MICHAEL SCHWILLE, ANTHONY ATLER, JONATHAN WELCH,
CHRISTOPHER PAUL, RICHARD C. BAFFA

Intelligence Support for Operations in the Information Environment

Dividing Roles and Responsibilities Between Intelligence and Information Professionals

For more information on this publication, visit www.rand.org/t/RR3161

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0570-8

Published by the RAND Corporation, Santa Monica, Calif.

Cover: lvcandy/Getty Images
Cover design: Rick Penn-Kraus

Preface

Planning and conducting operations in and through the information environment requires a significant amount of information and analytic expertise. Information operations (IO) often require an understanding of an adversary or potential adversary that is not common to traditional intelligence analysis and products on such topics as adversary decisionmaking processes, the beliefs and proclivities of adversary leaders, and adversary leaders' confidence in their subordinates and superiors. For this reason, intelligence support to IO can be challenging.

Although intelligence organizations have been established specifically to collect and analyze data on the human terrain, cultural factors, and other intelligence sources in support of IO and information-related capability planners and practitioners, such efforts were often short-lived. Moreover, existing collection and analytic practices *could* support IO intelligence requirements, but these requests are often crowded out by higher-priority needs elsewhere in a command. In some cases, low priority and attendant low levels of support have driven information professionals to gather needed intelligence themselves from alternative sources, raising concerns about analytic quality and oversight.

This report identifies requirements, highlights challenges, and offers solutions to improve IO intelligence integration from both an intelligence and IO perspective to help the joint force (specifically, the geographic combatant commands) better organize for, invest in, conduct, and support operations in the information environment. It should be of interest to both intelligence and information professionals at the combatant commands, as well as policymakers, force planners, and intelligence service center personnel.

This research was sponsored by U.S. European Command 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 The research reported here was completed in June 2019 and underwent security review

with the sponsor and the Defense Office of Prepublication and Security Review before public release.

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).

Contents

Figures and Tables

Figures

Tables

Summary

There is growing recognition within the U.S. Department of Defense (DoD) that information is a powerful tool and invaluable in support of military operations. The 2018 U.S. National Defense Strategy, 2017 National Security Strategy, and the National Defense Authorization Act for Fiscal Year 2018 all contained language calling on DoD to bolster its capability to produce effects in the information environment (IE).[1] Additionally, DoD's Strategy for Operations in the Information Environment, the Joint Concept for Operating in the Information Environment, and the elevation of information to the list of joint functions highlight how the department intends to aggressively pursue information-related activities.[2]

Meanwhile, the United States' near-peer competitors are already actively engaged in the IE. They have tailored their aggression to remain below the U.S. threshold for armed conflict, often allowing specialized forces to undertake operations unimpeded.[3] To counter these efforts, DoD needs a clear understanding of what relevant actors are doing in the IE, as well as an ability to conduct its own operations and undertake various other activities in and through the IE. The first capability is the responsibility of intelligence practitioners and the second, information operations (IO) practitioners. Both communities routinely deal with information and are at the forefront of U.S. information warfare efforts at the combatant commands (CCMDs). However, they

[1] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018; Executive Office of the President, *National Security Strategy of the United States of America*, Washington, D.C.: White House, December 2017; Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018, December 12, 2017. For a good summary of issues with "information" policy, see U.S. Senate, Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2018*, Washington, D.C., 2018.

[2] U.S. Department of Defense, *Department of Defense Strategy for Operations in the Information Environment*, Washington, D.C., June 2016; U.S. Department of Defense, *Joint Concept for Operating in the Information Environment (JCOIE)*, Washington, D.C., July 25, 2018; James Mattis, Secretary of Defense, "Information as a Joint Function," memorandum, Washington, D.C., September 15, 2017.

[3] Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-1925/1-A, 2018.

have long been beset by challenges that impede close coordination, resulting in missed opportunities to effectively conduct operations in the IE (OIE).

The recent surge in interest in the IE can make it appear that OIE are a new aspect of warfare, but both information efforts and intelligence have long been central to U.S. military practice. Information is the essence of both communities; what distinguishes them is how each community compiles, sorts, analyzes, and uses information. Furthermore, although both communities have undergone numerous reorganizations and name changes, perhaps to the chagrin of some who specialize in one or the other, they are indeed closely linked.

Methods and Approach

The goal of this study was to help the joint force (specifically, the CCMDs) identify and refine the requirements, opportunities, and challenges associated with providing intelligence support to OIE so that it can better organize for, invest in, conduct, and support these operations. Accordingly, our study was guided by three sets of questions:

1. What data, information, analysis, and level of understanding are required to plan, integrate, and execute OIE?
2. Who could collect the needed information and conduct the required analyses, and through what processes? What are the barriers or challenges to doing so?
3. What terms are appropriate to describe what is collected and what is produced? Where is the boundary between routine information-gathering and formal intelligence collection? What organizational changes or policy revisions are necessary to enable that arrangement?

We answered these questions through a three-step process: a literature review, interviews with subject-matter experts, and an analysis of 40 challenges facing CCMD and joint force commanders as they explore how information is provided in support of OIE and where improvements could be warranted and subsequently implemented. We then mapped each of the challenges we identified to between one and five of 67 unique solutions.

Understanding the Information Environment

Perhaps the greatest point of friction between the IO and intelligence communities is over whose responsibility it is to collect the information and conduct the analyses necessary to support OIE. Words matter. Doctrine and terminology are constantly changing, but they have not necessarily kept pace with changes to the operational environment—a challenge that is at the core of the IO intelligence integration (IOII)

problem. The joint force is still developing capabilities, undergoing reorganization, and testing concepts that will dramatically affect the future of intelligence support for OIE.

Recent guidance and information's designation as the seventh joint function highlight the growing importance of information to warfighting, but this idea is not new. The U.S. IO and intelligence communities have shared a close connection since the official recognition of both as important elements of national power. However, their interconnectedness organizationally and in practice has, by turns, strengthened and weakened throughout U.S. history. Information is the essence of both communities; how each compiles, sorts, analyzes, and uses information is a key difference.

Military actions designed to affect the attitudes, decisionmaking, and behaviors of others are effectively timeless, but the means by which the desired effects are achieved, at a minimum, overlaps with—and, at times, may directly compete with—intelligence. The intelligence cycle of collection, processing, integration, evaluation, and analysis is critical to OIE, which aim to shape how an adversary perceives (or misperceives) changes in the IE.

The primary goal of CCMDs is to deter conflict and fight to win in the event that deterrence fails.[4] Most if not all CCMD activities contribute to keeping the peace, primarily through deterrence. To ensure successful deterrence—or deescalation, in the event of a conflict—the campaigns planned by CCMD staffs must be capable, credible, and communicated effectively.[5] OIE have a critical role to play in deterrence. These activities often, though not always, achieve effects through nonlethal means. Should deterrence fail, the CCMDs' responsibilities also include planning for and responding to crises and contingencies.[6]

Six Types of Challenges Hinder Intelligence Support for OIE

Planning and conducting OIE requires a great deal of information and strong analytic capabilities. To clarify the roles and responsibilities involved in providing intelligence support for OIE, we compiled a set of 52 challenges that the joint force will need to consider and possibly address moving forward. Through a deliberate analytical process, we synthesized, refined, and combined the initial 52 challenges into a condensed

[4] U.S. Code, Title 10, Section 164, Commanders of Combatant Commands: Assignment; Powers and Duties.

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

[6] As we discuss later, *campaigning* refers to a whole-of-staff effort that involves planning and executing operations in the short term, as well as developing detailed contingency plans for a range of potential scenarios and future developments.

list of 40 unique challenges in six categories, with some challenges spanning multiple categories:

- Coordination and collaboration: This category focuses on common interactions between the IO and intelligence communities.[7] Challenges stem from a lack of mutual understanding, underdeveloped or nonexistent relationships, and immature or absent processes.
- Division of labor: Includes tensions over who should be responsible for which tasks, such as staffing decisions and information fusion, as well as expectations regarding analytic rigor.
- Missing expertise: Gaps in the skills and knowledge necessary for effective intelligence support for OIE. Most of these challenges are the result of shortfalls in training and education, which have led to a lack of personnel with the necessary expertise to perform required tasks.
- Prioritization: Includes challenges stemming from a command or other organization's failure to sufficiently prioritize OIE. Requirements related to these challenges could be met but are not because scarce resources are devoted to perceived or actual higher priorities. These challenges were cited in our discussions with subject-matter experts about the request for information (RFI) process, the value of IO assessments, and a command's need to balance limited resources.
- Gaps in concepts or doctrine: Identifies challenges stemming from a gap in concepts or doctrine. It can be easy to blame deficiencies in doctrine, but in this case, new concepts have been disseminated at both the joint and service levels and accompanying doctrine is being written. When doctrine and concepts are in a state of flux, practice inevitably lags.
- Intelligence authorities: Addresses the rules and oversight mechanisms that apply to the intelligence community (IC), including legal and policy restrictions that limit its ability to collect information on U.S. persons. The debate surrounding open-source intelligence and research highlights the importance of addressing challenges in this category.[8]

---

[7] Note the distinction between the IO and intelligence communities and information and intelligence as warfighting or joint functions. Joint functions are integrated like any other maneuver warfare approaches. This category of challenges is instead concerned with the interactions among the people, processes, and resources that constitute each respective community. Commands should continue to seek better ways to integrate the intelligence function with the newly designated information function.

[8] Analysis of open-source intelligence relies on publicly available information to meet intelligence requirements or to answer, non–intelligence-related questions. Within DoD, its users are generally IO practitioners and operators outside the intelligence profession.

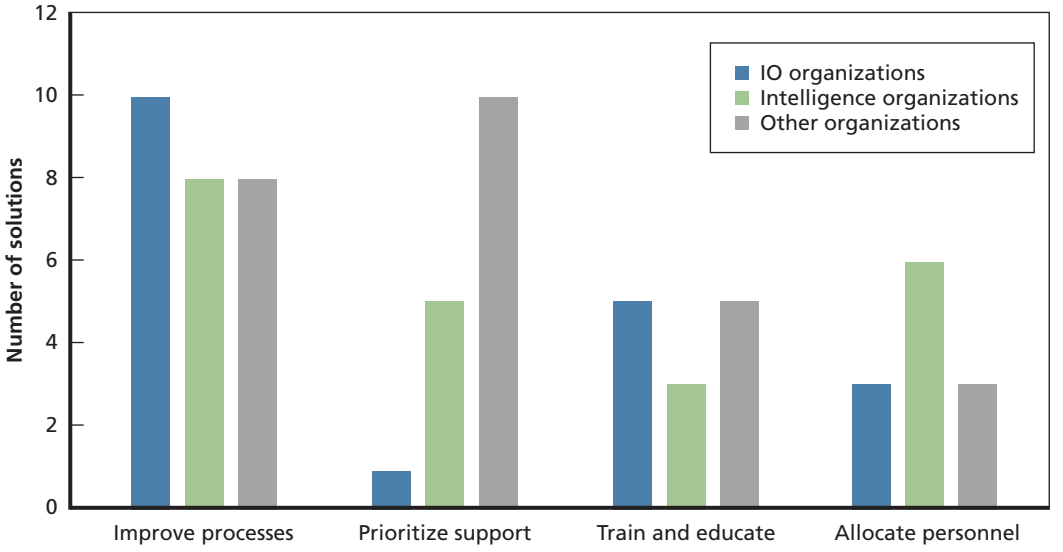
Four Ways to Improve Intelligence Support for OIE

We drew on interviews with subject-matter experts, our literature review, and the research team's expertise to develop solutions to these 40 challenges. We identified 91 potential solutions, which we then synthesized to reduce redundancy, leaving 67 unique solutions. We matched the solutions to specific challenges on our shortlist of 40 to ensure their utility and then validated them through a careful analytic review. We grouped the final 40 solutions into the following four categories:

- Improve processes: Solutions in this category address challenges that expose shortcomings or deficiencies in existing processes. Such challenges are common to both the intelligence and information communities. In fact, there were more solutions assigned to this category than any other. The first step to implementing them involves increasing awareness of processes and practices across the two communities. This will increase the type and amount of support that can be offered. Each community has its own established culture, and it will likely be necessary to push them to interact to a greater degree. In addition to coordination in support of OIE, the targeting and tasking processes are both areas for improvement.
- Prioritize support: These solutions address gaps in how support for OIE is prioritized. Commander and institutional priorities hinder effective support when they are in competition. Intelligence organizations need to dedicate personnel to conducting IOII, and IO practitioners need to be better at requesting support. Implementing the bulk of solutions in this category will require a command-level or institutional champion who can advocate for greater support from the IC; otherwise, intelligence organizations and entities will not see a need to give a higher priority to supporting OIE or to extend and grow their capabilities to do so.
- Train and educate: Both IO and intelligence personnel need additional training and educational opportunities to increase their familiarity with IOII and acquire related skills. There is also a general lack of understanding of roles and responsibilities across both forces.
- Allocate personnel: These solutions focus on addressing near-term personnel shortages. A dedicated body of intelligence professionals is needed to support OIE, but that would be a longer-term effort.

We first divided the solutions according to which community would be primarily responsible for implementing them: the information community, the IC, or other organizations. Figure S.1, which shows the results of this process, reflects a relatively balanced division between solutions that will need to be implemented by information professionals and organizations and those that will need to be implemented by intelligence professionals and organizations.

Figure S.1
Analysis of Solutions and Organizations Responsible for Implementation



Insights from This Research

Here, we outline several conclusions from our analysis and present a series of actionable recommendations to improve intelligence support for OIE across commands. Our six general conclusions are as follows:

- There is growing awareness of OIE and the effects that these operations generate, but there is not sufficient appreciation for what OIE can achieve or how they can shape the operational environment.
- IOII is a two-sided problem. Intelligence and IO professionals need to work together to address the challenges identified.
- There is insufficient support for OIE and little emphasis on the IE within the defense intelligence enterprise. This hinders efforts to plan and execute OIE.
- Current processes are insufficient to effectively support OIE, including for targeting and producing estimates and assessments.
- Challenges fall into six categories: coordination and collaboration, division of labor, missing expertise, prioritization, gaps in concepts or doctrine, and intelligence authorities. Potential solutions fall into four categories: improve processes, prioritize support, train and educate, and allocate personnel.
- Support for IO/OIE required from intelligence professionals spans the conflict continuum and varies across that spectrum.

Recommendations for IO Organizations

To implement solutions that will improve how the joint force organizes for, invests in, conducts, and supports OIE, we recommend that IO organizations take ownership of specific tasks and responsibilities where possible. They should make use of their available planners and practitioners and be champions for OIE within the joint force. Although there is clear recognition that information plays a key role across the conflict continuum, there is still little appreciation for how to execute OIE. Even when commanders and staffs *do* have the requisite understanding and awareness, they often do not fully consider or adequately integrate information activities, capabilities, and operations into military exercises and campaigns. To address this shortfall, we suggest that IO organizations take the following four steps:

1. Increase understanding and awareness of OIE and IOII. Work with commanders, staffs, and, especially, intelligence personnel to increase their knowledge of OIE. Be champions of OIE for commanders and staffs, and volunteer to teach and mentor them in how OIE should be conducted.
2. Make use of existing personnel to improve coordination and routinize processes that are currently ad hoc or nonexistent. Address knowledge shortfalls in the RFI process, and ask intelligence personnel to help IO practitioners craft answerable RFIs.
3. Assign IO liaison officers to intelligence organizations to establish better communication, build a shared understanding of OIE and IOII, help educate intelligence personnel, and create products that are more focused on the IE.
4. Ensure that nonlethal effects are included in targeting process. IO personnel should receive instruction on the targeting process and methodology. Improved understanding will lead to better articulation and advocacy for targets in the IE.

Recommendations for Intelligence Organizations

Intelligence organizations also have a part to play if the joint force is to get better at OIE. These organizations already have a firm base on which to build in the form of well-developed doctrine and analytic processes. Analysts are well trained and bring critical-thinking skills to complex problems. However, intelligence organizations need greater awareness of OIE and, subsequently, need to expand training and dedicate personnel to collecting and analyzing data and producing intelligence products focused on the IE. We offer three recommendations to help intelligence organizations pursue these objectives:

1. Formalize and expand training. This training should be institutionalized, broadened, and systematized across the defense intelligence enterprise. Both

military and civilian intelligence personnel need training, but the focus should be on personnel slated to work at CCMDs.

2. Empower an organization to own analysis of the IE. This organization will create the foundational structures through which intelligence support for OIE is institutionalized. To help achieve this, the Defense Intelligence Analysis Program, managed by the Defense Intelligence Agency, should treat intelligence support for OIE as a complex analytical issue. This will raise awareness of this challenge, help align resources and, potentially, lead to the creation of an IE specialization for intelligence personnel.
3. Create cross-functional teams to better integrate intelligence functions and direct greater attention to the IE. These teams should use existing doctrine and templates to ensure that IE-related tasks are properly executed.

Implementing these recommendations will increase the effectiveness of intelligence support for OIE. It will also help standardize processes, ensure that training and education are provided to both IO and intelligence professionals, and improve understanding of OIE across the joint force.

Acknowledgments

We would like to express our gratitude to a number of people in our sponsoring office, U.S. European Command's information operations directorate (J39), including COL Michael Jackson, Alan Ball, and LTC Dan Welsh. We are also indebted to U.S. European Command's intelligence directorate (J2), without whose support this report would not have been possible, including BG Laura Potter, CAPT Charles Pratt, and LT Mark Nicollet. There are also several personnel in the greater IO and intelligence communities who deserve a special thanks for their helpful insights and comments: Dwayne Hanford, LTC Wayne Sanders, MAJ Jason Romanello, Tom Evans, LTC Daniel "Dip" Schnick, Christian Andros, Kevin Doyle, Ray Colston, and Randall Munch. We received valuable contributions and ideas from too many to name individually, so if you have helped us better understand the challenges of integrating intelligence support and operations in the IE, thank you! We owe a debt of gratitude to the reviewers who read and commented on this document as part of RAND's quality assurance process: Michael Williams and Arturo Muñoz. We would also like to thank Maria Falvo for her administrative assistance and Lauren Skrabala for her editorial support.

Abbreviations

CCMD	combatant command
COLISEUM	Community On-Line Intelligence System for End Users and Managers
COP	common operational picture
DIA	Defense Intelligence Agency
DIAP	Defense Intelligence Analysis Program
DoD	U.S. Department of Defense
IC	intelligence community
IE	information environment
IO	information operations
IOII	information operations intelligence integration
IRC	information-related capability
J2	intelligence directorate
J25	intelligence operations, plans, and policy directorate
J39	information operations directorate
J5	strategy, plans, and policy directorate
JC HAMO	Joint Concept for Human Aspects of Military Operations
JCOIE	Joint Concept for Operating in the Information Environment
JIOC	joint intelligence operations center
JIPOE	joint intelligence preparation of the operational environment
JOA	joint operations area

JP	joint publication
JS	Joint Staff
MILDEC	military deception
MISO	military information support operations
OE	operational environment
OIE	operations in the information environment
OPLAN	operational plan
OPSEC	operational security
OSCAR-MS	Open Source Collection Acquisition Requirements-Management System
OSINT	open-source intelligence
PIR	priority intelligence requirement
PSYOP	psychological operations
RFI	request for information
SOP	standard operating procedure
STO	special technical operations
USEUCOM	U.S. European Command

CHAPTER ONE

Introduction

Information operations (IO) have been part of the U.S. Department of Defense (DoD) lexicon for nearly 30 years. In this short time frame, the terminology, concepts, and activities associated with IO have evolved dramatically—from highly classified to widely discussed, studied, and debated as an integrating staff function that leverages the range of information-related capabilities (IRCs). The first unclassified publication dedicated to IO was a DoD directive issued in 1992, and IO have since been enshrined in publicly available joint doctrine.[1]

However, IO and the terminology, concepts, and activities associated with these operations continue to evolve. The current doctrinal definition describes IO as follows:

> The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[2]

This definition may not have kept pace with changes in how IO are conceived, exercised, and executed, and it does not fully account for many of the goals of IO, the activities that these operations entail, or the capability development that they require. For example, the doctrinal definition of IRC reads 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.[3]

---

[1] Originally issued in 1992, U.S. Department of Defense Directive 3600.1, *Information Operations (IO)*, Washington, D.C., incorporating change 1, May 4, 2017, is the current iteration of the directive. Also see Joint Publication (JP) 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

[2] U.S. Joint Chiefs of Staff, *DoD Dictionary of Military and Associated Terms*, Washington, D.C., last updated January 2020, p. 104.

[3] U.S. Joint Chiefs of Staff, 2020, p. 104.

By 2016, DoD had come to refine the vocabulary used to describe IO and the range of other activities associated with U.S. forces' engagement in the information environment (IE). The broader term of art has become operations in the information environment (OIE).[4]

New terms are regularly introduced and incorporated into the DoD lexicon, and new capabilities and concepts frequently emerge that must be described and are subsequently operationalized. As a consequence, there is little in the way of standardization across staff sections, offices, organizations, and even individuals. Many of the concepts and terms associated with IO and OIE are viewed as esoteric and are not well understood across the joint force. Nowhere is this lack of shared understanding more apparent than in the relationships between intelligence and IO personnel in the combatant commands (CCMDs).

