CMO)			
Unit PA rep (S1)	Public affairs (PA)		
Service member camera	Combat camera (COMCAM)		
Operations security (OPSEC)			
		Military deception (MILDEC)	
Tactical deception (TAC-D) and deception in support of OPSEC (DISO)			
Social media monitoring	Social media analysis		
Civil affairs operations (CAO)			Extrinsic capabilities
Military information support operations (MISO)			
		Electronic warfare (EW)	
Limited cyber operations		Cyber operations	
		Space operations	
		Technical effects	

SOURCE: Adapted from ATP 3-13.1, *The Conduct of Information Operations*, Washington, D.C., October 2018, Table 3-1.

We have arranged and emphasized the capabilities that are intrinsic at battalion and below: These are contributions that you—as a tactical echelon commander or staff—can make to OIE using capabilities that are already part of your formation.

Methods

The empirical foundation for this handbook came from a range of sources, including the Joint Lessons Learned Information System, Center for Army Lessons Learned, and Marine Corps Center for Lessons Learned. We also consulted with subject-matter experts, who participated in a workshop and interviews to help us identify gaps and possible solutions. Their feedback helped ensure that this handbook is in line with current doctrine and that it reflects emerging tactics, techniques, and procedures.

Who Is CPT Aaron Murphy?

As noted, there are several ways to use this handbook. While you could read it cover to cover as part of a program of self-study, you might also use it as a reference when confronted with specific types of problems in planning or operations, or when you're seeking to better understand specific available capabilities.

Regardless of how you approach this handbook, the experiences of CPT Aaron Murphy—presented as a series of vignettes—are intended to reinforce the lessons and guide you in applying them. This young captain has recently completed the Captain's Career Course and arrived at his unit, which has just deployed as part of a U.S.-led joint combined task force to the occupied nation of Centralia. Murphy's service and military occupation do not matter (although Navy practitioners are invited to mentally substitute *lieutenant* as his rank). His experiences illustrate how the IRCs should or should not be applied in a real operational scenario.

The Capabilities

The following sections provide an overview of each IRC, the activities it encompasses, and relevant tactics, techniques, and procedures for

Montanya Occupies Western Centralia; U.S.-Led CJTF Responds

Montanya and Centralia have an uneasy relationship at the best of times. An economic downturn in the region has heightened regional tensions to an unbearable level. When Centralian forces put down a protest of Montanyans living in western Centralia, it was painted as a massacre. Montanyan forces responded by sending three brigades of armor and infantry into western Centralia to “protect” the ethnic Montanyans living there. The international community, led by the United States, swiftly responded by forming a combined joint task force (CJTF) to evict the Montanya forces from Centralia.

Montanyan forces are well equipped with some of the most advanced military hardware from Russia and China. They have modern tanks, armored fighting vehicles, planes, and an integrated anti-aircraft defense system. They also have access to unmanned aerial vehicles, and intelligence suggests that they even have electronic attack and defense equipment.

Based on the Montanyans’ rapid movement into Centralia, it also seems likely that they have access to satellite-based imagery and other communication capabilities. The Montanyan 23rd Brigade is the best in the force. It is currently occupying Borrisville and the surrounding area. Centralia’s southernmost city, Borrisville, is diverse, with approximately half of its population claiming to be ethnic Montanyan. The 23rd has the best equipment and most motivated soldiers in the Montanyan military, and they will not be dug out of the city easily!

As part of the CJTF response force, A Company is deployed on the eastern side of Borrisville. A Company is commanded by CPT Aaron Murphy and has three platoons:

- 1st Platoon, led by 1LT Samantha Alvarez, the most seasoned platoon leader
- 2nd Platoon, led by 2LT Jorge Williams, who always has good intentions but less-than-stellar execution
- 3rd Platoon, led by 2LT Pete Johnson, the most recent addition to the company’s leadership.

A Company has access to heavy armor, artillery, and close air support. It also has access to several additional “enabler” forces that accompany the CJTF: civil affairs (CA), PSYOP, EW, and cyber operations. There are also a number of civilians wearing tactical pants and polo shirts who frequent the command post from time to time.

Although the United Nations authorized the deployment of military forces to Centralia, it has not yet voted to approve the use of force. So, A Company is deployed in a defensive perimeter 5 km to the east of Borrisville.

The rules of engagement allow A Company forces to protect themselves but do not yet allow them to take offensive action.

This vignette is loosely based on Christopher Paul, “Two Vignettes: How Might Combat Operations Be Different Under the Information Joint Function,” *Mad Scientist Laboratory Blog*, October 8, 2020.

employing it or for supporting tactical maneuver formations. Remember that these capabilities aren't intended to stand alone; rather, they must be synchronized with other activities to support the commander's mission, intent, and end state. When multiple capabilities are employed together, they can often achieve effects greater than the sum of their individual parts. The "Bottom Line" at the end of each section tells you what you can do as the commander (or staff) of a tactical formation, how to access the capability, and where to find more information.

1

Inherent Informational Aspects of Military Operations

Overview

The joint force has fallen into the habit of thinking about informational power as something to enable physical power instead of *using information as an element of power itself*. Think about a tank and the physical power it brings to a fight. It can shoot large-caliber rounds at targets miles away and drive through or over most obstacles, and it is largely invulnerable to small arms. Now take a minute and think about what type of informational power a tank brings. It is large, loud, and certainly intimidating. To accomplish a mission with a tank, do you need it to destroy enemy forces, intimidate a hostile population, or provide reassurance to partners? The point is that there are many inherent informational aspects to all military activities and capabilities that are not always considered or used to the best advantage.

These inherent informational aspects of different military activities can influence the perceptions and attitudes of adversaries, civilians, and other relevant actors in a local AO. This can lead to desired behavioral changes and cause actors to think, believe, and act in a certain

Having recently completed his captain's training at the Maneuver Center, CPT Murphy was excited to lead A Company. In fact, A Co. could be the best in the battalion. For the past three months, Murphy had drilled the company in all aspects of maneuver and fires. He felt confident in its proficiency in everything from conducting a deliberate attack to calling for fire or requesting a 9-line MEDEVAC. The young lieutenants understood troop-leading procedures and how to incorporate armor, artillery, and air into combined arms warfare.

"We definitely have what we need to kick the Montanyan 23rd out of Borrisville, no problem," he thought.

Now, as Murphy read through the operations order (OPORD) for his first major operation, he continued to see references to how the brigade intended to use operations in the information environment to achieve critical objectives—and he felt his confidence flagging. He knew he could ask the S3 or battalion commander or the commanding officer to explain, but the OPORD talked about a lot of things Murphy hadn't really considered. "They'll think I'm not ready for this," he thought.

way (do what you want them to do). We focus here on two capabilities that are intrinsic to any maneuver capability down to the lowest echelon: **presence, posture, and profile** and **physical attack**.

Activities

Presence, Posture, and Profile

When U.S. forces arrive in a place, they bring with them a lot of people and materiel, including things that local people have never seen before. This can be exciting or threatening to locals. Moving forces around can add or diminish credibility, depending on the type of forces and what they are doing. The mere presence of these forces has an impact.

Whenever forces enter an area, leave a base, or cross a line of departure, they both send messages and are potential sensors to collect information. These activities must be deliberate, or they will appear uncoordinated and send the wrong message. *Remember that someone is always watching.*

Presence can be physical or virtual (think social media). Presence can be threatening or reassuring. Even the absence of presence sends a message. Presence is a powerful driver of behavior and an influential tool, so plan accordingly.

Just as important as presence is **posture**, which refers to the unit’s “attitude.” You can have an active or passive posture; your posture can be warm and welcoming or hostile and intimidating. Posture can be deliberately changed to send a message. Wearing full body armor, keeping weapons at the ready, and keeping your “head on a swivel” are all active (or aggressive) postures. Having a more relaxed posture could include not wearing Kevlar and keeping weapons in the low-ready position. The problem is that some of these posture decisions are made at echelons far above the tactical level, at least when it comes to conventional maneuver forces. Regardless of guidance from higher, you still have an influence on the personal aspects of posture: whether or not you and your unit are smiling, waving, or otherwise interacting with civilians in a friendly manner.

Profile describes the amount of presence and how locals perceive the unit. It reflects the size of the unit, the number of patrols it conducts, and how those activities are conducted. Are you a constant



Murphy expected a warmer reception as elements of 1st Platoon entered the town. Why were the locals hurrying off the street and into their homes and businesses? He could see why the kids would be a little scared, but he didn't understand why the adults were intimidated by the platoon's presence. If only they'd open up and connect a little bit, he was sure they could find common ground. "Don't they know we're here to help?" he thought.

Murphy knew his troops were aggressive; that's the way 1LT Alvarez trained them to be. She wanted to bring them all home, just like Murphy did. Why take unnecessary chances? 1LT Alvarez and the platoon sergeant made sure the troops had the highest level of protection and an active defensive posture, wearing full kit with weapons at the ready, regardless of the risk assessment.

Was the sight of armor and weapons making the locals feel *less* safe? Murphy wondered.

friendly presence or a scary and anxiety-producing group that thunders through a few times a week? Are locals afraid to interact with the unit, or are they warm and welcoming? Is the unit viewed as a source of security, an economic opportunity, or an occupying force? Profile contributes to the unit's reputation in the AO.

Physical Attack

Shooting artillery, dropping bombs, and assaulting an enemy with maneuver formations can directly contribute to mission accomplishment. It also can dramatically affect combatants' mental state. Combat power can intimidate and deter future adversary activities. After all, eliminating an enemy will certainly impede its decisionmaking capability, as will blowing up its communication equipment. Physical attack can be the mission, or it can support OIE.

When used alone, physical attack is one of the most powerful psychological tools at a unit's disposal. However, it is more effective when combined with other capabilities. Table 3 highlights additional capabilities that could be used in conjunction with physical attack. As the list reveals, physical attack as part of OIE typically supports or complements other capabilities, such as military deception, electronic warfare, or cyber operations. In addition to the psychological consequences of physical attack, also remember that physical destruction can affect the



TABLE 3
Use Cases: Inherent Informational Aspects of Military Operations

Problem	Tactic/Technique	Effect
Enemy reconnaissance is surveilling your position	Conduct a physical attack as part of tactical deception operations.	Lure the enemy away from where you are actually conducting operations.
Enemy is in a defensible position	Use movement and maneuver to increase your presence in an unexpected location, but leave an evacuation route open. Combine with MISO and physical attack for added effect.	Isolate the enemy to raise anxiety levels, then inspire enemy forces to withdraw to less-defensible positions.
Local nationals feel threatened by U.S. forces	Increase presence patrols, build rapport, and downgrade personal protective equipment to the extent possible.	Increase support for (or at least tolerance of) U.S. activities in the AO.
Adversaries are intimidating local nationals in your AO	Increase physical and virtual presence. Work with PA and PSYOP units to increase U.S. messaging. Conduct more KLEs.	Reassure locals that you are there and able to protect them.
Enemy is operating in your area operations	Physically attack enemy communication nodes in conjunction with EW and cyber operations to block communications.	The enemy is isolated and less likely to act.

physical aspects of the IE. Make sure you won't need that communication infrastructure or equipment later before destroying it.

Bottom Line: Inherent Informational Aspects of Military Operations

What can my unit do now?

A lot! To a large extent, many decisions related to presence, posture, and profile fall to the tactical level. The gear you carry may be dictated by higher tactical echelons, but you can determine both the posture and profile of your unit. You can also largely determine how much presence you have in the AO. Determining how aggressive or passive a unit needs to be is up to junior leaders, but it should be a conscious decision that is based on desired effects.

In terms of physical attack, as a fighting element of the U.S. military, your unit brings quite a bit of destructive power to any operation. The key is to consider not only what you need to destroy but also



how that destruction will affect enemy combatants and local civilians. Sometimes, you want to bring overwhelming firepower and destruction. Other times, you need to be more selective in what you destroy.

Where do I go for this capability?

You're it! More than almost any other capability, you can determine presence, posture, and profile. While higher command may dictate some things, you can influence the posture of your forces and how (and to what degree) they interact with locals.

Higher echelons will determine when and where you conduct an attack, but you must consider physical power in light of informational objectives and effects. Think about your presence, posture, and profile in all operations and consider what message you want to send to the enemy and civilians. *Remember, everything you do (or don't do) sends a message.*

Murphy called for a ceasefire across the net. Now that shots were fired and the "hot" war had started, he wanted to ensure that the mission was accomplished with minimal combat losses. He knew he had a follow-on mission to capture the village 5 km to his front and needed to conserve combat power. Intel reports had told him he was facing off against a second-tier unit that had questionable vehicles and equipment. After the pasting he just gave them with the BN's 120-mm mortars and 2nd Platoon's .50 cal's, he knew they weren't going to stay in place. True to form, he saw ones and twos then groups of enemy abandoning their positions. Good for him and bad for them; he knew they had no idea that Alvarez and her 1st Platoon were waiting in concealed positions to their rear.



2 Key Leader Engagement

Overview

Deployed units often conduct operations amid complex cultural, social, and political dynamics. In the AO, physical proximity to civilians means that personnel will inevitably encounter local communicators and leaders. These interactions provide an opportunity to strengthen relationships and security—if they are effectively planned and executed. Military personnel conduct **key leader engagements** (KLEs) to engage in critical dialogue and better understand and more effectively operate within a given cultural, social, and political environment.¹ These engagements can help build alliances, encourage cooperation and noninterference, and boost support for U.S. objectives.

Activities

KLEs are deliberate, planned, and purpose-driven dialogues that require research, preparation, and specific objectives. They offer an avenue to approach diverse problems and can be used to engage and influence foreign leaders at the strategic, operational, and tactical levels.

KLEs typically involve a scheduled meeting, but you should also be prepared for a chance encounter with a leader. Interactions can occur in person or via telephone or videoconference. In either instance, there should always be someone present to take notes. The person leading the KLE should focus on the engagement and not on taking notes.

KLEs support mission accomplishment by informing or influencing actors in the AO. Engaging in dialogue with key leaders can provide new information, resolve problems with civilian populations, and even forge new alliances within the battlespace. KLEs may also be directed toward specific key communicators, such as religious, academic, or tribal leaders. These interactions can be used with a wide range of operations, such as stability operations, counterinsurgency

¹ The Army now uses the term **soldier and leader engagement**, reflecting the importance of all engagements, not just those executed by unit leadership.

