Improving C2 and Situational Awareness for Operations in and Through the Information Environment

Christopher Paul, Colin P. Clarke, Bonnie L. Triezenberg,
David Manheim, Bradley Wilson

RAND
CORPORATION

For more information on this publication, visit www.rand.org/t/RR2489

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0131-1

Published by the RAND Corporation, Santa Monica, Calif.
© Copyright 2018 RAND Corporation
RAND® is a registered trademark.

Cover: U.S. Army photo

Limited Print and Electronic Distribution Rights

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

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

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

Support RAND
Make a tax-deductible charitable contribution at
www.rand.org/giving/contribute

www.rand.org

Preface

This is the final report for a RAND project that identified and refined concepts for organizing for, executing, and supporting command, control, computers, coordination, and intelligence, surveillance, and reconnaissance activities in the information environment (IE). The project's goal was to improve the integration of information operations and information considerations more broadly in military operations to achieve desired effects in and through the IE. The project further considered the organizational implications for meeting the requirements of these concepts at the geographic combatant commands (GCCs).

The observations and findings in this report should be of particular interest to stakeholders in the Joint Staff, the Office of the Secretary of Defense, and the GCCs, particularly in GCC J39 (or equivalent), as well as chiefs of staff and combatant commanders, who ultimately decide how GCC staffs are organized. This report may also be of interest to those responsible for staff organization at the geographic service component commands and in the broader information operations and information-related capability community of practice.

This research was sponsored by the Information Operations Directorate, Office of the Under Secretary of Defense for Policy, and conducted within the International Security and Defense Policy Center of the RAND National Defense Research Institute, 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 Community.

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

Contents

Figures and Tables

Figures

Tables

Summary

Recent operational experiences and Russian information aggression are among the many reasons that the information environment (IE) is ascending as a consideration in the planning, exercise, and conduct of U.S. military operations. Despite this growth in interest in the U.S. Department of Defense (DoD), attention to the IE remains insufficient. Ever-increasing technological sophistication and global adoption of advanced communication networks have rendered the IE more extensive, complicated, and complex than ever before. Efforts to coordinate and conduct military operations in and through the IE are beset with a "fog-of-war" problem not unlike that experienced in the traditional domains of air, land, and sea.

How can U.S. forces maintain situational awareness of the IE? What exactly does situational awareness mean in the context of the IE? Given the difficulties associated with bounding, comprehending, and meaningfully observing even small portions of the operationally relevant IE, what steps must DoD take to be able to effectively assert command and control (C2) and situational awareness over operations in and through the IE, including the ability to organize, understand, plan, direct, and monitor these operations?

Once concepts for C2 and situational awareness are identified, how should they be integrated and implemented at the geographic combatant commands (GCCs)? Which staffs, structures, or organizations should have responsibility for C2 and situational awareness in the IE? At what echelons?

This report identifies and refines concepts for organizing for, executing, and supporting C2 and situational awareness of the IE to improve the integration and execution of military operations, as well as the organizational implications of these requirements for the GCCs.

We pursued two central research questions:

- How should DoD conceptualize C2 and situational awareness of the IE?
- How should DoD organize at the GCC level to maintain C2 and situational awareness of the IE?

Methods and Approach

To answer these questions, we first framed the problem by drawing on our diverse experiences with different aspects of the IE and various defense challenges. An extensive literature and document review revealed conceptual and practical challenges and opportunities related to the IE. We supplemented these sources of information with interviews with stakeholders and subject-matter experts to further refine our definitions of relevant concepts and to identify requirements. We also conducted case studies across the range of military operations and, in the process, both expanded and validated our lists of challenges and requirements.

We conducted more than 30 unstructured interviews with a wide range of defense stakeholders. The interviews were conducted on a not-for-attribution basis, but we sought input from personnel at several GCCs (not just J39/Information Operations staff, but also J2/Intelligence staff and J3/Operations staff), various service component commands, a range of DoD schoolhouses and educational institutions, and several service-level proponency offices, as well as a range of stakeholders within the Office of the Secretary of Defense.

The Importance of the Information Environment

The IE is growing in importance as a consideration across DoD, and the importance of operations in and through the IE is growing, too. Our discussions with subject-matter experts, distillation of the literature, and observations suggest several strong reasons to further promote recognition of the importance of the IE.

What Happens in the IE Does Not Remain in the IE

To paraphrase and invert a phrase popularized by the Nevada Tourism Board, "What happens in the IE does not stay in the IE."[1] Effects and changes in the IE can influence the actions and behaviors of physical actors and systems, which then deliver effects in the various spatial dimensions. This is only noteworthy because military mindsets give primacy to the spatial domains, treating the IE as an afterthought and implicitly assuming that it is its own separate realm of contestation. It does not and cannot work like that. Actions in the spatial domains resonate in the IE, and actions in the IE have consequences in the physical domains. As others have noted,

> In spite of its lack of physical existence, the content and flow of information within a specific geographic area produces real, tangible effects in the physical world and on military forces present in the operating environment.[2]

---

[1] The original phrase is "What happens in Vegas stays in Vegas."

[2] Robert Cordray III and Marc J. Romanych, "Mapping the Information Environment," *IO Sphere*, Summer 2005, p. 7.

One Cannot *Not* Communicate

Foundational work in psychology by Watzlawick, Bavelas, and Jackson rightly noted that one cannot *not* communicate.[3] Every action, utterance, message, depiction, and movement of a nation's military forces influences the perceptions and opinions of populations that witness them, both in the area of operations (firsthand) and in the broader world (second- or thirdhand).[4] Furthermore, actions do speak louder than words, often making the inherent informational aspects of maneuver more important than official communications about those actions.

Every military activity has inherent informational aspects—creating information, changing information, or affecting one or more of the dimensions of the IE, intentionally or otherwise. It would be best if the inherent informational aspects of military operations were planned, coordinated, and intentional rather than left to chance.

War Is Politics by Other Means, and a Great Deal of Politics Takes Place in the IE

"War is politics by other means" is one of the central (and most quoted) principles of Carl von Clausewitz's military thinking.[5] This observation has recurring salience for U.S. military thinking, especially when recent U.S. military efforts "have produced many tactical and operational gains, but rarely achieved desired political objectives and enduring outcomes in an efficient, timely and effective manner."[6]

Enduring strategic outcomes are usually political in nature, and "military power alone is insufficient to achieve sustainable political objectives."[7] Furthermore, politics increasingly takes place in the IE—not just in the cognitive dimension of the IE in terms of the decisionmaking of national leaders and their constituents, but also in terms of the increasing volume of political discourse taking place through social media and mobile technology. Global penetration of technology is increasing, and the available modes of communication associated with that diffusion are increasing, too. Civilian populations in countries that are relevant to U.S. strategic interests have access to more information and a greater variety of conduits than ever before. They also have a greater ability to share their views with their leaders, even in autocratic or other nondemocratic regimes.

---

[3] Paul Watzlawick, Janet Beavin Bavelas, and Don D. Jackson, *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes*, New York: W. W. Norton and Company, 2014.

[4] Christopher Paul, *Strategic Communication: Origins, Concepts, and Current Debates*, Santa Barbara, Calif.: Praeger, 2011.

[5] Carl von Clausewitz, *On War*, J. J. Graham, trans., London: Wm. Clowes and Sons, 1909, chapter 1.

[6] U.S. Joint Chiefs of Staff, *Joint Concept for Human Aspects of Military Operations*, Washington, D.C., October 19, 2016b.

[7] U.S. Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, Washington, D.C., March 16, 2018, p. 4.

Greater attention to the IE could improve DoD's ability to influence political outcomes, through both warfare and other types of activities across the range of military operations.

Defeat Is a Cognitive Outcome

Defeat of an adversary, by whatever mechanism, is a cognitive outcome. Throughout history, very few battles or engagements have concluded with the death or wounding of every combatant on one side or the other, but battles typically conclude with one side being defeated. The accumulated stresses of combat and combatants' perceptions of a situation lead to fear, flight, or surrender. Alternatively, a force's commander perceives the opponent's relative advantages as a battle unfolds and concludes (through cognition) that the cost of continuing will exceed the possible benefits.

Defeat can also be a matter of perspective, something negotiated through the IE. Even if a force suffered more casualties or retreated, if it met all or some of its objectives, it may be able to plausibly claim victory. The objectives on which these claims of success are based may have been loosely defined or specified after the fact, but this may not be an obstacle to victory.[8] Nonstate actors (such as insurgents and terrorist groups) are often adept at turning their tactical failures into strategic successes when they reinterpret the meaning of tactical engagements for their adherents.

As the U.S. Marine Corps capstone doctrinal publication frames it, war is fundamentally a contest of wills.[9] If the goal of warfare is to defeat the adversary's will, then planners must recognize *will* as a variable in the operational environment—one that substantially exists in and is influenced through the IE. Fighting a perceptual, moral, and mental battle in and through the IE to defeat the will of future adversaries will require much greater U.S. attention to the IE going forward than has heretofore been the case. Too often, the joint force focuses on the destruction of enemy capabilities, attacking will only as a second-order consequence of destruction.[10] As then top leaders of the U.S. Army, Marine Corps, and Navy noted in a joint white paper, "War is inarguably the toughest of physical challenges, and we therefore tend to focus on the clash and lose sight of the will."[11]

Adversaries Are Fighting in and Through the IE

A host of state and nonstate adversaries and potential adversaries are already using disinformation, engagement, propaganda, and other efforts in and through the IE to target

---

[8] Gideon Avidor and Russell W. Glenn, "Information and Warfare: The Israeli Case," *Parameters*, Vol. 46, No. 3, Autumn 2016.

[9] Marine Corps Doctrinal Publication 1, *Warfighting*, Washington, D.C., June 20, 1997, p. 7.

[10] U.S. Joint Chiefs of Staff, 2016b.