A considerable amount of information and understanding is required to plan for OIE and mobilize IRCs to conduct these operations. These activities require not just awareness of friendly force capabilities and objectives but also extensive insight into the aspects of the IE that are relevant to the mission.[5] One common requirement is an understanding of the "human terrain," including relevant populations' cultural and linguistic patterns, beliefs, and attitudes; their modes of communication; and the content and tone of their discourse. OIE can also require an awareness of aspects of the *physical* terrain (e.g., the locations and significance of broadcast or network nodes, broadcast footprints, cellular service coverage), as well as an understanding of adversary decisionmaking processes, the beliefs and proclivities of leaders, and leaders' confidence in their subordinates and superiors.[6]

For commanders and operation planners, the question is quickly raised: Who is responsible for providing this type of data and analysis? Should the information professionals who plan or coordinate OIE be responsible for gathering the inputs necessary to inform their understanding of the IE, or should that knowledge and analysis come from *intelligence* professionals?

The answer probably involves some sort of division of labor between information and intelligence personnel, which begs questions of which community should be responsible for which types of information requirements and how relevant data and intelligence should be shared. This report revisits how these operations are planned, supported, and executed. It reconceives OIE as a set of discrete tasks and decisions requiring the expertise and input of specific types of specialists or organizations. Finally,

---

[4] DoD, *Department of Defense Strategy for Operations in the Information Environment*, Washington, D.C., June 2016.

[5] Christopher Paul, 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.

[6] Paul, Clarke, Triezenberg, et al., 2018.

it provides guidance on how to most appropriately assign these roles and responsibilities when it comes to providing intelligence and analytical support for OIE.

Analytic Challenges

The defense intelligence enterprise is vast—comprising all defense intelligence organizations and military intelligence personnel—and has a mission to provide information and analysis in support of operations. However, collaboration and coordination between DoD's intelligence and IO communities can be challenging when it comes to providing intelligence support for IO, sometimes referred to as IO intelligence integration (IOII). The defense intelligence organizations excel in providing detailed enemy orders of battle and other related and valuable products, but many of these products fail to encompass important aspects of the IE.

Even when the defense intelligence enterprise has spawned sections or organizations specifically dedicated to collecting and analyzing data on human terrain, cultural factors, and other intelligence sources for OIE and IRC planners and practitioners, such efforts have often been short-lived. Although existing data collection and analytic practices should support OIE intelligence requirements, OIE-related requests are often sidelined by higher-priority requests from elsewhere in a command. Low priority and attendant low levels of support have occasionally driven OIE and IRC personnel to gather needed data themselves from alternative sources, which, in turn, has raised concerns that such self-support might fall outside of appropriate intelligence authorities. It also raises questions about the quality and accuracy of the analysis. In fact, the boundary between the information-gathering and analysis that *should* be the responsibility of IO and IRC professionals and the collection and analysis that should be provided as part of intelligence support is often unclear.

Doctrine and defined processes are in place for IOII, but standardized processes have not been broadly adopted across the joint force. And both the providers and users of intelligence to support OIE are responsible for this lack of coordination at the command level.

There is a growing perception within DoD that information is a powerful tool to be used and weaponized. The National Defense Strategy, National Security Strategy, and 2018 National Defense Authorization Act all contain language that calls on DoD to bolster the capability to produce effects in the IE.[7] Additionally, the Strategy for

[7] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018; Executive Office of the President, *National Security Strategy of the United States of America*, Washington, D.C.: White House, December 2017; Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018, December 12, 2017. For a good summary of issues with "information" policy, see U.S. Senate, Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2018*, Washington, D.C., 2018.

Operations in the Information Environment, the Joint Concept for Operating in the Information Environment (JCOIE), and the creation of the information joint function highlight how DoD should be aggressively pursuing information-related activities.[8]

Doctrine and policy are still catching up with the demands of operating in the IE, and they do not sufficiently address many of the challenges that U.S forces will continue to face moving forward. Indeed, the forces, processes, and authorities necessary to understand and act in the IE are still not fully in place. This all comes at a critical time when the lines between peace, crisis, and war are blurrier than ever.[9] New technologies and techniques are expanding capabilities, and there is an appetite for campaigns short of war, often referenced as "gray zone" competition.[10]

Meanwhile, the United States' near-peer competitors are fully engaged in the IE and have explicitly designed their systems to operate below the threshold for armed conflict.[11] They have created specialized forces for this purpose and have been able to conduct operations unimpeded. To counter these efforts, DoD needs to better understand the IE and better prepare to conduct OIE.

This report explores several considerations for commanders, OIE planners, intelligence agencies, and others in a position to implement the solutions and recommendations identified here to improve how the joint force integrates intelligence processes and products for OIE.

Understanding the Information Environment

Perhaps the greatest point of friction between the IO and intelligence communities is over whose responsibility it is to collect the information and conduct the analyses necessary to support OIE. Joint Publication (JP) 3-13, *Information Operations*, addresses this issue directly by defining IOII as "the integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine

---

[8] DoD, 2016; U.S. Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, Washington, D.C., July 25, 2018b; James Mattis, Secretary of Defense, "Information as a Joint Function," memorandum, Washington, D.C., September 15, 2017.

[9] See, for example, Scott W. Harold, Yoshiaki Nakagawa, Junichi Fukuda, John A. Davis, Keiko Kono, Dean Cheng, and Kazuto Suzuki, *The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains*, Santa Monica, Calif.: RAND Corporation, CF-379-GOJ, 2017.

[10] For a more in-depth discussion of the gray zone, see Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*, Carlisle Barracks, Pa.: U.S. Army War College Press, April 2016, and Michael J. Mazarr, "The Challenge of the Gray Zone," briefing, U.S. Department of Defense, Strategic Multilayer Assessment Program, Washington, D.C., February 2016.

[11] Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-1925/1-A, 2018.

effects, and assess the information environment."[12] The same definition appears in JP 2-0, *Joint Intelligence*; JP 5-0, *Planning*; and JP 3-0, *Operations*.[13] JP 3-0 was updated in October 2018 specifically to incorporate the addition of "information" as the seventh joint function.[14] It very clearly addressed the importance of intelligence support for OIE and collaborative contributions to improving understanding of what information is needed and how it can support OIE, stating,

> In conjunction with activities under the intelligence joint function, this activity facilitates the [joint force commander's] understanding of the pervasive nature of information in the OE [operational environment], its impact on relevant actors, and its effect on military operations.[15]

DoD released the JCOIE in July 2018 to "institutionalize and operationalize the Joint Force's approach to information."[16] The central idea behind the concept document is to provide direction for the joint force to "build information into operational art to design operations that deliberately leverage the inherent informational aspects of military activities."[17] That goal is supported by three primary directives:

1. Understand information, the informational aspects of military activities, and informational power.
2. Institutionalize the integration of physical and informational power.
3. Operationalize the integration of physical and informational power.[18]

These ideas led to an examination of the capabilities that the joint force requires to fully leverage information for operation planning and in pursuing military objectives. The JCOIE identifies 17 capabilities organized into the following four categories of objectives:

1. Characterize and assess the informational, physical, and human aspects of the security environment.
2. Formulate options that integrate physical and informational power.

---

[12] JP 3-13, 2014, p. GL-3.

[13] JP 2-0, *Joint Intelligence*, Washington, D.C.: U.S. Joint Chiefs of Staff, October 22, 2013; JP 5-0, *Joint Planning*, Washington, D.C.: U.S. Joint Chiefs of Staff, June 16, 2017; JP 3-13, 2012.

[14] The other six joint functions are as follows: command and control, intelligence, fires, movement and maneuver, protection, and sustainment. See JP 3-0, *Joint Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, October 22, 2018.

[15] JP 3-0, 2018, p. III-18.

[16] U.S. Joint Chiefs of Staff, 2018b, p. vii.

[17] U.S. Joint Chiefs of Staff, 2018b, p. viii.

[18] U.S. Joint Chiefs of Staff, 2018b, p. ix.

3. Execute and modify options.
4. Institutionalize the integration of physical and informational power.[19]

The JCOIE is not so much a roadmap for IO practitioners as a vision for the entire joint force to pursue collaboratively. The first capability required by the joint force is focused on understanding the environment. However, this is also a key intelligence function during joint intelligence preparation of the OE (JIPOE), a process described in greater detail in Chapter Three. More specifically, it is about understanding the IE as a subset of the broader OE.

At the time of this writing, the most recent DoD definition of *IE* could be found in JP 3-0, which stated that the IE

> comprises and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, worldviews, and, ultimately, actions of an individual, group, system, community, or organization. The IE also includes technical systems and their use of data. The IE directly affects all OEs.[20]

Clearly, this is not a task to be handled solely by IO and IRC practitioners, but, rather, one that requires inputs from across the staff, with a heavy reliance on intelligence personnel.

Capabilities that fall into the third and fourth categories ("Execute and modify options" and "Institutionalize the integration of physical and informational power," respectively) focus on the ability to undertake information-related activities in coordination with physical activities. They address both means and processes. The fourth type of required capability focuses on the joint force itself. It advocates for culture change within the organization and for enhancing its ability to work with other organizations and partners.[21]

Key Terms and Use

To capture the evolving language, policy, and thinking surrounding the creation of a joint function for information and the associated changes it has prompted, we need to define some of the terms and concepts used in DoD documents and throughout this report. In the current lexicon, there is a significant emphasis on information, the inherent informational aspects of military power, and operations that are conducted primarily to generate effects in the IE.

---

[19] U.S. Joint Chiefs of Staff, 2018b, p. xi.

[20] JP 3-0, 2018, p. IV-2.

[21] U.S. Joint Chiefs of Staff, 2018b, p. 39.

Although many of these terms are defined in the *DoD Dictionary of Military and Associated Terms*, these definitions and related concepts are evolving. At the time of this research, JP 3-13, *Information Operations*, was being rewritten, and there was ongoing debate about the continued use of the term *IO*.[22]

Because words matter—and to minimize confusion and maximize clarity—Table 1.1 presents a list of commonly used terms and our reason for using, or for minimizing their use, throughout this report. With policy and doctrinal terminology and definitions in flux at the time of this writing, it is important to both acknowledge the official context for their use and highlight how this context differs in thought and practice in the communities that were the focus of this study.

Note that we try not to use *IRC* extensively in this report because it is quickly becoming a legacy term and engenders a stovepipe mentality. However, it is important to acknowledge the critical role of the functions it refers to. See Appendix A of this report for a list of IRCs, their varying definitions, and their inclusion or exclusion in selected key publications.

Table 1.1
Terms, Definitions, and Notes on Usage

Term	Definition	Source	Notes on Usage
Information environment (IE)	"Comprises and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The information environment also includes technical systems and their use of data. The information environment directly affects all OEs."	JP 3-0, 2018, p. IV-2	This report uses the standard definition of *IE*
Information operations (IO)	"The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."	JP 3-13, 2014, p. GL-3	When IO are viewed as "just a staff function," the concept does not reflect the complexities and breath of activities conducted in the IE. *IO* is likely to be replaced by *OIE*. In this report, we use *IO* sparingly and only to refer to the staff function in the sense of coordinating, integrating, or synchronizing capabilities and activities to leverage the informational aspects of military power.

[22] See U.S. Joint Chiefs of Staff, 2020, and JP 3-13, 2014.

Table 1.1—Continued

Term	Definition	Source	Notes on Usage
Information operations intelligence integration (IOII)	"The integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities, determine effects, and assess the information environment."	JP 3-13, 2014, p. GL-3	These activities were formerly referred to as *intelligence support to IO*, with the stated goal to provide analysis of the IE and improve understanding of the interrelationships of its physical, informational, and cognitive dimensions. The new term does not capture all relevant activities, and it is highly likely that it will change again when a new joint publication replaces JP 3-13. In this report, we use the current definition in JP 3-13 with the understanding that it will likely be replaced.
Information-related capability (IRC)	"A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions."	JP 3-13, 2014, p. GL-3	This term is currently up for debate as DoD explores what the establishment of information as a joint function means for joint warfighting. JP 3-0, updated in October 2018, is the most recent relevant doctrinal publication but does not use the term *IRC* at all.[a]
Operations in the information environment (OIE)	Not yet formally defined in doctrine. Somewhat ironically, the most recently published JCOIE does not concisely define the term and instead focuses on the objective—informational power—which it defines as follows: "The ability to leverage information to shape the perceptions, attitudes, and other elements that drive desired behaviors and the course of events. This includes the ability to use information to affect the observations, perceptions, decisions, and behaviors of relevant actors; ability to protect and ensure the observations, perceptions, decisions, and behaviors of the Joint Force; and the ability to acquire, process, distribute, and employ data (information). . . ."	JCOIE, 2018, p. 42 (*OIE* not explicitly defined)	The joint concept notes that informational power "helps commanders and staffs incorporate the concept of the *preeminent nature* of information into the design of all operations to maximize military power" (emphasis in original). This acknowledges the value of information to the range of U.S. military operations, including, presumably, OIE. In this report, we use *OIE* to refer to all operations and other activities in the IE.

SOURCES: JP 3-0, 2018; JP 3-13, 2014; U.S. Joint Chiefs of Staff, 2018b.

[a] The most recent version of JP 3-0 at the time of this writing used *capabilities that can create nonlethal effects* to describe some means that were traditionally IRCs: cyberattack, electronic attack, and military information support operations (MISO). The JCOIE, released in July 2018, used *IRC* twice, first as a tool for the commander and then, at the end, when discussing potential risks associated with the concept. Another term used in JP 3-0 is broader but also a mouthful: *joint force capabilities, operations, and activities for leveraging information*. It essentially covers all the traditional IRCs: key leader engagement, public affairs, civil-military operations, military deception (MILDEC), MISO, operational security (OPSEC), electronic warfare, combat camera, space operations, special technical operations (STO), cyber operations, and commander's communication synchronization. (See JP 3-0, 2018, p. III-36.)

Study Methods and Approach

The goal of this study was to help the joint force (specifically, the CCMDs) identify and refine the requirements, opportunities, and challenges associated with providing intelligence support for OIE so that they can better organize for, invest in, conduct, and support these operations. Accordingly, our study was guided by three sets of questions:

1. What data, information, analysis, and level of understanding are required to plan, integrate, and execute OIE?
2. Who could collect the needed information and conduct the required analyses, and through what processes? What are the barriers or challenges to doing so?
3. What terms are appropriate to describe what is collected and what is produced? Where is the boundary between routine information-gathering and formal intelligence collection? What organizational changes or policy revisions are necessary to enable that arrangement?

We answered these questions through a three-step process that consisted of a literature review, interviews with subject-matter experts, and an analysis of 40 challenges for CCMDs and joint force commanders to consider as they explore how information is provided in support of OIE and where improvements could be warranted and subsequently implemented.

The literature review was wide-ranging and included scholarly, policy, and doctrinal documents. We used a broad search methodology that initially identified 313 documents of interest. We grouped these documents into six initial categories:

- intelligence, data, and analytic requirements for IO
- indirect and implicit discussion of requirements in the broader IO literature
- lessons learned from IO after-action reports or lessons-learned compendia
- distinctions between intelligence and other forms of data collection and analysis
- examinations of existing intelligence products that address the IE
- procedures for and constraints on IO collection and analysis in statutes, authorities, and policies.

We coded the documents as "highly relevant," "relevant," or "not relevant." The initial pull of documents yielded 43 that we categorized as highly relevant. We analyzed these documents and used the results to identify a general list of topics for our interviews with subject-matter experts.

The goal of our interviews was twofold: We wanted to identify the challenges facing both intelligence personnel and IO practitioners, and we wanted to solicit their suggestions for responding to those challenges. We spoke with military personnel ranging from junior officers to general officers, along with civilians and contractor personnel. Most interviewees were GS-13s or GS-14s or held an equivalent military rank.

In total, we spoke with 62 personnel from 20 organizations. These organizations included those at the strategic level (Office of the Secretary of Defense, Defense Intelligence Agency [DIA], Joint Staff [JS]) and operational level (geographic CCMDs, service component commands), as well as institutional organizations (U.S. Army Training and Doctrine Command, Naval Information Warfighting Development Center) and force provider organizations (1st Information Operations Command, 151st Theater Information Operations Group).

Interviews were almost equally spilt between intelligence organizations (28 personnel) and IO organizations (33 personnel). These discussions provided us with a wealth of firsthand accounts and gave us valuable insight into how intelligence support for OIE is perceived across the joint force. We categorized insights from the interviews into six emerging themes: coordination and collaboration, division of labor, gaps in concept or doctrine, missing expertise, prioritization, and intelligence authorities.

Drawing on our literature review and interviews, we synthesized the challenges we identified, first combining and reducing them and then refining and matching them to solutions. Solutions emerged in four categories: improve processes, prioritize support, train and educate, and allocate personnel.

Overview of This Report

This report presents a detailed analysis of intelligence support for OIE and its attendant challenges and potential solutions. Chapter Two provides a brief history of OIE and describes recent changes to doctrine and policy. Chapter Three looks more closely at the six categories of challenges that we identified. Chapter Four presents solutions to the challenges discussed in Chapter Three, from both an intelligence and IO perspective. Chapter Five presents conclusions and recommendations from our analysis. The report also includes two appendixes providing background on key joint force IRCs and categories of information-related operations and activities (Appendix A) and a list of intelligence product categories reflecting the types of intelligence sources available to support OIE (Appendix B).

CHAPTER TWO

The Evolution of Operations in the Information Environment

The 2018 JCOIE and an out-of-cycle change to Publication 1, *Doctrine of the Armed Forces of the United States*, that established "information" as the seventh joint function demonstrated the Joint Staff's acknowledgement of an urgent need to update its doctrine. Technology diffusion has provided individuals and groups with an ability to access vast amounts of information that can be easily shared and acted upon by local and global audiences. This information can also be manipulated and distributed by state and nonstate actors more easily than ever. As such, the JCOIE concludes, "Information is changing the character of modern warfare."[1]

The JCOIE is not an outlier. There has been an explosion of interest and much productive thinking about information and its role in conflict in recent years.[2] The Joint Staff has produced a great deal of guidance related, both directly and indirectly, to information as a result. Part of this is a dramatic shift in how the defense establishment views conflict. These changes are only the beginning of a reframing of the interrelationship between information and intelligence and their roles in operations. At the time of this writing, the most recent military publications to address these topics included the following:

- *Joint Information Environment White Paper*, January 22, 2013[3]
- *Department of Defense Strategy for Operations in the Information Environment*, June 2016[4]
- JP 2-01, *Joint and National Intelligence Support to Military Operations*, July 5, 2017[5]

---

1 The quote is from the foreword by Vice Chairman of the Joint Chiefs of Staff Gen Paul J. Silva; U.S. Joint Chiefs of Staff, 2018b, p. iii.

2 Paul, Clarke, Triezenberg et al., 2018.

3 Martin E. Dempsey, Chairman of the Joint Chiefs of Staff, *Joint Information Environment White Paper*, Washington, D.C., January 22, 2013.

4 DoD, 2016.

5 JP 2-01, *Joint and National Intelligence Support to Military Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, July 5, 2017.

- *Joint Concept for Integrated Campaigning* (JCIC), March 16, 2018[6]
- *Joint Concept for Human Aspects of Military Operations (JC-HAMO)*, October 19, 2016[7]
- *Joint Concept for Operating in the Information Environment (JCOIE)*, July 25, 2018[8]
- JP 3-0, *Joint Operations* (updated to include "information" as a joint function), October 22, 2018.[9]

As evidenced by the recent publication dates, the joint force is still developing capabilities, undergoing reorganization, and testing concepts that will dramatically affect the future of OIE. Although there has been a great deal of innovation in this field, it is important to remember that these issues are not entirely new. U.S. IO and intelligence organizations have shared a close connection since both were officially recognized as important elements of national power. Their interconnectedness organizationally and in practice has strengthened and weakened throughout U.S. history. The following discussion clarifies the distinction between IO and intelligence organizations and explores the history and potential future of intelligence support for OIE.

IO and Intelligence: What's the Difference?

Military actions designed to affect the attitudes, decisionmaking, and behaviors of others are effectively timeless, but the ways and means by which the desired effects are achieved overlaps with—and may even directly compete with—intelligence activities. *Intelligence* is defined, in joint doctrine, as the products, activities, or organizations that execute the intelligence cycle of "collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations."[10] Many of these processes are also important to OIE, which aims to shape how enemy organizations perceive (or misperceive) changes made in the IE.

The recent surge in public interest in the IE can make it seem like OIE are a new aspect of warfare. However, both information efforts and intelligence have been a major part of the U.S. military operations for the duration of the nation's existence. Information is the essence of both communities; what distinguishes them is how each

---

6 U.S. Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, Washington, D.C., March 16, 2018a.

7 U.S. Department of Defense, *Joint Concept for Human Aspects of Military Operations (JC-HAMO)*, Washington, D.C., October 19, 2016.