Sometimes, it seemed like all Murphy did was KLEs when he'd rather be doing something exciting, like maneuvering his company or blowing something up. He particularly dreaded talking to the local mayor. Murphy knew it would be at least an hour of talking in circles and the mayor presenting a laundry list of all the things the unit was not doing for the community.

When he asked the S3 if it was really necessary, she gave him a terse reply. "Lieutenant, do you know division is reading every report you write about that mayor to help the PSYOP bubbas generate messages targeting the local Montanyans, baseline how effective our operations are, and assess our OPSEC?" As Murphy prepared to brief the next OPORD, he felt better about the importance of every one of those tedious meetings.

operations, noncombatant evacuation operations, security cooperation activities, and humanitarian operations. When fully integrated with other IRCs, KLEs can effectively shape and influence leaders and, in turn, foreign audiences.

Deliberate Engagements

Deliberate engagements are anticipated and planned interpersonal interactions to achieve a specific effect or objective. Planning and research should include the creation of a face-to-face engagement outline. Sketching an outline can help you plan, conduct, monitor, and assess all forms of engagement with foreign leaders, key communicators, and local populations.

Dynamic Engagements

Interactions with foreign leaders or communicators may be impromptu or dynamic engagements. This could include spontaneous face-to-face conversations with local civilian leadership while conducting dismounted patrols or unsolicited visits from local leaders to an operating base or combat outpost. Although they are unplanned, it is important to prepare for them. Preparation for dynamic engagement starts as early as initial entry training and should be reinforced through continued professional development. Displaying respect for others, communicating honestly, and remaining mindful of the local culture will inevitably increase the likelihood of a positive outcome in any human



TABLE 4
Use Cases: Key Leader Engagement

Problem	Tactic/Technique	Effect
Local population lacks awareness of U.S. security cooperation with the host nation	When permissions exist and OPSEC requirements are met, public affairs or combat camera document KLEs, and MISO or public affairs disseminates the documentation to target audiences.	Increase local trust in U.S. forces, with validation from host-nation leadership enhancing force posture.
Civilian non-interference	Conduct KLEs to ensure the safety of local populations and permit movement of military vehicles and establishment of defensive positions.	Enhance force protection, mitigate civilian casualties, and increase confidence in rules of engagement.
Crisis management	Engage in dialogue following a crisis (e.g., accident, enemy attack, disease outbreak) to mitigate social and political fallout, which could reduce force effectiveness.	Mitigate civil disturbances from fear or lack of security, increase effectiveness of operations, and increase public trust.
Cultural misunderstandings	Engage with local leaders, including religious leaders, and media to mitigate potential or actual misunderstandings and navigate culturally complex situations.	Mitigate civil disturbances from soldier misconduct and increase public trust.
Hostile or neutral leader/population	Engage with leaders of hostile or neutral populations to shift public perceptions and create a more favorable AO.	Increase public trust, increase potential for tips, mitigate civil disturbances, and enhance force protection.
Cordon-and-search or clearing operations	Coordinate or be prepared for a KLE on short notice (e.g., having trained personnel at the ready) to facilitate and streamline operations.	Enhance force protection, mitigate civilian casualties, increase confidence in rules of engagement, and mitigate civil disturbances.
Civil disturbance and rioting	Plan ahead and be prepared for KLEs, either deliberate or dynamic. Leaders can more effectively dissuade groups engaged in civil disturbance.	Mitigate or dispel civil disturbance events and enhance force presence, posture, and profile.
Missing service member or duty status—whereabouts unknown (DUSTWUN)	During a DUSTWUN, both deliberate and dynamic engagements could result in information or support.	Establish a force multiplier to increase the likelihood of locating or extracting missing persons.
Unreported criminal or enemy activity	Use KLEs to help local populations understand U.S. force commitment to resolving the conflict, as well as when and how to report activities.	Increase the likelihood of reporting on criminal or enemy activities and decrease U.S. and civilian casualties.



interaction. Role-playing exercises can help prepare service members and leaders for productive interactions.

Bottom Line: Key Leader Engagement

What can my unit do now?

You can do a lot! It's up to you to understand local leaders and prepare for deliberate and dynamic engagement. You need to understand their behaviors and what drives them. Think about what they want and where that might overlap with what you want. Ask, "If I were the local mayor, what would I try to get from these Americans?" Plan for routine engagements, learn as much about the local culture and current situation as you can, and be prepared for chance engagements.

Where do I go for this capability?

You have it, and you are it. And you might consult your commander if you find you are engaging with leaders who significantly outrank you. You can also ask public affairs and PSYOP personnel to help you practice engagements. Both capabilities will help you think through how an engagement could unfold and prepare you for likely questions. Public affairs can also provide you with higher command's talking points. Finally, don't forget about intelligence reports. Put in a request for information with the S2 on the key leaders in your AO. You may be surprised by what you didn't know. And remember to debrief with the S2. What you learn during an engagement might not be widely known across the force.

In preparation for engagements, consider referencing the graphic training aids and the Center for Army Lessons Learned quick reference guide to information operations, which are included in the references for this topic.



3 Civil-Military Operations and Civil Affairs Operations

Overview

Civil-military operations (CMO) and **civil affairs operations** (CAO) seek to mobilize civil networks to enable and empower military operations, leveraging cooperation and communication with civilian agencies and organizations to achieve common goals. These operations can enhance situational understanding, mitigate threats to civil society, and consolidate gains from security and stability operations. There is often confusion between CMO and CAO—namely, who has the appropriate authorities and who typically executes them. Below are the formal definitions from joint doctrine.¹

CMO are intrinsic:

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.

CAO are extrinsic:

Actions planned, coordinated, executed, and assessed to enhance awareness of, and manage the interaction with, the civil component of the OE; identify and mitigate underlying causes of instability within civil society; and/or involve the application of functional specialty skills normally the responsibility of civil government.

Put simply, CMO are conducted by any military unit or person (intrinsic) in coordination with the civil population, whereas civil affairs forces (extrinsic) conduct CAO, a subset of CMO. What does this mean for a tactical maneuver unit? It means that you don't need to involve civil affairs or worry about accessing tightly controlled authori-

¹ JP 3-57, *Civil-Military Operations*, Washington, D.C., July 9, 2018, p. GL-6.

Man, was this farmer MAD! Did it really matter that they killed the donkey? Murphy couldn't believe he was still at the farm four hours after LT Johnson's 3rd Platoon accidentally ran it over. He could totally believe that Johnson got his platoon lost—can't spell "lost" without "LT," after all. If that farmer would have just fixed the ditch next to the road, they would have been able to swerve. By now, he should be back at base eating chow instead of filling out paperwork. Too bad he couldn't just fix the ditch himself.

ties to interact with civilians. But it is still important to be deliberate. Every engagement with civilians matters and should be thought of as an opportunity.

One additional note on terminology: Understand that **civil-military cooperation** is what NATO and many U.S. partners call the joint function of **civil-military interaction**.² This is relevant because U.S. forces contribute to combined, multinational operations that involve extensive interaction with civilian populations. Partner and allied forces commonly use civil-military cooperation (abbreviated as CIMIC) to refer to what U.S. forces would call **CMO** or **CAO**, as well as the forces conducting such activities.

Finally, it's important to remember that these types of operations are ultimately about *increasing operational effectiveness* rather than just *being nice*. There is far more to CMO than simply handing out soccer balls or making local populations *like* the U.S. military.

The Army is the largest provider of civil affairs capabilities to the joint force. Army civil affairs capabilities can be found at every echelon—from theater planning teams to tactical teams—and in the active component, special operations, and reserve component as part of conventional forces. The Marine Corps also has a limited civil affairs

² NATO defines **civil-military interaction** as “a group of activities, founded on communication, planning and coordination, that NATO military bodies share and conduct with international and local non-military actors, both during NATO operations and in preparation for them, thereby mutually increasing the effectiveness and efficiency of their respective actions in response to crises” (NATO Standardization Office, *Allied Joint Doctrine for Civil-Military Co-Operation*, AJP-3.19, Edition A, Version 1, November 2018).



capability, which resides almost exclusively in the reserve component. The Navy and Air Force do not have formal civil affairs organizations.³

Activities

The requirement for CMO exists at all levels, but civil affairs is a high-demand/low-density capability. Ideally there would be specialists to support all maneuver units, but that is not practical. If you are fortunate enough to be assigned a civil affairs team, make use of it. Civil considerations are part of the mission variable set (mission, enemy, terrain and weather, troops available, support available—time, and civil considerations, or METT-TC). They also include political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) factors. While these concepts should be familiar, civil affairs personnel are the experts.

Couldn't someone get these locals out of the AO?! There were literally hundreds of locals sitting outside the base asking for jobs. They were thirsty, hungry, and generally impeding operations. Wasn't there some local group to help with this kind of thing? Murphy really wanted to ask someone to deal with these people, but he didn't know who to ask.

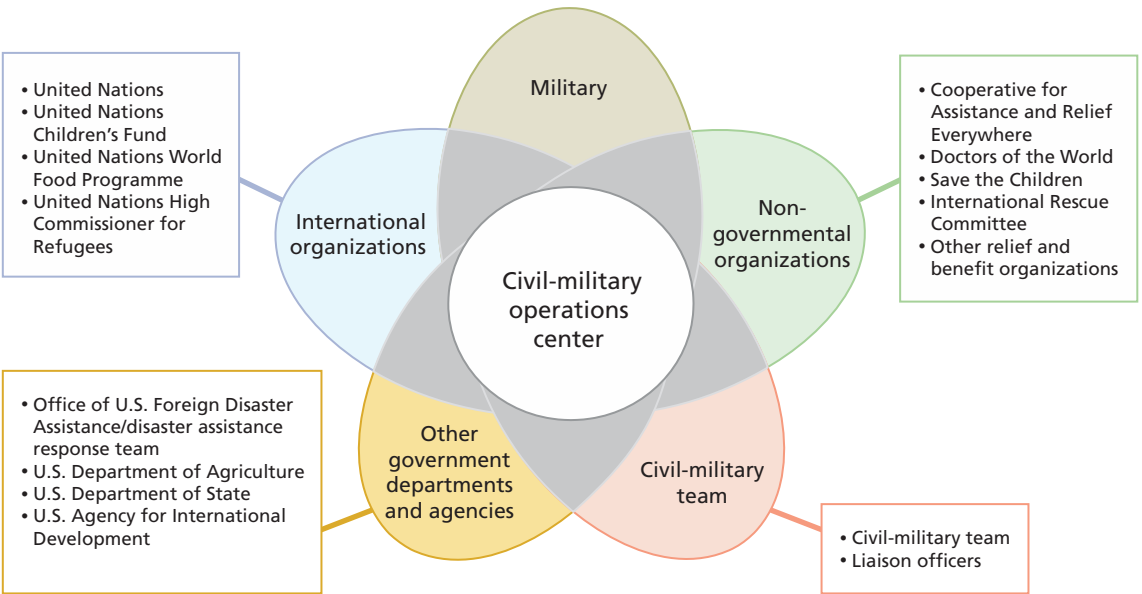
“CMO are inherently joint, interagency, and multinational,”⁴ meaning that, in addition to indigenous personnel and institutions, this is one way the U.S. military connects with other U.S. government actors (e.g., the U.S. Department of State, U.S. Agency for International Development), the United Nations and other international entities, and nongovernmental organizations, like the Red Cross/Red Crescent. At times, these organizations might work directly with a tactical unit, or civil affairs might support their mission. These organizations can enhance mission effectiveness and support a commander's mission. Although a civil affairs team can help navigate this complex web of stakeholders, a maneuver unit at the tactical level is likely to have access to a civil-military operations center (CMOC), like the one

³ JP 3-57, 2018, p. A-2.

⁴ FM 3-57, *Civil Affairs Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, April 2019.



FIGURE 1
Notional Civil-Military Operations Center



SOURCE: Adapted from JP 3-57, 2018, p. II-6.

shown in Figure 1. The CMOC is a place to engage with interagency, host-nation, and other partners.

Civil affairs activities at the tactical level enhance understanding of the civil component of the OE. The following are the key

TABLE 5

Use Cases: Civil-Military Operations and Civil Affairs Operations

Problem	Tactic/Technique	Effect
Potential civilians in combat area	Conduct clearing operations with civil affairs teams and maneuver teams to address unexpected misunderstandings with civilians.	Enhance tactical maneuver, mitigate civilian casualties, and identify threats and opportunities.
Cultural misunderstandings	Advise the commander/supported unit on cultural mores and mitigate risks of unintended insult to local civilians.	Mitigate civil disturbances resulting from soldier misconduct and increase public trust.
Lack of information about the local area	Advise the commander on local requirements and infrastructural centers of gravity and ensure cultural understanding.	Identify threats or opportunities, refine targeting inputs, and provide context for decisions.
Ineffective communication with local leaders	Advise the commander on effective modes of engagement with local leaders, facilitate discussions, and offer solutions.	Increase public trust and increase potential for tips on enemy activities.
Lack of trust from local noncombatants	Build rapport and develop lines of communication with local populations, facilitating cooperation and information sharing.	Increase public trust and increase potential for tips on enemy activities.
Damaged (or just weak) civilian infrastructure	Engage with local leaders to identify root causes of damage/destruction of civilian infrastructure or property and deconflict possible reparations.	Increase public trust, increase potential for tips on enemy activities, and identify centers of gravity.
Ineffective humanitarian relief coordination	Engage with nongovernmental organizations and interagency contacts on management and logistics of medical supplies or aid materials in the AO.	Improved public image with local population, better relationship with partner organizations, and more trust.
Deconflict patrol tensions	Conduct presence patrols and engage with local leaders with civil affairs teams, build rapport, communicate U.S. intentions, and ease tensions related to U.S. force patrols.	Mitigate civil disturbances, improve force posture, gather passive intelligence.
Ineffective coordination with host-nation authorities	Conduct civil-military operations with civil affairs teams to facilitate effective dialogue with host-nation civil authorities.	Identify threats and opportunities.



tasks or missions that civil affairs can conduct in support of mission accomplishment:

- **Civil reconnaissance** is a planned observation and evaluation of civil aspects of the OE. Data are collected to enhance situational understanding and aid the commander in decisionmaking.
- **Civil engagement** is an activity or interaction between civil affairs forces and nonmilitary individuals designed to build relationships, reduce interference or causes of instability, gather information, and promote trust between U.S. forces and others.
- **Civil information management/civil knowledge** integration is the process by which data related to the civil component of the OE are gathered, stored, processed, and analyzed. These data are used to develop collection plans, evaluate civil information, and enhance the civil component of a commander's common operating picture.