[11] Raymond T. Odierno, James F. Amos, and William H. McRaven, *Strategic Landpower: Winning the Clash of Wills*, white paper, U.S. Army, U.S. Marine Corps, and U.S. Special Operations Command, October 28, 2013.

and influence the perceptions, opinions, alliances, and decisions of local, regional, and transregional populations.[12] These adversaries and potential adversaries have gained effectiveness by generously resourcing information power and information-related capabilities (IRCs), giving prominence to information effects when planning and executing operations, and integrating physical and informational power.[13]

If the joint force is to counter or compete with these efforts, DoD needs to increase attention to operations in and through the IE.

A Summary of Possible Visions for Operations in and Through the Information Environment: Three Tiers

Chapter Two in this report reviews several emerging concepts and discussions about the IE, along with the older and more traditional literature on information operations (IO) and IRCs. When we considered this literature in light of our discussions with subject-matter experts and stakeholders, we concluded that there are three possible levels or tiers of visions of the future role of information in operations. Each has implications for the C2 and situational awareness requirements for operations in the IE (OIE). The three-tiered framework is shown in Figure S.1.

The tier 1 vision is the legacy view, the antiquated vision that has dogged IO planners in numerous campaigns and operations. Under this vision, operations in and through the IE are an afterthought. The focus of planning and execution is on physical objectives, physical capabilities, and physical effects. The IE and IRCs are considered only to the extent that they can contribute to or support physical capabilities—for example, using information to increase lethality or to disrupt the adversary so it is easier to achieve a physical advantage. The IE is overlooked and ignored at this tier, and when it is considered, it is considered late. Planners complete their work, then invite an information stakeholder to "sprinkle some of that IO stuff" on the plan.[14] This vision is attractive to no one but serves as a reminder of a prior baseline, something to which DoD could return if attention to the IE wanes.

Tier 2 is the realization of what the IO and IRC communities have aspired to offer and what is implied by several of the concepts described in this report. Under this vision, capabilities to conduct operations in and through the IE are embraced as valuable military capabilities. The IRCs are resourced appropriately and used by com-

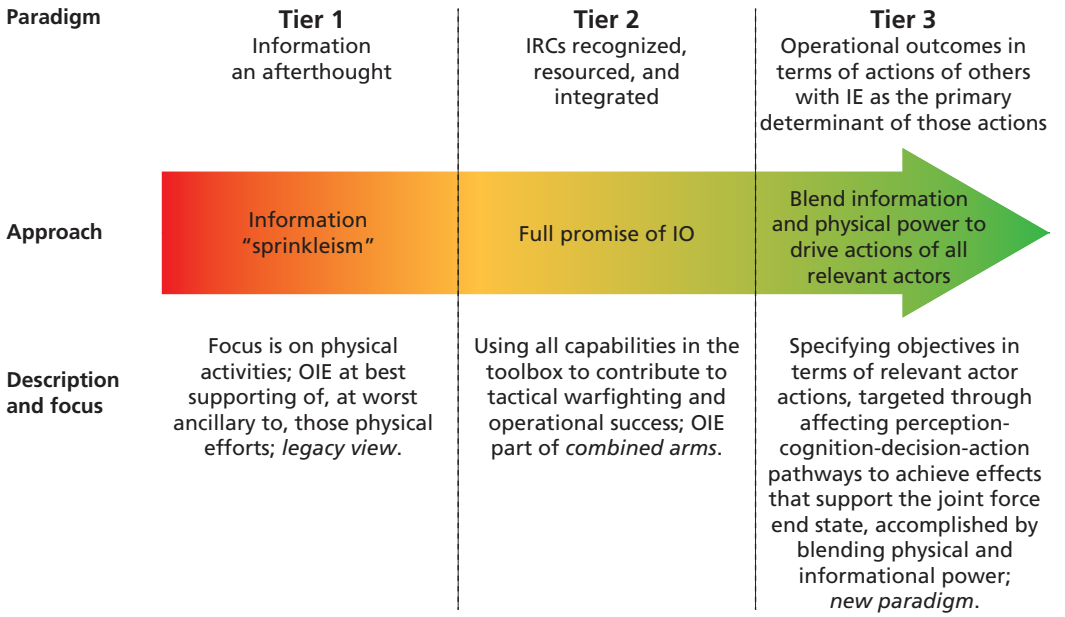
---

[12] U.S. Army, *Unified Quest: Fighting on the Battleground of Perception*, Washington, D.C., October 4, 2016.

[13] Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub 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.

[14] Dennis M. Murphy, *Talking the Talk: Why Warfighters Don't Understand Information Operations*, Carlisle, Pa.: U.S. Army War College, Center for Strategic Leadership, Issue Paper 4-09, May 2009, p. 2.

Figure S.1
Three Tiers of Visions of the Role of Information in Operations



RAND *RR2489-S.1*

manders and planners just like any other military capability. Information and IRCs become just another tool in the commander's toolbox, seamlessly integrated with other tools used to accomplish the mission as part of combined arms. Sometimes, information is *supporting* the main effort, but sometimes information is *supported*, and information is the main effort.

This tier 2 vision is strong. If fully realized, it would represent a significant improvement over the tier 1 baseline, in which information is a secondary or tertiary concern and IRCs are poorly understood, mistrusted, and used only hesitantly or when no other capability could deliver the required effect. However, in our discussions and literature review, we identified a third, deeper vision for operations in and through the IE.

Tier 3 represents a true paradigm shift.[15] Tier 3 encompasses all the characteristics of tier 2: Commanders comfortably employ and integrate physical and informational capabilities as part of combined arms as they pursue their objectives. However, under the tier 3 vision, how those objectives are specified is different. In tier 3, all military objectives are phrased in terms of the desired actions and behaviors of relevant actors; then, all military activities seek to drive, lead, push, herd, cajole, coerce, constrain, persuade, or manipulate relevant actors down perception-cognition-decision-action paths that ultimately lead to those objectives.

[15] Scott K. Thomson and Christopher E. Paul, "Paradigm Change: Operational Art and the Information Joint Function," *Joint Force Quarterly*, Vol. 89, 2nd Quarter 2018.

Getting others to do what one wants is called *influence*, so influence becomes the lingua franca of operational art. Both physical and informational power contribute to influence. (This vision is not a pacifist vision.) Commanders operating under this vision understand that destruction is a powerful form of influence that deprives actors of alternative courses of action. A relevant actor who has been killed has been successfully influenced from performing any undesired behavior ever again. However, short of this most extreme form of influence, there are a host of ways in which physical and informational power can be used collectively to achieve behavioral objectives that (ideally) accumulate to support enduring strategic end states.

Although DoD has not unambiguously committed to the tier 3 vision, there is enough promise and interest in this vision for us to emphasize it here. In identifying requirements for C2 and situational awareness for the IE, we sought to identify requirements necessary to support the tier 3 vision, should DoD choose that path. Tier 2 is wholly included within tier 3, and tier 1 is unattractive to today's military planners. Should DoD's ultimate ambition for operations in and through the IE fall short of tier 3, some of the requirements and criteria discussed in later chapters would see a reduction in relative importance or weight alongside options for meeting those requirements.

The Current State of C2 and Situational Awareness of the IE

When it comes to the IE, the current state of C2 and situational awareness at the GCCs and other major headquarters is underwhelming. Our interviews revealed that the IE is predominantly an afterthought; when it is considered, the emphasis tends to be on noncombatant populations rather than threat or adversarial actors. Commanders and staffs largely fail to appreciate the potential of OIE, IO and the IRCs are generally excluded from battle-oriented processes and procedures, and IE-related displays are virtually negligible on the watch floor and all but absent from the commander's update briefing. OIE are often crowded out by busy (and faster) physical capability–oriented battle rhythms. C2 and situational awareness for OIE are handled in a piecemeal fashion, out of sight of the commander. The IE rarely plays much of a role in exercises, and most staff have limited or no experience with OIE under wartime conditions (even exercises).

Requirements for C2 and Situational Awareness

Numerous conceptual advances related to operations in and through the IE have occurred in recent years or are currently under way. Because of these advances, requirements for operations in and through the IE remain a moving target; subsequent

research on optimal organization may need to consider revised and expanded requirements based on revised and expanded concepts related to operating in the IE.

We identified 17 summary requirements for effective C2 and situational awareness for operations in and through the IE.

Effective C2 for OIE requires

1. understanding the capabilities available to affect the IE (not just IRCs), as well as inherent informational aspects of operations
2. understanding authorities and procedures
3. understanding what you want in the IE (clear goals)
4. knowing what progress toward those goals will look like (assessment)
5. having some concept of how you will get there (logic of the effort)
6. sufficient capacity to staff OIE
7. that OIE are considered in all staff sections and processes
8. that OIE are included/integrated with other operations
9. being able to staff OIE as supported or supporting
10. commander interest in OIE.

Effective situational awareness of the IE requires

11. a responsive and capable intelligence, surveillance, and reconnaissance apparatus
12. adequate observation and collection of intelligence on the IE
13. points of focus narrower than the entire IE
14. commander interest.

Additional organizational requirements for C2 and situational awareness of the IE include

15. the ability to sustain activities under a low-demand steady state
16. the ability to handle steady and contingency states and the ability to transition between the two
17. understanding of the place of IE-related staffs, structures, and organizations in the chain of command/organizational hierarchy.

Analysis of Seven Organizational Alternatives to C2 in the IE

Using the requirements that depend in whole or in part on organizational arrangement, we conducted a provisional analysis of seven organizational alternatives that emerged from our research: "as is" (in the staff); in the staff but more prominent; in the staff but with an element in each directorate; the equivalent of a domain component

command; a subunified command (e.g., theater special operations command); a joint task force (JTF); and a standing JTF or joint interagency task force (JIATF).