8 U.S. Joint Chiefs of Staff, 2018b.

9 JP 3-0, 2018.

10 JP 3-0, 2018, p. GL-8.

compiles, sorts, analyzes, and uses information. Both have existed in a variety of constructs and under different names, and, perhaps to the chagrin of some who specialize in one or the other, they are indeed closely linked.

Going beyond doctrinal definitions, it is important to understand the desired outputs of these two functions. With intelligence, the bottom line is to enable the commander to make sense of the immensely complex OE so that he or she can make better decisions. By contrast, OIE are about devising ways to affect the OE through operations.

Both intelligence and OIE are intensely process-oriented. The development of intelligence is an analytical process that often results in some type of product; the term intelligence also describes the enterprise that executes the process. OIE are part of the operational planning process, which relies on the intelligence enterprise's characterization of the OE to achieve effects and thereby reshape the OE.

The Past: Intelligence and Psychological Warfare

The importance of information and its ability to affect adversary decisionmaking has long been recognized as a persistent characteristic of warfare. The integration of influence and intelligence in the U.S. military activities is also as old as the nation itself. Some of the first official U.S. intelligence operations included covert influence efforts during the American Revolution. For example, a 1776 campaign by the Continental Congress included establishing "a free press" in Canada to publish writings that attempted to persuade Canadians to join the American colonies in ousting the British and planting stories in a Dutch newspaper to influence that country's credit markets.[11] And General Washington directed multiple deception operations, often by using fabricated intelligence documents and procurement records that were allowed to be "captured" by the British.[12]

IOII, or what is increasingly characterized as intelligence support for OIE, has waxed and waned in importance due to changes in philosophical and organizational approaches. However, an emphasis on well-informed and coordinated information efforts as a permanent and significant fixture in military operations began taking shape early in World War II, despite a wide range of terminology being used to refer to what we now know as OIE.

In 1941, Colonel William B. Donovan observed Britain's system of "coordinating and combining intelligence, counterintelligence, psychological warfare and unortho-

[11] Central Intelligence Agency, Public Affairs, *Intelligence in the War of Independence*, Washington, D.C., last updated September 6, 2017.

[12] Central Intelligence Agency, 2017.

dox methods of sabotage, subversion, and guerrilla warfare."[13] On his recommendation, the U.S. government established the Office of the Coordinator of Information, which included a division for research and analysis, the Foreign Information Service, and sections for special intelligence and sabotage. The office was later split into two organizations; psychological warfare fell under the purview of the Office of War Information, and special operations were overseen by the Office of Strategic Services.

At the same time, the War Department stood up what would become the Psychological Warfare Branch as part of the intelligence structure. These early attempts to integrate intelligence, psychological warfare, and special operations at the national level caused friction, as military theater commanders were given the authority to determine the relationship between the Office of War Information and the Office of Strategic Services in their theaters.[14] Nonetheless these changes established the precedence and importance of integrating intelligence and psychological operations (PSYOP).

The need for effective international strategic influence was exacerbated during the Cold War as the United States sought to counter Soviet propaganda. The central role of intelligence in achieving that influence was underscored by the 1947 National Security Council Memorandum 4/4A, "Coordination of Foreign Information Measures," which tasked the Central Intelligence Agency (CIA) with covert psychological operations. Numerous IO-related committees, groups, and military units were developed and disbanded over multiple presidential administrations and achieved varying degrees of IOII. However, the CIA maintained a central role, along with the U.S. Department of State, DoD, and the U.S. Information Agency, through the end of the 20th century.[15]

The Recent Past and Present: IOII After 9/11

Discourse on IOII continued during the early stages of Operations Enduring Freedom and Iraqi Freedom, although it often emphasized requirements and deficiencies in the context of support to tactical counterterrorism and counterinsurgency operations. Commanders struggled, in some cases, because they insufficiently appreciated or even overlooked the IE as a critical part of the OE.[16] What commanders needed, whether they realized it or not, was a more holistic picture, developed through intelligence collection and analysis, that included such dimensions as sociocultural interactions,

---

[13] Susan L. Gough, *The Evolution of Strategic Influence*, Carlisle Barracks, Pa.: U.S. Army War College, April 2003, p. 3.

[14] Gough, 2003.

[15] Gough, 2003.

[16] Dennis M. Murphy, *Talking the Talk: Why Warfighters Don't Understand Information Operations*, Carlisle Barracks, Pa.: U.S. Army War College, Center for Strategic Leadership, Issue Paper 4-09, May 2009.

economic factors, and political perspectives, in addition to the more traditional enemy- and terrain-focused intelligence products.[17]

Another challenge identified early on was that successful operations in the IE required early and intense intelligence collection to support IO planning, particularly for PSYOP, computer network attacks, and MILDEC, which could require months of preparation.[18]

The intelligence community's (IC's) ability to support IO during this period was mixed. Generally, there was a concentration on the enemy at the expense of collecting and analyzing population-centric data to support IO. Intelligence sections often lacked an IO mindset. For example, one report on Operation Enduring Freedom found that useful intelligence was not being collected, analyzed, and disseminated, listing as examples

> census data and patrol debriefs; minutes from shuras with local leaders; after-action reports from civil affairs officers and Provincial Reconstruction Teams; polling data and atmospherics reports from psychological operations and female engagement teams; and translated summaries of radio broadcasts that influence local farmers, not to mention the field observations of Afghan soldiers, United Nations officials, and non-governmental organizations.[19]

There were some successes as well, such as Operation Al Fajr in Fallujah, Iraq, in late 2004. There, intelligence sections supported MILDEC (by diverting attention away from areas where U.S. forces were building up) and PSYOP (by drafting messages "encouraging insurgents to surrender and noncombatants to depart the city" prior to the assault).[20] Intelligence officials also identified a Fallujah hospital as a key node of enemy propaganda; the hospital was then prioritized as a target for an Iraqi commando raid that disrupted the enemy's ability to disseminate information early in the battle. Coalition forces conducted electronic attacks on insurgents' means of communication, forcing them to use channels that could be monitored and providing intelligence that would inform the conduct of the operation.[21]

---

[17] David Sloggett, "Intelligence Support to Contemporary Information Operations," *IO Sphere*, Spring 2007.

[18] Carrie Gray and Edwin Howard, "IO MOE Development and Collection: A Paradigm Shift," *IO Sphere*, Spring 2005.

[19] Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Washington, D.C.: Center for a New American Security, January 2010, p. 7. Also see Damian Spooner, *Improving MAGTF Intelligence Support to Information Operations in the Four Block War*, thesis, Quantico, Va.: Marine Corps Command and Staff College, 2010.

[20] Spooner, 2010, p. 7.

[21] Spooner, 2010.

Learning from Failure in the Capture of Fallujah

In contrast to Operation Al Fajr, the First Battle of Fallujah, known as Operation Vigilant Resolve, was marred by significant failures in U.S. strategic communication at both the strategic and operational levels. The April 2004 operation was a response to the ambush of Blackwater contractors whose bodies were burned and hung from a bridge that served as an entrance to the city. The fighting ended in a U.S. withdrawal from the city and subsequent defection of U.S.-trained Iraqi forces to the insurgents' cause.

The U.S. military learned from the experience and took those lessons into account in planning its second attempt to take the city. Perhaps the most visible example was the renaming of the operation from Phantom Fury to Al Fajr, Arabic for *dawn*. This demonstrated a better understanding of not just U.S. adversaries but also U.S. partners and the importance of empowering them. Another important change was that the commander of Multi-National Corps–Iraq established an "IO threshold" to "visualize a point at which enemy information based operations (aimed at international, regional, and local media coverage) began to undermine the Coalition forces' ability to conduct unconstrained combat operations."[a]

[a] Thomas F. Metz, Mark W. Garrett, James E. Hutton, and Timothy W. Bush, "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," *Military Review*, Vol. 86, No. 3, May–June 2006, p. 6.

The Future: Campaigning in the Information Environment

Historically, the preponderance of OIE have been tactical actions that support a larger operation, often with limited tactical-level objectives. However, the concept of a conflict continuum and a focus on campaigning point to a need for greater appreciation of influence capabilities at the strategic level. This does not mean that OIE will go away; in fact, quite the opposite is likely to be true. But it has become increasingly important that these operations directly support combatant commanders' objectives.

The JCOIE states that joint forces need to better "understand information, the informational aspects of military activities, and informational power" to "shape perceptions, attitudes, and other elements that drive desired behavior and the course of events."[22] The emphasis on *understanding* the environment is pervasive. Persistent intelligence and data collection and analysis are required to inform the integration of physical and informational activities. The JCOIE encourages the joint force to leverage multiple intelligence sources to understand how competitors and adversaries operate within the IE and to plan for and assess joint force informational activities.[23]

According to Title 10 of the U.S. Code, the primary duties of a CCMD include planning for contingencies, deterring conflict, and executing the missions assigned by

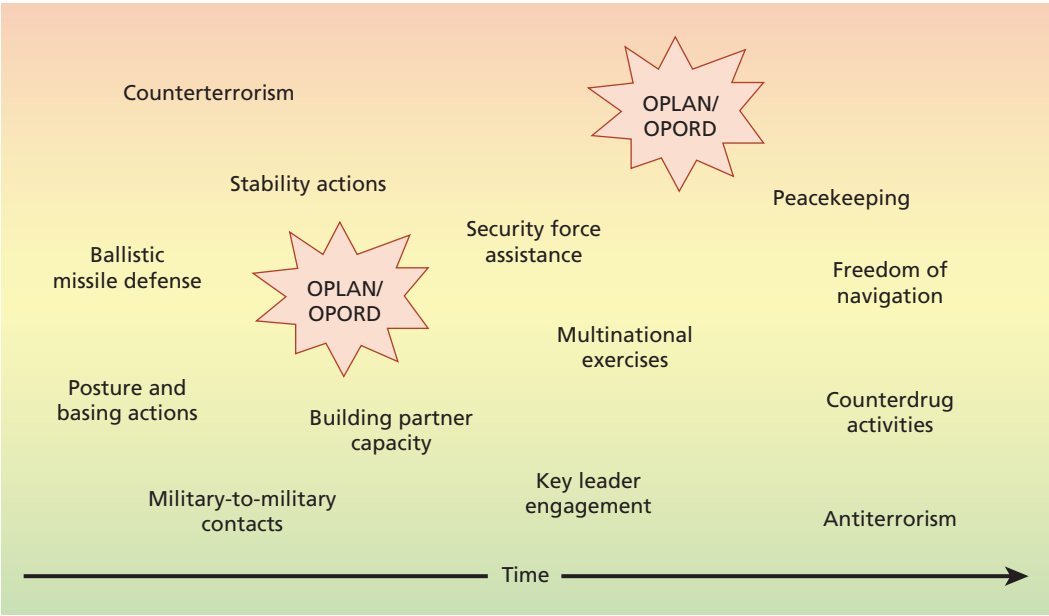
[22] U.S. Joint Chiefs of Staff, 2018b, p. viii.

[23] U.S. Joint Chiefs of Staff, 2018b.

the National Command Authority.[24] This means that the default goal of day-to-day operations is deterring conflict. Most (if not all) of a CCMD's activities contribute to keeping the peace, primarily through deterrence. Maintaining peace, and even deescalation in the event of conflict, is achieved through campaigns planned by CCMD staffs. For deterrence to succeed, the deterring party must be capable, credible, and able to communicate effectively.[25]

Figure 2.1, from JP 3-0, illustrates the myriad activities that a CCMD might undertake in pursuit of its stability-focused objectives. All the operations in the figure have an informational component, whether they contribute directly or indirectly to deterring an adversary. For example, security force assistance, building partner capacity, and military-to-military engagements are conducted with the intention of building the capability of U.S. and allied or partner forces, which can increase credibility and have a deterrent effect on adversaries. Leveraging both information and the inherent

Figure 2.1
Notional Joint Operations in a CCMD Campaign Context



SOURCE: JP 3-0, 2018, Figure V-5.

NOTE: The geographic combatant commander's theater campaign encompasses and provides context for all planned and ongoing theater activities, crisis response requirements, and combat operations. The goal is to preclude the need for a combat solution to problems while maintaining an acceptable level of stability. OPLAN = operation plan. OPORD = operational order.

[24] U.S. Code, Title 10, Section 164, Commanders of Combatant Commands: Assignment; Powers and Duties.

[25] JP 3-0, 2018, p. xxii.

informational aspects of other military activities to achieve behavioral effects (being deterred is clearly a behavior), this process can generally be considered part of OIE.

Unfortunately, OIE do not achieve their intended effects—at least not reliably—by accident. Operating in the IE involves a complex process that ties together seemingly disparate activities to achieve desired effects. OIE, while often tactical, are a significant part of campaigning. Campaigning is a whole-of-staff effort that involves planning and executing operations in the short term, as well as developing detailed contingency plans for a range of potential scenarios and future developments.

Both short-term operations and long-term planning require the aid of intelligence to succeed. An intelligence section's greatest contribution to a staff is its analytical capability. OIE planners and practitioners benefit from intelligence assistance in several ways: in understanding the IE, as discussed; in identifying and analyzing potential targets; and in conducting assessments to determine how effective OIE were in achieving their desired effects.

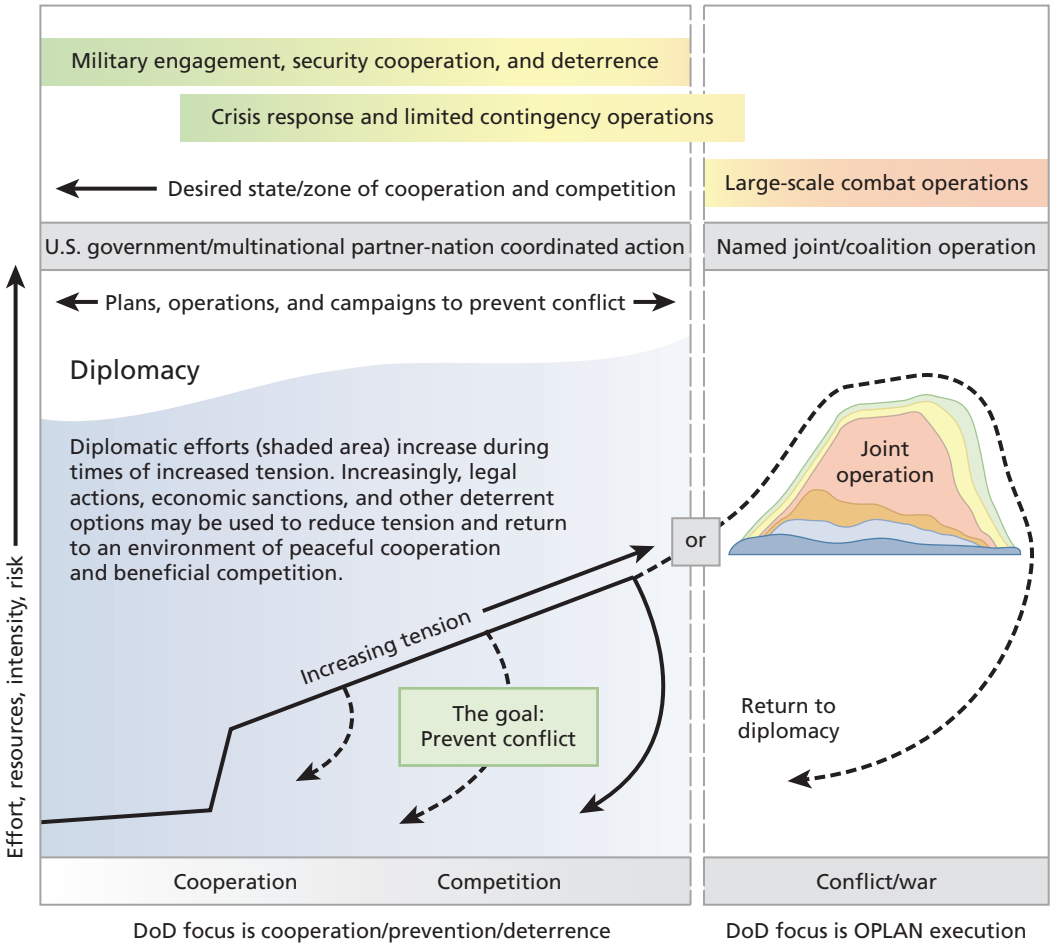
At the time of this writing, DoD was experiencing a paradigm shift in how it approached campaign planning. The key theme has been a shift away from a narrow focus on the conflict or a war-centric, linear phasing model that presumes sequential actions in discrete phases, as shown on the right-side of Figure 2.2. Instead, DoD is broadening its perspective, with the realization that the preponderance of time and effort is actually spent on cooperation, prevention, and deterrence, as shown on the left side of Figure 2.2. One of the key implications of this shift is an acknowledgement that CCMDs are not simply engaging in security cooperation while they simultaneously develop and update OPLANs for contingencies. Rather, they are perpetually campaigning and competing with potential adversaries in their area of responsibility.[26] At the tactical level, this does not change things much, other than potentially placing greater attention on operating in the IE.

Shaping and Dominating in the Short and Long Terms

The context presented in this report helps illustrate that, independent of the phase of a conflict, a CCMD must perpetually take short- and long-term actions simultaneously. If a CCMD's area of responsibility escalates toward conflict, it may have a small surge capacity, but that capacity will quickly be consumed by the demand to conduct operations and planning. Command leadership will need to redistribute its finite resources to address the challenges it is facing until it can obtain additional help (if such support is available). With intelligence capacity as one of the most finite resources, we found in our interviews that there is often dissonance between what type of intelligence support

[26] For more on this, see U.S. Joint Chiefs of Staff, 2018a.

Figure 2.2
The Conflict Continuum



SOURCE: U.S. Joint Chiefs of Staff, 2018b, p. 17, Figure 4.

IO personnel believe they should receive and what intelligence personnel believe they are providing.

Successfully conducting OIE requires different intelligence support at different points on the conflict continuum. The nature of this intelligence support depends on several factors and will change as an operation evolves. Whereas one type of support may be enough to enable shaping activities, it may be wholly inadequate for OIE as a conflict escalates. Regardless of the support required, it will not be easy to provide, and it will require dedicated effort.

Figure 2.3 explores how intelligence support might look at the CCMD level in support of OIE in the short term and planning or campaigning in the long term across

Figure 2.3
Short- and Long-Term Intelligence Support for Shaping and Dominating Activities

Tactical Actions	Short Term Shaping Activities
Examples	Web operations, monitoring indicators and warnings
Time horizon	0–6 months (JIOC support)
Resource investment	Increasing
Specificity	Narrow
IRC focus	PSYOP and strategic communication

Operational Actions	Short Term Dominating Activities
Example	Battle damage assessment
Time horizon	As quickly as possible (hours)
Resource investment	Unified focus; all contribute
Specificity	Most specific intelligence available: geographic, personality, temporal
IRC focus	Full-spectrum information warfare to targeting

Short term

Shaping activities

Dominating activities

Planning Actions	Long Term Shaping Activities
Examples	Foundational intelligence: intelligence mission data, target audience analysis
Time horizon	Months (not fast)
Resource investment	Sustained
Specificity	Broadest
IRC focus	MILDEC/OPSEC, PSYOP, electronic warfare

Campaigning Actions	Long Term Dominating Activities
Examples	Intelligence, surveillance, and reconnaissance degradation, leader OODA (observe, orient, decide, act) loop
Time horizon	"Normal" crisis battle rhythm
Resource investment	Unified focus; all contribute
Specificity	Broad
IRC focus	Full-spectrum information warfare to targeting

Long term

the categories of the Joint Combat Operational Model.[27] The figure shows the time horizon of each activity, analytical resources available, the level of specificity needed, and the chief IRC.

For example, the top left quadrant explores tactical actions, short-term activities executed during shaping activities. Ideally these actions are tied to achieving the

[27] JP 3-0, 2018, p. V-8.

campaign effects prescribed by the combatant commander. The IO/IRC activities are supported by the intelligence directorate's (J2's) joint intelligence operations center (JIOC), at least by design, but our interviews indicated that that there were challenges in receiving this support for a variety of reasons. Concurrent with these tactical actions are the long-term contingency planning efforts, mandated by law, that compete for the same intelligence resources: Intelligence personnel may be focusing on very different parts of the CCMD's vast areas of responsibility, or perhaps the analytical skill set required for these two functions is dramatically different. The top left quadrant reflects a need for sentiment analysis and quick-turn assessment whereas actions in the bottom left quadrant require a more methodical, long-term approach.

In the event of escalation up through dominating activities, for example, all timelines are accelerated, but the competition for finite intelligence resources endures. The top right quadrant is fully focused on targeting, traditionally with a bias toward achieving effects in the physical dimension. The intelligence personnel assigned to this problem rapidly cycle through building or updating target packages, conducting battle damage assessment, and repeating this process. Similarly, in the bottom right quadrant the focus is on full-spectrum information warfare, but, over the course of the campaign, it is important for actions to fit together in a more comprehensive manner rather than simply "servicing targets."