Bottom Line: Civil-Military Operations and Civil Affairs Operations

What can my unit do now?

For CMO, there is a lot that your unit can do. You can help to pick up trash, clean out an irrigation canal, or repair a building. You don't need special authorities for these activities, but you should coordinate with higher for materials and supplies, if needed. Keep in mind that these activities build rapport and send a message. U.S. forces don't dig wells and hand out supplies without a purpose. Listen to local concerns to get information about the enemy while winning over civilian populations. For CAO, civil affairs forces may be tasked to conduct missions in your AO. Be aware that they are working on behalf of the commander and have their own mission requirements. You may be asked to help provide security for them or assist them as they work with local civil society groups, nongovernmental organizations, or other aid groups.



Where do I go for this capability?

The CMOC or S/G-9, if one exists for your organization, is where a CMO planner is likely to be located. This individual should have purview over the command's CMO and a thorough understanding of civil considerations in the AO. Personnel at the CMOC may have suggestions for CMO activities. See the following annexes in the operations/execute order for more additional guidance: Annex G, Civil-Military Operations (J9/G-9/S9); Annex K, Civil Affairs Operations (G-9/S9); Annex P, Host-Nation Support (G-4/S4); and Annex V, Interagency Coordination (G-3/S3 and G-9/S9).

There are many Army and Marine CA doctrinal publications and graphical aids that can assist you with planning or executing CMO. You can also reach out to your S/G-9 planner for additional support. If you don't have one of those, coordinate through your S/G-3 section. The CIMIC Centre of Excellence is also a great resource. It is a NATO-accredited organization that leads doctrine development, maintains a repository of lessons learned, and provides training and education. It offers a wealth of resources for executing CMO/CAO/CIMIC, most of which are publicly available.



4 Public Affairs and Combat Camera/Service Member Camera

Overview of Public Affairs

Public affairs have three major roles: (1) monitoring and reporting on public messaging and mass media to identify risks and opportunities, (2) planning and implementing public information and outreach to achieve mission goals and objectives, and (3) coordinating with higher echelon public affairs staff on regional and multinational narratives.¹

Public affairs professionals develop public affairs communication plans to support the execution of the commander's communication strategy. This is the commander's blueprint and design for coordinating and synchronizing themes, messages, images, and actions to support information-related objectives. Synchronizing messaging ensures the integrity and consistency of command themes to the lowest tactical level.

Activities

Engaging with Media

Public affairs professionals take the lead in public-facing operations and can facilitate media engagements. In the Army, they are among the few who can directly communicate service-level and commander messages directly to the global and American public. They will have the most recent Public Affairs Guidance (PAG), with relevant topics and talking points. While tactical units are conducting operations, public affairs can amplify the effects through public exposure, such as by releasing video or other evidence of KLEs.

You might find yourself in a position where there are reporters in the AO that aren't embedded with your unit because they are acting independently, are locals, or are uncredentialed aspiring journalists. You need to understand how to act if this happens. Getting guidance

¹ The Marine Corps has combined public affairs and combat camera into what it calls **COMMSTRAT** (communication strategy). We elected to leave them separate in this handbook.

It wasn't true, but now it was on the news. A few hours ago, someone had posted a video claiming that a U.S. military vehicle had struck and killed a small girl in the outskirts of Borrisville, in Murphy's AO.

It started on a dubious social media account linked to a local group that was sympathetic to Montanyan forces. The video then jumped to several other, more reputable sites before it was picked up by the local news. Now, it had been viewed tens of thousands of times. Murphy needed help to combat this false story. He knew that higher had a smart PA officer who he saw on the local news from time to time. She always seemed to have the right answers. Maybe he could ask her.

beforehand from your battalion S1 or PA officer can help with this. This guidance is also helpful if you have an embedded journalist with your unit. In these instances, view the journalist as a way to tell your story and the good things that your unit is doing to help achieve the command's mission. Stay in your lane and speak to the things your unit is doing. Don't speculate, get dragged into a political conversation, or find yourself cornered into discussing something that you aren't qualified to address.

Building the Common Operating Picture

Public affairs professionals support tactical units by managing public information and its impact on operations. They also coordinate with leadership and staff to mitigate operational surprises and achieve objectives through public messaging and engagements—for example, by monitoring social and mass media for trends that could affect operations.

Coordinating Reachback

Depending on the unit mission, public affairs staff will reach back to a higher command for additional support and coordination with DoD, interagency, and other partner efforts.

Tactical Support

Public affairs detachments (PADs) are often dispatched with combat patrols and small units that deploy to remote locations. Tactical digi-



tal media kits allow these teams to gather, process, and deliver audio files, digital imagery, and other media in austere environments with cameras and video equipment, laptops, night-vision devices, and audio gear. The kits aid globally deployed combat camera (COMCAM) teams, public affairs detachments and MISO teams operating from tactical command posts, forward operating bases, combat outposts, and forward-deployed combat patrols. PADs may be expected to create products for internal and external audiences, such as a newspaper, magazine, or newscast, and interact with civilian media outlets. It can also provide release authority and guidance on casualty and mortuary affairs and prisoner-of-war/missing-in-action matters.

Tactical digital media kits help to uphold a policy of “maximum disclosure, minimum delay.” Timely use of visual imagery can effectively counter adversary propaganda, such as accusations of civilian casualties. In that same vein, the PA officer can enact media embargoes, which are designed to enforce OPSEC while also ensuring the timely release of appropriate and accurate information.

Over the past few years, Montanya had made a point of buying out struggling radio and television stations in western Centralia and replacing them with Montanyan-language programming that was, of course, very pro-Montanyan. After the initial invasion, Montanya made sure its messages dominated, targeting both ethnic Montanyans in Centralia and Centralians using media it already controlled. Murphy couldn't control the media, but he could get his own story out.

IRC Coordination: Defining the Narrative

PA professionals collect, develop, and disseminate public information, command information, and community engagement themes, messages, and talking points, requiring an understanding of potential second- and third-order effects on intended and unintended publics. To avoid information fratricide, public affairs officers synchronize themes, messages, and talking points with other operational and tactical IRCs as needed.



Overview of Combat Camera and Service Member Camera

Combat camera (COMCAM) is a primary supplier of operational imagery and is a fundamental tool for decisionmakers and commanders at the tactical level. It helps counter misinformation, disinformation, and propaganda; provides legal and evidentiary documentation; facilitates battlefield and environmental assessments; and supports other IRC documentation.²

Service members can perform a similar function using their own camera or smartphone cameras (if allowed in the AO), allowing them to document activities as they unfold, refute false claims, and provide evidence of activities conducted during operations.

Activities

Support to Operations

A picture is worth a thousand words. Imagery is a vital component of commanders' decisionmaking and civil affairs, public affairs, KLE, and MISO. It also supports sensitive site exploitation activities. To maximize the use of digital imagery, a designated photographer in the unit should be selected. This unit photographer should be given specific guidance on what kinds of images are required.

Documentation

Documentation of operations and events for the historical record, legal and evidentiary purposes, or to support investigations is another important activity.

Assessments

Visual imagery is used for battle damage and environmental assessments to show, respectively, damage sustained or inflicted and environmental conditions before, during, and after an operation or exercise.

² The Navy and Marine Corps no longer maintain a deployable COMCAM capability.



TABLE 6
Use Cases: Public Affairs and Combat Camera/Service Member Camera

Problem	Tactic/Technique	Effect
Responding to crisis and disaster	Work with visual imagery and COMCAM to cover the event while reaching back to major command for messaging and guidance on host-nation actions.	Quickly set the narrative and response.
False claims	Work with visual imagery and COMCAM to cover the event while reaching back to higher for messaging and host nation actions.	Quickly, publicly refute false claims and reinforce the narrative.
Media personnel on the battlefield	Engage with media, instruct soldiers on how to engage with media, prepare talking points.	Ensure OPSEC and that the right story is provided.
Media engagements	Schedule media engagements to inform the public about operations, sharing as much as you can as soon as you can.	Conduct good interviews.
Damaged civilian infrastructure	Respond quickly with COMCAM to document extent of damage, then respond as directed.	Limit collateral damage, negative press, and fallout from the event.
Civilian casualties	Respond quickly with COMCAM to document extent of casualties and respond as directed.	Limit collateral damage, negative press, and fallout from the event.
Propaganda and false narratives	Establish battle-tempo of informing public with COMCAM documentation and other appropriate information materials.	Demonstrate transparency and gain trust.

Bottom Line: Public Affairs and Combat Camera/Service Member Camera

What can my unit do now?

For PA, there isn't much that you can do at the tactical level. PA is handled by PA professionals. Don't try to get into their lane by using social media and going directly to the American public. Remember to stay in your lane and only talk about things that you have knowledge about. You don't want to become the strategic private that appears on the nightly news talking about something you are not qualified or approved to discuss.

However, you should be aware of PAG and always have a copy of the most up-to-date talking points, themes, and messages. You can



request that PA provide media or interview training so that you are more prepared when you run into a journalist on the battlefield. In these instances, refer to your PAG or your battalion S1 for guidance, because they will usually be filling in the PA role at the battalion level.

For combat camera, you have access to a camera, either through a smartphone (if allowed in the AO) or COMCAM personnel assigned to your unit. Use it! Make sure that you document who took a photo, when it was taken, and where it was taken. Document as much as possible to support your operations, provide information to the S2, and document damage and activities.

One thing you can't do is use your device in an unauthorized manner, such as inadvertently or intentionally disseminating imagery that could compromise the security of an operation, forces, or noncombatants. Also, PSYOP personnel may have cameras that can be leveraged for mission support.

Where do I go for this capability?

If your unit does not have a PAD, consult with your commander before making a request for PA support. There will be PA personnel at either the regiment or brigade level. You can also request support through your S/G-1. All the services have PA professionals who have access to products, training materials, and courses that can assist tactical leaders. They can provide additional insight and instruction on the use of social media and cameras in the AO. They should be your first stop in seeking guidance or training on any aspects of PA.

Fortunately, one of Murphy's NCOs had a video of the actual incident clearly showing that the victim was an animal, not a small girl. The PA officer pointed out several sources of disinformation, including stock footage of outdated vehicles, to present the truth. She actually got the local news to run a segment on the manipulation, turning the tables just a bit. Unfortunately, the false narrative that U.S. forces were careless and ignorant persisted on regional social media.



5 Operations Security and Signature Management

Overview of Operations Security

The purpose of OPSEC is to ensure mission success by preventing an adversary from observing and exploiting critical information and indicators.¹ It is a **capability that employs a process** to systematically identify, control, and protect critical information. It plays a vital role in protecting the force and the mission. Identifying what the enemy can observe alerts commanders and units to vulnerabilities. Once a vulnerability is identified, OPSEC can assist in developing countermeasures, including support for deception activities. Employing trained OPSEC personnel to test your unit for vulnerabilities—from traffic patterns to social media use—protects lives and missions.

The first step is to identify the essential secret(s) needed for the planned activity. Essential secrets are **operational aspects of friendly operations** that carry a risk of mission failure or other severe consequences if compromised, discovered, or leaked. OPSEC personnel identify and mitigate these vulnerabilities.

The following are some examples of operational aspects of friendly operations:

- Presence: current physical or virtual location
- Capability: what you can do
- Strength: number of forces or amount of capability
- Intent: what you plan to do
- Readiness: preparedness for the mission
- Timing: when an action will occur
- Location: where an action will occur
- Method: how you intend to accomplish objectives.

For every plan, activity, patrol, or anything else that might be of interest to an adversary (or should otherwise not be shared), figure

¹ This section draws heavily on a draft OPSEC smart card provided by a subject-matter expert in the Joint Information Operations Warfare Center's Joint OPSEC Support Element.

The enemy's spotter network was driving everyone in the BN crazy, Murphy included. Whenever they left the gate, the enemy seemed to know their every move. And SIGINT couldn't tell which selectors were civilian and which were used by the enemy. The BN commander finally got fed up and convinced the JAG to allow jamming as a matter of force protection. The next time they went on patrol, all civilian comms were jammed, which irritated the locals. But Murphy's unit could finally move without spotters communicating their route. Yet, for some reason, all they did on the patrol was go to an isolated area. That was dumb, thought Murphy. Why are we going into the middle of nowhere?

A few days later, Murphy got his answer. When they turned off the jammers, the first people on the net in that remote area had been spotters—and now intel knew who they were.

out which aspects might ruin the commander's plan—or *your* plan—if leaked. The next step is to identify some **indicators** or observables that could give them away.

Here are some examples of indicators:

- Changes to security procedures
- Visual observation of specialized equipment
- Specialized equipment emanations
- Tracking of flights and ships
- Increase (or decrease) in activity
- Changes in operational tempo
- Reception, staging, onward movement, and integration:
 - Troop and equipment arrivals/movements
 - Staging of cargo vehicles
 - Bag drops, muster, or formations outside normal hours
- Geolocation features.

Once you have selected your indicators, you need to ask two questions:

1. What are the enemy's collection capabilities (e.g., signals intelligence, human intelligence, open-source intelligence)? Plan for the worst case, not the easiest case!



2. What countermeasures can I employ? Be specific: Detail which countermeasure you plan to employ against which collection capability and which operational aspect it will protect. More countermeasures are not necessarily better and will be challenging to coordinate. Think it through, deconflict, and communicate.