Table S.1 presents a summary of our provisional analysis of the seven organizational alternatives against the eight explicitly organizational requirements of the 17 listed on the previous page. In keeping with the provisional nature of the analysis, evaluations of the extent to which each organizational alternative satisfies each requirement is also somewhat provisional. Where the organizational alternative appears to wholly or sufficiently satisfy the requirement, a cell contains a check mark (√). Where the organizational alternative appears to be significantly lacking or likely to fail to sufficiently meet the requirement, the cell contains an X. Where the organizational alternative partially satisfies the requirement criteria, the cell is marked with a ½. These three scoring levels are always ordinal to each other; that is, a check is always better than a ½, which is always better than an X. However, we acknowledge the potential for unscored variation within the categories: some halves may be better than others, though still falling short of wholly meeting the requirement, and some Xs may be worse than others, with some being merely inadequate while others are complete failures. Fine-grained comparison within a given level requires care or perhaps additional analysis. Finally, a question mark (?) indicates "it depends." This score appears only in the column for the requirement "Commander attentive to OIE," which under three of the alternatives is wholly dependent on the proclivities of the individual commander; under the four other alternatives, the commander is exclusively and specifically responsible for the OIE and so is organizationally constrained to be attentive to it.

Each of the seven organizational alternatives has different strengths and weaknesses. This provisional analysis does not unambiguously endorse any of the alternatives as the obvious solution for every GCC. It does, however, provide useful decision support for any GCC. Any GCC considering how to organize for C2 for OIE should first consider the relative importance of the eight requirement criteria within the context of its command. An organizational alternative that satisfies the most important of those criteria (recognizing that priorities may vary across GCCs)—and satisfies other organizational criteria (such as cost-efficiency, organizational consistency, or commander preference)—should be strongly considered.

Further Insights from the Research

This report documents a range of other challenges related to C2 and situational of the IE. Our observations and analyses produced the following additional insights.

Doctrine Can Support Improved Practice

There is a gap between emerging concepts for operations in and through the IE and current practice at the GCCs and other commands. However, our review of relevant

Table S.1
Summary of Provisional Organizational Analysis

	Alternatives						
Criteria	**As is**	**In the staff but more prominent**	**In the staff, with an element in each directorate**	**Equivalent of domain component command**	**Subunified command**	**JTF**	**Standing JTF or JIATF**
Commander attentive to OIE	?	?	?	√	√	√	√
Sufficient capacity to staff OIE	X	½	½	√	√	√	√
OIE considered in all staff sections and processes	X	½	√	√	√	√	√
OIE included/ integrated with other operations	½	√	√	√	½	√	X
Able to staff OIE as supported or supporting operations	X	½	√	√	√	√	X
Able to handle steady-state and contingency operations	X	½	√	√	√	X	X
Able to function in low-demand steady state	√	½	√	X	X	X	X
Understood/ accepted place in chain of command/ organizational hierarchy	√	√	½	X	½	½	X

NOTE: √ indicates that the organizational alternative wholly or sufficiently satisfy the requirement. X indicates that the organizational alternative is significantly lacking or likely to fail to sufficiently meet the requirement. ½ indicates that the organizational alternative partially satisfies the requirement criteria. ? indicates that the ability to meet the requirement depends on any of a number of factors.

doctrine found that many existing processes could easily accommodate a greater focus on the IE.

For example, the joint operation planning process described in Joint Publication (JP) 5-0 provides ample opportunity to consider the IE and plan for operations in and

through it.[16] The process also provides an opportunity to completely ignore the IE. If the commander's guidance to initiate planning at the beginning of the operational design process includes an interest in the IE, then everything that follows (including problem framing, specification of objectives and military end state, and courses of action developed) can also be mindful of the IE and its role in the planned effort. With the simple addition of the IE as a consideration, the other elements of the planning process can accommodate it.

Similarly, while numerous stakeholders reported to us that intelligence support for planning and operations in and through the IE is inadequate, it is our view that this is due to practice (especially habit and priorities) rather than a lack of opportunity in doctrine. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, includes numerous hooks amenable to greater inclusion of the IE and OIE-relevant considerations.[17]

Other aspects of other doctrinal processes may need more substantial adjustment in order to incorporate OIE.

C2 and Situational Awareness of the IE Face Huge Seams

Both C2 and situational awareness of the IE face significant seams—areas that either overlap with or fail to cover the roles and responsibilities of those tasked with conducting operations in and through the IE. First, there is the issue of whether C2 and situational awareness are functionally aligned to operate in the IE alone or as part of broader (and more kinetic) operations. Second, there is a substantial difference between undertaking steady-state OIE and undertaking OIE as part of broader crisis or contingency operations. Third, baseline steady-state OIE will be far different from operations that set the conditions for future contingencies. Fourth, there are differences between integrating the IE into deliberate planning versus integrating the IE into rapid-reaction planning. Fifth, C2 and situational awareness of the IE need to be able to handle and move between operating against a nation-state and operating against violent nonstate actors, as well as working together with non-adversaries in a range of situations and scenarios. As the world moves further into the information age, the capabilities of both state and nonstate actors to operate in and through the IE are only growing.[18] Sixth, and finally, there are also seam issues when operating with partners, whether interorganizational, interagency partners, international, or multinational partners.

---

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

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

[18] William R. Gery, SeYoung Lee, and Jacob Ninas, "Information Warfare in an Information Age," *Joint Force Quarterly*, Vol. 85, 2nd Quarter, 2017, p. 24.

Situational Awareness Solutions Are Not One-Size-Fits-All

In reviewing the literature and discussing current and possible practice for situational awareness of the IE with stakeholders, we were struck by the diversity of possibly useful information about the IE. Not only does the IE have three dimensions (the cognitive, the informational, and the physical), but there is also considerable variation in context (the IE as relevant to a specific geographic area or region, or for a specific actor or audience of interest), and considerable variation in interest, depending on the types of missions, operations, or activities on which a specific command might focus. For example, one command might be interested in monitoring social media networks for expressions of support for violent extremists (as indicators of supportive behavior toward terrorist organizations or as possible routes to radicalization or recruitment). Another might be interested in aggressor-nation propaganda and its impact on democratic participation and perceptions of government legitimacy among citizens in an allied country. Yet a third command might be watching potential aggressor command networks for indications that deterrence is failing and the aggressor intends to launch an invasion. A fourth may be interested in permutations of all three of the previous examples.

Supporting this insight is the observation that a command cannot know everything about the IE. There is simply too much that could be known. Any plan for situational awareness that aspires to track and present everything about the IE will collapse under its own weight. Instead, command staffs must identify the elements of the IE that are relevant to their missions and responsibilities, then tailor presentations and visualizations (and supporting data collection and analyses) accordingly.

Recommendations

Based on these conclusions and the detailed findings of this research, we make six recommendations.

First, *DoD should make changes across doctrine, processes, education and training, and tactics, techniques, and procedures to appropriately emphasize the importance of OIE and the role of OIE in combined arms and multidomain operations*. Addressing many of the gaps, shortfalls, and requirements that we identify in this report demands greater understanding of the IE, new concepts for OIE, and details of IRCs across the joint force. This understanding must be inculcated in junior officers as they progress through their careers to senior staff and command positions. These processes and the necessary appreciation and understanding must be introduced in training and education, and they should be routinized and standardized in doctrine and procedures.

Second, building on the first point, *DoD should make OIE an integral part of joint force staffing and operations—always*. If DoD aspires to the tier 3 vision shown in Figure S.1, under which all operations are conceived of as seeking to shape the behaviors of relevant actors to achieve enduring strategic outcomes, then influence must

become the lingua franca of operational art. Existing doctrine and practice include *opportunities* to consider the IE, should the commander and staff be so inclined. We recommend changes to doctrine and processes that make consideration of the IE and articulation of problems and objectives in terms of relevant actor behavior *compulsory*.

Third, when GCCs decide how to staff and organize for C2 of the IE, they should *choose C2 structures that align with priorities in the specific theater*.

Fourth, when preparing presentations or visualizations of the IE, *match visualizations to specific situations or operations and specific commanders*. Do not expect one-size-fits-all situational awareness or presentational solutions for the IE; it is too complex, diverse, and extensive.

Related to the fourth point, we recommend that *visualization tools offer a host of default options to help ensure that at least one meets any given contextual need*. No single combined information overlay or display of the IE will be sufficient in all areas of operations and all types of missions. Instead, where possible, display and visualization designers should offer numerous customizable layouts so that end users do not have to start from scratch and can easily consider a range of possible displays, select the visualization that best meets their needs, and then refine or customize it as required.

Finally, we recommend that the DoD intelligence apparatus and the supporting intelligence community *refocus existing capabilities and develop new capabilities to better observe the IE, with a particular emphasis on the proclivities, intentions, and decisionmaking processes of relevant actors*. New ways of operating and a new emphasis on operating in and through the IE require a new understanding of the operational context. The exact details of the changes and improvements required will need further research or experimentation.

Acknowledgments

We wish to thank our various points of contact and interlocutors in the sponsoring office: Rob Presler, John Zabel, Gerald Miller, COL Michael Lwin, COL Scott Thomson, and LTC Jason Cullinane. We further extend our thanks to the various staff officers and civilians we spoke to at the combatant commands, joint task force headquarters, supporting components, and other elements that we visited. The terms of our interviews protect your anonymity, but you have our gratitude nonetheless. At RAND, Maria Falvo provided invaluable administrative support to this effort. We also appreciate the thoughtful comments provided by the quality assurance reviewers of this report, Arturo Muñoz and Edward Fisher of the DoD Information Operations Center for Research at the Naval Postgraduate School. We are also grateful to the RAND editorial team, Matt Byrd, Babitha Balan, Lauren Skrabala, and Katherine Wu, who put this report into its final form. Any errors or omissions that remain are the responsibility of the authors alone.