This chapter provided an overview of the evolving nature of information in the DoD lexicon, described the interplay between intelligence and information, and illustrated how OIE will likely play a role in future military operations across the conflict continuum. Next, we turn to the individual challenges that hinder effective intelligence support for OIE, detailing how both IO and intelligence organizations are responsible for the effective integration of intelligence processes.

CHAPTER THREE

Categorizing Challenges to Intelligence Support for Operations in the Information Environment

Planning and conducting OIE requires a great deal of information and analysis. The central inquiry of this report concerns roles and responsibilities for intelligence support for OIE and related challenges. We identified 52 challenges through our literature review, stakeholder interviews, and our own analysis (as described in Chapter One). We deliberately chose the term *challenges* as not all are gaps or shortcomings. They range in intensity and require various levels of effort to surmount or avoid. We synthesized, refined, and combined the initial 52 challenges into a condensed list of 40 unique challenges. We then grouped these 40 challenges into six categories (generated inductively based on possible groupings of the 40 challenges):

1. coordination and collaboration
2. division of labor
3. missing expertise
4. prioritization
5. gaps in concepts or doctrine
6. intelligence authorities.

The challenges were not mutually exclusive; some should be (and therefore were) included in multiple categories. After our analysis was complete, we assigned each challenge to a single overarching or "top" category to facilitate cross-referencing with solutions. However, to illustrate this overlap, in the discussion that follows, we indicate which challenges span multiple categories.

Coordination and Collaboration

The challenges in this category pertain to common interactions between the OIE and intelligence communities.[1] Many of the challenges in integrating these two commu-

[1] Note the distinction between the IO and intelligence communities and information and intelligence as warfighting or joint functions. Joint functions are integrated like any other maneuver warfare approaches. This cat-

nities stem from a lack of mutual understanding and underdeveloped or nonexistent relationships. Even with established doctrine, many of the processes that these two communities are supposed to rely on are immature or absent. There is a lack of understanding in both communities about what should be done, and standard operating procedures (SOPs) are often lacking. Where there are pockets of effectiveness, there is no institutional foundation to support them; rather, individual personalities often make the process work. The 14 coordination and collaboration challenges are listed in Table 3.1.

When individuals in one community do not understand the tasks and requirements of another, the greatest amount of friction will occur where their respective community practices or processes intersect. The processes by which intelligence is gathered, analyzed, and disseminated may be fully conducive to IO practitioners' needs, but IO practitioners might have little interaction with intelligence personnel. Likewise, available intelligence products could be directed toward supporting IO but remain sequestered by intelligence personnel who do not understand what IO practitioners would do with the knowledge.

Finally, combatant command J2 and J39 (IO) staff sections operate differently and are sourced by individuals with different backgrounds and experiences. This can result in variations in staff "cultures." Individual personalities can generally overcome these cultural differences in practice when a command is driven toward a common goal. However, these considerations are important to acknowledge when trying to improve coordination and collaboration within and across the two communities.

Under the broader category of coordination and collaboration, there are several types of challenges. In the following sections, we examine in greater detail the challenges that arise from a lack of shared understanding, processes, and community characteristics.

Common Understanding

Integrating the intelligence and IO communities requires a common understanding of fundamental elements of each community and their functions. To support IO, intelligence personnel must be familiar with the types of information that are relevant to the physical, informational, and cognitive dimensions of the IE. Conversely, IO practitioners must be familiar with intelligence resources and processes for how that information is collected, analyzed, and disseminated.[2] Both must also understand how to access that information and how to request assistance when needed through an RFI.[3]

---

egory of challenges focuses instead on the interactions among the people, processes, and resources that constitute each respective community. Testing and development should continue to seek better ways to integrate the intelligence function with the newly designated information function.

[2] JP 2-01, 2017.

[3] We discuss RFIs at greater length in the context of prioritization challenges, later in this chapter.

Table 3.1
Challenges Associated with Coordination and Collaboration

Coordination and Collaboration	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concepts or Doctrine	Intelligence Authorities
Lexicon/terminology does not align between IO and intelligence.	X					
Coordination between J2 (intelligence directorate) and J39 (IO directorate) is hampered by not being collocated.	X					
Cultural and perceptual differences between J2 and J39 impede close coordination.	X					
Coordination between J2 and J39 is hampered by not having shared understanding or SOPs to support their interaction.	X					
Not all intelligence related to OIE and the IE is shared with appropriate staff sections within the command.	X					
Pockets of effectiveness are not institutionalized and are mostly the result of individual personalities.	X					
IO analysis of the IE does not meet intelligence professionals' standards for analytic tradecraft.	X	X	X			X
Not enough personnel to undertake activities that require IO expertise. Too many meetings, events, operations, activities for the current force structure to accommodate.	X	X				
Lack of understanding of a common operational picture (COP), staff procedures, and SOPs to produce and share a COP of the IE.	X		X		X	
There are no intelligence information reports (finished intelligence) specific to OIE foreign military intelligence collection activities, hindering the ability to search intelligence products.	X				X	
IO reachback organizations provide IE-related materials that are useful for IO and OIE, but they do not produce finished intelligence products. Thus, these materials are not indexed in intelligence systems and cannot be found through intelligence channels or inquiries.	X	X		X	X	
Targeting working groups and targeting doctrine do not adequately consider nonlethal effects. OIE are typically categorized as nonlethal, so intelligence support for targeting does not include the IE, reinforcing the exclusion of OIE.	X	X		X	X	
Some critical IO requests for information (RFIs) would require unique analysis and production methods at the tactical level.	X	X	X	X		
Some IO priority intelligence requirements (PIRs) would require unique intelligence collection methods at the tactical level.	X	X	X	X		

NOTE: Top challenges appear in bold.

Both the literature review and interviews with intelligence and IO practitioners indicated that intelligence personnel lacked understanding of the information function, and IO personnel lacked understanding of the intelligence function.

That said, in practice, there are plenty of overlapping concepts and goals between the two groups. Intelligence personnel have been collecting, analyzing, and reporting on human, cultural, and infrastructure aspects of the OE for decades. However, these activities have mostly supported operational staffs and commanders who are making planning and operational decisions regarding maneuver, fires, and how to engage with civilian populations. Much of the same information would be valuable to J39 staffs during their planning, operations, and assessments as well. The two communities have their own lexicons and ways of describing things, and the terms related to IO are often misunderstood in the rest of the force.[4]

Processes

In addition to a common understanding of what each community does and how it uses various terms, coordination and collaboration between intelligence and IO professionals is often challenged by a lack of shared processes. As stated, intelligence staffs collect, analyze, and report on much of the information that IO practitioners seek and from which they would benefit. In addition to incongruent terminology making this disconnect less obvious, finished intelligence products may never reach the J39 staff section, IO cell, or other IO practitioners due to gaps between respective IO and intelligence processes. Each community should have a rudimentary understanding of the other's most common activities and then seek to understand its respective command's activities in detail.

Effective intelligence support for OIE does not require changes to the fundamental purpose or processes of intelligence collection, analysis, and reporting. Commanders already require accurate and timely intelligence to support decisionmaking and provide reasoned insight into future conditions or situations.[5] As Army doctrine defines it, "The intelligence warfighting function is the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment."[6] Of course, knowledge of the enemy and surrounding environment can only reduce uncertainty to a reasonable level, as absolute certainty on any battlefield will remain impossible. However, the ultimate purpose remains to provide relevant knowledge to support decisionmaking.[7]

---

[4] See, for example, Christopher Paul, "Is It Time to Abandon the Term Information Operations?" *Strategy Bridge*, March 11, 2019.

[5] JP 2-01, 2017; JP 2-0, 2013.

[6] Army Doctrine Publication 2-0, *Intelligence*, Washington, D.C., July 31, 2019, p. 2-2.

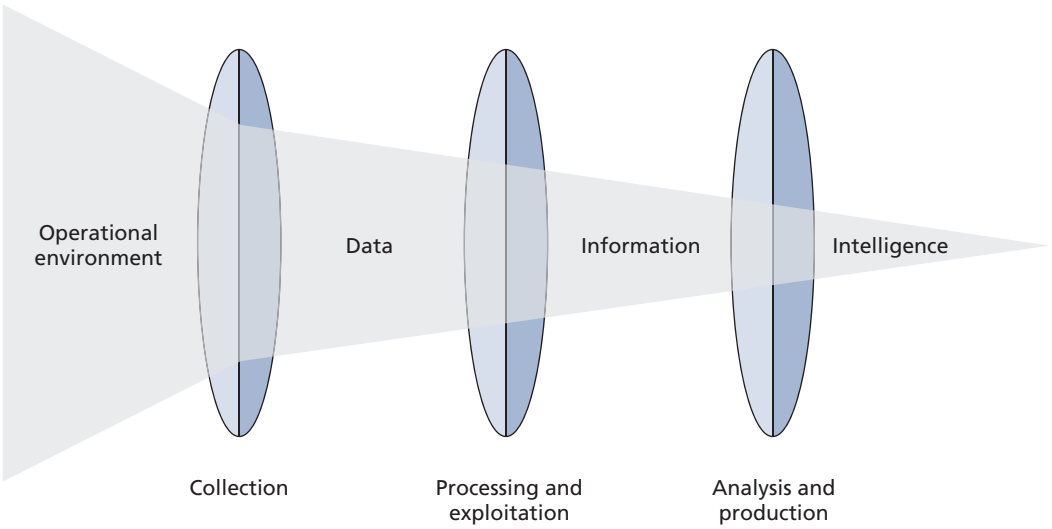
[7] For the Marine Corps version of the Army doctrine publication, see Marine Corps Doctrinal Publication 2, *Intelligence*, Washington, D.C., incorporating change 1, April 4, 2018.

The integration of intelligence into military operations is an inherent responsibility of commanders at every echelon and across the range of military operations.[8] There are a variety of methods to collect raw input from the OE. Collected data are then processed and exploited to develop usable information. After that, the information is analyzed and, finally, packaged as intelligence products. Figure 3.1 illustrates this process.

However, IO personnel must also understand the process by which intelligence products are developed if they are to know when and how to best integrate the intelligence function. The processes by which intelligence personnel develop relevant intelligence from the OE consists of the following six steps, as shown in Figure 3.2:

- planning and direction
- collection
- processing and exploitation
- analysis and production
- dissemination and integration
- evaluation and feedback.

Figure 3.1
Relationship Among Data, Information, and Intelligence



SOURCE: JP 2-0, 2013, p. I-2, Figure I-1.

[8] JP 2-0, 2013.

Figure 3.2
The Intelligence Process

SOURCE: JP 2-0, 2013, p. I-6, Figure I-3.

Although they are described as a process, the steps are not always taken sequentially. At times, activities are conducted simultaneously or bypassed altogether, as JP 2-0, *Joint Intelligence*, explains:

> For example, a request for imagery requires planning and direction activities but may not involve new collection, processing, or exploitation. In this case, the imagery request could go directly to a production facility where previously collected and exploited imagery is reviewed to determine if it will satisfy the request. Likewise, during processing and exploitation, relevant information may be disseminated directly to the user without first undergoing detailed all-source analysis and intelligence production. Significant unanalyzed operational information and critical intelligence should be simultaneously available to both the commander (for time-sensitive decision-making) and to the all source intelligence analyst (for the production and dissemination of intelligence assessments and estimates).[9]

In addition to IO personnel being familiar with intelligence processes, successful support for OIE requires that intelligence personnel develop an appreciation for the knowledge that IO practitioners require and how it is employed. OIE attempt to influence the decisionmaking of relevant actors, such as adversaries or noncombatant

[9] JP 2-0, 2013, p. I-5.

populations in areas where adversaries are operating. So, it is important to understand those actors, how they interact within the IE, and how they make decisions. As the JC-HAMO states, a critical and enduring challenge in warfare is the "need to understand relevant actors' motivations and the underpinnings of their *will*."[10]

JC-HAMO recognizes four imperatives in affecting the will and decisionmaking of relevant actors (the first three of which indicate a clear role for intelligence support):

- *Identify* the range of relevant actors and their associated social, cultural, political, economic, and organizational networks.
- *Evaluate* relevant actor behavior in context.
- *Anticipate* relevant actor decision making.
- *Influence* the will and decisions of relevant actors.[11]

With those general imperatives in mind, intelligence and IO personnel require a more detailed common understanding of how to categorize the IE. This is readily apparent in how OIE are used to influence a relevant actor's decisionmaking and subsequent behavior. IO personnel must consider relevant actors, and how they might be influenced, to achieve the desired effects. The process of doing so is less formalized than the intelligence operations process described earlier. However, key steps in planning, execution, and assessment have clear requirements for intelligence support.

The first step is to identify and understand the relevant actor to be influenced, including how the relevant actor perceives and interacts with the IE. This includes how the relevant actor collects, processes, perceives, disseminates, and acts on information. Next, IO practitioners evaluate various means of interacting with the IE. These means can be diplomatic, informational, military, or economic, and they can involve governmental, academic, cultural, and private institutions. Once a mean or combination of means are identified, IO practitioners determine which IRCs, including capabilities, techniques, or activities, should be employed and then continuously assess, monitor, and evaluate the operation.[12] These steps have clear implications for intelligence support.

Community Characteristics to Consider

The importance of relationships between IO practitioners and intelligence personnel is emphasized in doctrine but lacking in practice. These relationships must be established early and include continuous interaction. Part of cultivating such relationships is mutual awareness of the characteristics of each community, including an understanding of organizational and leadership structures, roles in the planning process, the long

[10] U.S. Joint Chiefs of Staff, 2016, p. i. Emphasis in the original.

[11] U.S. Joint Chiefs of Staff, 2016, p. 2.

[12] JP 3-13, 2014.

lead times required to support IO, and practical requirements for the intelligence staff to satisfy IO needs.

Most CCMDs have a staff to conduct IO planning and manage the integration of operations, activities, and capabilities to achieve effects in the IE. Joint force commanders may also establish an IO cell that brings together cross-functional expertise and encourages coordination. In addition to OIE specialists, these staffs and cells may include, or be closely tied to, intelligence support personnel. IO cell chiefs are responsible for coordinating the planning and execution of IRC capabilities and any requested intelligence support.[13] IO staffs and IO cells are likely to remain a central component of IOII.

It is critical for intelligence personnel to understand how—and from where—information requirements are likely to originate. A joint intelligence support element may establish an IO support office to assess affects in the IE, producing intelligence products to support IO, and aiding with collection management tasks.[14] This may represent the "supply" side of the supply-and-demand dynamics for intelligence support to IO in many commands.

IO planners are part of the Joint Operations Planning Process, like all other staff planners. IRCs are an important component of every phase of operations, but they often require long lead times for proper planning.[15] IO practitioners must not rely solely on information from the IRCs, which can provide only some of the information that they require. IO personnel are responsible for providing a holistic understanding of the IE, a prerequisite for effectively influencing decisionmaking. This highlights the importance of early planning and cross-functional coordination, including between IO planners and J5 (strategy, plans, and policy) and J25 (intelligence operations, plans, and policy) personnel.

The IO staff/cell must take a proactive approach to intelligence support and consider the long lead times required to support JIPOE, in addition to authorities associated with IRCs. IO practitioners are responsible for identifying and communicating intelligence gaps that impede their understanding of the IE.[16] Effective intelligence support for OIE requires active engagement from both sides of the supporting-supported relationship. Improving intelligence support to IO is not synonymous with abdicating the role of initiative within IO staffs/cells.

To provide effective intelligence, the intelligence staff must have adequate communication and network-enabled capabilities. Commanders and staffs must ensure that communication support and resources are allocated to appropriate intelligence

[13] JP 3-13, 2014.

[14] JP 3-13, 2014.

[15] JP 3-13, 2014.

[16] JP 3-13, 2014.

staffs.[17] Demand for the attention of intelligence personnel is well acknowledged across the joint force, particularly for personnel with highly specialized capabilities. But the intelligence function also relies on established infrastructure, communication, preapproved access to classified information and computer systems, and other services to achieve the coordination and collaboration necessary to support OIE.

This discussion of intelligence and IO processes highlighted the importance of integration in the abstract. However, without dedicated resources and strong leadership support for integration at the system and user levels, coordination and collaboration will not occur in practice.

Division of Labor

The challenges in this category focus on tensions over who should be responsible for what tasks. Key challenges span differences of opinion regarding responsibility for staffing decisions, information fusion, and expectations of analytic rigor. All 22 tasks in this category are listed in Table 3.2.

Staffing Gaps

Before addressing division of labor, it is important to address labor capacity. At the CCMDs, there are myriad boards, bureaus, centers, cells, and working groups that demand the involvement of IO practitioners, and there are not enough military or civilian personnel to routinely participate in all of them. Although virtually all CCMD J39s have a contracted workforce, these personnel are not allowed to perform inherently governmental functions or officially represent the government at any of these meetings. J39s are forced to use interim sourcing solutions to satisfy a demand that has grown rapidly without commensurate enduring manpower growth. We heard in our interviews that staff augmentation, in a surge situation, goes disproportionally to intelligence rather than IO. This staffing gap presents an enduring deficit in steady-state conditions that can be greatly exacerbated in the event of a crisis or contingency.

Analytic Rigor

The IC produces multiple products to answer commanders' PIRs, although many of these products do not sufficiently address the IE. Where products are produced by IO personnel, they either do not adhere to IC Directive 203 standards of analytic tradecraft, or, when they do, they are not widely disseminated.[18] Additionally, there is a

[17] Army Doctrine Publication 2-0, 2018.

[18] Intelligence Community Directive 203, *Analytic Standards*, Washington, D.C.: Office of the Director of National Intelligence, January 2, 2015.

Table 3.2
Challenges Associated with Division of Labor

Division of Labor	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concepts or Doctrine	Intelligence Authorities
Web operations are not an intelligence activity but involve monitoring and engaging in real time on social media. (They are also not Title 50 covert operations, which would require additional intelligence oversight.)		X			X	X
IO analysis of the IE does not meet intelligence professionals' standards for analytic tradecraft.	X	X	X			X
There is a limited ability to compile data across intelligence-gathering disciplines to produce an integrated and credible product to inform leadership decisions (for example, to conduct integrated social media monitoring, compile publicly available information, and establish a robust IE COP).		X	X	X		
J39 uses interim sourcing solutions to acquire additional manpower and expertise.		X	X			
Not enough personnel undertake activities that require IO expertise. Too many meetings, events, and operations for the current force structure to accommodate.	X	X				
Intelligence does not produce adequate products focused directly on the IE, so the default is to use existing intelligence products that may have some IE-related data but were not created specifically to answer IO RFIs.		X	X	X		
The processes described in doctrine for JIPOE actually includes quite a bit of good IE-related material; however, JIPOE as practiced does not include very much (if anything) about the IE.		X	X	X		
Intel analysts at the service component commands need to provide more analysis of the IE and should use the most recent doctrine to update baseline analyses (a process similar to intelligence preparation of the battlefield).		X	X		X	
There is no organization dedicated to or responsible for providing IE-related training to intelligence analysts.		X				
IE-related estimates and assessments from J2 have much more credibility with commanders and staffs than similar products produced by J39.		X				
IO reachback organizations provide IE-related materials that are useful for IO and OIE, but they do not produce finished intelligence products. Thus, these materials are not indexed in intelligence systems and cannot be found through intelligence channels or inquiries.	X	X			X	X
Targeting working groups and targeting doctrine do not adequately consider nonlethal effects. OIE are typically categorized as nonlethal, so intelligence support for targeting does not include the IE, reinforcing the exclusion of OIE.	X	X		X	X	

Table 3.2—Continued

Division of Labor	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concepts or Doctrine	Intelligence Authorities
IO RFIs are difficult to service and require high level of effort to sufficiently address.		X	X			
Effective training material and courses are not available for IOII.		X	X	X		
IOII is not included in professional military education.		X	X			
J2 does not contribute estimates of the IE or help assess OIE.		X		X		
OIE can be very challenging to measure/assess; some of these effects might be observable though national technical means of verification, but such support is lacking.		X		X		
Some critical IO RFIs would require unique analysis and production methods at the tactical level.	X	X	X	X		
Some IO PIRs would require unique intelligence collection methods at the tactical level.	X	X	X	X		
Responses to intelligence requests (via the Community On-Line Intelligence System for End Users and Managers [COLISEUM] and the Open Source Collection Acquisition Requirement Management System [OSCAR-MS] are slow.		X	X	X		
OIE is not considered in J2 red-teaming for the command.		X	X	X		
Increased steady-state demands equate to increased J2 support but not increased IO support.		X		X		

NOTE: Top challenges appear in bold.

limited ability to compile intelligence across multiple disciplines to create products that are credible and useful to senior leadership.

Intelligence Product Focus

Products generated by the intelligence enterprise are designed to satisfy traditional intelligence questions for consumers who have a traditional perspective on what those products should look like. We found that these products do not sufficiently consider the IE, at least in the eyes of those who focus on the IE. However, we also heard about "pockets of effectiveness." One particularly noteworthy example is U.S. European Command (USEUCOM). USEUCOM's J39, J2, public affairs office, and other staffs collaborate to generate products that describe the IE for senior leadership. They

have built a credible brand and, in the process, have helped educate leaders on what to look for as consumers of IE products. It took them a long time to get there, but this case provides a lesson in overcoming staff divisions.