Overview of Signature Management

In 2018, Marine Corps Commandant Gen. Robert B. Neller cautioned,

The next fight will be a battle of signatures. Assume everything we do, can and will be observed. On tomorrow's battlefield, *to be seen is to be targeted, to be targeted is to be engaged, to be engaged is to be killed, at range and with precision!*²

Signature management (SIGMAN), like OPSEC, is a capability and a process. It is a way to understand friendly force signatures and indicators, identify adversary methods to collect those signatures,

Murphy was frustrated. Why had the BN suddenly started conducting mission rehearsals inside that giant metal warehouse? It was a million degrees in there, while it was only about a thousand degrees outside and at least there was a breeze. Sure, outside made their sand table and rehearsals a bit more visible, but who was around? The OPSEC geeks were probably worried about some fantasy enemy drone.

Then one day, it happened. They started a patrol just as they had rehearsed, when there was a burst of comms and they were ordered to return. What the hell?

The little game became clear when they got back and were ordered into formation. Suddenly the counterintelligence sergeant appeared with a couple of MPs and arrested one of their local partners! Turns out, she'd been tipping their plans. The boss had switched the rehearsals to inside to make sure it wasn't a drone or a spotter, while intel, counterintel, and OPSEC put together a plan. They rotated which host-nation partner was present at the rehearsals, then monitored comms and enemy activities as patrols started. Luckily, they caught it early, before someone walked into a nasty ambush.

² Gen. Robert B. Neller, Commandant, U.S. Marine Corps, *Message to the Force 2018: "Execute,"* January 26, 2018. Emphasis in original.



and develop countermeasures to mask those signatures. Some liken the term **SIGMAN** to “offensive OPSEC,” because, through the process of analyzing own-force signatures, you can develop ways to lead the adversary to incorrect conclusions while concealing your true intentions.

Whether the challenge is managing physical signatures through camouflage, concealment, and deception or technical signatures on the electromagnetic spectrum, Neller feared that a decline in signature management capabilities could have grave consequences.³

SIGMAN can limit your vulnerability to, for example, indirect fires, ambush, and detection that would prevent surprise. Military units often generate enormous physical, electronic, thermal, acoustic, and other signatures that can be detected even by unsophisticated adversaries. (Imagine tanks rolling through your local mall.) Emission control measures (e.g., frequency hopping, limiting transmission times, PACE [primary, alternate, contingency, and emergency] communication plans, cellphone discipline) increase combat effectiveness, survivability, and deception opportunities.

Physical Signature

Physical signatures are things that the adversary can observe through direct observation, drones, or satellite imagery. They can be a large concentration of forces, recently dug foxholes or tracks in the mud, a command post, or just a solitary military vehicle. These types of signatures can be detected by electro-optical, infrared, or synthetic aperture

The trouble all started with an out-of-office email. Murphy and his unit were going to the field for a weeklong exercise and wouldn't have email access. During the exercise, someone red-teaming the exercise saw the out-of-office emails, did a few quick searches on social media, and found that posts had stopped when the company left for the field. Even worse, a couple of posts mentioned the departure. Assembling a list of people involved in the exercise and how long they would be away was not difficult. When the report on OPSEC violations reached the BN commander, Murphy and the rest of the company were called in for a very unpleasant “discussion.”

³ Neller, 2018.



radar assets and can detect heat signatures and compare before and after images of a location.

Technical Signature

These types of signatures are generated by friendly force use of the electromagnetic spectrum. They include radio frequency (RF), radar, acoustic, scent, chemical, or radiation emissions outside the RF spectrum. They are typically collected through signals or measurement intelligence assets.

Administrative Signature

Administrative signatures are created by an individual or unit while conducting routine or combat operations. They include planning or research material, Defense Travel System orders or reservations, passport requirements, social media posts, official media releases, and logistics or contracting requests. Both open-source and human intelligence can collect these types of signatures.

Bottom Line: OPSEC and Signature Management

What can my unit do now?

You should definitely be concerned about OPSEC and signature management at the tactical level, including controlling the signals your unit emits and the observable information that can be collected by an enemy. Most OPSEC planning is done at the brigade or regimental levels, though it is still a concern of companies and battalions.

Where do I go for this capability?

Higher echelons should have OPSEC officers. However, you will rarely go directly to these individuals. Instead, work through the command channels and your S3. You can work with your S6 or EW personnel to monitor and track your digital emissions. If you are concerned about deception in support of OPSEC or foreign intelligence monitoring, your S2 can direct you to a counterintelligence officer.



TABLE 7
Use Cases: OPSEC and Signature Management

Problem	Tactic/Technique	Effect
Enemy locations unknown	Attract enemy to reveal positions, suppress signatures for illusion of safety, mislead enemy about your location.	Encourage enemy to reveal their locations.
Need enemy to concentrate or disperse forces	Suppress or amplify signatures in key areas, mislead or distract the enemy (e.g., shiny objects, deception materials), and overload sensors in selected areas.	Redirect enemy focus and influence movement of its forces.
Need to conduct surprise attack	Repackage known organizational or capability signatures, suppress signatures, overload enemy sensors, mislead or distract the enemy, and increase OPSEC.	Prevent enemy knowledge of attack planning or preparations and prevent enemy detection of attack.
Need enemy not to commit reserves	Repackage known organizational or capability signatures, amplify selected signatures, and mislead or distract the enemy.	Prevent the enemy from committing reserves to the right location, at the right time, or at all.
Enemy has detection capability	Repackage known organizational or capability signatures (e.g., electromagnetic spoofing), overload sensors, suppress signatures, increase OPSEC, support deception activities by feeding selected information to detection capability. • Use your own drone to monitor your footprint. Once you understand your signature, you can better conceal it. • Bury your electronic cables and operate radios and electronic equipment remotely.	Fool, overload, or disable enemy detection capability and support deception activities.
Enemy is monitoring social media ^a	Increase OPSEC and mislead or distract the enemy.	Prevent enemy from assessing unit and support friendly deception activities.
OPSEC violations	Provide or increase OPSEC training, conduct OPSEC red-teaming, and publicly punish, embarrass, or arrest violators.	Violations decrease, and unit can harness previous violation methods for deception activities.

^a It can be difficult to get approval for unit-level social media activities.



6 Military Deception

Overview

The purpose of a deception, at whatever level, is not just to trick someone; the purpose is to cause adversary decisionmakers to take **actions** or **inactions** harmful to themselves and favorable to you.

Tactical deception (TAC-D) is an activity that can fall within the authority, assets, and AO of tactical-level commanders with an approved plan. The intelligence requirements and planning timelines are typically shorter than for MILDEC.

Deception in support of OPSEC (DISO) is a deception activity that conveys (or denies) selected information or signatures to a foreign intelligence entity. It makes friendly force activities harder to interpret. This focus on deceiving foreign intelligence organizations instead of adversary commanders is the primary way it differs from TAC-D and MILDEC.

Military deception (MILDEC) is conducted at the operational and strategic levels of war and is designed to support major campaigns and operations. It typically requires detailed intelligence on the target (e.g., beliefs, activity patterns, training), high-level approval, and lengthy planning timelines. It uses a wide range of resources, some of which are outside your chain of command and can be difficult to acquire (e.g., social media support, aircraft platforms, certain cyber and electronic capabilities).

Activities

Several common tactics can be used to help deceive an adversary. The two most

Murphy smiled as the Montanyan UAV overflew his position. Well, it wasn't really the A Co. position anymore, but it sure looked like it was.

The company had worked hard to make it look like their hastily prepared fighting position was still in use. The camouflage and concealment made the new position, inside the treeline and several hundred meters to the east, practically undetectable—especially from overhead angles.

He couldn't see Alvarez or Williams's platoons at all and was glad that he put Johnson deep in the woods.

common tactics are **feints** and **demonstrations**. Additional tactics include diversion, ruse, and displays.

Feint

A **feint** is an offensive action that *involves contact with an adversary* for the purpose of deceiving the enemy about the real time and purpose of the main offensive action. It aims to lead the adversary to wrong conclusions about friendly force locations and intentions. Repeated feints in an area can lull the adversary into a false sense of security.

Demonstrations

A **demonstration** is a show of force that *does not initiate contact with the adversary*. It is usually conducted in an area where the unit does not plan to conduct offensive operations and is intended to make the adversary believe that offensive operations are immanent in a location where there are not.

Planning

Backward planning is key to effective deception activities:

- 1. What do you want to happen (deception goal)? (This can come from commander’s guidance.)
- 2. What does the target need to *do* or *not do* for you to achieve that goal (deception objective)?
- 3. What does the target need to sense (see, hear, intercept) to make the decision you want (desired perception)?
- 4. What assets do you have (or can you request)? When creating deception events, think broadly and creatively: dust clouds,

Every time Murphy’s unit tried to find a particular target, they would ask local leaders and elders for help. Somehow, the target always disappeared suddenly after these inquiries. One day, the IO guy at HQ had them try something different. At first Murphy thought it was a waste of time, asking about some low-level target. But pretty soon, thanks to all of the attention, locals started to think the low-level guy Murphy sought was actually important. When word got around, the actual VIP target got so angry that he came out of hiding to set things straight and punish the low-level “pretender.”



spikes in electronic emissions, vehicle movements, force deployments/positioning, loudspeaker broadcasts, media stories, leave-behinds, loud versus quiet drones, and so on. All of elements should play a role in creating a convincing deception story.

5. What assets, in what order, and at what times will convey the story (deception plan)?
6. Who will know about the deception (limited is better), and how will you protect the plan (OPSEC)?
7. How will you know whether your plan worked (assessment plan), and what steps will you take to end the deception? (Ending too suddenly could jeopardize future deceptions!)

Cause a target to take an action:

Reveal a position, commit reserve forces, take a certain route at a certain time, leave an area, relax (believing an attack is not imminent). Whatever you specifically want the target to **DO**.

Cause a target to take an inaction:

Avoid committing reserve forces, attacking at a certain time or location, or using a certain route; avoid placing an improvised explosive device (IED); avoiding the location of a downed pilot. Whatever you specifically want the target to **NOT DO**.

Here are some techniques for achieving deception objectives:¹

- Truth: To make a deception story more believable, include as much truth as possible.
- Amplifying signatures: Make a force appear larger and more capable or simulate a deployment of critical capabilities.
- Suppressing signatures: Make a force appear smaller and less capable or conceal the deployment of critical capabilities.
- Overloading enemy sensors: Confuse or corrupt enemy collection assets by providing multiple false indicators and displays.

¹ Some of these can be found in FM 3-13.4, *Army Support to Military Deception*, Washington, D.C.: Headquarters, U.S. Department of the Army, February 2019.



Murphy's unit had really loud drones that weren't doing much good. The enemy always heard them and then hid or ran away. But one day, A Co. assaulted one end of a narrow valley with the drones in front. As LT Williams's unit noisily led the company north through the valley, the Montanyans avoided contact and stayed well ahead, then walked into a very well-concealed blocking position of special operations forces secretly inserted a couple of days prior. That was a bad day for the Montanyans.

- Creating shiny objects: Misdirect enemy attention. This can also be done by “seeding” the rumor mill.
- Repackaging known organizational or capability signatures: Generate new or deceptive profiles (e.g., visible, thermal, acoustic, electromagnetic) that increase or decrease the ambiguity of friendly activity or intent.
- Conditioning the enemy by pattern/repetition: Create patterns of friendly behavior to mislead the enemy.
- Leading the enemy by substitution: Make it appear that nothing has changed, such as through the use of decoys and selectively leaked “intelligence.”
- Leading the enemy by mistake: Make the enemy believe that it has valuable information when it does not (also called *tactical leave-behinds*). Beware of overusing this technique.

Intelligence

Intelligence is *vital* to successful deception. Without careful coordination, success is unlikely, and you may endanger your unit, friendly forces, and the entire mission. Unless you understand the target—including biases, practices, activities, and training—a deception story may be ineffective or even *harmful*. The risk and the need for solid intelligence are why MILDEC (more than TAC-D) can be so difficult to get approved and take so long to plan.

Increasing Versus Decreasing Ambiguity

Deception stories are built around either *increasing ambiguity* or *decreasing ambiguity* in the mind of the target. If the target is already behaving



as you prefer (making a mistake), the deception story and related events should be designed to **decrease ambiguity** to prevent a change in this behavior. That is, they should convince the enemy that it's business as usual, possibly leading to an enemy maneuver to the wrong place, at the wrong time, and with the wrong equipment. In an ambiguity-decreasing deception, the story and events are built around no complications, no changes, no confusion, no stress; every event reinforces continuing the current belief, practice, or activity, until such time you can take advantage. A lack of intelligence on the target makes this type of deception unpractical and unwise.

Deception stories that **increase ambiguity** are designed to confuse, mislead, and stress the target to prevent an accurate assessment of your intent, location, or capabilities. This type of deception is most

Murphy quickly realized that the D-Day invasion was an easy way to understand the deception process. The deception goal was keeping the Germans from knowing Normandy was the location of the landings and moving to reinforce it. The plan used ambiguity-decreasing deception events to convince Hitler that Calais was the landing site. The deception objective was no action—for Hitler not to commit German reserves to Normandy.

The techniques included truth (the allies were going to invade France), with General Patton employing a classic decoy to draw attention to his fake 1st Army Group (leading the enemy by substitution) and its fake equipment (repackaging known signatures) to help hide (suppress signatures) the actual force buildup. Repeated air raids to the wrong sites meant the Germans were conditioned to the raids not signaling an invasion, while numerous (movie-worthy!) insertions of fake information helped reinforce Hitler's belief in the wrong landing site. The deception objective was no deployment of German reserves for two weeks. The plan worked so well that the Germans waited seven weeks before shifting their reserves, helping the allies secure Normandy and saving thousands of lives in one of history's most elaborate and successful military deceptions.

By now, the Montanyans knew Murphy's unit always did a route recon with aircraft or a drone prior to a patrol or attack, which gave him an idea. He presented it to the S3 and was surprised when she agreed. A few days later, they conducted a normal route recon, and sure enough, the Montanyans had committed additional forces to that route—and LT Alvarez's platoon unsurprisingly faced little resistance when it attacked using a different route scanned in secret a few days before.



successful with an indecisive and risk-averse target. The more intelligence you have, the more you can refine your deception story, but these types of deceptions are possible with limited intelligence, too.

Whatever your objective, keep in mind **Magruder’s principle**: It is generally easier to get the target to maintain an existing belief, so you might look first at deceptions that decrease ambiguity.