Abbreviations

AGI	artificial general intelligence
AI	artificial intelligence
ANI	artificial narrow intelligence
AOR	area of responsibility
C2	command and control
C4ISR	command, control, communication, computers, intelligence, surveillance, and reconnaissance
CIO	combined information overlay
CVE	countering violent extremism
DoD	U.S. Department of Defense
FM	field manual
GCC	geographic combatant command
GPS	Global Positioning System
HA/DR	humanitarian assistance/disaster relief
iCOP	integrated common operating picture
IE	information environment
IO	information operations
IRC	information-related capability
ISR	intelligence, surveillance, and reconnaissance
JC-HAMO	Joint Concept for Human Aspects of Military Operations
JCIC	Joint Concept for Integrated Campaigning

JCOIE	Joint Concept for Operating in the Information Environment
JIATF	joint interagency task force
JOPP	joint operation planning process
JP	joint publication
JTF	joint task force
MADCOM	machine-driven communication
MCO	major combat operations
MOC	Marine Corps Operating Concept
NASIC	National Air and Space Intelligence Center
OIE	operations in the information environment
OODA	observe, orient, decide, act
TSOC	theater special operations command

CHAPTER ONE

Introduction, Research Questions, and Research Approach

For many reasons—including recent operational experiences and Russian information aggression—the information environment (IE) is an increasingly prominent consideration in the planning, exercise, and conduct of military operations. However, levels of interest in and attention to the IE across the U.S. Department of Defense (DoD) remain insufficient. Ever-increasing technological sophistication and global adoption of sophisticated communication networks have rendered the IE more extensive and complex than ever before. The result is that efforts to coordinate and conduct military operations in and through the IE are beset with a "fog-of-war" problem not unlike that experienced in the traditional domains of land, sea, and air.

Can U.S. forces maintain situational awareness in the IE? What exactly does *situational awareness* mean in the context of the IE? Given the difficulties associated with bounding, comprehending, and meaningfully observing even small portions of the operationally relevant IE, what steps must DoD take to effectively assert command and control (C2) and situational awareness over operations and activities in or through the IE?

Once C2 and situational awareness in this space are defined, how should they be integrated and implemented at the geographic combatant commands (GCCs)? Furthermore, which staffs, structures, or organizations should be responsible for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) in the IE? At what echelons?

This report is part of a RAND project that identified and refined concepts for organizing for, executing, and supporting C2 and situational awareness to improve and support the integration and execution of military operations in and through the IE. The project further considered the organizational requirements for effectively integrating these concepts at the GCCs.[1]

[1] The decision to focus this analysis at the GCC level was made in coordination with our project sponsors in the Office of the Secretary of Defense and a result of resource constraints. Organizational and practical considerations for lower echelons could be the subject of future research, as suggested in Chapter Six.

We pursued answers two central research questions:

- How should DoD conceptualize C2 and situational awareness of the IE?
- How should DoD organize at the GCC level to maintain C2 and situational awareness of the IE?

Research Approach

To answer these questions, we first framed the problem by drawing on our diverse experiences with different aspects of the IE and various defense challenges. From there, we conducted an extensive literature and document review, which revealed both conceptual and practical challenges and opportunities related to the IE. We supplemented this review with interviews with stakeholders and subject-matter experts to further refine the concepts examined in this study and to help identify requirements. Brief case studies across the range of military operations allowed us to both expand and validate lists of challenges and requirements.

We conducted more than 30 unstructured, not-for-attribution interviews with a wide range of defense stakeholders. We sought input from personnel at several GCCs (including J39, Information Operations; J2, Intelligence; and J3, Operations), service component commands, DoD schoolhouses and educational establishments, and service-level proponency offices. We also spoke with a range of stakeholders in the Office of the Secretary of Defense.

Organization of This Report

The remainder of this report defines the concepts that were central to this study and describes challenges and solutions to DoD's need to better organize for operations in and through the IE. Chapter Two defines the IE and the related lexicon, presents a number of perspectives on the IE, justifies the importance of operations in and through the IE to DoD's mission, and details new conceptual developments related to the IE. Chapter Three describes current concepts and practices for C2 and situational awareness—first for the spatial domains and then as specific to the IE. Chapter Four enumerates requirements for effective C2 and situational awareness for operations in and through the IE. Chapter Five presents a provisional analysis of the ability of each of seven organizational alternatives to meet requirements at the GCC level, as identified in Chapter Four. Chapter Six presents our conclusions and recommendations. An appendix discusses automation, machine learning, and computational propaganda to inform DoD efforts to advance these capabilities in support of C4ISR.

CHAPTER TWO

What Is the Information Environment, and Why Is It Important?

Before considering concepts or organizational structures for C2 and situational awareness in the IE, it is important to address some foundational questions. What is the IE, and how should we think about it? What role does the IE play in joint force operations, and how should we think about that? Is the role of the IE in joint force operations significant enough that C2 and situational awareness actually matter? This chapter prepares the necessary groundwork for answering these questions by examining different ways to conceive of and define the IE. It then turns to the DoD lexicon of terms related to the IE. This is followed by a discussion of the ways in which the IE is operationally relevant to the joint force. We conclude this chapter with a brief review of recent and emerging concepts related to the IE within DoD.

Conceptions of the Information Environment

The domains in which military operations take place, as defined in U.S. doctrine, are primarily physical. The earliest wars were fought in the land domain, but as technology progressed, warfare expanded to the sea, then the air, and then to space. Forces operating in these domains move around them at calculable rates of speed, and force elements have relative positions. Each domain has intuitive positional advantages (such as "the high ground") and physical boundaries (albeit sometimes fuzzy). The IE is different, and although we speak and write about information warfare, the IE has yet to be defined as a warfighting domain in U.S. military doctrine.

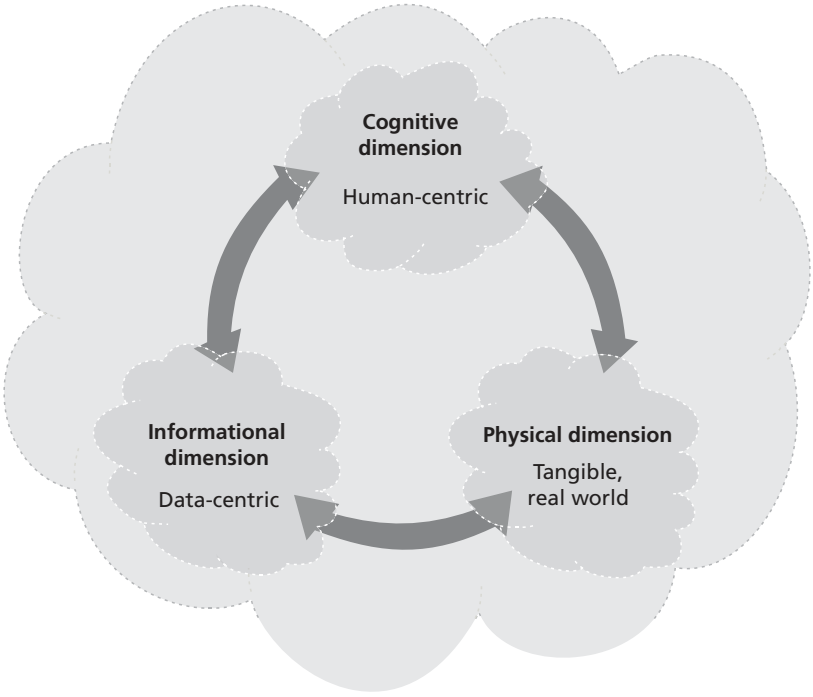
We largely cannot reach out and touch the IE. Targets in the IE include human perceptions or behaviors: Weapons are ideas, and defenses are norms, beliefs, and traditions. If we think of conflict as requiring both the means and the will to engage the enemy, the *domains* of warfare are primarily concerned with *means*, while the *IE* is primarily concerned with influencing the *will* to act. Given that the IE does not conform to spatial boundaries, it is difficult to conceptualize it visually and verbally. In this section, we review four ways that the IE can be conceptualized and explore how those concepts clarify dynamics of will and decisionmaking.

A Doctrinal View of the IE

Joint Publication (JP) 3-13, *Information Operations*, depicts the IE as three interrelated "dimensions" (see Figure 2.1): physical, informational, and cognitive.[1] The cognitive dimension is at the top, perhaps implying a dependency on the lower two dimensions, informational and physical. In fact, the formal definition of the cognitive dimension states that it is the most important component of the IE:

> The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Defining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision

Figure 2.1
The IE as Conceptualized in JP 3-13



SOURCE: JP 3-13, 2014, Figure 1-1.
RAND *RR2489-2.1*

[1] Joint Publication 3-13, *Information Operations*, Washington D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014, p. I-2.

> maker and create the desired effects. As such, this dimension constitutes the most important component of the information environment.[2]

Interestingly, the definition of the physical dimension includes humans but not human decisions:

> The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries.[3]

Finally, the definition of the informational dimension covers the means by which information flows, which can also be human-based.[4] The formal definition is as follows:

> The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information.[5]

When adding a "target audience" to the diagram in Figure 2.1, JP 3-13 shows the human target as enclosed within the triangle formed by the cognitive, informational, and physical dimensions. As conceptualized in this manner, the IE is an environment that both shapes and confines the target audience. Both the IE and its dimensions are notionally depicted as clouds. The cloud symbol might communicate several characteristics of the IE: (1) that its boundaries are soft and, perhaps, changeable; (2) that its impact is largely cognitive (i.e., it concerns the realm of the mind); and (3) that it is ephemeral and has unclear physical boundaries.[6]

With this doctrinal overview of the IE in mind, we next examine how the IE is conceptualized in three different disciplines: by the behavioral influence analyst whose focus is primarily on the cognitive dimension, by the knowledge management scientist

---

2 JP 3-13, 2014, p. I-3.

3 JP 3-13, 2014, p. I-2.

4 All three of the dimensions of the IE can be human-developed, but even the cognitive dimension could also include automated decisionmaking through artificial intelligence (AI) or other forms of autonomy. See the extended discussion in the appendix for more on this topic.

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

6 Rebecca Rosen hypothesizes that clouds "get traction as a metaphor because they are shape shifters, literally" (Rebecca Rosen, "Clouds: The Most Useful Metaphor of All Time?" *The Atlantic*, September 30, 2011).

whose focus is primarily on the infomational dimension, and, finally, by a strategic decisionmaker whose primary focus is not the IE at all.[7]

Behavioral Influence Analysis View of the IE

The National Air and Space Intelligence Center (NASIC) offers a behavioral influence analysis view of the IE.[8] Behavioral influence analysis ultimately seeks to assess and draw conclusions about a target's decisionmaking. Specifically, analysts want to know *who* is an appropriate target and *what factors* influence the target's decisionmaking, such as worldview, cultural experience, and social identity. Furthermore, *why* would a particular target behave in a particular way as a result of, for example, motivations or behavioral norms. Behavioral influence analysis also considers *how likely* a particular target is to choose one behavior over other possible behaviors. In this respect, behavioral influence analysis is squarely aimed at understanding the cognitive dimension of the IE from the cultural or societal level to the highly personal level of the individual decisionmaker. Like JP 3-13 (Figure 2.1), NASIC conceives of cognitive dimension analysis as a triangle, as shown in Figure 2.2. However, the target audience in this case is not confined to the IE but is, rather, at the point of the triangle. Conceptually, behavioral influence analysis in the IE focuses on understanding a target's position and features in the cognitive dimension and seeks to assess influences on organization, group, and individual decisionmaking.