Leadership preference for intelligence products was another challenge that emerged in our interviews and is presumably a function of individual proclivities and what commanders are familiar and comfortable with. Accounts from USEUCOM personnel clearly indicate that this is a surmountable hurdle.

Creating a Comprehensive IE Common Operational Picture

Ideally, the outcome of good staff collaboration would be a comprehensive COP that accurately portrays relevant aspects of the IE. This is not currently the case. There are several reasons for this, not all of which are attributable to divisions of labor.

Generally, intelligence personnel support the intelligence cycle, with a focus on conducting analysis. They generally work on a slower timeline that facilitates the nature of their deliberate work. IO practitioners do some of this as well, with a focus on analyzing the IE—everything from the use of the electromagnetic spectrum to relevant actor behaviors. Unfortunately, the analysis by both parties is not yet fused into a comprehensive IE COP. This is not just an issue at the CCMD level; a comprehensive IE COP would be almost wholly dependent on inputs from the service components and their assigned forces, who are the real eyes and ears of a CCMD.[19]

Using JIPOE to Explore the Information Environment

JP 2-01.3, *Joint Intelligence Preparation of the Operating Environment*, states that irregular warfare seeks to "erode an adversary's power, influence, and will" by controlling, influencing, or gaining the support of a relevant population "through political, psychological, and economic methods."[20] As such, intelligence personnel who develop the JIPOE must convey a detailed understanding of "the impact of ethnic groups and religions, to include their associated leadership, the locations of places of worship and cultural/historical significance, languages being spoken, population density, age, living conditions, allocation of wealth, and means of income."[21] Furthermore, JIPOE products must assess an area's cultural landscape by describing how "key social and political factors revolve around understanding previous political systems, parties, formal and informal leaders, affiliations, political grievances, loyalty to former local, regional,

[19] Paul, Clarke, Triezenberg et al., 2018.

[20] JP 2-01.3, *Joint Intelligence Preparation of the Operating Environment*, Washington, D.C.: U.S. Joint Chiefs of Staff, May 21, 2014, pp. VII-1–VII-2. Note that JP 2-01.3 was undergoing revisions when this report was in production.

[21] JP 2-01.3, 2014, p. VII-2.

and national government officials, patterns of political tolerance or violence, and the education system."[22]

Intelligence support to IO planning is often described in terms of common but flexible planning tools and products. Many of the suggested products represent an extension of widely familiar analyses of the OE, including mission, enemy, troops available, terrain, time, and civilian considerations (better known as METT-TC); political, military, economic, social, infrastructure, information, physical environment, and time (PMESII-PT); and area, structures, capabilities, organizations, people, and events (ASCOPE). Additional products could include closer analyses of friendly and enemy IO capabilities, vulnerabilities, opportunities, and threats, along with their potential effects on the IE and OE. Furthermore, target audience goals, psychological mindsets, and motivations represent a focus on the cognitive dimension of the IE and are examples of required intelligence products.

Missing Expertise

The challenges in this category concern gaps in the skills and knowledge necessary to complete tasks related to intelligence support for OIE. Most of these challenges are a result of gaps in training and education among relevant personnel. Just as policy and doctrine are continually adjusted and updated, training and education must evolve as needs change if the joint force is to effectively engage in the IE. This is not to say that there are no courses available; rather, the courses that do exist provide limited instruction. All 21 tasks in this category are listed in Table 3.3.

Analyst Training and Education

The service schoolhouses, DIA, the Joint Force Staff College, and other organizations and commands do have some courses that focus on OIE or the IE—for example, the Information Environment Advanced Analysis course. This is the most advanced course available that teaches IOII to both IO and intelligence practitioners. Course attendance is voluntary, and attendees do not receive an additional skill identifier or other designation showing that they have attended the course. This means that future billet assignments for graduates of the course will not consider the OIE-specific skills acquired. Yet, it is just one course and will not, by itself, educate the joint force.

Indeed, both intelligence and IO professionals need training to effectively support and conduct OIE, and there is no comprehensive approach to addressing these shortfalls across both communities. Courses are not part of professional military education, nor are they offered to any great extent though elective courses. For both military and civilian occupations, in both communities, the dearth of curricula focusing

[22] JP 2-01.3, 2014, p. VII-2.

Table 3.3
Challenges Associated with Missing Expertise

Missing Expertise	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concept or Doctrine	Intelligence Authorities
Open-source intelligence (OSINT), collected by intelligence professionals, can make an important contribution to situational understanding of the IE.			X		X	
Intelligence staffs/cells do not have the required expertise to analyze the IE.			X			
IO professionals are unable to adequately articulate IO PIRs.			X			
IO RFIs are difficult to service and require a high level of effort to sufficiently address.		X	X			
J39 personnel do not have targeting process experience or training like J2 targeteers.			X			
Tools and systems to collect, monitor, and analyze the IE are lacking.			X			
Effective training material and courses are not available for IOII.		X	X	X		
Senior leaders lack awareness and knowledge of OIE.			X	X		
IOII not included in professional military education.		X	X			
IO analysis of the IE does not meet intelligence professionals' standards for analytic tradecraft.	X	X	X			X
There is a limited ability to compile data across intelligence-gathering disciplines to produce an integrated and credible product to inform leadership decisions (for example, to conduct integrated social media monitoring, compile publicly available information, and establish a robust IE COP).		X	X	X		
J39 uses interim sourcing solutions to acquire additional manpower and expertise.		X	X			
Intelligence does not produce adequate products focused directly on the IE, so the default is to use existing intelligence products that may have some IE-related data but were not created specifically to answer IO RFIs.		X	X	X		
The processes described in doctrine for JIPOE actually include good IE-related material; however, JIPOE as practiced does not include very much (if anything) about the IE.		X	X	X		
Intelligence analysts at the service component commands need to provide more analysis of the IE and should use the most recent doctrine to update baseline analyses (a process similar to intelligence preparation of the battlefield).		X	X		X	
Lack of understanding of a COP, staff procedures, and SOPs to produce and share a COP of the IE.	X		X		X	

Table 3.3—Continued

Missing Expertise	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concept or Doctrine	Intelligence Authorities
IO-related requirements lack visibility and are not captured in a consolidated list.			X	X		
Some critical IO RFIs would require unique analysis and production methods at the tactical level.	X	X	X	X		
Some IO PIRs would require unique intelligence collection methods at the tactical level.	X	X	X	X		
Responses to intelligence requests (via COLISEUM and OSCAR-MS) are slow.		X	X	X		
OIE is not considered in J2 red-teaming for the command.		X	X	X		

NOTE: Top challenges appear in bold.

on IOII is a great impediment. These deficiencies are apparent at the highest levels of DoD, as reflected in guidance published by the Chairman of the Joint Chiefs of Staff instructing the joint force to prioritize efforts to train for OIE.[23] However, many aspects of IOII need to be examined for the joint force to see improvements in the basic understanding of OIE.

OSINT is one area in which intelligence personnel should focus efforts to improve OIE. They need this training to expand their ability to gather and analyze publicly available information. However, IO practitioners are not trained in the intelligence cycle, leading to problems with RFI or intelligence request process. IO practitioners need training on the targeting process and the philosophy that underpins it. Leadership, often not well trained or versed in OIE, is not asking the right questions of their staff sections or fully incorporating OIE into plans and assessments.

The IE is becoming more complex and difficult to understand. Increasing volumes and rates of data on the IE, the ability of state and nonstate actors to adapt to data collection and actions in the IE, and the proliferation of more data and noise continue to cloud understanding the environment. This trend is likely to continue, so stakeholders will increasingly depend on both IO and intelligence personnel to help

[23] Chairman of the Joint Chiefs of Staff Notice 3500.01, *2017–2020 Chairman's Joint Training Guidance*, Washington, D.C., January 12, 2017.

them understand the IE, visualize operations, make decisions, and improve mission command.[24]

Intelligence Organizations and Programs of Analysis

To further explain why intelligence professionals are not versed in OIE, it is important to look at the organizations from which intelligence professionals are drawn. The IC is a robust federation of 16 intelligence organizations and has the capabilities and expertise to provide analytic support to U.S forces operating in the IE. DoD agencies and military service staffs account for eight of the 17 elements of the IC.[25] However, there are relatively few qualified personnel and fewer products in the defense intelligence enterprise addressing the IE. Rather, these organizations are responsible for producing foundational intelligence for the joint force to enhance the understanding and baseline knowledge needed for plans and operations. The world is complex, and the defense intelligence enterprise cannot focus on all problems at once. Therefore, these organizations have to prioritize efforts.

The Defense Intelligence Analysis Program (DIAP) outlines the analysis and production responsibilities for the elements of the defense intelligence enterprise, including DIA, the command joint intelligence operation centers, and the service intelligence centers. The DIAP is a knowledge-based construct, as opposed to a customer-based one. It comprises intelligence functional codes that task organizations to provide intelligence on a given subject or problem set for a diverse customer base. For example, the National Ground Intelligence Center is responsible for fulfilling requests for intelligence on Russian ground forces for any customer across the U.S. government. This federated approach to intelligence analysis and production allows for specialization; it allows organizations to build up a large body of expertise on a given topic. For many problems, this approach works and makes sense.

However, the DIAP does not contain an intelligence functional code for support to IO. Therefore, no single element is responsible for providing this type of support. This is a major reason that relatively little emphasis is placed on support operations in the IE from an intelligence perspective.

At the same time, there is a lack of expertise in the IC to support requests that focus on the IE. This starts with a general lack of understanding of basic terminology, such as *IO*, *OIE*, and associated functions, capabilities, and activities that leverage information. This extends to the intelligence personnel who are supposed to be providing this support.

---

[24] Paul, Clarke, Triezenberg et al., 2018.

[25] Office of the Director of National Intelligence, *United States Defense Intelligence Strategy*, Washington, D.C., 2019, p. 28.

Organizations That Support and Operate in the Information Environment

There are a variety of organizations involved in the IE outside of the geographic CCMDs or their subordinate components. These organizations may appear, in name, to fall soundly into either the IO or intelligence category, but they actually provide excellent case studies in how, at the individual and organizational levels, intelligence and IO professionals have endeavored to mature the working relationships among their functional areas in the interest of the mission. There are essentially two types of organizations that support IO: reachback or support organizations and operational headquarters, which provide a range of support to deploying units.

The support organizations have a longer history than their operational counterparts. They provide, at a minimum, a repository of what has and has not been tried in their fields, including efforts to improve intelligence support for OIE. It is noteworthy that organizations of both types have been standing up and evolving rapidly in the past decade. The recent establishment of information as a joint function and its cascading effects within DoD will ensure the continued evolution of these organizations. Finally, what is conspicuously absent is a federal government entity, above DoD, to fulfill (at a minimum) a strategic communication function. Under the current arrangement, guidance on national objectives and strategic narratives is distributed across a variety of entities, something that is particularly problematic when "information" is one of the four instruments of national power. Key stakeholders include the National Security Council, the U.S. Department of State's Global Engagement Center, and the U.S. Agency for Global Media (formerly the Broadcasting Board of Governors). However, there is no longer an organization like the U.S. Information Agency to serve as the cross-governmental coordinator.[26]

Prioritization

We identified ten challenges in the prioritization category. This category includes challenges stemming from failures to sufficiently prioritize OIE within a command or other organization. Requirements related to these challenges could be met but are not because scarce resources are devoted to perceived or actual higher priorities. These challenges were highlighted in our discussions with subject-matter experts about the RFI process, the value of IO assessments, and the need to balance limited resources in a given command. All 16 tasks in this category are listed in Table 3.4.

---

[26] Shuttered in 1999, the U.S. Information Agency was not a panacea for this very complex problem. The agency's mission was to

> Promote the national interest and national security of the United States through understanding, informing and influencing foreign publics and broadening dialogue between American citizens and institutions and their counterparts abroad. (U.S. Information Agency, *Strategic Plan 1997–2002*, 1997)

Table 3.4
Challenges Associated with Prioritization

Prioritization	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concepts or Doctrine	Intelligence Authorities
J2 does not contribute estimates of the IE or help assess OIE.		X		X		
OIE can be very challenging to measure/assess; some of these effects might be observable though national technical means of verification, but such support is lacking.		X		X		
J2 does not provide baseline estimates of the IE in support of OIE and does not have dedicated collection and analysis resources to support OIE assessment.				X		
IO RFIs are a low priority; none are PIRs/commander's critical information requirements.				X		
IO-related requirements lack visibility and are not captured in a consolidated list.			X	X		
Some critical IO RFIs would require unique analysis and production methods at the tactical level.	X	X	X	X		
Some IO PIRs would require unique intelligence collection methods at the tactical level.	X	X	X	X		
Responses to intelligence requests are slow (via COLISEUM and OSCAR-MS).		X	X	X		
OIE is not considered in J2 red-teaming for the command.		X	X	X		
Increased steady-state demands equate to increased J2 support but not increased IO support.		X		X		
There is a limited ability to compile data across intelligence-gathering disciplines to produce an integrated and credible product to inform leadership decisions (for example, to conduct integrated social media monitoring, compile publicly available information, and establish a robust IE COP).		X	X	X		
Intelligence does not produce adequate products focused directly on the IE, so the default is to use existing intelligence products that may have some IE-related data but were not created specifically to answer IO RFIs.		X	X	X		
The processes described in doctrine for JIPOE actually includes quite a bit of good IE-related material; however, JIPOE as practiced does not include very much (if anything) about the IE.		X	X	X		
Targeting working groups and targeting doctrine do not adequately consider nonlethal effects. OIE are typically categorized as nonlethal, so intelligence support for targeting does not include the IE, reinforcing the exclusion of OIE.		X		X	X	
Effective training material or courses are not available for IOII.		X	X	X		
Senior leaders lack awareness and knowledge of OIE.			X	X		

NOTE: Top challenges appear in bold.

How Commanders and Staff Prioritize Resources

Commanders at all levels must prioritize limited resources to best accomplish their missions. Intelligence staffs are particularly vulnerable to the unquenchable thirst for knowledge that comes from every other staff section. Demands from IO practitioners must be considered in this context, with conflicts adjudicated by thoughtful commanders.

Some interviewees expressed concerns that IE-related information requirements were rarely raised to a level that they considered a priority that resulted in intelligence support. As noted in the discussion of coordination and collaboration challenges, this may be the result of IO practitioners not being aware of existing intelligence products due to differing terminology or the fact that the intelligence was intended to support other staff functions. It is also possible that IO practitioners fail to access the intelligence capabilities of their commands to the same degree as other staff sections due to a lack of engagement with the intelligence and information requirements processes.

Assessing the outcome of IO is a challenging endeavor. Intelligence resources will most likely be required to collect the requisite data and apply analytic techniques that can accurately attribute causation between a relevant actor's actions, their implied decision making, and the IO-directed IRC activities. This level of intelligence involvement in IO is generally not available at the CCMD level.

Intelligence and Information Requirements

One of the most important stages of the intelligence process with which IO practitioners should familiarize themselves is the role that information requirements play in the planning and direction of intelligence operations. IO practitioners who do not understand or participate in official RFI processes may not be able to properly express their needs when competing for finite intelligence resources.

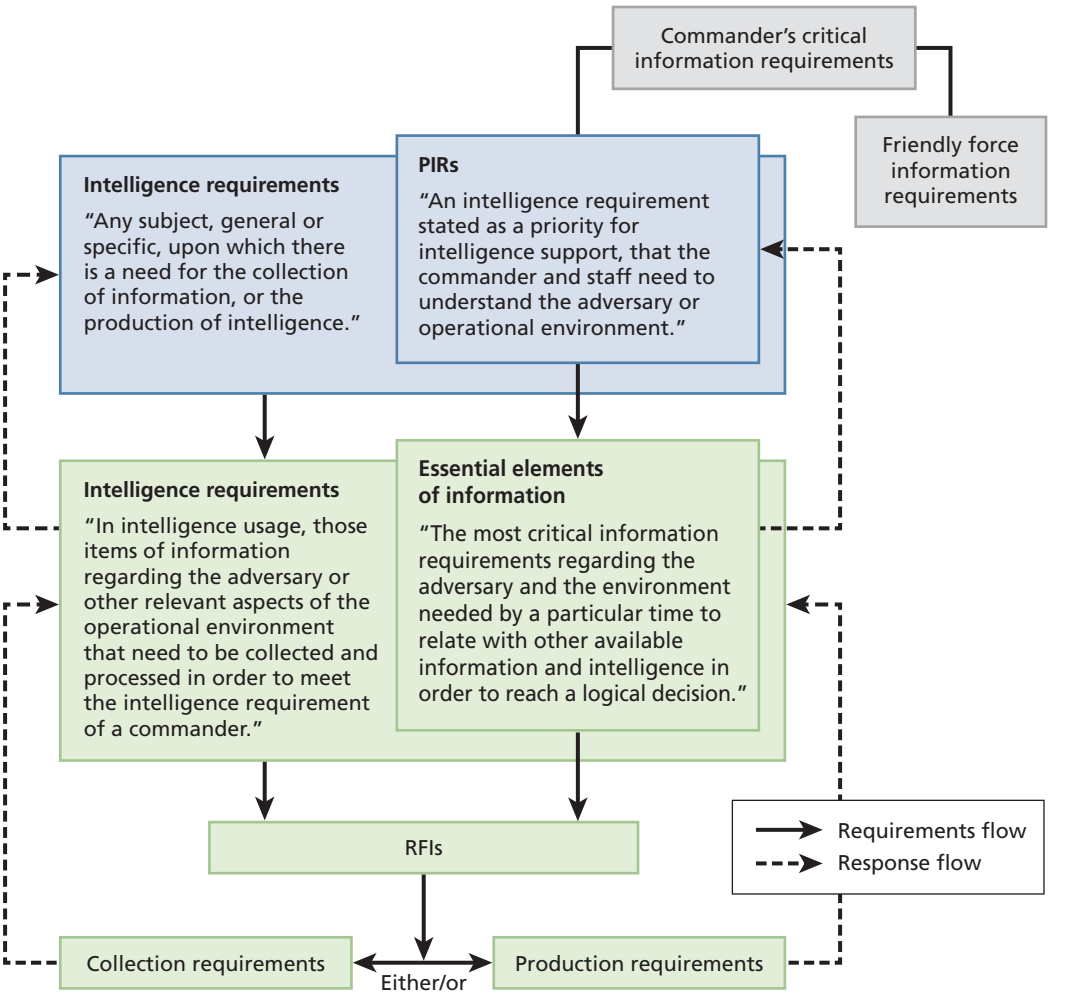
All staff sections involved in mission planning help identify information gaps, knowledge about the enemy or OE that are significant and unknown. Gaps in information that require collecting information or producing intelligence get formulated as intelligence requirements. Staff sections, including IO practitioners, may then recommend that some be designated PIRs. The J2 then consolidates the requirements and refers them to the commander for final decision and prioritization of PIRs, a process that determines the level of intelligence support and priority that each requirement receives.

Intelligence requirements, including the subset of PIRs, are then analyzed to determine which specific questions must be answered to satisfy the requirement. These are known as *information requirements*, a subset of which are essential elements of information required to satisfy PIRs. When combined with friendly force information requirements, all these requirements constitute the commander's critical informa-

tion requirements.[27] Figure 3.3 shows the relationships among these various types of requirements.

IO planners and integrators must understand how to communicate information needs via supporting intelligence personnel and official procedures, such as RFIs and the full range of commander's critical information requirements.

Figure 3.3
Relationship Between Intelligence Requirements and Information Requirements



SOURCE: JP 2-0, 2013, p. I-8, Figure I-4.

[27] JP 2-0, 2013.

Intelligence Support to IO Assessment

IO assessments are similar to other forms of combat assessment in that they estimate the effectiveness of selected plans, analyze collateral damage, and inform recommendations for future decisionmaking. Traditionally, the intelligence staff is responsible for accumulating, consolidating, and reporting information regarding combat assessments to facilitate current and future operations.[28] IOII involves similar doctrinal relationships among IO and intelligence personnel who assess IO, but the characteristics of the IE suggest that attempts to achieve integration raise unique challenges. It was also reported that intelligence support to IO assessments is rarely a priority for command leadership.

JP 3-13, *Information Operations*, has a chapter dedicated to IO assessment that emphasizes many important points related to IOII without explicitly using that term. For example, assessments require a baseline from which to measure change. This requires a well-planned analysis of the IE prior to the start of operations, followed by continuous collection and observations of effects during operations. The complexity of the IE, including the difficulty observing the cognitive dimension, can also require specific capabilities for collection and analysis that are not organic to many commands and organizations. Therefore, these capabilities and specific requests must be transformed into information requirements and requests to be satisfied with external support, such as the IC and other reachback support.[29] JP 3-13 also recommends an eight-step IO assessment framework, shown in Table 3.5.