Access Versus Secrecy

Once you have developed a deception plan, you have to determine whom to share it with. Typically, the commander and operations officer are read in, but who else? It depends, and there is no rule. Units (such as supply personnel or fuelers) that are meant to serve as decoys may not behave normally if they know they are part of a deception. Conversely, not reading someone in while using them as a deception prop can create ill will. There is no perfect formula for how to balance this trade-off. Instead, realize that trade-offs will always exist, maintain mission focus, and manage accordingly.

Bottom Line: MILDEC

What can my unit do now?

You can do TAC-D at your level; it requires little coordination, but it can be quite effective. All you need is an approved plan from your commander to execute. Actual MILDEC requires longer lead times and more in-depth knowledge of the enemy, and approval is held at high echelons. DISO is all about the information that you convey or deny to **adversary intelligence forces**. You want to confuse them by creating multiple false or misleading indicators, so think about what confuses you about enemy forces and use that as a starting point.

Where do I go for this capability?

Higher echelons should have MILDEC officers. However, you will rarely go directly to these individuals. Instead, work through the command channels and your S3. You can work with S6 or EW personnel to monitor and track your digital emissions. If you are concerned about deception in support of OPSEC or foreign intelligence monitoring, your S2 can direct you to a counterintelligence officer.



7

Electronic Warfare

Overview

Electronic warfare (EW) is broken into three separate activities:

- **Electronic attack** focuses on the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment to degrade, neutralize, or destroy enemy capability. Electronic attack is considered a form of fires.
- **Electronic protection** consists of actions to protect personnel, facilities, and equipment from the effects of friendly or enemy use of the electromagnetic spectrum.
- **Electronic support** is a set of actions—requested by (or under direct control of) an operational commander—to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conducting operations.¹

The **electromagnetic spectrum** (EMS) is “the range of electromagnetic radiation frequencies from zero to infinity. For simplicity, it is divided into 26 alphabetically designated bands.”² Figure 2 provides an overview of these bands and example frequency uses.

EW Stakeholders

The EMS is wide-ranging, and numerous stakeholders are involved with EW planning, execution, and assessment.³ In the Army, at the bri-

¹ Electronic support is distinct from signals intelligence (SIGINT); they have different tasks from different authorities and serve different purposes. For more on this distinction, see, for example, JP 3-85, *Joint Electromagnetic Spectrum Operations*, Washington, D.C., May 22, 2020, p. 1-6.

² ATP 3-12.3, *Electronic Warfare Techniques*, Washington, D.C.: U.S. Department of the Army, July 2019, p. 1-2.

³ See ATP 3-12.3, Chapter 2, which lists key personnel.

gade level and higher, the lead for EW is the cyber and electronic warfare officer (electronic warfare officer elsewhere, including in joint doctrine), in the cyberspace and electromagnetic activities section, S-3/G-3 operations staff section.⁴ However, increased EW capability will be coming online in the near future with the addition of an Army EW platoon with brigade combat teams. Below the brigade level, there may be an EW representative in the S3 or S6. Company-level units may have counter–radio-controlled IED EW (CREW) specialists to manage assets, train and assist equipment operators, and advise company leadership. Marine forces have access to a radio battalion, which provides signals intelligence, EW, and limited cyber operational capability to tactical units.

Activities

For tactical maneuver units, the key question is *How can EW enable or impede my unit’s operations?* Most EW assets are retained at higher echelons, so when it comes to tactical missions, the focus is primarily on defensively navigating the EMS. The Army’s EW techniques publication calls out enemy use of geolocation and jamming as “the greatest threat to mission command information systems at the tactical level.”⁵ Of the three divisions of EW, **electronic protection** is often the most relevant to tactical maneuver units.

Before writing off “comms troubles,” take steps to troubleshoot electromagnetic interference. It could be friendly or enemy forces using the same frequencies, the proximity other equipment, atmospheric conditions, or a radio malfunction—or the enemy could be jamming your radio.

Equipment

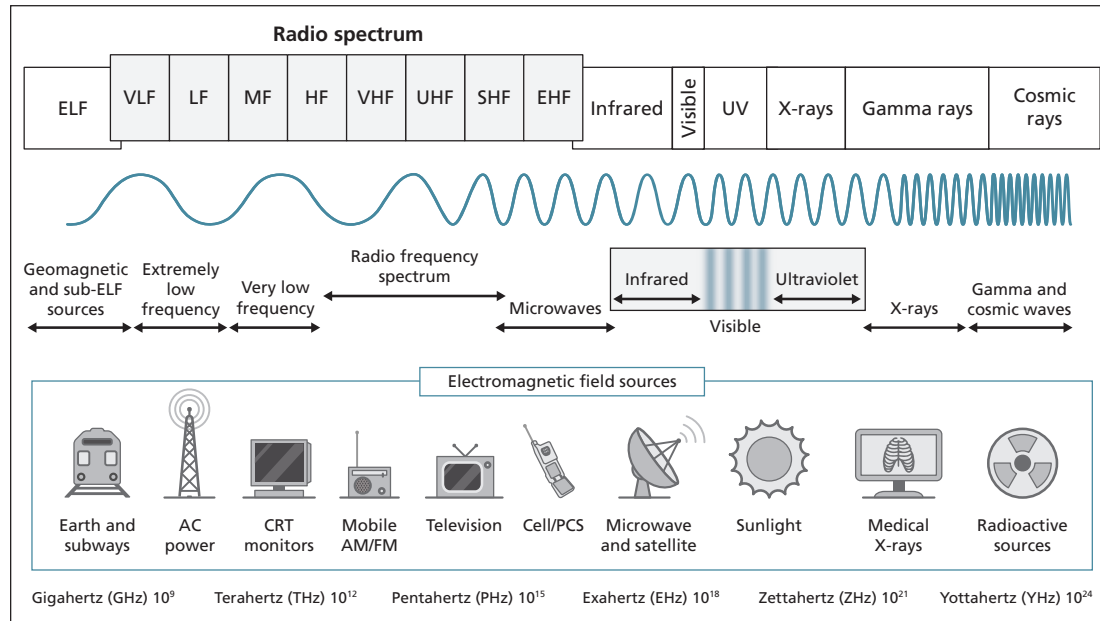
Mission-specific equipment configurations for EW might include a manpack, vehicle-mounted, fixed-site, airborne, or seaborne platform or some combination of these equipment types.

⁴ EW is primarily a type of operation, not a signal/mission command issue, which is why it is under the purview of the Army G-3 versus G-6.

⁵ ATP 3-12.3, 2019, p. 7-1.



FIGURE 2
The Electromagnetic Spectrum



SOURCE: Adapted from FM 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, April 2017, p. 1-12, Figure 1-5.

NOTES: AC = alternating current, AM = amplitude modulation, CRT = cathode ray tube, EHF = extremely high frequency, ELF = extremely low frequency, FM = frequency modulation, HF = high frequency, LF = low frequency, MF = medium frequency, PCS = personal communication systems, SHF = super high frequency, UHF = ultra high frequency, UV = ultraviolet, VHF = very high frequency, VLF = very low frequency.

Every time one of Murphy's platoons approached NAI (named area of interest) 4, his comms went out. At first, he thought it was Hill 244 blocking line of sight, but the S6 he mentioned it to said, "No way. There's a retrans station up there. You should be good." Then Murphy considered the possibility that their own CREW systems were jamming the signals. But those checked out fine. The enemy must be employing some sort of EW asset in the area.

Technical Assets and EW Systems at the Tactical Level

Detecting enemy radio signals, sensing enemy vehicles and aircraft, deceiving enemy systems with EMS signature spoofing, and directional jamming are EW capabilities that can be employed with technical assets that are available at the tactical level.

- Versatile Radio Observation and Direction (VROD) and VROD Modular Adaptive Transmit (VMAX) is a combined EW backpack system that surveys the field from an electromagnetic perspective and provides limited electronic assault capabilities, such as signal interception and jamming.
- Raven Claw is a mobile computer system that offers on-the-ground planning and management without any network connection.
- The Terrestrial Layer System (TLS) integrates signals intelligence, EW, and cyber capabilities and will be fielded to EW and intelligence platoons.

Bottom Line: Electronic Warfare

What can my unit do now?

This is one of the capabilities that you can't employ with assets that are organic to most tactical formations; you'll need equipment or personnel attached to your unit, or you'll need airborne support. Under some operational conditions, some units have jammers installed on their vehicles, but this capability is limited.

Where do I go for this capability?

In a battalion, the S6 is the starting point. At higher-level commands, cyber and electronic warfare officers may reside in either the G-6 or



G-3. In the Army, at the battalion level and above, there should be a designated EW representative to conduct relevant planning with the S2, S6, fire support officer, and others. At the brigade/regiment and higher level, coordinate with the cyber and electronic warfare officer or electronic warfare officer.

The Montanyans knew how to combine EW and fires to devastating effect. One day, Murphy watched through his binoculars as a Centralian motorized rifle company prepared to assault a village with the help of B Co. in the valley below. He noticed several of the Centralian soldiers texting when their NCOs weren't looking. He even saw one private hide behind a truck and make a call! It wasn't three minutes later that artillery rounds started to land all over the Centralian forces. The intel folks told Murphy that the Montanyans had the ability to find and target unmasked electromagnetic signatures. Murphy guessed this was proof of that.



TABLE 8
Use Cases: Electronic Warfare

Problem	Tactic/Technique	Effect
Enemy has jamming capability (electronic attack)	Use approved devices and avoid compromised communications systems, like commercial phones. Use prescribed encryption keys to bolster security.	Limit the ability of the enemy to monitor or jam your communications.
Enemy has EMS detection capability	Limit electromagnetic emissions. Ensure transmissions are necessary, preplan them to keep them short, and transmit them quickly and precisely. Use burst-enabled equipment and brevity codes.	Limit the emissions that and enemy can detect and target.
Enemy can monitor transmissions	Use an alternate means of communication. Use burst-enabled equipment. Change network frequencies and call signs to misdirect the enemy.	Enemy cannot locate your position and listen to your conversations.
Enemy positions are unknown	Use electronic support and attack to identify signatures in the EMS.	Locate concealed or unknown enemy positions.
Enemy spoofs GPS or communications	Rely on maps and compasses for navigation. Revisit legacy solutions for communication.	Degrade enemy confidence in spoofing tactic while ensuring redundancy for navigation and communication.
Interference is detected but the origin is unknown	Conduct an EMS survey (electronic support).	Develop battlespace awareness of EMS.
Enemy has electronic attack capability	Use electronic countermeasures, such as flares, chaff, radar jammers, CREW, and decoys, to disrupt capability.	Confuse enemy electronic detection assets, like radar, and remain concealed in the EMS.
Enemy is trying to locate your position with EW or drone assets	Use deception to misdirect the enemy (false transmissions, emissions from assets other than those present). • Be prepared to maneuver quickly while taking steps to limit electronic footprint. • Adjust launch and recovery operations for drones. Do not launch and recover a drone in the same location. • Reemphasize camouflage, concealment, and deception. When not moving, use camo nets.	Increase or decrease enemy confidence.

SOURCES: This table draws extensively from FM 3-12, 2017, and ATP 3-13.1, *The Conduct of Information Operations*, Washington, D.C., October 2018, Chapters 5–7.



8

Cyber Operations

Overview

Cyber operations can be offensive or defensive, with potential effects across all domains. They use computer hardware, software, code, or devices to target enemy and hostile adversary activities and capabilities or to protect data, networks, net-centric capabilities, and other designated systems. As a component of operational planning, these operations are used to detect, identify, and respond to attacks against friendly networks.

Activities

Cyber missions and actions are interrelated; synchronizing and supporting efforts is imperative to maintaining freedom of maneuver in cyberspace. Cyber operations can be offensive or defensive.

Intelligence Preparation of the Environment

Cyber can be integrated into intelligence preparation of the environment as a systematic and continuous process of analyzing the OE. Cyber specialists can provide intelligence on the means and motives of threat actors and the digital environment to help units prepare for threat scenarios.

Using its EW and cyber capabilities, the Montanyan military hacked into cellular networks and sent targeted messages to Centralian troops and their families. It also used aggressive cyber operations to disrupt Centralian government and business activities. This hurt commerce and decreased confidence in the Centralian government, both domestically and internationally.

Tactical Defensive (Cyber Operations)

Infrastructure

Tactical networks leave an electronic footprint that is often easy to discover. Military tactical networks are distributed, and the close proximity of adversaries increases the risk of intercepted communications. Cyber defenders need to protect friendly tactical cyber terrain, prevent the enemy from interfering with force maneuver, and counter cyber

threats to ensure the reliability of critical networks. Tactical defensive infrastructure in the Army, for example, consists of prepositioned tools on dedicated computer and storage systems at corps and below.

Cyber Situational Understanding

Cyber situational understanding requires input from a range of assets and supports planning and coordination across activities, such as electronic warfare, deception, and OPSEC. It also helps detect changes to the cyber environment that could indicate a threat.

Bottom Line: Cyber Operations

What can my unit do now?

There isn't much that you can do at the tactical level, and you certainly shouldn't get on your own laptop and try to hack into a local network. That's a surefire way to end up in hot water. The authorization to conduct cyber offensive operations typically rests at a very high level and will require extensive coordination and lead times to plan.

Where do I go for this capability?

You need a good idea of what kind of capability you need. What is it that you want to do, and for how long? Do you want to turn off the lights in a section of town as you conduct a raid? Do you want to open up the flood gates on a river to stop your enemy from crossing? Whatever you want to happen, you need to be specific in your request. Cyber operations are not all-encompassing activities like you might imagine, and you will not be granted unlimited access. Often, the EW officer will be co-located with the cyber officer at brigade or regiment. Don't be afraid to ask for their advice as you plan an operation.



9 Military Information Support Operations/Psychological Operations

Overview

Psychological operations (PSYOP) forces execute **military information support operations** (MISO). MISO are a vital part of U.S. political, military, economic, and ideological activities in peacetime, contingencies, and declared war. They are used to inform and influence target audiences. Themes, messages, and narratives can be disseminated through a variety of mediums; TV, social media, radio, posters, billboards, and leaflets are all methods to distribute a message.