Figure 2.2 recognizes that individuals are the core unit of the groups, organizations, societies, and cultures that surround them. The lines between the domains are wavy to convey that boundaries are fluid. Analysts are instructed to consider these domains as holistically as possible while managing the potentially overwhelming amount of data available at any level on any particular target.

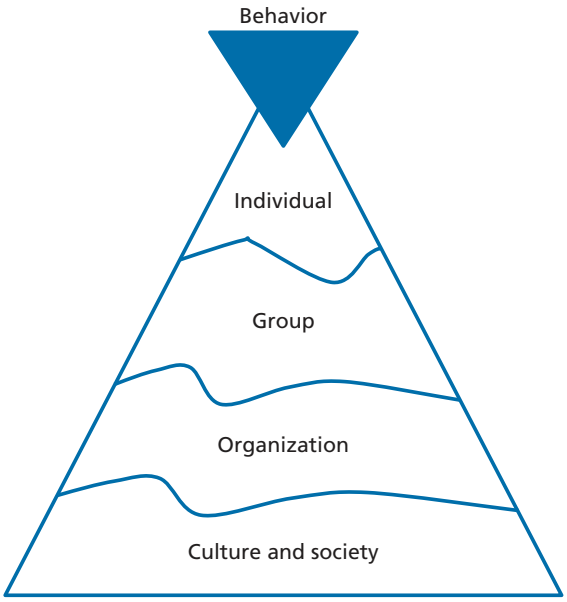
This concept of analysis relates to the physical, informational, and cognitive dimensions in JP 3-13 in that the physical and information dimensions supply tangible indicators that are then interpreted to assess the cognitive dimension.

---

[7] Although all these analytic disciplines consider the whole of the IE, each emphasizes a different dimension. The IE is a complex concept; developing an understanding of views that emphasize each dimension may give us a more nuanced view of the whole. In addition to the views discussed in this section, we reviewed concepts from Richard A. Poisel, *Information Environment and Electronic Warfare*, Norwood, Mass.: Artech House, 2013; Martin C. Libicki, *What Is Information Warfare?* Washington, D.C.: National Defense University, August 1995; Marc J. Romanych, "A Theory-Based View of Information Operations," *IO Sphere*, Spring 2005; Robert Cordray III and Marc J. Romanych, "Mapping the Information Environment," *IO Sphere*, Summer 2005; Thomas H. Davenport and Laurence Prusak, *Information Ecology: Mastering the Information and Knowledge Environment*, Oxford, UK: Oxford University Press, 1997; and Jandria S. Alexander, "Achieving Mission Resilience for Space Systems," *Crosslink Magazine*, Spring 2012.

[8] Beth Waina, National Air and Space Intelligence Center, "Behavioral Influences: Mission, Methodology and Analysis," presentation at the RAND Corporation, Santa Monica, Calif., October 7, 2016.

Figure 2.2
Domains of Analytic Interest in Behavioral Influence Analysis



SOURCE: Waina, 2016.
RAND *RR2489-2.2*

Knowledge Management View of the IE

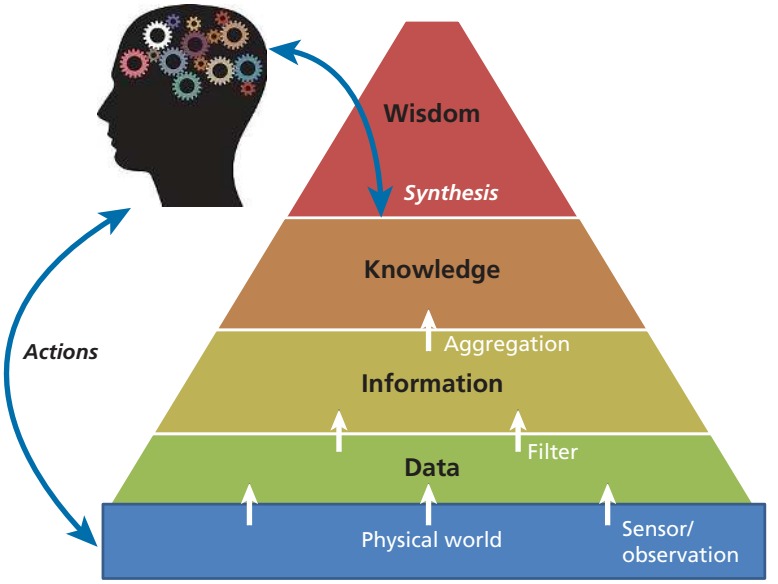
While the behavioral influence analysis view is focused on cognition driving behavior, the knowledge management view considers how data drive action. NASIC's concept seeks to explain how human and social influences ultimately shape an individual's decisionmaking. The knowledge management perspective focuses on how the processing and shaping of information can affect individual decisionmaking.

The knowledge management scientist describes the dynamics of the IE as a "closed-loop" process in that an individual is able to observe how past actions influence future decisions and actions. The processing of data to inform decisions is hierarchical, as shown in Figure 2.3. Data from the physical world are first sensed and filtered to produce information, then aggregated to produce knowledge, and, finally, synthesized to produce wisdom.[9] Actions taken according to that wisdom then alter the physical world, producing new data.

Like the previously discussed concepts of the IE, the knowledge management view again takes the form of a triangle. This visual theme implies something important about the IE. In the words of Army manual ATP No. 6-01.1, "The volume of available

[9] Milan Zeleny was one of the first to articulate these principles, commonly known as the DIKW (data, information, knowledge, and wisdom) or wisdom hierarchy. See Milan Zeleny, *Human Systems Management: Integrating Knowledge, Management and Systems*, Hackensack, N.J.: World Scientific, 2005.

Figure 2.3
Knowledge Management View of the IE



SOURCE: Based on Zeleny's model of knowledge management (Zeleny, 2005).
RAND *RR2489-2.3*

information makes it difficult to identify and use relevant information."[10] At each step in the process, some data are discarded and may be replaced with newly filtered, aggregated, or synthesized data. This process of discarding and creating information, which we call *synthesis*, is shaped by both physical and social/human factors. For example, data filtering may occur because we did not have the right sensor at the right place and time, but it can also occur when we reject data that do not fit our preconceived notions of the world. Furthermore, the process of synthesis affects both the target audience and the analyst who is trying to understand or influence that target audience. Conceptually, some mechanism must be used to reduce the breadth and complexity of the IE to produce cognition, behaviors, or actions, respectively, as denoted by the triangle structure in the doctrinal, behavioral influence analysis, and knowledge management views.

A Strategist's View of the IE

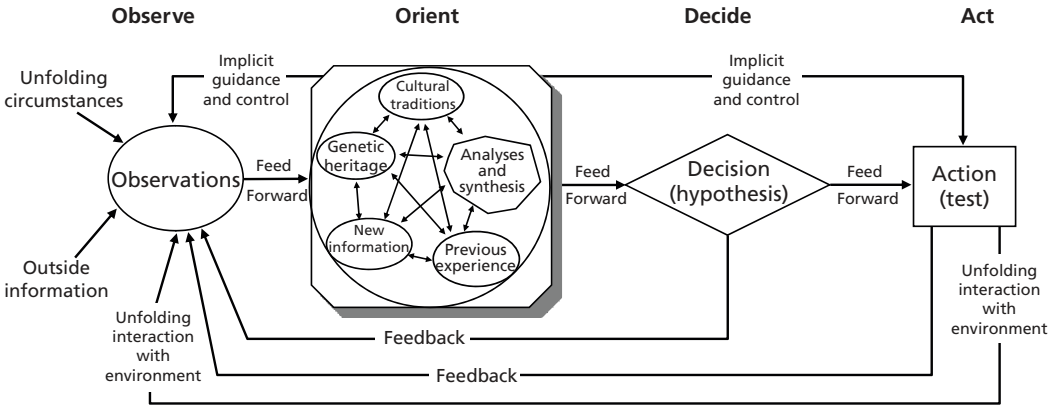
This final view of the IE comes from the physical world of fighter pilots. It shows the IE in the context of warfare in the air domain, as interpreted by John Boyd in his observe, orient, decide, act (OODA) loop of strategic decisionmaking. Like the knowl-

[10] Army Techniques Publication 6-01.1, *Techniques for Effective Knowledge Management*, Washington D.C., March 2015, p. vi.

edge management view, it is a closed-loop process, but, according to Boyd, it adapts as we try new things and rapidly learn based on feedback from the physical environment. The diagram in Figure 2.4 is the only known instance in which Boyd drew the model. Although Boyd described the OODA loop in simple terms, the diagram reveals a complex process that depends on "heritage, cultural traditions, and previous experiences" to develop an implicit repertoire (shown as *guidance and control*) of what he called *psychophysical* skills—automatic responses to unfolding circumstances.[11] In this way, the OODA loop acknowledges the importance of the cognitive dimension of the IE to what subsequently happens in the relevant spatial domain.

The first steps in OODA are to observe the environment and then to orient—that is, to "find one's position in relation to unfamiliar surroundings."[12] Orientation is followed by a decision to either act or integrate new information into one's thought processes (to develop a hypothesis), which is later tested. In later work, Boyd described the OODA process as a "continuing whirl of reorientation, mismatches, analyses/synthesis [that] enables us to comprehend, cope with, and shape as well as be shaped by the novelty that literally flows around and over us."[13] While operations in the IE tend to have a slower pace or cadence than fighter jet operations, the novelty, complexity, and closed-loop process are relevant to any discussion of operations in the IE. Perhaps more

Figure 2.4
A Strategist's View of the IE



SOURCE: J. Boyd, 2010, p. 3.
RAND *RR2489-2.4*

[11] John R. Boyd, *The Essense of Winning and Losing*, Washington, D.C.: Project on Government Oversight, August 2010, p. 1. Boyd's original version of the briefing dates to 1995 or 1996. He passed away in 1997 and there have since been several efforts to compile his briefings and and other unpublished materials in online archives.