Table 3.5
IO Assessment Framework

Step	Description
1	Analyze the IE
2	Integrate IO assessment into plans and develop the assessment plan
3	Develop IO assessment information requirements and collection plans
4	Build/modify an IO assessment baseline
5	Coordinate and execute IO and coordinate intelligence collection activities
6	Monitor and collect focused IE data for IO assessment
7	Analyze IO assessment data
8	Report assessment results and make recommendations

SOURCE: JP 3-13, 2014, p. VI-3, Figure VI-1.

[28] JP 2-01, 2017.

[29] JP 3-13, 2014.

Each step in the IO assessment framework has a potential role for intelligence support, but such support is clearly more central in some steps. For example, analyzing the IE in step 1 includes establishing an IE baseline to serve as the reference point for future comparison, while additional intelligence activities are conducted in step 5. Intelligence expertise is also certainly beneficial to properly developing information requirements and collection plans in step 3.

Monitoring and collecting information in step 6 may require a diverse array of collection capabilities, including human intelligence; signals intelligence; air- and ground-based intelligence; surveillance and reconnaissance; open-source intelligence, including from the internet; contact with the public; an ability to establish networks of culturally appropriate informants; press inquiries and comments; U.S. Department of State polls; reports and surveys; nongovernmental organizations; intelligence from international organizations; and commercial polls. The publication also emphasizes the need for personnel who are capable of employing unbiased analytic techniques in step 7, something that may require relying on expertise not organic to IO staffs.[30]

The above framework was developed and is managed by the Joint IO Warfighting Center for use at the operational and tactical levels, but it certainly applies at the strategic level as well. There is not a single step that does not have an intelligence component, and, therefore, collaboration with intelligence counterparts is critical to ensuring the effectiveness of IO planning and execution. However, acquiring intelligence support throughout this process requires that it be made a priority of the command during IO planning phases.

Finite Resources, Training, and Personnel

The IC, and the intelligence warfighting function, have finite resources and capabilities. Intelligence personnel and systems, like all resources, are not unlimited, and there are multiple demands for their specialty skills and capabilities. If lost to action or accident, intelligence resources are not easily replaced. Specialists who are trained in low-density languages or skills are particularly valuable and difficult to replace or augment quickly. Furthermore, different categories of intelligence products discussed in Appendix B may require unique resources and techniques that cannot be easily applied across the full range of intelligence products.

New products and solutions are needed to address the complex challenges inherent in the IE. To address these challenges, intelligence analysts will need additional skills and training to help stakeholders understand the IE. This will include ways to visualize operations, facilitate decisionmaking, and improve mission command.[31] Thus, the problem set will only increase—and in a nonlinear fashion.

---

[30] JP 3-13, 2014.

[31] Paul, Clarke, Triezenberg et al., 2018.

Intelligence reduces uncertainty; it does not eliminate it. This consideration is central to how commanders assess risk. Collecting information and developing it into intelligence takes time. Thus, commanders and IO practitioners must weigh the benefits of operating sooner, with less-developed intelligence, against the advantages of delaying operations to gather more intelligence, with the understanding that perfect clarity will never be achieved.[32] IO leaders will have to operate with an imperfect understanding of the environment while making assumptions founded in experience and personal research and education, like all other military leaders. The integration of communities will not always place IO as a top priority, and, even with unlimited resources, the IC could never eliminate all uncertainty. IO practitioners must learn to practice their trade in the fog and accept risk along with their operations-minded brethren.

Technological advancements are providing new opportunities to increase the timeliness of relevant information and lower its cost. Advances in data processing, such as artificial intelligence, big data analytics, knowledge bases, and iterative search tools, have created a new paradigm in which the timelines of intelligence operations and the intelligence process are greatly compressed. Exploitation and dissemination of information now occur nearly simultaneously as multimedia products are automatically updated with new information as it is collected and processed.[33] Understanding how to quickly access resident knowledge bases can save time and effort associated with more-formal information or intelligence requirements processes. Intelligence personnel who develop these tools should be building in the IO-related fields and data from the ground up. IO practitioners must provide feedback and maintain relevancy as these new tools are developed so they represent the information warfighting function. This is perhaps the most important consideration in addressing prioritization challenges. The manner in which automated systems of the future are designed will dictate the prioritization of information and intelligence support far beyond what any SOP, official policy, or personal relationship ever has. It is up to today's IO practitioners to get involved and lobby as those development efforts evolve.

Gaps in Concepts or Doctrine

Several challenges we encountered reflected gaps in concepts or doctrine. It can be easy to blame deficiencies in doctrine, but, in this case, new concepts are emerging and doctrine is changing and evolving at both the joint and service levels. When doctrine and concepts are in a state of flux, practice inevitably lags. All eight challenges in this category are listed in Table 3.6.

---

[32] Army Doctrine Publication 2-0, 2019.

[33] Marine Corps Doctrinal Publication 2, 2018.

Table 3.6
Challenges Associated with Gaps in Concepts or Doctrine

Gaps in Concepts or Doctrine	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concepts or Doctrine	Intelligence Authorities
Lack of common understanding of a COP, staff procedures, and SOPs to produce and share a COP of the IE.	X		X		X	
There are no intelligence information reports (finished intelligence products) specific to OIE foreign military intelligence collection activities, hindering the ability to search intelligence products.	X				X	
IO reachback organizations provide IE-related materials that are useful for IO and OIE, but they do not produce finished intelligence products. Thus, these materials are not indexed in intelligence systems and cannot be found through intelligence channels or inquiries.	X	X			X	X
Targeting working groups and targeting doctrine do not adequately consider nonlethal effects. OIE are typically categorized as nonlethal, so intelligence support to targeting does not include the IE, reinforcing the exclusion of OIE.	X	X		X	X	
Lack of clarity about operators' routine awareness of the IE and expectations concerning restrictions. (For example, no one accuses aircraft pilots of "doing intelligence" when they look out the canopy, and they are not expected to look away when they see a civilian airliner that might have U.S. persons on board.)					X	X
Web operations are not an intelligence activity but involve monitoring and engaging in real time on social media. (They are also not Title 50 covert operations, which would require additional intelligence oversight.)		X			X	X
Intel analysts at the service component commands need to provide more analysis of the IE and should use the most recent doctrine to update baseline analyses (a process similar to intelligence preparation of the battlefield).		X	X		X	
OSINT, collected by intelligence professionals, can make an important contribution to situational understanding of the IE.			X		X	

NOTE: Top challenges appear in bold.

Intelligence Versus Information Products

Perhaps the most vexing challenge is that, because of the recent surge in interest in the IE, the process for understanding it is immature and the products developed to communicate that information are still evolving. Specifically, IO products are not formally indexed like intelligence information reports and finished intelligence products. This limits the ability of both the intelligence and IO communities to search, share, and

collaborate. Reachback organizations, such as the 1st IO Command, the Marine Corps Information Operations Center, theater information operations groups, and Marine Expeditionary Force information groups, generate an immense volume of quality products that fall into this category. However, because they are not formally part of the IC, they are not beholden to analytic tradecraft standards, and their products are not indexed in the various IC databases or dissemination channels. Too often, key IE observations and insights have been left out of the intelligence process and not used to inform commanders and their staffs, who do not yet rely on IO products as a staple of their information diet. J39s are working through this challenge, which admittedly involves addressing challenges in other areas as well, from training and system development to leadership attention.

Applying Understanding

Military doctrine serves as a set of guidelines or, at times, a how-to manual, especially at the CCMD level or in a joint environment. This can be a lifesaver for a staff officer who is working in a functional area with which he or she has limited experience. However, there are numerous examples of doctrine lagging behind practice. It takes a long time to draft, approve, and produce doctrine; therefore, it will rarely be current. We heard many instances of the same problems being pointed out repeatedly. In these circumstances, there is a need to harmonize and update doctrine to help practitioners achieve results and accurately measure the effectiveness of OIE.[34]

U.S. military doctrine is generally quite comprehensive, but the nexus of information and intelligence leaves something to be desired. The JCOIE helps provide some direction, but it is still only a concept and therefore more aspirational than executable. The latest rewrite of JP 3-0, *Operations*, began to clarify the implications of the new information function and explain its intended relationship with its sibling, intelligence.[35] JP 3-0 specifically addresses how intelligence should support the information function:

> Intelligence is critical to the effectiveness of information activities. The intelligence function supports the information function by providing all-source intelligence analysis of processed information. Intelligence facilitates understanding the interrelationship of the informational, physical, and human aspects that are shared by the OE and the information environment. By providing population-centric, sociocultural understanding of relevant actors, intelligence can greatly assist planning, integration, execution, and assessment of information activities to create desired

[34] Arturo Muñoz and Erin Dick, *Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness,* Santa Monica, Calif.: RAND Corporation, PE-128-OSD, 2015.

[35] JP 3-0, 2018.

> effects. Intelligence in support of information activities may require greater-than-normal lead times to establish behavior baselines for human decision making.[36]

It is important to remember that the information function and IO, while inseparable, are not the same. If one were to replace *information activities* with *information operations* in the above quotation, IO dependence on intelligence would become even clearer. Ultimately, IO involve the coordination, integration, and synchronization of disparate information activities, executed by IRCs. Therefore, the criticality of intelligence support to IO or information activities is highlighted in the latest joint doctrine.

Intelligence Support to Targeting

An explicit task of the intelligence warfighting function is to "provide intelligence support to targeting and information operations" to achieve lethal and nonlethal effects.[37] Targeting, "the process of selecting and prioritizing targets and matching the appropriate response to them," is fundamentally an integration and synchronization activity.[38] Targeting is traditionally associated with the joint fires function and seeking lethal effects, but it requires the integration of planning, intelligence, maneuver, and other activities. The integration of IO and targeting to synchronize lethal and nonlethal effects is increasingly a topic of interest. Intelligence support to IO planning, execution, and assessment are all required for successful targeting. Although doctrine addresses nonlethal targeting, it may not be sufficient to guide a process that remains inherently focused on lethality. Targeting working groups do not give nonlethal assets sufficient consideration when addressing how to achieve desired effects.

Along similar lines, one of the most critical ways in which intelligence enables or can even drive operations is through its support to targeting. This is addressed in JP 3-0:

> Information activities and capabilities are integrated in the targeting process during planning and execution to create and synchronize effects in support of [joint force commanders'] objectives. Many information activities and capabilities have interagency execution approval levels that may increase time required to plan, coordinate, and integrate into the joint force targeting process. Other [U.S. government] departments and agencies lack trained personnel and procedures to satisfy interagency planning, execution, and assessment requirements. Fully analyzing and developing target sets for nonlethal action may also increase coordination time required. Information activities may be compartmented. However, effective integration of information activities and capabilities in the targeting process

---

[36] JP 3-0, 2018, p. III-27.

[37] Army Doctrine Publication 2-0, 2019, p. 2-3, Table 2-1.

[38] JP 3-60, *Joint Targeting*, Washington, D.C.: U.S. Joint Chiefs of Staff, January 31, 2013, p. I-1. Note that JP 3-60 was undergoing revisions when this report was in production.

> results in improved understanding for the entire joint and multinational force and increased opportunities to achieve [joint force commanders'] objectives.[39]

The lethal or nonlethal effects sought by targeting represent a change in the physical or behavioral state of a target system, a target system component, a target, or a target element that help achieve an associated objective. The intelligence function helps planners, operators, and commanders understand targets. Understanding a target's "cognitive characteristics" has long been considered necessary for assessing critical nodes within a target system, for example. However, as we have discussed, these cognitive characteristics can be difficult to identify.[40]

Intelligence support to targeting occurs throughout the joint targeting cycle, but key contributions that are relevant to targeting in the IE will typically be made in the planning phase. Intelligence products support target system analysis and target development during JIPOE. Intelligence personnel are then involved in validating nominated targets added to a joint target list, restricted target list, and no-strike list. Information must then be collected and analyzed to develop a more complete picture of targets and identify remaining intelligence gaps.[41]

Intelligence Authorities

Challenges involving intelligence authorities pertain to the rules and oversight mechanisms that apply to the defense intelligence enterprise; however, they affect IO personnel as well. There are legal and policy restrictions placed on the IC that limit these organizations' ability to collect information on U.S. persons. This category highlights some of the challenges with this and other intelligence authorities. All four tasks in this category are listed in Table 3.7.

Routine Monitoring, Publicly Available Information, and Open-Source Research

There is a lack of clarity about what constitutes routine awareness of the IE and what that should look like. For example, no one accuses aircraft pilots of "doing intelligence" when they look out the canopy of their aircraft and see a civilian airliner. Pilots are not expected to look away because there might be U.S. persons on board; it is understood that they are merely maintaining situational awareness in the air domain. In much the same vein, practitioners who monitor various social media platforms are just maintaining situational awareness in their environment. However, this quickly becomes an intelligence oversight issue when U.S. intelligence personnel are doing the monitoring.

---

[39] JP 3-0, 2018, p. III-27.

[40] JP 3-60, 2013.

[41] JP 2-0, 2013.

Table 3.7
Challenges Associated with Intelligence Authorities

Intelligence Authorities	Coordination and Collaboration	Division of Labor	Missing Expertise	Prioritization	Gaps in Concepts or Doctrine	Intelligence Authorities
Web operations are not an intelligence activity but involve monitoring and engaging in real time on social media. (They are also not Title 50 covert operations, which would require additional intelligence oversight.)		X			X	X
IO analysis of the IE does not meet intelligence professionals' standards for analytic tradecraft.	X	X	X			X
IO reachback organizations provide IE-related materials useful for IO and OIE, but they do not produce finished intelligence, so these materials are not indexed in intelligence systems and cannot be found through intelligence channels or inquiries.	X	X			X	X
Lack of clarity about operators' routine awareness of the IE and expectations concerning restrictions. (For example, no one accuses aircraft pilots of "doing intelligence" when they look out the canopy, and they are not expected to look away when they see when they see a civilian airliner that might have U.S. persons on board.)					X	X

NOTE: There were no top challenges in this category.

Indeed, there are many guidelines, laws, and policies that prevent intelligence organizations from collecting information on U.S. citizens.[42] However, there is a difference between monitoring the IE and actively collecting information in that space. This leads to confusion for both IO and intelligence practitioners. Indeed, the differences between OSINT and open-source research are at the crux of this debate. Some organizations have policies that actively distinguish between the two, while others do not. Currently, DoD faces challenges in developing a clear policy for collecting information on U.S. persons in the IE and what mitigating actions to take should it occur.

It is difficult to implement oversight mechanisms on fast-paced mediums. One example is U.S. Central Command's WebOps program, which has been operational for several years and is designed to actively counter adversary messaging and engage

[42] U.S. Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, Washington, D.C., August 8, 2016.

selected relevant actors across various social media platforms.[43] Yet, this program routinely pushes both intelligence and IO practitioners into uncharted territory. That is to say, because social media platforms allow for rapid engagement, and conversations happen fast, operational guidelines for IO practitioners need to be preestablished. WebOps is not an intelligence program, but it does rely on intelligence professionals, who must adhere to intelligence rules, regulations, and oversights. Because of this, the lines between what IO practitioners need to do their jobs and what they can obtain from intelligence organizations are widening. Intelligence processes and products are also not created at the speed of engagement on social media; operators who are engaging in this space need to respond quickly to maintain relevancy.

Open-Source Collection Management Tools

Another area of concern pertains to the tools that are used to collect and collate intelligence requirements. COLISEUM and OSCAR-MS are two of these requirement management tools. RFIs that require OSINT collection and analysis are coordinated through COLISEUM, and RFIs that require new OSINT collection are entered into OSCAR-MS. In both systems, collection managers are required to deconflict existing requirements with emergent requirements. Both of these systems allow collection managers to add new RFIs and assign organizations to fulfill requests. Both COLISEUM and OSCAR-MS are maintained by DIA.

This chapter identified 40 unique challenges in six categories addressing roles and responsibilities for intelligence support for OIE. We described each challenge and provided context to highlight why it was important for effective intelligence support for OIE. The next chapter proposes solutions to these challenges.

---

[43] Associated Press, "U.S. Bid to Counter ISIS Online Recruiting, WebOps, Inept, AP Finds," CBS News, January 31, 2017.

CHAPTER FOUR

Solutions to Improve Intelligence Support for Operations in the Information Environment

With the 40 challenges presented in Chapter Three in mind, we sought to identify solutions to these disparate and complex problems. Candidate solutions came from our interviews, our literature review, and the expertise of the research team.[1] We synthesized candidate solutions to reduce redundancy, matched them to specific challenges to ensure their utility, and validated them through careful analytic review.

In our analysis, we explicitly matched solutions to the challenges, with between one and five potential solutions addressing each challenge. Across the 40 challenges, we identified a total of 91 solutions, which we then synthesized to reduce redundancy, leaving 67 unique solutions.

To highlight the dual nature of the IOII problem, we first divided the solutions by which community would be primarily responsible for implementing them: the IO/OIE/IRC community, the IC, or other organizations. Figure 4.1 clearly shows a relatively balanced division between solutions that will need to be implemented by information professionals and organizations and those that will need to be implemented by intelligence professionals and organizations.

The solutions we identified fell into four general categories:

1. Improve processes.
2. Prioritize support.
3. Train and educate.
4. Allocate personnel.

These solution categories are intentionally phrased as directives. To address the challenges identified in Chapter Three, it is necessary to prioritize support for IO/OIE, improve related processes, allocate additional personnel to related intelligence and coordination tasks, and ensure that personnel are sufficiently trained and educated in required tasks. The remainder of this chapter summarizes the solutions according to these themes.

[1] Some challenges clearly imply a solution. Following the logic of Charles Kettering, "A problem well stated is a problem half-solved."

Improve Processes

The solutions in this category address challenges that expose shortcomings or deficiencies in existing processes. Because some challenges apply to both the intelligence and information communities, process solutions address both intelligence and IO/OIE/IRC processes. There were 30 solutions in this category. Removing duplicates left us with 26 unique solutions. We identified ten that were IO/OIE/IRC-related, eight that addressed intelligence processes, and eight that addressed the processes of other organizations. There were more solutions assigned to this category than any other.

Processes in both the information and intelligence communities need to be improved. This can start with each becoming more aware of the other's processes and practices. Each community has its own established culture, and it will likely be necessary to push the two toward greater interaction. Additionally, the targeting and tasking processes both need to be improved. All 26 tasks in this category are listed in Table 4.1.

Table 4.1
Solutions to Improve Processes

Responsibility for Implementation	Solution
IO organizations	IO personnel need training to better understand how to write well-scoped, articulate intelligence requests that are practical and feasible.
	J39 should create a consolidated list of actionable PIRs, with the help of IRC personnel, that is endorsed by the commander and submitted quarterly to the JIOC.
	J39 should work to streamline processes, create SOPs, and procure tools that help visualize the IE, as well as pursue further research on concept and tool development.
	J39 or IRC personnel should brief the J2 on past and future OIE at quarterly working group meetings.
	J39 should brief the IRCs, J2, and other staff elements to increase awareness of OIE, primarily through the IO working group.
	Products created by J39, IRC personnel, or organizations outside the IC that provide valuable insight into the IE need to be socialized with the command and staff to demonstrate their value.
	J2 should vet products created by J39, IRC personnel, and organizations outside the IC to ensure accuracy and agreement.
	J39 should take the lead to garner J2 engagement in OIE and write the first draft of a J2-J39 SOP.
	J39, IRC personnel, and J2 should have a common process to collaborate, develop observable metrics to support OIE measurement and assessment, and determine who (J39, IRC personnel, J2, other intelligence entity) will collect information.
	J39 and J2 should have a process to collaborate to determine what kinds of estimates of what target populations or regions will be required to support OIE and to prioritize them for J2 action.

Table 4.1—Continued

Responsibility for Implementation	Solution
Intelligence organizations	Using existing guidebooks, templates, and doctrine, intelligence analysts at the service component commands should provide more-extensive descriptions and analyses of the IE.
	The Judge Advocate General, in coordination with J2, should ensure that there are appropriate authorities for OSINT collection and craft a clearly articulated policy that delineates between OSINT and open-source research.
	The JIOC should aggressively pursue requests that it receives from IO personnel.
	OIE products should be serialized and made searchable.
	J2 should create IE-specific products that adhere to IC Directive 203 standards.
	Trained J2 red team personnel should be included in OIE planning efforts.
	J2 should ensure that doctrine is followed and that the IE is comprehensively analyzed during JIPOE.
	Roles, responsibilities, and authorities for IE monitoring, estimates, and collections related to WebOps should be clarified, and there should be processes to determine who (WebOps, J2) should gather needed information and on what timeline.
Other organizations or entities	Extraneous meeting requirements should be reduced.
	Products such as the IO synch matrix already exist, but a more streamlined process to task needs to be incorporated, like an air tasking order.
	If possible, J2 and J39 should be located in close proximity to support interaction.
	Doctrine aligning IOII terminology should be updated, and all staff sections should adopt a common lexicon.
	J2 and J39 (or other OIE/IRC) personnel should have a process by which they work together to prioritize RFIs, make them as practical as possible, leverage existing collections where possible.
	A working group consisting of O-4/O-5 or GS-13/GS-14 J2 and J39 personnel should meet quarterly to discuss products, support mechanisms, and future operations and to routinize relationships and consultations.
	An organization other than J39 or J2 needs prioritize efforts that focus on OIE.
	The targeting process should include lethal and nonlethal targeting in a commensurate manner.