Activities

Previously and still fairly commonly referred to as “PSYOP,” MISO are planned operations intended to convey information to foreign audiences to influence emotions, motives, objective reasoning, and, ultimately, behaviors. At the tactical level, tactical PSYOP teams execute or coordinate actions and disseminate messages in person, in writing, and through audio and visual media with such goals as encouraging enemy forces to defect, disperse, surrender, or take some other action beneficial to friendly forces. At brigade and above, the focal point is the staff PSYOP officer or NCO, who closely coordinates with the IO officer or representative. The commander or officer-in-charge of an attached PSYOP unit may also contribute to synchronizing IRC activities. Both are core members of the unit’s IO working group.

Face-to-Face Engagement

Building rapport is critical in establishing the legitimacy and credibility of U.S. forces in an AO, as well as building and improving relationships with local populations. For this reason, tactical PSYOP teams are trained and skilled in face-to-face engagements for the following purposes:

- KLEs: Engage with local leaders to establish support and build critical relationships.

- Gathering atmospherics: Determine and understand what drives local sentiment on U.S. force presence.
- Working with interpreters: Ensure effective communication and culturally appropriate dialogue.

Messaging Capabilities

Media and loudspeakers offer options for communicating with wider audiences. Goals might include gaining access to denied or restricted areas, outreach to combatants, or protecting civilians.

- Surrender appeals: Announce opportunities and incentives for enemy forces to surrender.
- Civil disturbance control: Engage with populations at risk of unrest.
- Internally displaced persons control: Mitigate challenges posed by noncombatants on the battlefield.
- Noncombatant evacuation coordination: Warn and direct non-combatants during evacuation operations.
- Sonic deception: Use loudspeakers to deceive the enemy about the size and positions of units.

Local Assessment

Tactical PSYOP teams are made up of regional or cultural experts who understand political, cultural, ethnic, and religious subtleties and enhance understanding of the OE. They use a variety of assessment and analysis tools and can provide recommendations for dynamic targeting and optimizing the U.S. force presence in an AO:

- Rapid local assessment or deliberate local assessment: Provide social, political, and economic assessments of the AO.
- Media analysis: Identify media centers of gravity and perceptions of local populations.
- Propaganda analysis: Analyze enemy motives and interpret capability-related messages.



TABLE 9
Use Cases: MISO/PSYOP

Problem	Tactic/Technique	Effect
Enemies in an urban zone	Use coordinated messaging (e.g., surrender appeals, loudspeaker operations) for clearing operations and to flush out enemy positions. Coordinate with EW and cyber personnel on tactical maneuver and defeat capabilities.	Mitigate casualties, increase the likelihood of enemy surrender, increase confidence in target acquisition, and use nonlethal options to reduce enemy will to fight.
Enemy locations unknown	Use loudspeaker operations, face-to-face engagement, and public messaging to encourage civilians reports of enemy locations and activities.	Increase potential for tips, enhance targeting inputs, and increase public trust.
Enemy knows your location	Use loudspeakers to produce misleading signatures in support of DISO.	Get the enemy to think you are somewhere you are not.
Civilian interference in defensive positions or convoy movements	Use preapproved messaging via loudspeaker, radio, or TV to keep civilians away from operations.	Enhance force protection, mitigate civilian casualties, and increase confidence in rules of engagement.
Civilians/internally displaced persons in urban combat area	Use loudspeaker operations, face-to-face engagements, and public messaging via radio/TV to tell civilians to stay indoors and close windows, as well as to direct internally displace persons to collection points or safety areas.	Enhance operation speed and efficiency and reduce civilian casualties.
Noncombatant evacuation operation	Use loudspeaker operations, face-to-face engagements, and public messaging to facilitate noncombatant evacuation and direct civilians.	Enhance operation speed and efficiency and reduce civilian casualties.
Missing service member or duty status—whereabouts unknown (DUSTWUN)	Use loudspeaker operations, face-to-face engagements, and public messaging locate and protect missing U.S. forces.	Create a force multiplier to increase the likelihood of locating and protecting missing personnel.
Cultural misunderstandings	Call on PSYOP forces to advise unit on cultural mores to mitigate risk of insulting locals.	Prevent civil disturbances from soldier misconduct and increase public trust.
IEDs on main supply routes	Use preapproved messaging via loudspeaker operations, face-to-face engagements, radio, or TV to encourage civilians to report IEDs/ enemy activity.	Increase potential for tips about IEDs and enemy activities near key routes.
Lack of trust from local noncombatants	Build rapport and foster better relationships with locals.	Increase public trust, increase potential for tips on enemy activities, and mitigate civil disturbances.



TABLE 9—Continued

Problem	Tactic/Technique	Effect
Lack of information about the local area	Conduct rapid and deliberate local assessment, aiding commander in identifying local centers of gravity.	Increase passive intelligence, refine targeting inputs, and identify threats/opportunities.

Bottom Line: MISO/PSYOP

What can my unit do now?

MISO is one of the capability areas that requires specially trained forces (PSYOP personnel), who can help you craft messages and design talking points for KLEs. If you want to hang up a poster, send out a message on a local social media platform, or use a loudspeaker, you should probably talk to PSYOP first. Messaging campaigns are carefully coordinated, and there is a risk of doing more harm than good if you are unfamiliar with other messaging activities in an AO.

Where do I go for this capability?

Coordinate on the use of MISO capabilities through your battalion S3, who will be able to request tactical PSYOP support from PSYOP elements in theater. Keep in mind that while MISO authorities are held at a relatively high level, PSYOP forces are tactically focused and are usually more than willing to accompany you on a patrol or help plan a mission. PSYOP also have access to preapproved messages and all manner of printed leaflets, posters, and handbills for your use. Ask your S3 to see what preprinted products are available. Even if you don't have direct PSYOP support, you can request and use these preapproved

Montanya knows the importance of public opinion. The Montanyan government has disseminated a consistent justification for its involvement in Centralia: It is intervening to protect ethnic Montanyans from a Centralian government that has persecuted them. Both before and during the conflict, Montanyan propaganda units disseminated messages via social media, local newspapers, radio, and local television to delegitimize the Centralian government and generate support for Montanyan intervention in western Centralia. This effort has increased perceptions of the legitimacy of its operations, as well as support for its activities.



products. These can range from tip lines, arrest warrants, and information flyers to surrender appeals.

Just remember that any product that is developed must be done so via PSYOP personnel and go through a rigorous approval process. Don't go making your own leaflets to hand out to locals. That's a sure-fire way of getting yourself in trouble.



10 Space Operations

Overview

Space-based capabilities are critical for successful land domain operations. Nearly every operation relies on the advantages that space provides. They are expected to just work, but how they work is something we don't give much thought to.

Military satellites in geosynchronous orbit (the same speed as the Earth's rotation, so they seem to stay in one place) provide forces on the ground with **positioning, navigation, and timing** (PNT) and **satellite communication** (SATCOM) capabilities. This enables freedom of maneuver and intelligence preparation of the battlefield, reliable communication, and accurate targeting, fires, and navigation. Military space capabilities are unique in that they are the product of partnerships across DoD and the U.S. government.

Activities

Most enemies will have access to at least some space-based capabilities, particularly for communication and navigation. There are ten identified space capabilities, of which five are particularly relevant to tactical operations:

- **PNT:** GPS satellite signals help you know where you are (positioning) and how to get where you want to go (navigation), but the role they play in timing is less understood. Precise and reliable timing information is essential for virtually every modern weapon system, as well as tactical digital networks, wide-area networking, and advanced communications. The loss of PNT would have a devastating effect on nearly all aspects of modern warfighting.
- **SATCOM:** Small, portable devices link to satellites to enable connectivity and communication over large, dispersed areas and remote areas.

Murphy had to assault the top of a mountain and needed a good plan because the Montanyans had anti-aircraft artillery up there. For accurate fires, he needed precise geolocations, but where could he get those? Thinking about it, he used GPS to pull up some satellite imagery of the mountain and the location of the firing battery, then he plotted the enemy's location on the satellite map. Next, he compared the elevations of the firing location and the target and pulled up the local weather forecast. He had to request that the firing battery be available on call for tomorrow. Over the SATCOM, he told the BN fire support officer that he would provide an update to the meteorological data tomorrow at 0500 via Blue Force Tracker text.

Reflecting, Murphy realized that everything he had just done relied on satellites in some form or fashion. He'd never really thought about how much he depended on space-based capabilities.

- **Space-based intelligence, surveillance, and reconnaissance (ISR):** Long-duration, persistent monitoring via satellite enables detailed analysis to enhance targeting and intelligence collection.
- **Environmental monitoring:** Operation planning and execution require reliable data on weather patterns.
- **Missile warning:** Early warning of changes force posture is essential for threat detection and cueing friendly force missile defenses.

Bottom Line: Space Operations

What can my unit do now?

You have what you have in terms of GPS-enabled and SATCOM equipment. Other than that, space-based capabilities are largely out of the realm of tactical operations. However, you should keep your equipment updated with the most current encryption and always have a map and compass. You should also have a backup communication plan that includes SATCOM, line of sight, Blue Force Tracker, and other secure methods.

Where do I go for this capability?

You can request imagery through your S2, and your S6 can help keep your communications up and running. If you want to deny enemy satellite capabilities for a mission, go through your S3. (It will be nec-



TABLE 10
Use Cases: Space Operations

Problem	Tactic/Technique	Effect
GPS electromagnetic interference or jamming	Point the GPS device at your chest and spin. As the satellite signal goes up and down, it can help you determine where the jamming signal is emitting. - Mask your signature behind a vehicle or in a ditch. - Ensure that you have the right fill and encryption and that your receiver is turned on at least monthly to allow encryption to be updated.	Determine where a jamming signal is emitting.
		Block the jamming signal.
		Stop enemy attempts to jam.
SATCOM electromagnetic interference or jamming	Ensure that your PACE [primary, alternate, contingency, and emergency] plan is robust. It is hard to recognized when you are being jammed.	Change the physical satellites and spectrum satellites you are accessing for communication.
Unmanned aerial system interference	Determine whether GPS or SATCOM capabilities are at fault.	Identify the problem to better understand how to avoid it.
Cloud cover	Be aware that just because it's cloudy, that doesn't mean that enemy satellites can't see you. Your physical presence can be picked up via synthetic aperture radar satellites, so take other steps to prevent detection.	Prevent enemy forces monitoring friendly force locations.
Enemy use of Google Earth or other detailed imagery	For offensive operations, request space support to degrade or deny enemy satellite capability in a selected region for a selected period of time. Commercial imagery is prolific and almost as good as U.S. military capabilities.	Deny the enemy access for a given period of time. This can help a patrol get out of the gate unseen. However, be aware that everything you do can be monitored.

While out on patrol in their regular sector, Murphy was with Alvarez's 1st Platoon as they came across LT Williams from 2nd Platoon at an intersection. Williams thought he was at an intersection three grid squares to the east. When Murphy pulled out his DAGR and confirmed their location, Williams raised his wrist Garmin to compare locations. Murphy lost his mind. This confirmed that his personal GPS was wrong: He was being spoofed. Murphy pulled out his map and compass and pointed Williams in the right direction. Williams had a bit of a walk to get back into his own sector. Murphy had the next three hours to think up what additional detail Williams would be on for using a personal GPS instead of issued gear.



essary to request access from higher echelons.) If enemy use of satellite imagery is a concern, think OPSEC and signature management, and enhance camouflage and concealment. See the sections “Military Deception” and “Operations Security and Signature Management” in this handbook for more detail on these and other options.

There won’t be a subject-matter expert on space capabilities below the division or Marine Air-Ground Task Force level.

There was enemy on that rocky outcrop overlooking the valley. Murphy could see them on the UAS terminal but not with his own eyes because he was in heavy woods. It looked like they were setting up an ambush on the road exiting the town several clicks away. Using the UAS grid location, Murphy had the forward observer call for a fire mission. When the BN fire support officer reported, “Rounds complete,” Murphy didn’t see any impacts. When the UAS scanned out, there was smoke coming from the nearby village. Had the UAS given Murphy a bad grid coordinate for his call for fire? What the heck happened!?!



11

Technical Effects

Overview

Technical effects are unique, highly classified, often technical capabilities designed to provide an edge for certain use cases. Depending on the mission and unit, related tools might be a regular part of operations. An IO officer is often responsible for coordinating these capabilities and their effects with the unit and mission.

Activities

To request this support you need to work through your chain of command. Typically, an IO or technical effects officer at higher headquarters is contacted, reviews your problem, and communicates your request through the appropriate channels. Aside from the most elite, specialized units and the most critical missions, this is rarely a quick process. If a capability is found (or can be developed within the required timeline), it may be allocated to your request. You may not even be aware of the decision or involved in the capability's employment. You might simply observe the desired effect with no details on how it was accomplished. This opacity is not meant to discourage the use of these tools; it is to avoid leaks, protect the capabilities from enemy countermeasures, and ensure maximum longevity of what can be very costly items. Be patient, be clear about your mission needs, and work with your chain of command to harness these unique capabilities.

Murphy was sitting in the BN targeting meeting one morning when a high-value target came up for discussion. Someone in the back of the room he'd never seen before spoke up and said she had a capability that could help. The boss turned to her, said, "See me after," and quickly moved on. Murphy frowned, confused.

Bottom Line: Technical Effects

What can my unit do now?

There's not much that can be discussed at an unclassified level.

Just as Murphy was getting ready for the next patrol, the S3 pulled him aside and told him someone would be joining the patrol. The guest turned out to be a captain carrying a backpack she wouldn't let anyone near. During the patrol, the captain fiddled with the backpack several times, but no one was sure what she was doing. Once back on base, she thanked Murphy for the help and left. When Murphy asked the S3 what that was all about, she just shrugged her shoulders. "Be glad you could help out."

Where do I go for this capability?

Think about what you want to happen and what effect you need to achieve mission success, which you must be able to clearly articulate in your CONOPS. Write a request for technical effects that you want to achieve and forward that request up through the S3/G-3. As this request goes through the routine approval channels, if the tool or capability exists, that should be the starting point for further discussion.