[12] Oxford Dictionaries, *Orient*, webpage, Oxford University Press, undated 2017.

[13] John R. Boyd, *Conceptual Spiral*, Washington, D.C.: Project on Government Oversight, November 2011, p. 28. Boyd presented the briefing in 1992.

importantly, Boyd's description of orientation as the outcome of shaping observations through the prism of human and social factors echoes the behavioral influence analysis view of the IE, shown in Figure 2.2.

Lexicon Related to Military Activities in or Through the IE

This report is about C2 and situational awareness in DoD operations in and through the IE. There is a diverse and growing collection of terms used to talk about such efforts. Although we prefer *operations in and through the IE* for its specificity, in this section, we present and critique the available lexicon. This discussion differentiates among *information operations (IO)*, *information-related capabilities (IRCs)*, *operations in the IE*, *IE operations*, *maneuver in the IE*, and *information warfare*.

Information Operations

The first term that likely comes to mind when imagining military activities in and through the IE is *information operations*. The common-sense and colloquial understanding of *information operations* takes the term at face value, assuming that information operations are *operations* that have something to do with *information*. This common-sense understanding further suggests that IO personnel are operators who engage in these operations by employing information in some manner. This makes perfect sense, but it is not what *IO* is supposed to mean (and therein lies the problem).

IO, as formally described and practiced, is a planning, coordinating, and integrating function. In other words, it is a staff function, overseen by a staff officer, who integrates the efforts of IRCs (next in our lexicon list)—efforts that are then executed by IRC personnel. These activities (or operations) should probably be called *information-related capability executions* or described by one of the other, newer terms in the lexicon. Unfortunately, such efforts have traditionally been (and will likely to continue to be) colloquially mislabeled as *information operations*.

The relationship between the planning and integrating function known as *information operations* and actual operations using information is certainly similar to the relationship between *fire support coordination* and *fires*. Each pair of terms describes a staff function and a capability to execute or operate that function. But no trained member of the joint force would ever conflate fire support coordination with fires or expect a fire support coordination officer to leave a command post, travel to an artillery battery, and lay a gun. However, members of the joint force routinely conflate information operations as a coordinating and integrating function with the execution of any effort in the IE (collectively and incorrectly referred to as *information operations*). They might well expect a staff officer whose task is planning and integration to go and lay out a storyboard for leaflets, get on a computer and do some cyber reconnaissance, or otherwise execute IRC tasks as part of operations (because, *operations*).

Not only does the current colloquial use of *information operations* confuse the relationship between the planning and integration function and the actual execution of efforts in and through the IE, but the term is often used as shorthand for psychological operations/military information support operations.[14] This ignores the rest of the traditional IRCs and the inherent informational aspects of other military activities, including the presence, posture, and profile of deployed forces. Worse, a 2017 report by Facebook (which likely has a much larger readership than most DoD doctrinal publications) on false news and disinformation defined *information operations* as "actions taken by organized actors (governments or nonstate actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome."[15] This definition promotes an understanding of information operations that is inconsistent with both the colloquial and the formal DoD usage—and one that is quite pejorative. DoD would not want the joint force's use of the phrase *information operations* to invoke the Facebook report's definition for the wider public.

Because of these concerns, we limit our use of *information operations* throughout and cite it only in its narrow, denotatively correct sense to describe a planning and integrating function.

Information-Related Capabilities

Less often misused than *information operations*, but not wholly without contentiousness, is *information-related capability*. An IRC is doctrinally defined as "[a] tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions."[16]

This is a perfectly reasonable and usable definition, except it lacks clear boundary conditions. Almost anything members of the joint force do or say can send a message or otherwise affect the IE, so almost anything could be an IRC, depending on circumstances and consequences. This lack of clear boundaries is a problem. Some stakeholders do not want to think about or have their capability coordinated or deconflicted as an IRC.

While the joint definition is intentionally unbounded, certain capabilities are traditionally considered *information-related*. In fact, past IO doctrine listed five core capabilities alongside a number of supporting and related capabilities.[17] The traditional core capabilities were psychological operations/military information support operations, military deception, operations security, electronic warfare, and cyber operations.

---

[14] Curtis D. Boyd, "Army IO Is PSYOP: Influencing More with Less," *Military Review*, May–June 2007.

[15] Jen Weedon, William Nuland, and Alex Stamos, *Information Operations and Facebook*, version 1.0, Menlo Park, Calif.: Facebook, 2017.

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

[17] See Christopher Paul, *Information Operations Doctrine and Practice: A Reference Handbook*, Westport, Conn.: Praeger, 2008.

The listed supporting or related capabilities included public affairs, civil-military operations, defense support to public diplomacy, information assurance, physical security, physical attack, counterintelligence, and combat camera. Contemporary lists cite all of the above as IRCs. Service-specific materials have further listed key leader engagement and special technical operations as IRCs. Australian Army concepts have additionally included presence, posture, and profile in this category.[18]

Every action and utterance of the force can communicate a message or otherwise affect the IE, so we embrace the broad conception of IRCs and do not subscribe to specific or constrained lists.[19] Under this conception, some capabilities are *always* and only information-related, as their effects are only ever in or through the IE. Other capabilities are *sometimes* or *secondarily* information-related; they are often used for other purposes and capable of having effects independent of the IE. Pretty much any DoD capability could be included in that second category under certain circumstances. This conception does include a C2 challenge related to the IE, however. If any capability can be information-related and affect the IE, then the necessary scope of C2 is accordingly broader.

Operations in the IE

Relatively new on the lexical scene is the term *operations in the information environment*. The term was first embraced by DoD in the 2016 *Department of Defense Strategy for Operations in the Information Environment*.[20] A related term is embedded in the title of the *Joint Concept for Operating in the Information Environment*, still in draft form at the time of this writing. Interestingly, neither source defined *operations in the information environment* as its own term of art. Both define *IE* according to the doctrinal definition cited earlier in this chapter (consisting of three interrelated dimensions: physical, informational, and cognitive). Both then allow the standard definition of *operations* or *operating* to precede it, without any additional definitional discussion. We admire the implied simplicity: Once you have defined the IE, these are the operations you undertake there.

IE Operations

The same words are used in a slightly different construction by the U.S. Marine Corps. A 2017 draft concept of employment defined *information environment operations* as

---

[18] See James Nicholas, "Australia: Current Developments in Australian Army Information Operations" *IO Sphere*, Special Edition 2008.

[19] Christopher Paul, *Strategic Communication: Origins, Concepts, and Current Debates*, Santa Barbara, Calif.: Praeger, 2011.

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

> [t]he integrated planning and employment of [Marine Air Ground Task Force], Naval, Joint, and Interagency information capabilities, resources, and activities that enhance the Marine Corps single-battle concept and provide defensive, offensive, exploitative effects and support in order to operate, fight and win in and through a contested information environment.[21]

The document that offered this definition explicitly distinguished it from *information operations*, noting that IO seek only cognitive advantage, while IE operations seek any and all kinds of military advantage, including temporal, spatial, and technological. Marine Corps IE operations, then, are clearly envisioned as an umbrella concept that encompasses IO. The document further identifies seven functions of IE operations, which are to be employed across six operational capability areas: electromagnetic spectrum operations, cyber operations, space operations, influence operations, military deception operations, and inform operations.[22] These operational capabilities areas appear to parallel the traditional core of IRCs.

A U.S. Marine Corps interviewee informed us that, after seeing the rest of DoD employing *OIE* instead of *IE operations*, the Marine Corps would subsequently be calling its concept *OIE* (with the definition and treatment unchanged).

Maneuver in the IE

Another term or concept that has come into currency takes the time-honored military concept of *maneuver* and either applies it to the cognitive dimension of the IE or expands it to encompass the IE. According to a U.S. Army Special Operations Command white paper, "Maneuver is a principle of Joint operations that involves the employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy."[23] It notes that seeking advantage in the human domain can also be thought of as maneuver, albeit of a very different kind—one based on cognitive maneuver that seeks to shape contextual conditions and influence decisionmaking.[24]

The term and concept have both virtues and weaknesses. To its credit, *maneuver* mobilizes a concept familiar to all uniformed personnel and generalizes it to the

---

[21] U.S. Marine Corps, *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, Washington, D.C., July 6, 2017b, p. 1. The single-battle concept emphasizes that a unified operational environment in which actions in one area can affect all parts of the environment.

[22] U.S. Marine Corps, 2017b, p. 22. The seven functions are (1) assure enterprise C2 and critical systems, (2) provide IE battlespace awareness, (3) attack and exploit networks, systems, and information, (4) inform domestic and international audiences, (5) influence foreign target audiences, (6) deceive foreign target audiences, and (7) control IW capabilities, resources, and activities.

[23] U.S. Army Special Operations Command, *Cognitive Maneuver for the Contemporary and Future Strategic Operating Environment*, white paper, May 13, 2016, p. 2.

[24] U.S. Army Special Operations Command, 2016.

less familiar area, the IE. Incorporating information and IRCs conceptually as part of combined-arms maneuver would help joint force personnel plan and execute operations that leverage both physical and informational power. Thinking about the IE as just another part of the operating environment—and one that can be approached using familiar concepts from the spatial domains—could increase conceptual comfort and promote the acceptance and adoption of IE-related ideas across the broader force.