Improve Processes in IO Organizations

For IO organizations, we identified a several overarching solutions. The IO community must continue to explain to intelligence professionals the foundational concepts of OIE. Across the IC, there is a lack of understanding of OIE and how to support it. One way to address this challenge is through an open and continuous dialogue. Establishing a common lexicon, so that both parties are talking to and not past each other, would help build common understanding. A quarterly IO and intelligence forum

could be one way to encourage engagement. This group could focus on creating standard processes and procedures to raise awareness of each community. It could also be used to socialize intelligence processes for IO practitioners while simultaneously helping to educate the IC on IO needs.

The need for IO practitioners to be able to write clear, understandable RFIs and intelligence requirements is another process to be improved. Without the ability to clearly and articulately ask intelligence professionals for support, in a manner that facilitates understanding, there is little hope to have RFIs answered. Several interviewees mentioned that they would write an RFI only to have it returned to their own office to be answered.

Although there are some pockets of effectiveness, overwhelmingly, products that are created by IO organizations are rarely vetted with intelligence professionals. One way to improve the level of trust associated with an IO product would be to have intelligence professionals vet the product. Indeed, some CCMDs are already creating a "brand" of products that are always vetted through multiple staff sections, including intelligence professionals. This has dual effect of increasing brand awareness for senior leaders and forcing disparate staff sections to coordinate their efforts.

The assessment process is another area in which intelligence personnel could provide valuable input. However, it is unlikely that the IC will willingly volunteer their assistance; rather, IO practitioners need to request assistance from the IC.

Improve Processes in Intelligence Organizations

The IC could provide more-extensive analysis of the IE by using existing doctrinal templates and guides. JIPOE already calls for intelligence analysts to contribute significantly to characterizing the IE, yet they often do not do so to a sufficient degree. There are multiple pages dedicated to explaining the IE and how to characterize it, but this analysis is not often followed as completely as it should be. JIPOE is foundational analysis; it is critical to the development of all plans and orders that a CCMD publishes.

Just as the IO community needs to be better at requesting RFIs, the IC needs to be more responsive in addressing those requests. As IO practitioners get better at asking the right questions, intelligence personnel should aggressively pursue answers. One change that will support this process would be to clearly identify OIE and IE PIRs. Not only would this help to raise awareness of these issues in the IC, but it would also help to focus processes on answering them.

The ability to serialize IO/IE products so that they are searchable is another process in which the IC could assist. Currently, there is no easy way to determine whether an intelligence product is useful to an IO practitioner. One easy way to change this would be to have a special serialization for IE-related products. That way, analysts, practitioners, and operators could easily search systems for the information they need to support and conduct OIE.

Creating plans to conduct OIE requires more than just IO practitioners and planners. It requires input from the entire staff. Although J2 should be providing analysis and input for these plans, red team personnel—specifically, those charged with thinking like an adversary—should also be engaged throughout the planning process. Often, intelligence personnel are too busy or are not asked to participate in OIE planning. This needs to change. Red team personnel must be used extensively throughout the planning process to ensure that operations and activities fully leverage the inherent informational aspects of military power.

Prioritize Support

The challenges in this category highlight efforts that need to be prioritized. Too often, effective support is possible but not fully provided (or not provided at all) because of commanders' or institutional priorities. In this category, we identified 17 solutions, 16 of which were unique. Of those, one was associated with IO organizations, while five focused on intelligence organizations and ten pertained to other organizations or entities, as shown in Table 4.2. The bulk of these solutions were derived from outside the IO and intelligence communities, illustrating that other organizations and entities need to prioritize intelligence support for OIE.

Prioritize Support in IO Organizations

The prioritization of intelligence support for OIE largely falls outside the scope of IO organizations. However, one solution that we identified relates to RFIs. That is, IO practitioners need to ensure that only the most important RFIs are sent to intelligence personnel, increasing the likelihood of receiving an answer from the intelligence organizations. These RFIs need to be clearly and concisely written and should be crafted in a way that aligns with the tools and analytic tradecraft that the analyst will use to answer the question.

Prioritize Support in Intelligence Organizations

Intelligence organizations need to dedicate more time, energy, and resources to OSINT, an important capability that has not received a proper amount of support from the defense intelligence enterprise. A dedicated OSINT capability added to an existing cross-functional intelligence capability could greatly increase the value of intelligence support for OIE. To date, this capability has not been prioritized.

Intelligence organizations must commit to providing more in-depth analysis of the IE during the creation of foundational intelligence processes. They should closely follow JIPOE and ensure that specific characteristics of the IE are identified and analyzed. Without this foundational knowledge, it is extremely difficult for the joint force to realign in the lead-up to hostile actions.

Table 4.2
Solutions to Prioritize Support

Responsibility for Implementation	Solution
IO organizations	J39/OIE/IRC personnel should send only the most important intelligence requests to the JIOC.
Intelligence organizations	J2 should prioritize OSINT collection and analysis in support of OIE and dedicate additional analysts to OSINT.
	Intelligence organizations should increase the production of intelligence products that addresses IO PIRs and leverage production centers within and outside the IC for IE-related products.
	Intelligence personnel are already creating products that could be valuable to IO planners and operators, but they may not be discoverable, available in useful formats, or reaching those who need them. Thus, J2 should push these products to J39 and IRC personnel.
	J2 should commit to providing baseline estimates of the IE in support of OIE and dedicate collection and analysis resources to support OIE assessment.
	The JIOC should house a red team with targeting expertise and an understanding of OIE.
Other organizations or entities	Commanders should prioritize analysis and production of OIE-related products to build foundational intelligence across the IE.
	J3 should prioritize OIE efforts that have achievable outcomes. If they are sufficiently important, national technical means should be leveraged to measure their effects.
	Commanders should create OIE- and IE-focused PIRs.
	DIA should add intelligence support for OIE as a complex problem in the DIAP.
	Commanders at the service component commands need to prioritize analysis of the IE so that additional intelligence analysts are dedicated to these activities.
	J2 and J39 (or other OIE/IRC personnel) should have a process for working together to prioritize RFIs and make them as specific as possible.
	Commanders should prioritize the collection of IE PIRs through tactical means.
	An IC organization should be the functional manager for IOII.
	J2 and J39 should procure information technology/tools (e.g., command and control of the information environment, pulse) that can help visualize and analyze the IE for both operators and analysts.
	J3 (operations) should prioritize OIE as part of theater-shaping activities across the conflict continuum.

Other Organizations or Entities

Although there has been renewed interest in OIE within DoD, there are still communities that are struggling to support these efforts. The reasons for this are myriad, but elements within the defense intelligence enterprise are particularly resistant to expanding support for evolving OIE concepts. DIA, the center of gravity for military intel-

ligence, should take ownership of IE analysis and intelligence support for OIE. This will involve designating intelligence support for OIE as a complex analytical issue in the DIAP, which will help focus efforts, secure resources, and create the institutional backbone needed to effectively address associated challenges. DIA should also designate an IOII functional manager to help adjudicate and assign responsibilities across the defense intelligence enterprise. Part of this solution could be to designate a lead organization with responsibility for IOII.

Another solution would be to treat intelligence support for OIE like the defense intelligence enterprise treats targeting. There is a cadre of professional analysts assigned to various commands who are trained as targeteers. They are intelligence professionals first but are sent to targeting school to learn targeting methodology. After this training, these personnel are awarded a particular functional skill identifier. They then go on to complete a utilization tour as a targeteer, usually with a CCMD. In much the same vein, a cadre of intelligence professionals could be trained as IE analysts. Once trained with an IO sub-specialty, these individuals would be assigned utilization tours to conduct IOII at a service intelligence center, DIA, CCMD or component command.

Commanders and senior leaders across DoD also have a role to play in ensuring that IOII is fully supported. They must prioritize OIE across the conflict continuum and ensure that these operations are considered concurrently with other operational planning, not as an afterthought.

Acquiring the tools and information technology to successfully conduct IOII and support analytic processes is another area that needs to be prioritized. As processes evolve and new personnel are trained to conduct IOII, new systems will be needed. Analysts will need ways to compile data for OIE, commanders and staffs will need to visualize OIE, and operators will need a way to implement their decisions.

Train and Educate

We identified 29 solutions that related to training and education, 13 of which were unique. IO organizations were identified five times, intelligence was identified three times, and other organizations were identified five times. Both IO and intelligence personnel need additional training and educational opportunities to increase their knowledge, and there is a general lack of understanding of roles and responsibilities across both communities.

Train and Educate IO Professionals

IO personnel need additional training in writing acceptable, well-scoped IRs. This will lessen the burden on the IC and go a long way toward ensuring that RFIs are answered.

To help raise the awareness of OIE, which will necessitate better IOII, training objectives that highlight OIE should be included in joint exercises. Although this has

Table 4.3
Solutions to Facilitate Training and Education

Responsibility for Implementation	Solution
IO organizations	J39 should ensure that training objectives in joint exercises reinforce OIE.
	J39 and IRC personnel need training to better understand how to write well-scoped, articulate intelligence requests that are practical and feasible.
	Commanders and staff need to be educated on the importance of OIE.
	J39 should help train selected J2 personnel on OIE so that they are better prepared to red-team OIE as part of broader operations.
	IO organizations should educate leaders on OIE so that they better understand the concepts and how to operationalize information. They should start by leveraging existing courses and mobile training teams.
Intelligence organizations	J2 personnel (or other intelligence personnel who support J39) should receive OIE-related intelligence training.
	Using JIPOE as a guide, intelligence analysts should create foundational intelligence estimates that specifically incorporate the IE.
	J2 personnel should train J39 personnel on targeting procedures.
Other organizations or entities	DIA (or the IC organization that is assigned to or takes responsibility for the IE) should create and implement curricula on OIE.
	Common lexicon should be reinforced in training for both J39/IRC personnel and J2 personnel.
	Courses on integrating IO into the intelligence process need to be created and included in professional military education and for civilian analysts (at service centers and DIA).
	DIA (or another designated IC organization) should create additional courses on IOII and OIE, to be offered in the Advanced Global Intelligence Learning Environment (AGILE).
	Additional courses specific to IOII should be offered at the service centers for new analysts and through AGILE general analyst training.

happened in some joint exercises, more often than not, OIE is still a secondary objective, if it is mentioned at all.

Additionally, commanders and staffs need to be educated on OIE more generally. Until senior leadership understands the importance of OIE, these operations will not be a priority for commands.

Train and Educate Intelligence Professionals

Intelligence organizations need training and educational opportunities to raise their overall understanding of OIE and IOII. Our interviews revealed that many intelligence professionals do not understand OIE or how intelligence processes can support these operations. To address this gap, more topics related to IOII need to be incorpo-

rated into introductory analytical courses. Educational opportunities need to continue throughout an analyst's career to continue to grow their expertise and understanding of these issues.

One area in which intelligence personnel should take the lead is in helping IO practitioners increase their understanding of the targeting process. Whereas selected intelligence personnel receive a significant amount of training on the targeting process and can receive an identifier after completion, IO practitioners do not often have this opportunity. Having trained intelligence personnel train IO practitioners on the targeting process will increase the relevance and utility of OIE at the CCMD level.

Finally, intelligence personnel need to ensure that JIPOE is meticulously followed and that they create foundational estimates of the IE.

Other Organizations or Entities

Intelligence personnel need training courses, whether they are analysts, collection managers, branch chiefs, or senior leaders. There needs to be an overall increase in the types of analysis that these personnel provide, as well as a better general understanding of OIE. IO practitioners need to better understand intelligence processes to more effectively request assistance and to ensure that IO products incorporate existing intelligence. However, responsibility for creating additional courses and content for IOII resides primarily outside the CCMDs. The services and IC are more likely to have the requisite skills and capability to conduct this training.

Allocate Personnel

We identified 14 total solutions pertaining to the allocation of personnel, 12 of which were unique. IO organizations were the primary organization for three of these solutions, intelligence organizations were identified six times, and other organizations were identified three times. The solutions focus primarily on near-term personnel shortages rather than creating a large body of intelligence and IO personnel dedicated to OIE. Although a dedicated body of intelligence professionals is needed to support OIE, that development will take a long time.

Allocate IO/OIE/IRC Personnel

IO organizations should consider expanding their liaison presence in intelligence organizations.[2] The addition of one person or more IO practitioners embedded in intelli-

[2] Liaison officers must represent their home organizations' equities and avoid either over-assimilating or becoming just another body in the new organization. Parent organizations must maintain control over liaison officers. One way to do this could be to have parent organization be the primary rater for liaison officers and not give this responsibility to personnel in the liaised organization. For a fuller discussion of liaison officers see Christopher Paul, Harry J. Thie, Katharine Watkins Webb, Stephanie Young, Colin P. Clarke, Susan G. Straus, Joya Laha,

Table 4.5
Solutions to Allocate Personnel

Responsibility for Implementation	Solution
IO organizations	J39 should create at least one liaison officer position to promote additional interaction with J2 staff elements.
	J39 should continue to leverage the expanding capabilities of the theater information operation groups to augment staffing shortages
	J39 should utilize all personnel options (civilian, military, contractor) to fulfill meeting obligations and delegate to IRC personnel, where possible; this may require additional manpower.
Intelligence organizations	J39 should be augmented with an intelligence collection manger to help validate RFIs, enter RFIs into COLISEUM or OSCAR-MS, and ensure that RFIs are answered in a timely manner.
	Intelligence organizations should dedicate additional intelligence analysts to the IE.
	J2 should provide dedicated analyst support to WebOps to help with targeting and vetting.
	J2 should shift analytical support to OIE.
	JIOC should build cross-functional teams to provide better analysis of the IE, which will be useful for IO planning purposes.
	J2 should provide dedicated analytical support to J39 to help with collection, production, and assessments.
Other organizations or entities	An IC organization (preliminarily, we recommended DIA) should be designated as the proponent for IOII, and specific IC organizations should focus on creating IE-focused content (like the 1st IO Command but in the IC or at the Joint Staff level).
	The IC should assign a member organization (DIA, or whichever IC element takes responsibility for OIE) to serialize all IE-related products.
	DIA (or another designated IC organization) should create a training pipeline for intelligence analysts to become subject-matter experts in IOII.

gence organizations would have multiple benefits. It would help educate intelligence professionals on IO processes and procedures. It would also help ensure that the intelligence that is generated is of maximum value to IO planners and practitioners. A small investment in liaison personnel could have a dramatic impact on the quality and amount of support that IO organizations receive. This cell would additionally help increase the level of interaction between these two communities, break down cultural barriers, and increase overall understanding.

IO organizations at the CCMDs should also consider what mechanisms should be used to bring additional expertise onto their staffs. The IO community is not large

Christine Osowski, and Chad C. Serena, *Alert and Ready: An Organizational Design Assessment of Marine Corps Intelligence*, Santa Monica, Calif.: RAND Corporation, MG-1108-USMC, 2011, p. 64.

in any of the services, and there is no civilian occupation equivalent in the federal workforce. Therefore, the CCMD IO organizations should leverage the theater information operation groups as much as possible to fulfill staffing needs. The Army Reserve and Army National Guard theater information operation groups are an available force pool for CCMD IO organizations. Another way to overcome staffing shortfalls in IO organizations would be to leverage personnel who are well versed in OIE whenever possible. Because J39 must be represented at many events and meetings, having knowledgeable personnel attend is important. Therefore, being able to draw on civil affairs, PSYOP, MILDEC, OPSEC, public affairs, or other specialists to attend events that IO personnel cannot would help ensure that IOII considerations are addressed.

To increase planning efforts for OIE, IO cells should be supported by a functionally integrated staff, including intelligence. This will ensure that OIE are considered early in the planning process. These efforts should take place in every step of the Joint Operations Planning Process, JIPOE, and intelligence preparation of the battlefield.

Allocate Intelligence Personnel

One area in which IO organizations need assistance is collection requirements. Intelligence collection managers should augment J39 to help it validate requests and leverage intelligence systems. Most IO practitioners are unfamiliar with COLISEUM and OSCAR-MS, how they operate, or how tasks are assigned. An intelligence collection manager could help IO personnel ask refined questions of their intelligence counterparts.

Assigning a collection manager would provide some support for IO RFIs, but, ultimately, more intelligence personnel need to focus on supporting OIE. There is also a need for dedicated analytical support for OIE to help with collection, production, and assessments. Another way to improve the quality of the intelligence provided to IO practitioners is to have cross-functional intelligence teams that can provide better analyses of OIE. A cross-functional team could include multiple analysts and collection and production personnel from a range of intelligence disciplines. A key member of this group would be an OSINT analyst or someone capable of analyzing publicly available information.

This chapter identified 67 unique solutions in four categories: improve process, prioritize support, train and educate, and allocate personnel. In total, IO organizations were identified 19 times, intelligence organizations 22 times, and other organizations or entities 26 times. Many organizations have the responsibility to improve intelligence support for OIE. Following these identified solutions will help to reach that goal. Next, we present the overarching conclusions and recommendations from our research.

CHAPTER FIVE

Conclusions and Recommendations

The changing nature of IOII and the growing influence and evolving character of OIE reflect the close relationship between the intelligence and IO communities—specifically, in how they collect, analyze, and create products focused on information. We illustrated that the dual nature of the IOII problem has a deep-seated history that has not yet been fully acknowledged or overcome. We explored six categories of challenges that highlight why there are problems with intelligence support for OIE in an effort to bring clarity to the contours of those problems.

We then presented four categories of solutions. For example, to resolve the challenges identified in Chapter Three, the joint force must prioritize support for IO/OIE, improve related processes, allocate additional personnel to related intelligence and coordination tasks, and ensure that personnel are sufficiently trained and educated in these required tasks.

Here, we outline several conclusions from that analysis and present a series of actionable recommendations to improve intelligence support for OIE at the command level. Our six general conclusions are as follows:

- There is growing awareness of OIE and the effects that these operations generate, but there is not sufficient appreciation for what OIE can achieve or how they can shape the OE.
- IOII is a two-sided problem. Intelligence and IO professionals need to work together to address these challenges.
- There is insufficient support for OIE and little emphasis on the IE within the defense intelligence enterprise. This hinders efforts to plan and execute OIE.
- Current processes are insufficient to enable effective intelligence support for OIE, including for targeting and producing estimates and assessments.
- Challenges fall into six categories: coordination and collaboration, division of labor, missing expertise, prioritization, gaps in concepts or doctrine, and intelligence authorities. Potential solutions fall into four categories: improve processes, prioritize support, train and educate, and allocate personnel.
- Support for IO/OIE required from intelligence professionals spans the conflict continuum and varies across that spectrum.

Recommendations for IO Organizations

To implement solutions that will improve how the joint force organizes for, invests in, conducts, and supports OIE, we recommend that IO organizations take ownership of specific tasks and responsibilities where possible. They should make use of their available planners and practitioners and be champions for OIE within the joint force. Although there is clear recognition that information plays a key role across the conflict continuum, there is still little appreciation for how to execute OIE. Even when commanders and staffs *do* have the requisite understanding and awareness, they often do not fully consider or adequately integrate information activities, capabilities, and operations into military exercises and campaigns. To address this shortfall, we suggest that IO organizations take the following four steps:

- Increase understanding and awareness of OIE and IOII. Work with commanders, staffs, and, especially, intelligence personnel to increase their knowledge of OIE. Be the champions of OIE for commanders and staffs, and volunteer to teach and mentor them in how OIE should be conducted.
- Make use of existing personnel to improve coordination and routinize processes that are currently ad hoc or nonexistent. Address the knowledge shortfalls in the RFI process, and ask intelligence personnel to help IO practitioners craft answerable RFIs.
- Assign IO liaison officers to intelligence organizations to establish better communication, build a shared understanding of IOII and OIE, help educate intelligence personnel, and create products that are more focused on the IE.
- Ensure that nonlethal effects are included in the targeting process. IO personnel should receive instruction on the targeting process and methodology. Improved understanding will lead to better articulation and advocacy for targets in the IE.

Recommendations for Intelligence Organizations

Intelligence organizations also have a part to play if the joint force is to get better at OIE. These organizations already have a firm base on which to build in the form of well-developed doctrine and analytic processes. Analysts are well trained and bring critical-thinking skills to complex problems. However, intelligence organizations need greater awareness of OIE and, subsequently, need to expand training and dedicate personnel to collecting and analyzing data and producing intelligence products focused on the IE. We offer three recommendations to help intelligence organizations pursue these objectives:

- Formalize and expand training. This training should be institutionalized, broadened, and systematized across the defense intelligence enterprise. Both military

and civilian intelligence personnel need training, but the focus should be on personnel slated to work at CCMDs.
- Empower an organization to own analyses of the IE. This organization will need to create the foundational structures through which intelligence support for OIE is institutionalized. To help achieve this, the DIAP should treat intelligence support for OIE as a complex analytical issue. This will raise awareness of related challenges, help align resources and, potentially, lead to the creation of an IE specialization for intelligence personnel.
- Create cross-functional analytic teams to better integrate intelligence functions and direct greater attention to the IE. These teams should use existing doctrine and templates to ensure that IE-related tasks are properly executed.