12 Social Media and Open-Source Intelligence

Overview

You might intuitively understand the power of social media, but what you can legally do with it for military purposes is not well defined. This section provides some clarity, but note that legal and policy frameworks have lagged behind the rapid evolution of social media. Anything broadcast on social media or elsewhere online or that is otherwise available to the public for free or for a fee can be considered **publicly available information** (PAI).¹

PAI can be used in two ways: **open-source intelligence** (OSINT) and **open-source research** (OSR), each of which has a specific purpose and is derived from different authorities. OSINT is the collection and processing of PAI for intelligence purposes; it is conducted by intelligence professionals under intelligence authorities and directed toward foreign audiences. OSR is conducted for operational needs and not typically conducted by intelligence analysts.

Although anyone can do OSR, it cannot be overstated that—before you get onto social media for any operational purpose—you must first check with your command’s policy on the use of social media. In many instances, this guidance won’t exist or it will be prohibitively restrictive.

To help distinguish between OSINT and OSR, it is helpful to consider what **OSINT** is:

- Conducted by intelligence personnel
- Uses certain types of PAI

¹ **Publicly available information** is defined as follows:

Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting a place or attending an event that is open to the public. (U.S. Department of Defense Directive 3115.18, *Access to and Use of Publicly Available Information (PAI)*, Washington, D.C., incorporating change 1, August 20, 2020, pp. 12–13)

- Can use advanced analysis techniques, such as social media analysis, lexical analysis, and sentiment analysis
- Can be conducted by selected capability areas, like MISO, PA, and civil affairs.

OSR can

- Help you maintain battlespace awareness
- Monitor the key influencers in your AO.

Social media monitoring can provide information on a group's demographics, size, organizational structure, pattern-of-life activities, and reach. This information can be used to craft detailed messages and inform or influence audiences. Keep in mind, however, that social media data may not be representative of those who do not participate on these platforms, so social media monitoring should not be used as the sole basis for planning or decisionmaking. There are also limitations on tactical units' collection and use of these data. You must comply with relevant DoD information security, OPSEC, and cyber policies.

OSR: Forbidden Activities

There are many restrictions on the use of PAI for OSR purposes, as well as accessing and using almost any kind of data on U.S. persons. Here are some examples of what you cannot do:

- Use a false identity or affiliation to access PAI
- Create your own cover persona or personality (this is an intelligence activity and requires specific permission)
- Store PAI on your devices
- Collect information on U.S. persons
- Send messages or set up an organizational profile for your unit (this is PA's domain)
- Release stories to news media
- Conduct any kind of analysis—text analysis, network analysis, or sentiment analysis—with these tools.



The police chief was usually all smiles at their weekly KLE. But today he wouldn't even look Murphy in the eyes. He kept making vague reference to something he'd seen online. Murphy couldn't leave this engagement on a sour note, but he didn't have time to send it up through the channels to learn more. During a break in the meeting, Murphy pulled his interpreter aside and asked him to search social media to find out what the local buzz was all about.

To avoid problems, carefully review DoD Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)*, 2020, and DoD Instruction 3115.12, *Open Source Intelligence (OSINT)*, 2020.

Messaging

Messaging or engaging on social media is something that you can do, although your ability to do so in a deployed environment may be limited. From both a personnel and unit standpoint, one of the best resources available to govern your actions on social media is *The Social Corps: The USMC Social Media Principles*, 2013. That handbook covers ways to engage on social media and sets out solid principles to guide posting. When engaging on social media, remember OPSEC and be aware that anyone (especially adversaries) could be intently watching what you post.

Bottom Line: Social Media and Open-Source Intelligence

What can my unit do now?

There are ways social media platforms can assist with operations. For OSR, here are a few examples of what you can do:

- Monitor local media sources for situational awareness
- Identify prolific posters and potential key influencers in your AO
- Gauge public opinion on a topic
- See whether operational cover has been compromised or illuminated
- Monitor for OPSEC violations.



Where do I go for this capability?

Your BN S2 will have some form of OSINT capability that will be more analytically robust than you going on a social media platform and seeing who is posting. You can also talk with PA or PSYOP, which monitor social media accounts.

A good place to start for guidance on social media use and engagement is the Marine Corps’ social media principles, listed below. 1st IO Command and the Marine Corps Information Operations Center both have analytic capabilities that you could draw on.



Conclusion

Overview

Capabilities that aren't central to your mission—and that take time to understand and utilize (like PA, PSYOP, and space operations)—might feel like add-ons that don't help with mission accomplishment. We hope this handbook provided some insight into OIE and how the capabilities presented here can help tactical formations. Tactical formations never have enough time to plan, prepare, and execute missions. Perhaps the next time a warning order comes down, a brief skim through this handbook will give *you* some ideas for how to leverage all available capabilities to achieve mission success.

Activities

There are several additional process and battle drills that tactical formations should be aware of as they plan and prepare for operations.

Processes

There are two forums that can be used to help synchronize and drive OIE. They are the Targeting Working Group (TWG) and the Information Operations Working Group (IOWG):

- The IOWG is chaired by the brigade/regimental IO officer. It prioritizes, requests, and synchronizes capabilities. Outputs of this working group include an IO running estimate, commander's critical information requirements, IO input for upcoming and ongoing operations, and an IO synchronization matrix. Many of these products feed directly into the TWG and operations process.
- The TWG is held at the battalion and brigade/regimental levels. It is chaired by a battalion or brigade/regimental fire support officer. In this forum, key targeting products, like the high-payoff targeting list and target synchronization matrix, are refined. The

TWG considers targets for execution using both kinetic and non-kinetic capabilities.

IO/OIE Battle Drills

Maneuver formations rigorously follow battle drills for mission accomplishment. One way to help leaders effectively integrate the capabilities in this handbook into tactics and operations is to include **IO battle drills** in existing battle drills. In current doctrine, there is little mention of IO or OIE in either offense or defense, only in stability operations. Table 11 is an example checklist, battle drill, or utilization matrix showing how certain capabilities could be employed to shape the operational environment and achieve commander’s intent. Although such a checklist or matrix resembles a nonlethal fires plan, it should be noted that—unlike fires—operations in the information environment continue throughout all phases of the mission.

TABLE 11
Example Employment Matrix for an Infantry Company Attack

Task Attack: Destroy or defeat enemy forces, seize and secure terrain, or both	
Supporting Tasks	IRC Support/Battle Drill
Suppress or neutralize enemy reserves	• EA: Jam signals of enemy command and control (C2) • PSYOP: Multimedia products to degrade enemy will to fight • Physical attack: Target barracks, roads, C2 elements, etc. • PA: Coverage of advancing troops, embedded media
Deceive the enemy as to the battalion's actual intentions	• TAC-D: Feint • PSYOP: Multimedia products targeting will to fight • PSYOP: Sonic deception along alternate axis of advance • EA: Jamming along alternate axis of advance • OPSEC: Monitor selected social media • Defensive cyber operations: Protect friendly command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), provide cybersecurity • PA: Media embargo of embedded reporters
Destroy enemy security and disruption forces	• PSYOP: Multimedia products to degrade enemy will to fight • EA: Jam signals of enemy C2 • Physical attack: target barracks, roads, etc.
Obscure friendly movements and deployment	• OPSEC: Enforce radio discipline until D-30 • SIGMAN: Support to technical means TAC-D • PSYOP: Sonic deception in vicinity of friendly forces • TAC-D: Execute feint in vicinity of friendly forces • PA: Media embargo until D+2
Destroy or neutralize the enemy's local C2 system	• EA: Jam enemy C2 signals • PSYOP: Multimedia products to degrade enemy will to fight • Physical attack: Target barracks, roads, C2 elements, radio antennas, etc.
Consolidate on the objective	• KLE: Prepare talking points on the operation • PSYOP: Multimedia products supporting key themes (mission legitimacy, degrading adversary's legitimacy) • SIGMAN: Set up of multispectral camouflage netting to minimize signatures • PAO: Release media embargo, prepare talking points • EA: Continued jamming of select adversary signals • COMCAM: Site exploitation

Capability Integration: What CPT Murphy Learned

It was H-1, just one hour until A Co. went on the offense. After months playing cat and mouse with the Montanyans, it was time for decisive action. A Co. was going to be the main effort to remove the Montanyan 3rd BN from Borrisville. Murphy had been to the battalion HQ every day this week for rehearsals, and he felt confident in the plan and his troops. He had air, artillery, and tank support. Surprisingly, though, it was some of the other capability areas—ones he didn't know much about before he started operations outside of Borrisville several months ago—that really helped settle his mind.

He just couldn't believe how many additional capabilities were assigned to A Co. for this mission. As he sat in the heavily wooded section to the west of the town, he watched the TAC-D plan go into full effect; the eastern skyline was ablaze with tracers and the sounds of tank movement from the PSYOP team. He knew that OPSEC was solid and their signatures were effectively masked from enemy detection. The Montanyans had no idea A Co. was sitting in these woods.

Each platoon also had a team of EW specialists attached. They were there to block enemy communications, disrupt remotely detonated devices, and identify locations that had a high volume of military communications for targeting by the field artillery support. He also had a PSYOP team attached to his company HQ element. They brought with them loudspeakers as part of the TAC-D plan, which were to be used to confuse and disorient the Montanyans. They also had a bunch of the same leaflets that the Air Force had been dropping all over the town for the past week, directing civilians to stay indoors and off the streets as A Co. attacked.

The battalion PA rep had coached Murphy on what to say—and what not say—after the attack had culminated and they had reached their objective. He knew that the Montanyan-friendly journalists were going to be there demanding to know why A Co. had caused so many civilian casualties and destroyed parts of the city (even if neither happened). He also knew that the media blackout and CA team would help with some of that until higher HQ could arrive to deal with the situation.

As H-hour approached, Murphy was confident the attack would go through, and he was thankful that he had, and understood, how all of these “extra” capabilities were both keeping his troops safe and helping him accomplish the mission.

Appendix. Stakeholder Organizations

Key DoD and NATO IE stakeholders range from policy-setting organizations and centers of excellence and lessons learned to training providers. This list is not exhaustive, and the debate continues over which organizations qualify as OIE stakeholders. More information about these organizations can be found on their respective websites. The descriptions here are largely drawn from the organizations' mission statements.

Joint and National

Joint Staff, J39, Deputy Director for Global Operations

Joint Information Operations Warfare Center (JIOWC) supports IRC development and coordinates across combatant commands and other DoD organizations.¹

- **JIOWC OPSEC Support Element (JOSE)** offers the two-week mobile training team Defense OPSEC Planners course for joint OPSEC certification.
- **Joint Forces Staff College (JFSC)/Information Operation Division** offers the Joint Information Operations Orientation Course (JIOOC), Joint Information Operations Planners Course (JIOPC), and Joint Military Deception Training Course (JMTC).

Joint MISO WebOps Center (JMWC), part of U.S. Special Operations Command, provides joint MISO capabilities worldwide.

U.S. Cyber Command (USCYBERCOM) directs, synchronizes, and coordinates cyber planning and operations alongside U.S. and international partners.

U.S. Government

Global Engagement Center, housed at the U.S. Department of State, directs, leads, synchronizes, integrates, and coordinates U.S. counterpropaganda efforts internationally.

¹ See Joint Staff, J7, Deployable Training Division, *Joint Officer Handbook: Staffing and Action Guide*, Washington, D.C., September 21, 2018.

Other

Additional OIE stakeholder organizations include the **Joint Lessons Learned Information System (JLLIS)**, **Joint Special Operations University (JSOU)**, and the **John F. Kennedy Special Warfare Center and School (SWCS)**, which is an Army entity but *the* provider of training for the joint community MISO/PSYOP, civil affairs, and more.

U.S. Army

Operational

U.S. Army Cyber Command (ARCYBER) integrates and conducts cyber operations, electronic warfare, and information operations.

Theater Information Operations Groups (TIOGs) are responsible for IO planning, synchronization, and assessment. Two are Army National Guard units and one is an Army Reserve unit.

Institutional

1st IO Command, part of U.S. Army Cyber Command, deploys IO support teams to Army and joint missions and provides IO planning, analysis, and reachback support. It also offers a wealth of training opportunities and products (such as information preparation of the environment).

U.S. Army Cyber Command Center of Excellence (CCoE) is responsible for force modernization, doctrine development, training and education, and related requirements for cyber operations, electronic warfare, and other functions related to Army networks, signals, communications, and information capabilities.

Center for Army Lessons Learned (CALL), which is responsible for guiding modernization and improvement initiatives, offers lessons-learned courses for personnel across the services that cover IE-related topics.

U.S. Marine Corps

Operational

Marine Expeditionary Force Information Groups (MIGs) oversee and coordinate IRCs in each of the three Marine Expeditionary Forces.

Marine Corps Forces Cyberspace Command (MARFORCYBER) conducts full-spectrum cyber operations in support of Marine Corps, joint, and coalition forces.

Institutional

Deputy Commandant for Information (DC I) is responsible for all OIE plans, policies, strategy, and requirement development and is the principal adviser and spokesperson for Marine Corps IE-related programs and activities.

Marine Corps Information Operations Center (MCIOC) provides operational support and subject-matter expertise for OIE.

Marine Corps Center for Lessons Learned (MCCLL) collects, synthesizes, and disseminates lessons learned to support operational improvement, including for OIE.

U.S. Air Force

16th Air Force (Air Forces Cyber) is dedicated to information warfare. It houses multisource ISR, cyber operations, electronic warfare, environmental monitoring, and cryptologic capabilities and performs other OIE-related activities.

U.S. Navy

U.S. Fleet Cyber Command/U.S. Tenth Fleet conducts full-spectrum cyber operations in support of Navy, joint, and coalition forces.

NATO

NATO Strategic Communications Centre of Excellence (StratCom COE) provides training, education, lessons learned, and guidance on conducting public diplomacy, PA, military PA, information operations, and PSYOP in accordance with NATO policies and objectives.

NATO Civil-Military Cooperation Centre of Excellence (CCOE) provides training, education, lessons learned, and guidance on CIMIC in accordance with NATO policies and objectives.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) provides training, education, lessons learned, and guidance on conducting defensive cyber operations in accordance with NATO policies and objectives.