However, although the analogy of cognitive maneuver being like physical maneuver is both attractive and promotes some productive thinking about efforts in and through the IE, it is not a perfect analogy. As noted earlier, the IE is not entirely like the spatial domains. The "seek advantage" part of maneuver generalizes to the IE, but "positional advantage" and "movement in combination with fires" are potentially problematic. The IE is not always meaningfully spatial in the way that the physical domains always are. Movement in the IE is also similarly nebulous. Technology allows a message to spread unpredictably while the message's originator does not physically move from the keyboard or microphone. *Suppression* may mean something in the IE, but it is surely not the same thing as directing suppressing fire at an enemy position so that friendly forces can move more safely (as in physical maneuver).[25] If the maneuver analogy is taken too literally, there is a risk that nonsense, such as the possibility of "outflanking" a firewall, could be propagated. While we embrace the virtues of integrating the IE into common military frameworks and practices, we urge caution when it comes to analogies like this example.

Information Warfare

Another term that appears occasionally in this context is *information warfare*. Information warfare is not currently defined in joint or service doctrine, but it was in the 1990s. Chairman of the Joint Chiefs of Staff Instruction 3210.01 defined *information warfare* in 1996 as follows:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based net-

[25] In fact, it would be plausible to argue that *suppression* is, in fact, an effect in and through the IE. When a position is under fire, return fire from that position is reduced. This is called *suppression*. It is not that the soldiers occupying a suppressed position are unable to return fire. It is that it would be very dangerous to do so; they perceive that increased danger, and they decide (in the cognitive portion of the IE) either to reduce the risk as completely as possible by remaining face down in cover or to minimize their exposure to risk, returning fire only sporadically or in short, poorly aimed bursts while maximizing their use of available cover. Suppression *in* the IE might mean nothing or might mean something entirely different. One possible equivalent might be social media: When a post by a user has been met with an inundation of opprobrium or "flaming" by other users, the initial user may be hesitant (*suppressed*) to post again expressing similar views. The point remains that, although suppression might mean something in the IE, it is not clear that the meaning will be directly analogous to the well-understood definition of suppression in the spatial domains.

> works while defending one's own information, information-based processes, information systems and computer-based networks.[26]

The late Dan Kuehl of National Defense University defined *information warfare* more simply: "Military offensive and defensive actions to control/exploit the environment."[27]

Information warfare has come up in many of the recent discussions of military operations in the IE, even appearing in draft documents. In fact, the July 2017 *Marine Air Ground Task Force Information Environment Operations Concept of Employment* was, while in draft form, titled *Information Warfare Concept of Employment* as late as May 2017, and the 2016 *Marine Corps Operating Concept* refers to information warfare and the integration of information warfare into the combined-arms approach.[28]

The term is attractive, as it connects clearly with military/defense roles. However, it also appears to confine these activities to "warfare." In fact, the joint force operates across the range of military operations, a spectrum that extends well outside of warfare (such as deterrence, shaping, humanitarian efforts, security cooperation efforts, and conflict short of warfare). In an era partially defined by gray-zone aggression among competitors seeking gains in conflicts short of warfare, it would be prudent to avoid terms for operations in the IE that unnecessarily constrain the scope or range of those activities.[29]

Essential Characteristics of a Term and Definition for Operations in and Through the IE

There are many terms that could be used to describe DoD plans and activities in and through the IE. Retired Army IO officer and long-time member of the DoD information community of interest Michael Williams has cautioned, "obsessing over the definition of information operations and what capabilities it may or may not include is a distraction."[30]

Whatever term ends up being embraced, it should have several characteristics. It should have all the usual virtues of a good definition. In particular, the common-sense

---

[26] Chairman of the Joint Chiefs of Staff Instruction 3201.01, *Joint Information Warfare Policy*, January 2, 1996.

[27] Dan Kuehl, National Defense University, "Information Warfare," briefing, undated.

[28] U.S. Marine Corps, *Information Warfare Concept of Employment*, Washington, D.C., May 10, 2017a; U.S. Marine Corps, *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, Washington, D.C., September 2016, p. 4.

[29] Christopher Paul, "Confessions of a Hybrid Warfare Skeptic," *Small Wars Journal*, May 3, 2016. A reviewer of this report noted that the dictionary definition of warfare is sufficiently broad in scope to encompass all the referenced activities. That may be so, but the generally accepted connotation and denotation of the term both inside and outside of DoD are narrower, prompting this concern.

[30] Michael Williams, "Speed, Volume, and Ubiquity: Forget Information Operations and Focus on the Information Environment," *Strategy Bridge*, July 26, 2017.

interpretation of the term should correspond closely with the technical definition, and the term should not be in use with a different definition in a different community. It should also have some features specific to the requirements of defense efforts in the IE. As we argue in the next section, the term and definition should capture efforts and effects not only *in* or *on* the IE but also *through* it. The effects and efforts of greatest concern to DoD *transit* the IE to have an impact in the spatial domains. The term of art should also allow that a broad range of activities have effects in and through the IE. Included capabilities should not be confined to those associated with messaging or with technical capabilities that affect C4ISR systems. Actions speak louder than words, and every action or utterance—or even the mere presence of the joint force—has potential echoes and consequences in and through the IE.

We would be satisfied with any term of art that meets all these requirements. In this report, we use the *efforts* or *operations in and through the IE* to describe the area of endeavor under discussion.

Why Is the IE Important?

Now that we have discussed different conceptualizations of the IE and different terms of art for military activities related to the IE, we turn to questions of motivation. Why is the IE important, such that C2 and situational awareness actually matter? Our discussions with subject-matter experts, distillation of the literature, and observations suggest several strong reasons for promoting recognition of the importance of the IE across DoD.

What Happens in the IE Does Not Remain in the IE

To paraphrase and invert a phrase popularized by the Nevada Tourism Board, "What happens in the IE does not stay in the IE."[31] Effects and changes in the IE can influence the actions and behaviors of physical actors and systems, delivering effects or changes in the various spatial dimensions. This is only noteworthy because of military mindsets that give primacy to the spatial domains, treating the IE as an afterthought and implicitly assuming that it is its own separate realm of contestation. It does not and cannot work like that. Actions in the spatial domains resonate in the IE, and actions in the IE have consequences in the physical domains. As others have put it, "In spite of its lack of physical existence, the content and flow of information within a specific geographic area produces real, tangible effects in the physical world and on military forces present in the operating environment."[32]

[31] The original phrase is, "What happens in Vegas stays in Vegas."

[32] Cordray and Romanych, 2005, p. 7.

One Cannot *Not* Communicate

Foundational work in psychology by Watzlawick, Bavelas, and Jackson has rightly noted that one cannot *not* communicate.[33] Every action, utterance, message, depiction, and movement of a nation's military forces can influence the perceptions and opinions of populations that witness them, both in the area of operations (firsthand) and in the broader world (second- or thirdhand).[34] And, of course, actions speak louder than words.

Every military activity has inherent informational aspects, whether creating information, changing information, or affecting one or more of the dimensions of the IE, intentionally or otherwise. It would be best if the inherent informational aspects of military operations were planned, coordinated, and intentional rather than left to chance.

War Is Politics by Other Means, and a Great Deal of Politics Takes Place in the IE

"War is politics by other means" is one of the central (and most quoted) principles of Carl von Clausewitz's military thinking.[35] This observation has recurring salience for U.S. military thinking, especially when U.S. military efforts "have produced many tactical and operational gains, but rarely achieved desired political objectives and enduring outcomes in an efficient, timely and effective manner."[36]

Enduring strategic outcomes are usually political in nature, and "military power alone is insufficient to achieve sustainable political objectives."[37] Furthermore, politics increasingly takes place in the IE—not just in the cognitive dimension of the IE in terms of the decisionmaking of national leaders and their constituents, but also in terms of the increasing volume of political discourse taking place through social media and mobile technology. Global penetration of technology is increasing, and the available modes of communication associated with that diffusion are increasing, too. Civilian populations in countries that are relevant to U.S. strategic interests have access to more information and a greater variety of conduits than ever before. They also have a greater ability to share their views with their leaders, even in autocratic or other nondemocratic regimes.

Greater attention to the IE could improve DoD's ability to influence political outcomes, through both warfare and other types of activities across the range of military operations.

---

[33] Paul Watzlawick, Janet Beavin Bavelas, and Don D. Jackson, *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes*, New York: W. W. Norton and Company, 2014.

[34] Paul, 2011.

[35] Carl von Clausewitz, *On War*, J. J. Graham, trans., London: Wm. Clowes and Sons, 1909, chapter 1.

[36] U.S. Joint Chiefs of Staff, *Joint Concept for Human Aspects of Military Operations*, Washington, D.C., October 19, 2016b.

[37] U.S. Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, Washington, D.C., March 16, 2018, p. 4.

Defeat Is a Cognitive Outcome

Defeat of an adversary, by whatever mechanism, is a cognitive outcome. Throughout history, few battles or engagements have concluded with the death or wounding of every combatant on one side or the other, but battles typically conclude with one side being defeated. The accumulated stresses of combat and combatants' perceptions of the situation lead to fear, flight, or surrender. Alternatively, a force's commander perceives the opponent's relative advantages as a battle unfolds and concludes (through cognition) that the cost of continuing will exceed the possible benefits.

Defeat can also be a matter of perspective, something negotiated through the IE. Even if a force suffered more casualties or retreated, if it met all or some of its objectives, it may be able to plausibly claim victory. The objectives on which these claims of success are based may have been loosely defined or specified after the fact, but this may not be an obstacle to victory.[38] Nonstate actors (such as insurgents and terrorist groups) are often adept at turning their tactical failures into strategic successes when they reinterpret the meaning of tactical engagements for their adherents.

As the U.S. Marine Corps capstone doctrinal publication frames it, war is fundamentally a contest of wills.[39] If the goal of warfare is to defeat the adversary's will, planners must recognize *will* as a variable in the operational environment—one that substantially exists in and is influenced through the IE. Fighting a perceptual, moral, and mental battle in and through the IE to defeat the will of future adversaries will require much greater U.S. attention to the IE going forward than has heretofore been the case. Too often, the joint force focuses on the destruction of enemy capabilities, attacking will only as a second-order consequence of destruction.[40] As then top leaders of the U.S. Army, Marine Corps, and Navy noted in a joint white paper, "War is inarguably the toughest of physical challenges, and we therefore tend to focus on the clash and lose sight of the will."[41]

Adversaries Are Fighting in and Through the IE

A host of state and nonstate adversaries and potential adversaries are already using disinformation, engagement, propaganda, and other efforts in and through the IE to target and influence the perceptions, opinions, alliances, and decisions of local, regional, and transregional populations.[42] These adversaries and potential adversaries have gained effectiveness by generously resourcing information power and IRCs,

---

[38] Gideon Avidor and Russell W. Glenn, "Information and Warfare: The Israeli Case," *Parameters*, Vol. 46, No. 3, Autumn 2016.