Enhancing Integration

This study focused on intelligence support for OIE. However, a complete and successful integration of the two joint functions requires that each be capable of transferring between the supported and supporting roles as necessary to ensure that objectives are achieved. Although we did not address IO support to intelligence in depth here, it is worth noting the potential value of that relationship for future study, experimentation, and implementation across the joint force.

IRCs represent unique capabilities for influencing the behavior of target audiences in ways that can be conducive to collecting information. For example, intelligence collection methods may require that actors or groups communicate with each other or activate technical systems. IO that produce reactions within the IE can be coordinated with preplanned or persistent observation to address information requirements more broadly.

Finally, joint operations rely on the integration and synchronization of all joint functions. As the information function continues to be developed across the joint force, OIE may serve as an example of how it is better integrated with the command-and-control, maneuver, fires, force protection, and sustainment functions as well.

Suggestions for Further Research

Over the course of this research, we identified multiple avenues for investigation that were tangential to our main research question but warrant further analysis. For example, we noted several critical training and education shortfalls. To address this problem, the joint force would benefit from a systematic approach to cataloging and identifying relevant courses that are available to IO practitioners, intelligence professionals, and other personnel. This would necessitate a curriculum and gap analysis, which could

be done by examining all IOII, IE analysis, and related courses (currently or recently available), along with a gap analysis to determine where training needs are not being met.

To help meet training needs at the CCMDs, an analysis of the Universal Joint Task Lists could identify where IOII content can be added to joint exercises. Joint exercises are the main training venue for CCMD forces, and planners should strongly consider including OIE training among their objectives. How to design this training and what measurable and achievable goals it should address should also be carefully considered.

Analytic tradecraft is also important. Systematic collection and synthesis of available OIE products and reports could help analysts produce better products that are focused on the IE. This can lead to the creation of templates and tradecraft checklists for intelligence analysts so that they are better prepared to conduct analysis in support of OIE.

APPENDIX A

Information-Related Capabilities, Operations, and Activities

Table A.1 defines some key joint force IRCs and categories of information-related operations and activities. It reflects the breadth of both the IE and the contexts in which the force relies on information to support OIE. When they were available, we used definitions from the *DoD Dictionary of Military and Associated Terms*.[1]

JP 3-13, *Information Operations*, defines the IRCs and discusses them at length, but it does not provide a comprehensive list of these capabilities. Instead, it includes a list of IRC specialties that is not intended to be all all-inclusive.[2] In Table A.1, the column labeled "IRC" indicates which of these specialties are included in JP 3-13. JP 3-13 goes even further, however, explaining that

> IO is not about ownership of individual capabilities but rather the use of those capabilities as force multipliers to create a desired effect. There are many military capabilities that contribute to IO and should be taken into consideration during the planning process.[3]

Those capabilities are reflected in the "Contributor" column. JP 3-0's list of IRC specialties and contributing capabilities is complemented by the broader list of capabilities, operations, and activities found in JP 3-0, *Joint Operations*, which retains those identified in JP 3-13.

Note that several terms in Table A.1 are used but not defined in the *DoD Dictionary* or otherwise entirely absent from that document. When this occurs, it may mean that the term will no longer be used or that a definition could not be agreed upon but could be included in a subsequent update.

---

1 U.S. Joint Chiefs of Staff, 2020.

2 JP 3-13, 2014, p. II-4.

3 JP 3-13, 2014, p. II-5.

Table A.1
Information-Related Capabilities, Operations, and Activities

Name	Acronym	Definition	Definition Source	IRC (JP 3-13, 2014)	Contributor (JP 3-13, 2014)	Capabilities, Operations, and Activities (JP 3-0, 2018)
Commander's communication synchronization	CCS	A process to coordinate and synchronize narratives, themes, messages, images, operations, and actions to ensure their integrity and consistency to the lowest tactical level across all relevant communication activities.	*DoD Dictionary*			X
Civil-military operations	CMO	Activities of a commander performed by designated military forces that establish, maintain, influence, or exploit relations between military forces and indigenous populations and institutions by directly supporting the achievement of objectives relating to the reestablishment or maintenance of stability within a region or host nation.	*DoD Dictionary*	X	X	X
Cyberspace operations	CO	The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.	*DoD Dictionary*	X	X	X
Combat camera	COMCAM	Specially-trained expeditionary forces from Service-designated units capable of providing high-quality directed visual information during military operations.	*DoD Dictionary*			X
Electronic warfare	EW	Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.	*DoD Dictionary*	X		X
Joint electromagnetic spectrum operations	JEMSO	Those activities consisting of electronic warfare and joint electromagnetic spectrum management operations used to exploit, attack, protect, and manage the electromagnetic operational environment to achieve the commander's objectives.	*DoD Dictionary*		X	
Intelligence		1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities.	*DoD Dictionary*	X	X	

Table A.1—Continued

Name	Acronym	Definition	Definition Source	IRC (JP 3-13, 2014)	Contributor (JP 3-13, 2014)	Capabilities, Operations, and Activities (JP 3-0, 2018)
Information assurance[a]	IA	IA is necessary to gain and maintain information superiority. The [joint force commander] relies on IA to protect infrastructure to ensure its availability, to position information for influence, and for delivery of information to the adversary. Furthermore, IA and [cyberspace operations] are interrelated and rely on each other to support IO.	JP 3-13		X	
Joint interagency coordination group	JIACG	A staff group that establishes regular, timely, and collaborative working relationships between civilian and military operational planners.	*DoD Dictionary*		X	
Key leader engagement[a]	KLE	KLEs are deliberate, planned engagements between US military leaders and the leaders of foreign audiences that have defined objectives, such as a change in policy or supporting the [joint force commander's] objectives.	JP 3-13		X	X
Military deception	MILDEC	Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.	*DoD Dictionary*	X	X	X
Military information support operations	MISO	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.	*DoD Dictionary*		X	X
Operations security	OPSEC	A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities.	*DoD Dictionary*		X	X
Public affairs	PA	Communication activities with external and internal audiences.	*DoD Dictionary*	X	X	X

Table A.1—Continued

Name	Acronym	Definition	Definition Source	IRC (JP 3-13, 2014)	Contributor (JP 3-13, 2014)	Capabilities, Operations, and Activities (JP 3-0, 2018)
Space operations[a]		Space capabilities are a significant force multiplier when integrated with joint operations. Space operations support IO through the space force enhancement functions of intelligence, surveillance, and reconnaissance; missile warning; environmental monitoring; satellite communications; and space-based positioning, navigation, and timing. The IO cell is a key place for coordinating and deconflicting the space force enhancement functions with other IRCs.	JP 3-13		X	X
(Integrated joint) special technical operations[a]	STO	IO need to be deconflicted and synchronized with STO. Detailed information related to STO and its contribution to IO can be obtained from the STO planners at CCMD or Service component headquarters. IO and STO are separate, but have potential crossover, and for this reason an STO planner is a valuable member of the IO cell.	JP 3-13		X	X
Strategic communication[b]	SC or STRATCOM	The SC process consists of focused United States Government efforts to create, strengthen, or preserve conditions favorable for the advancement of national interests, policies, and objectives by understanding and engaging key audiences through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.	JP 3-13		X	

SOURCES: U.S. Joint Chiefs of Staff, 2020; JP 3-13, 2014; JP 3-0, 2018.

[a] Used but not defined in the *DoD Dictionary*.

[b] Not included in the *DoD Dictionary*.

APPENDIX B

Intelligence Product Categories

Outputs from the intelligence process can be categorized into a variety of product types. Each product category, or an informational analog, presents opportunities for intelligence to support IO. In Table B.1 describes and provides examples of products in several intelligence product categories outlined in JP 2-01, *Joint and National Intelligence Support to Military Operations*. The information in the first three columns, "Product Category," "Description," and "Example Products," is from JP 2-01; the fourth column, "IO Relevancy," presents conclusions from our analysis of each product's relevancy to the IO community.

Table B.1
Intelligence Product Categories

Product Category	Description	Example Products	IO Relevancy
General military intelligence (GMI)	GMI is tailored to specific missions and includes information on enemy/foreign forces and pertinent information concerning the OE (political, economic, topographic, geodetic, demographic, and sociological aspects of foreign countries). Increasingly, GMI may become more concerned with non-traditional aspects of the OE to include cultural aspects and cyberspace capabilities.	• Tailored to specific mission: Political, economic, and social aspects of countries in the JOA [joint operations area]. Information on organization, operations, and capabilities of foreign military forces in the JOA. Counterintelligence on foreign intelligence capabilities and activities, as well as terrorism, which impacts the force protection mission • Formats: Military Capabilities Assessment, Military-Related Subject Assessment, Adversary Course of Action Estimate, Foreign Intelligence Threat Assessment	• Part of the foundational intelligence that is required for OIE • Specific sociocultural analysis, target audience analysis, intelligence mission data • MILDEC, OPSEC, MISO, electronic warfare: – Enemy force decisionmaking – Civilian communication infrastructure – Network nodes with the greatest influence
Current intelligence	Current intelligence involves producing and disseminating all-source intelligence on the current situation in a particular area. [It requires] continuous monitoring of world events and specific activities in the CCMD's [area of responsibility].	• Military and political events of interest from joint intelligence operations center (JIOC), joint intelligence support element (JISE), and national sources. Counterintelligence on current foreign intelligence activities • Reports on joint force operations • Summaries and briefings by JIOC, JISE, and national organizations • Open-source intelligence in the JOA	• Short-term shaping operations • WebOps and ongoing shaping operations • Strategic communication and messaging, MISO: – Current content resonating with target audiences – Ongoing flows of information

Table B.1—Continued

Product Category	Description	Example Products	IO Relevancy
Estimative intelligence	Once a basic understanding of the threat and pertinent military-related subjects has been gained, it is necessary to view the situation through the adversary's eyes and consider which COAs [courses of action] are available to the adversary. . . . The intelligence estimate should also contain an assessment of all adversary COAs, especially the adversary's most likely COA and the COA determined to be most dangerous to friendly mission accomplishment.	• Estimates provide forecasts on how a situation may develop and the implications for planning and executing military operations	• IRC running estimates: – Expected changes to decisionmaking – Planned changes to the physical information domain
Warning intelligence	The warning intelligence process analyzes and integrates operations and information to assess the probability of hostile actions and provides sufficient warning to preempt, counter, or otherwise moderate their outcome. The focus of warning intelligence varies at each echelon—from least specific at the strategic level, to most specific at the operational and tactical levels.	• Current intelligence reports from theater assets, theater warning intelligence support, and correlation of force movements in the joint operations area (JOA) • National level provides tip-off and warnings of imminent or hostile activity	• Specific intelligence (geographic, personality, temporal) • WebOps, social media analysis: – Indications that influential nodes are changing behaviors or opinions – Indications that reactions to MISO content have been as expected or not
Target intelligence	Target intelligence portrays and locates the components of a target or target complex, networks, and support infrastructure in support of joint targeting. Specific target intelligence products may include characterizing the target's physical or functional construct, significance, location, vulnerability, and other attributes. Intelligence forms the basis for target analysis and development, tracking and fixing information for moving or perishable targets, and weaponeering.	• Target systems analyses. • Electronic target folders containing target materials describing characteristics of selected targets • Target lists • Combat assessment products	• Enhances understanding of the enemy's decisionmaking cycle • Specific knowledge of enemy thoughts, beliefs, decisionmaking processes • Human factors analysis: – Description of relevant actors to be affected – Methods and messages resonant with target

Table B.1—Continued

Product Category	Description	Example Products	IO Relevancy
Scientific and technical intelligence (S&TI)	S&TI looks at foreign [scientific and technological] developments that have or indicate a warfare potential. This includes medical capabilities and weapon system characteristics, capabilities, vulnerabilities, limitations, and effectiveness; research and development activities related to those systems; and related manufacturing information. S&TI supports the research and development of friendly systems and countermeasures to known or postulated threats.	• Adversary weapon system capabilities and vulnerabilities • Medical capabilities and health services available in the JOA • Potential collateral effects from attacking weapons of mass destruction sites	• Enemy communication technological specifications • Enemy system vulnerabilities to electronic attacks
Counterintelligence (CI)	Multidisciplined CI threat analysis evaluates all foreign intelligence and security services disciplines, terrorism, foreign-directed sabotage, and related security threats. Analysis focuses on the [joint force's] ability to sustain forward operations and protect [its forces].	• Counterintelligence analyzes the threats posed by foreign intelligence and security services and the intelligence activities of non-state actors	• Friendly OPSEC vulnerabilities • Enemy collection capabilities • Friendly cyber vulnerabilities
Identity intelligence (I2)	I2 combines the synchronized application of biometrics, forensics, and [document exploitation] capabilities with intelligence and identity management processes to establish identity, affiliations, and authorizations in order to deny anonymity to the adversary and protect [friendly] assets, facilities, and forces. I2 products result from the collection, analysis, exploitation, and management of identity attributes and associated technologies and processes. All-source analysts fuse identity attributes (biologic, biographical, behavioral, and reputation) and other information and intelligence associated with those attributes collected as a result of information collection tasks.	• Biometric enabled watchlist • Document and media exploitation search results • Forensics studies	• Leadership decisionmaking biases and perceptions • Key individuals central to human networks • Key leaders' cyber presence

SOURCES: Intelligence product categories, descriptions, and example products are derived verbatim from JP 2-01, 2017. Conclusions regarding IO relevancy were generated through our analysis.

References

Army Doctrine Publication 2-0, *Intelligence*, Washington, D.C., July 31, 2019.

Associated Press, "U.S. Bid to Counter ISIS Online Recruiting, WebOps, Inept, AP Finds," CBS News, January 31, 2017. As of February 7, 2020: https://www.cbsnews.com/news/us-bid-to-counter-isis-online-recruiting-webops-inept-ap-finds

Central Intelligence Agency, Public Affairs, *Intelligence in the War of Independence*, Washington, D.C., last updated September 6, 2017. As of February 7, 2020: https://www.cia.gov/library/publications/intelligence-history/intelligence

Chairman of the Joint Chiefs of Staff Notice 3500.01, *2017–2020 Chairman's Joint Training Guidance*, Washington, D.C., January 12, 2017.

Dempsey, Martin E., Chairman of the Joint Chiefs of Staff, *Joint Information Environment White Paper*, Washington, D.C., January 22, 2013. As of February 7, 2020: https://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf

DoD—*See* U.S. Department of Defense.

Echevarria, Antulio J. II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*, Carlisle Barracks, Pa.: U.S. Army War College Press, April 2016.

Executive Office of the President, *National Security Strategy of the United States of America*, Washington, D.C.: White House, December 2017.

Flynn, Michael T., Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Washington, D.C.: Center for a New American Security, January 2010.

Gough, Susan L., *The Evolution of Strategic Influence*, Carlisle Barracks, Pa.: U.S. Army War College, April 2003.

Gray, Carrie, and Edwin Howard, "IO MOE Development and Collection: A Paradigm Shift," *IO Sphere*, Spring 2005.

Harold, Scott W., Yoshiaki Nakagawa, Junichi Fukuda, John A. Davis, Keiko Kono, Dean Cheng, and Kazuto Suzuki, *The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains*, Santa Monica, Calif.: RAND Corporation, CF-379-GOJ, 2017. As of February 7, 2020: https://www.rand.org/pubs/conf_proceedings/CF379.html

Intelligence Community Directive 203, *Analytic Standards*, Washington, D.C.: Office of the Director of National Intelligence, January 2, 2015.

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

Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, July 5, 2017.

Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operating 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 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

Joint Publication 3-60, *Joint Targeting*, Washington, D.C.: U.S. Joint Chiefs of Staff, January 31, 2013.

Joint Publication 5-0, *Joint Planning*, Washington, D.C.: U.S. Joint Chiefs of Staff, June 16, 2017.

JP—*See* Joint Publication.

Marine Corps Doctrinal Publication 2, *Intelligence*, Washington, D.C., incorporating change 1, April 4, 2018.

Mattis, James, Secretary of Defense, "Information as a Joint Function," memorandum, Washington, D.C., September 15, 2017.

Mazarr, Michael J., "The Challenge of the Gray Zone," briefing, U.S. Department of Defense, Strategic Multilayer Assessment Program, Washington, D.C., February 2016.

Metz, Thomas, Mark W. Garrett, James E. Hutton, and Timothy W. Bush, "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," *Military Review*, Vol. 86, No. 3, May–June 2006, pp. 2–12.

Muñoz, Arturo, and Erin Dick, *Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness*, Santa Monica, Calif.: RAND Corporation, PE-128-OSD, 2015. As of February 7, 2020:
https://www.rand.org/pubs/perspectives/PE128.html

Murphy, Dennis M., *Talking the Talk: Why Warfighters Don't Understand Information Operations*, Carlisle, Barracks, Pa.: U.S. Army War College, Center for Strategic Leadership, Issue Paper 4-09, May 2009.

Office of the Director of National Intelligence, *United States Defense Intelligence Strategy*, Washington, D.C., 2019.

Paul, Christopher, "Is It Time to Abandon the Term Information Operations?" *Strategy Bridge*, March 11, 2019. As of February 7, 2020:
https://thestrategybridge.org/the-bridge/2019/3/11/
is-it-time-to-abandon-the-term-information-operations

Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub P. Hlávka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-1925/1-A, 2018. As of February 7, 2020:
https://www.rand.org/pubs/research_reports/RR1925z1.html

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 February 7, 2020:
https://www.rand.org/pubs/research_reports/RR2489.html

Paul, Christopher, Harry J. Thie, Katharine Watkins Webb, Stephanie Young, Colin P. Clarke, Susan G. Straus, Joya Laha, Christine Osowski, and Chad C. Serena, *Alert and Ready: An Organizational Design Assessment of Marine Corps Intelligence*, Santa Monica, Calif.: RAND Corporation, MG-1108-USMC, 2011. As of February 7, 2020: https://www.rand.org/pubs/monographs/MG1108.html

Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018, December 12, 2017.

Sloggett, David, "Intelligence Support to Contemporary Information Operations," *IO Sphere*, Spring 2007.

Spooner, Damian L., *Improving MAGTF Intelligence Support to Information Operations in the Four Block War*, thesis, Quantico, Va.: Marine Corps Command and Staff College, 2010.

U.S. Code, Title 10, Section 164, Commanders of Combatant Commands: Assignment; Powers and Duties.

U.S. Department of Defense, *Department of Defense Strategy for Operations in the Information Environment*, Washington, D.C., June 2016.

———, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018.

U.S. Department of Defense Directive 3600.1, *Information Operations (IO)*, Washington, D.C., incorporating change 1, May 4, 2017.

U.S. Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, Washington, D.C., August 8, 2016.

U.S. Information Agency, *Strategic Plan 1997–2002*, Washington, D.C., 1997.

U.S. Joint Chiefs of Staff, *Joint Concept for Human Aspects of Military Operations (JC-HAMO)*, Washington, D.C., October 19, 2016.

———, *Joint Concept for Integrated Campaigning*, Washington, D.C., March 16, 2018a.

———, *Joint Concept for Operating in the Information Environment (JCOIE)*, Washington, D.C., July 25, 2018b.

———, *DoD Dictionary of Military and Associated Terms*, Washington, D.C., last updated January 2020.

U.S. Senate, Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2018*, Washington, D.C., 2018. As of February 7, 2020: https://www.armed-services.senate.gov/imo/media/doc/FY18%20NDAA%20summary2.pdf

NATIONAL DEFENSE RESEARCH INSTITUTE

Both information operations (IO) and intelligence have long been core components of U.S. military operations, and information is the essence of both communities. What distinguishes them is how each community compiles, sorts, analyzes, and uses information. Gaps in understanding of each community's roles, responsibilities, and processes have important implications for operations in the information environment (OIE), which require a significant degree of coordination between the personnel who provide intelligence support to these operations and the personnel who are responsible for planning and conducting them. To support information operations practitioners, intelligence personnel must be familiar with the types of information that are relevant to OIE. Conversely, information operations practitioners must be familiar with intelligence products and processes for how that information is collected, analyzed, and disseminated.

Despite the recent surge in interest in OIE, there is still not sufficient appreciation across the joint force for what these operations can contribute. As a result, intelligence organizations do not understand intelligence needs for OIE or routinely provide OIE-specific intelligence products, and related requests for intelligence support are not prioritized. This situation is compounded by a lack of awareness of intelligence organizations' processes and requirements among information operations staffs.

A review of guidance, doctrine, and documentation on the information requirements for OIE, along with interviews with subject-matter experts, highlighted 40 challenges to effective intelligence support to OIE, along with 67 potential solutions to address them.

$25.50

ISBN-10 1-9774-0570-3
ISBN-13 978-1-9774-0570-8

www.rand.org

RR-3161-EUCOM