Abbreviations

AO	area of operations
ATP	Army techniques publication
BN	battalion
C2	command and control
CA	civil affairs
CAO	civil affairs operations
CIMIC	civil-military cooperation
CJTF	combined joint task force
CMO	civil-military operations
CMOC	civil-military operations center
COMCAM	combat camera
CONOPS	concept of operations
CREW	counter–radio-controlled improvised explosive device electronic warfare
DISO	deception in support of operations security
DoD	U.S. Department of Defense
EMS	electromagnetic spectrum
EW	electronic warfare (transitioning to <i>electromagnetic warfare</i>)
FM	field manual
GPS	Global Positioning System
IE	information environment
IED	improvised explosive device
IO	information operations
IRC	information-related capability
ISR	intelligence, surveillance, and reconnaissance
JIOWC	Joint Information Operations Warfare Center
JP	joint publication
KLE	key leader engagement
MCWP	Marine Corps warfighting publication

MEDEVAC	medical evacuation
MILDEC	military deception
MISO	military information support operations
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
OE	operational environment
OIE	operations in the information environment
OPORD	operations order
OPSEC	operations security
OSINT	open-source intelligence
OSR	open-source research
PA	public affairs
PAD	public affairs detachment
PAG	Public Affairs Guidance
PAI	publicly available information
PNT	positioning, navigation, and timing
PPP	presence, posture, and profile
PSYOP	psychological operations
SATCOM	satellite communication
SIGINT	signals intelligence
SIGMAN	signature management
TAC-D	tactical deception
UAS	unmanned aerial system
UAV	unmanned aerial vehicle

References

Background Reading

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018.

ATP—See Army Techniques Publication.

Joint Publication 2-0, *Joint Intelligence*, Washington, D.C.: U.S. Joint Chiefs of Staff, October 22, 2013.

Joint Publication 3-0, *Joint Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, October 22, 2018.

Joint Publication 3-05, *Special Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, July 16, 2014.

Joint Publication 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

Joint Staff, J7, Deployable Training Division, *Joint Officer Handbook: Staffing and Action Guide*, Washington, D.C., September 21, 2018.

JP—See Joint Publication.

Marine Corps Warfighting Publication 3-32, *Marine Air-Ground Task Force Information Operations*, Washington, D.C.: Headquarters, U.S. Marine Corps, April 1, 2018.

Paul, Christopher, “Two Vignettes: How Might Combat Operations Be Different Under the Information Joint Function,” *Mad Scientist Laboratory Blog*, October 8, 2020. As of January 15, 2021:

<https://madsciblog.tradoc.army.mil/275-two-vignettes-how-might-combat-operations-be-different-under-the-information-joint-function>

Paul, Christopher, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-2489-OSD, 2018. As of January 15, 2021:

https://www.rand.org/pubs/research_reports/RR2489.html

Paul, Christopher, and William Marcellino, *Dominating Duffer’s Domain: Lessons for the 21st-Century U.S. Army Information Operations Practitioner*, Santa Monica, Calif.: RAND Corporation, RR-1166/1-A, 2017. As of January 15, 2021:

https://www.rand.org/pubs/research_reports/RR1166z1.html

———, *Dominating Duffer’s Domain: Lessons for the 21st-Century U.S. Marine Corps Information Operations Practitioner*, Santa Monica, Calif.: RAND Corporation, RR-1166-1-OSD, 2016. As of January 15, 2021:

https://www.rand.org/pubs/research_reports/RR1166-1.html

U.S. Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, Washington, D.C., July 25, 2018.

1. Inherent Informational Aspects of Military Operations

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018.

Marine Corps Warfighting Publication 3-32, *Marine Air-Ground Task Force Information Operations*, Washington, D.C.: Headquarters, U.S. Marine Corps, April 1, 2018.

U.S. Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, Washington, D.C., July 25, 2018.

2. Key Leader Engagement

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018, Chapter 3.

Field Manual 3-13, *Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, December 2016.

Graphic Training Aid 21-03-012, *Negotiations*, Washington, D.C.: Headquarters, U.S. Department of the Army, July 2012.

Graphic Training Aid 41-01-008, *Civil Affairs Negotiations and Mediation Guide*, Washington, D.C.: Headquarters, U.S. Department of the Army, September 30, 2016.

Joint Publication 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

U.S. Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, Washington, D.C., July 25, 2018.

3. Civil-Military Operations and Civil Affairs Operations

Army Techniques Publication 3-57.10, *Civil Affairs Support to Populace and Resources Control*, Washington, D.C.: Headquarters, U.S. Department of the Army, August 6, 2013.

Army Techniques Publication 3-57.20, *Multi-Service Techniques for Civil Affairs Support to Foreign Humanitarian Assistance*, Washington, D.C.: Headquarters, U.S. Department of the Army, February 2013.

Army Techniques Publication 3-57.30, *Civil Affairs Support to Nation Assistance*, Washington, D.C.: Headquarters, U.S. Department of the Army, May 1, 2014.

Army Techniques Publication 3-57.50, *Civil Affairs Civil Information Management*, Washington, D.C.: Headquarters, U.S. Department of the Army, September 6, 2013.

Army Techniques Publication 3-57.60, *Civil Affairs Planning*, Washington, D.C.: Headquarters, U.S. Department of the Army, April 27, 2014.

Army Techniques Publication 3-57.70, *Civil-Military Operations Center*, Washington, D.C.: Headquarters, U.S. Department of the Army, May 5, 2014.

Army Techniques Publication 3-57.80, *Civil-Military Engagement*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 31, 2013.

Field Manual 3-57, *Civil Affairs Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, April 2019.

FM—See Field Manual.

Graphic Training Aid 41-01-001, *Civil Affairs General Concepts*, Washington, D.C.: Headquarters, U.S. Department of the Army, January 1, 2019.

Graphic Training Aid 41-01-004, *Civil Affairs Reference Guide*, Washington, D.C.: Headquarters, U.S. Department of the Army, September 1, 2016.

Graphic Training Aid 41-01-007, *Civil Affairs Project Management*, Washington, D.C.: Headquarters, U.S. Department of the Army, November 26, 2012.

Graphic Training Aid 41-01-008, *Civil Affairs Negotiations and Mediation Guide*, Washington, D.C.: Headquarters, U.S. Department of the Army, September 30, 2016.

Graphic Training Aid 41-60-001, *Civil Affairs Operations Planning Considerations*, Washington, D.C.: Headquarters, U.S. Department of the Army, September 1, 2016.

Joint Publication 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

Joint Publication 3-57, *Civil-Military Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, July 9, 2018.

JP—See Joint Publication.

Marine Corps Tactical Publication 3-03A, *Marine Air-Ground Task Force Civil-Military Operations*, Washington, D.C.: Headquarters, U.S. Marine Corps, July 2016.

NATO Standardization Office, *Allied Joint Doctrine for Civil-Military Co-Operation*, AJP-3.19, Edition A, Version 1, November 2018.

4. Public Affairs and Combat Camera/Service Member Camera

Air Force Instruction 35-109, *Visual Information*, Washington, D.C.: Headquarters U.S. Air Force, June 1, 2017.

Army Regulation 360-1, *The Army Public Affairs Program*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 8, 2020.

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018.

Army Techniques Publication 6-02.40, *Techniques for Visual Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, January 2019.

Chairman of the Joint Chiefs of Staff Instruction 3205.01D, *Joint Combat Camera (COMCAM)*, Washington, D.C., October 20, 2014.

Cotton, CDR Tom, Joint Combat Camera Program Manager, “Combat Camera Support to Information Operations,” briefing, 2018. As of January 15, 2021: https://www.dimoc.mil/Portals/64/docs/DVI%20docs/COMCAM_Capabilities_Brief_APR_2018.pdf?ver=2018-04-13-150801-487

Joint Publication 3-61, *Public Affairs*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, August 1, 2016.

Marine Corps Order 3104.1B, *Marine Corps Combat Camera Program*, Washington, D.C.: Headquarters, U.S. Marine Corps, October 25, 2011.

Maryland National Guard, *Maryland National Guard Unit Public Affairs Representative Handbook*, undated.

U.S. Navy, *Joint Combat Camera (COMCAM)/Visual Information Smartbook*, Fort Meade, Md.: Defense Visual Information Joint Combat Camera Program, 2015.

5. Operations Security and Signature Management

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018, Chapters 5–7.

Army Techniques Publication 3-13.3, *Army Operations Security for Division and Below*, Headquarters, U.S. Department of the Army, July 2019.

Neller, Gen. Robert B., Commandant, *U.S. Marine Corps, Message to the Force 2018: “Execute,”* January 26, 2018.

U.S. Marine Corps, *Marine Corps Concept for Signature Management*, October 2017.

6. Military Deception

For a discussion of the role that deception played in the Gulf War, see Wyatt Olson, “‘Left Hook,’ Deception Hastened War’s End,” *Stars and Stripes*, January 17, 2016.

Field Manual 3-13.4, *Army Support to Military Deception*, Washington, D.C.: Headquarters, U.S. Department of the Army, February 2019.

Vertuli, Mark D., “A Myth Retold: The Army’s MILDEC Program in the 21st Century,” *IO Sphere*, Fall 2015.

Whaley, Barton, *Practice to Deceive: Learning Curves of Military Deception Planners*, Annapolis, Md.: Naval Institute Press, 2016.

7. Electronic Warfare

Air Force Doctrine Annex 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations*, Washington, D.C., July 30, 2019.

Air Force Instruction 10-703, *Electronic Warfare (EW) Integrated Reprogramming*, Washington, D.C., February 22, 2017.

Army Regulation 5-12, *Army Use of the Electromagnetic Spectrum*, Washington, D.C.: Headquarters, U.S. Department of the Army, February 8, 2020.

Army Regulation 525-22, *U.S. Army Electronic Warfare*, Washington, D.C.: Headquarters, U.S. Department of the Army, January 28, 2016.

Army Techniques Publication 3-12.3, *Electronic Warfare Techniques*, Washington, D.C.: U.S. Department of the Army, July 2019.

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018.

ATP—See Army Techniques Publication.

Chairman of the Joint Chiefs of Staff Instruction 3320.01C, *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment*, Washington, D.C., February 5, 2019.

Chairman of the Joint Chiefs of Staff Instruction 3320.02D, *Joint Spectrum Interference Resolution (JSIR) Procedures*, Washington, D.C., June 3, 2013.

Chairman of the Joint Chiefs of Staff Instruction 3320.02F, *Joint Spectrum Interference Resolution*, Washington, D.C., March 8, 2013.

Chairman of the Joint Chiefs of Staff Instruction 3320.03D, *Joint Communications Electronics Operating Instructions*, Washington, D.C., June 25, 2018.

Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, April 2017.

FM—See Field Manual.

Graphic Training 13-01-001, *Cyber and EW Threat Quick Reference Card*, Washington, D.C.: Headquarters, U.S. Department of the Army, April 2019.

Graphic Training 13-01-002, *Electronic Warfare Platoon Checklist, Lessons and Best Practices*, Washington, D.C.: Headquarters, U.S. Department of the Army, December 2019.

Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, May 22, 2020.

JP—See Joint Publication.

Marine Corps Order 2400.2A, *Marine Corps Management and Use of the Electromagnetic Spectrum*, Washington, D.C.: Headquarters, U.S. Marine Corps, October 7, 2009.

Neller, Gen. Robert B., Commandant, U.S. Marine Corps, *Message to the Force 2018: "Execute,"* January 26, 2018.

U.S. Army Training and Doctrine Command Pamphlet 525-8-6, *The U.S. Army Concept for Cyberspace and Electronic Warfare Operations, 2025–2040*, Fort Eustis, Va., January 2018.

8. Cyber Operations

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018.

Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, April 2017.

Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, Washington, D.C.: U.S. Joint Chiefs of Staff, May 21, 2014.

Joint Publication 3-0, *Joint Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, October 22, 2018.

Joint Publication 3-12, *Cyberspace Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, June 2018.

Presidential Policy Directive 20, *US Cyber Operations Policy*, October 2012.

U.S. Army Training and Doctrine Command Pamphlet 525-8-6, *The U.S. Army Concept for Cyberspace and Electronic Warfare Operations, 2025–2040*, Fort Eustis, Va., January 2018.

9. Military Information Support Operations/Psychological Operations

Army Techniques Publication 3-53.1, *Military Information in Special Operations*, Washington, D.C.: U.S. Department of the Army, April 2015.

Field Manual 3-53, *Military Information Support Operations*, Washington, D.C.: U.S. Department of the Army, January 2013.

Graphic Training 33-01-001, *Military Information Support Operations in Military Decisionmaking Process*, Washington, D.C.: U.S. Department of the Army, April 2014.

Graphic Training 33-01-004, *Military Information Support Operations Authoritative References*, Washington, D.C.: U.S. Department of the Army, November 2017.

Joint Publication 3-13.2, *Military Information Support Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, November 2014.

10. Space Operations

Center for Army Lessons Learned, *Operating in a Denied, Degraded, and Disrupted Space Operational Environment*, Fort Leavenworth, Kans., June 2018.

Joint Publication 3-14, *Space Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, October 26, 2020.

11. Technical Effects

These capabilities are tightly controlled, and you will not be able to access information on them.

12. Social Media and Open-Source Intelligence

Marcellino, William, Meaghan L. Smith, Christopher Paul, and Lauren Skrabala, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, Santa Monica, Calif.: RAND Corporation, RR-1742-OSD, 2017. As of January 15, 2021: https://www.rand.org/pubs/research_reports/RR1742.html

U.S. Department of Defense Directive 3115.18, *Access to and Use of Publicly Available Information (PAI)*, Washington, D.C., incorporating change 1, August 20, 2020.

U.S. Department of Defense Instruction 3115.12, *Open Source Intelligence (OSINT)*, Washington, D.C., incorporating change 2, July 16, 2020.

U.S. Marine Corps, *The Social Corps: The USMC Social Media Principles*, Washington, D.C., 2013.



NATIONAL DEFENSE RESEARCH INSTITUTE

Early-career officers in tactical units must understand and operate in an increasingly complex information environment. Poor communication with command-level decisionmakers and errors in judgment can be costly in the face of sophisticated adversary capabilities and while operating among civilian populations. There are few opportunities for formal education and training to help officers prepare for operations in the information environment (OIE), and it can be difficult to know how to employ the tactics, techniques, and procedures of tactical-level maneuver-focused operations in support of OIE-related capabilities and activities. With its quick-reference format and series of illustrative vignettes, this handbook is intended to facilitate tactical problem-solving and increase officers' awareness of when and how they can contribute to the goals of OIE.

\$32.00

www.rand.org