[39] Marine Corps Doctrinal Publication 1, *Warfighting*, Washington, D.C., June 20, 1997, p. 7.

[40] U.S. Joint Chiefs of Staff, 2016b.

[41] Raymond T. Odierno, James F. Amos, and William H. McRaven, *Strategic Landpower: Winning the Clash of Wills*, white paper, U.S. Army, U.S. Marine Corps, and U.S. Special Operations Command, October 28, 2013.

[42] U.S. Army, *Unified Quest: Fighting on the Battleground of Perception*, Washington, D.C., October 4, 2016.

giving prominence to information effects when planning and executing operations, and integrating physical and informational power.[43] If the joint force is to counter or compete with such efforts, DoD needs to increase attention to operations in and through the IE.

New Developments in Concepts Related to the IE

At the time of this writing, information and the IE were ascendant in DoD concepts and conversations. There was a great deal of productive thinking about the IE in 2016, 2017, and 2018. This explosion of interest in the IE coincided with this study, rendering the research somewhat complicated by creating something of a moving target. Identifying requirements for C2 and situational awareness of the IE (see Chapter Four) was made more challenging because of numerous changes in the concepts, characteristics, and scope of the operations for which these capabilities are required. In this section, we review relevant concepts and innovations that shaped this research effort.

Strategy for Operations in the IE/Joint Concept for Operating in the IE

Long-simmering interest in the IE achieved a steady boil with the release of the *Department of Defense Strategy for Operations in the Information Environment* in June 2016. Though only 20 pages, the strategy declared a bold, aspirational end state:

> Through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations.[44]

The strategy served as a catalyst for further conceptual development related to the IE, explicitly calling for updates to joint concepts and serving notice to DoD thinkers and stakeholders that the IE is important and that DoD is moving forward with concepts and capabilities related to the IE.

The *Joint Concept for Operating in the Information Environment* (JCOIE) was still in draft form at the time of this writing and is part of the implementation of the strategy. In drafts that we reviewed, the JCOIE advanced two main ideas:

1. The joint force must specify military objectives in terms of the actions and behaviors of relevant actors (e.g., adversary leaders, adversary forces, constituencies in a civilian population, leaders of a partner nation).

---

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

[44] DoD, 2016, p. 2.

2. The joint force must plan and conduct all operations to influence the behaviors and actions of relevant actors through the use of integrated informational and physical power, especially by leveraging the inherent informational aspects of all military activities.

The core of this draft concept is consistent with our own views and conclusions, and it has certainly informed our analysis of requirements for C2 and situational awareness for operations in and through the IE.

Marine Corps Efforts

Once the Marine Corps decided to embrace the IE, it moved forward swiftly. Guidance from the Commandant to invigorate information warfare and integrate it into the service's combined-arms approach was central to the September 2017 Marine Corps Operating Concept (MOC).[45] The MOC emphasizes the cognitive dimension of conflict, the importance of information as a weapon, the battle of signatures, future conditions under which "to be detected is to be targeted is to be killed," and the importance of information as part of combined arms.[46]

The MOC acknowledges that "the Marine Corps is currently not organized, trained, and equipped to meet the demands" of these IE requirements, so the service adjusted its force structure and introduced plans to develop new capabilities.[47] It established a three-star Deputy Commandant for Information, who converted the Marine Expeditionary Force's headquarters groups into *information groups*, changing their manning and composition for the new mission.[48]

Elaborating on the concepts outlined in the MOC, in July 2017, the Marine Corps published *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, which "introduces a comprehensive approach to fighting and winning in and through the information environment."[49] The concept outlines how IE operations will be integrated with combined arms by conceptually extending the Marine Corps' foundational concept of maneuver warfare to include the IE as part of the maneuver space. IE operations are described as "an integral component of [Marine Air Ground Task Force] operations."[50]

---

[45] U.S. Marine Corps, 2016.

[46] U.S. Marine Corps, 2016, p. 6.

[47] U.S. Marine Corps, 2016, p. 8.

[48] Mark Pomerleau, "Marines Look to Dominate in Information Environment," *C4ISRNET*, April 5, 2017.

[49] U.S. Marine Corps, 2017b, p. i.

[50] U.S. Marine Corps, 2017b, p. 1.

Army Unified Quest

The 2015 Army Unified Quest series of wargames and other events included the seminar "Fighting on the Battleground of Perception." The seminar report (released in 2016) contains many interesting observations. Building on the idea of IRCs as combined-arms capabilities, the report finds that individual IRCs need concepts and doctrine both for how they are employed individually and how they can best be integrated with other capabilities and assets during operations. The report noted the challenge of adversary aggression below the threshold of war, and competition to set conditions prior to the onset of hostility. The seminar report emphasized better use of IRCs to shape conditions and to counter adversary shaping in order to improve prospects for success during actual outbreaks of hostilities.[51]

Seminar participants also concluded, "The United States will have to adapt and innovate to counter adversary information warfare and influence campaigns occurring across all phases of operations."[52] Finally, the report cites a need for increased education, training, and practice for the employment of influence concepts for leaders at all levels in the Army.[53]

Information as a Joint Function

One of the biggest developments related to DoD's embrace of the IE came on July 12, 2017, when Chairman of the Joint Chiefs of Staff Joseph F. Dunford, Jr., approved *information* as the first addition to the joint functions since the other six were codified in doctrine. The information function is encapsulated in change 1 to JP 1, *Doctrine for the Armed Forces of the United States*. JP 1 now describes the information joint function as follows:

> The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant actor perceptions, behavior, action or inaction, and supports human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides [joint force commanders] the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of all military activities to achieve the commander's objectives and attain the end state.[54]

---

[51] U.S. Army, 2016.

[52] U.S. Army, 2016, p. 9.

[53] U.S. Army, 2016, p. 12.

[54] Joint Publication 1, *Doctrine for the Armed Forces of the United State*s, Washington, D.C., March 25, 2013.

Exactly what information as a joint function will mean and how it will be represented in down-trace doctrine and executed across the joint force remain open questions. However, elevation of information to the status of a joint function is a clear indication of DoD's commitment to increasing its emphasis on the IE and on efforts in and through the IE.

Joint Concept for Human Aspects of Military Operations

Released in late 2016, *Joint Concept for Human Aspects of Military Operations* (JC-HAMO) "describes how the Joint Force will enhance operations by impacting the will and influencing the decision making of relevant actors in the environment, shaping their behavior, both active and passive, in a manner that is consistent with U.S. objectives."[55]

JC-HAMO introduced language and ideas echoed in the draft JCOIE, including an emphasis on influencing behavior and defining the subjects of that influence as "relevant actors." *Relevant actors* does not refer only to adversaries and potential adversaries but includes any "individuals, groups, and populations whose behavior has the potential to substantially help or hinder the success of a particular campaign, operation, or tactical action."[56] This makes JC-HAMO (and other concepts that use the term *relevant actors*) more clearly applicable across the range of military operations.

To achieve the objectives laid out in JC-HAMO, the concept identifies four imperatives for the joint force, all of which have implications for C2 and situational awareness requirements for the IE. The joint force must be able to

- *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 ("influence" is the act or power to produce a desired outcome on a target audience or entity).[57]

Joint Concept for Integrated Campaigning

Released in draft form less than six months after JC-HAMO, *Joint Concept for Integrated Campaigning* (JCIC) sought to identify solutions to the problem of competitors combining conventional and nonconventional methods (such as gray-zone aggression) to achieve their objectives.[58] The solution offered in the concept is "integrated cam-

[55] U.S. Joint Chiefs of Staff, 2016b, p. 1.

[56] U.S. Joint Chiefs of Staff, 2016b, p. 1.

[57] U.S. Joint Chiefs of Staff, 2016b, p. 2; emphasis in original.

[58] U.S. Joint Chiefs of Staff, 2018.

paigning," which integrates and aligns military and nonmilitary activities "of sufficient scope, scale, simultaneity, and duration across multiple domains."[59]

JCIC connects to the IE and to other concepts and documents discussed here in several ways. For example, it recognizes the need to coordinate and integrate across all activities and capabilities (including information) to achieve desired effects, and JCIC follows the logic that commanders and staffs arrange their operations and activities to produce desired conditions, behaviors, and outcomes (rather than attrition or unspecified victory conditions).[60]

Expanding Maneuver and Cognitive Maneuver White Papers

Two white papers by U.S. Army Special Operations Command have shared ideas for extending the concept of maneuver to the IE: the 2016 *Cognitive Maneuver for the Contemporary and Future Strategic Operating Environment*, cited earlier, and the 2017 *Expanding Maneuver in the Early 21st Century Security Environment*. Both take the insight that the joint force can have both physical and cognitive objectives, and both suggest that while the joint force maneuvers physically in pursuit of its physical objectives, it should also maneuver cognitively toward its cognitive objectives.[61]

The earlier paper lists six specific types of cognitive maneuvers: narrative cultivation, narrative attack, marginalization, proxy mobilization, disorientation, and fostering relationships.[62] The later argues for a broad understanding of *influence*, noting that influence causes an adversary or relevant population to behave in a manner that broadens strategic options or supports objectives. It also notes that influence can come from many different types of military activities:

> This could mean a broad application of actions and messages that promote a narrative. It could also mean precision targeting operations that create multiple dilemmas for an adversary's ability to maintain unity.[63]

A Summary of Possible Visions for Operations in and Through the IE: Three Tiers

We considered these emerging IE-related concepts and alongside the older and more traditional literature discussing IO and IRCs, as well as discussions with subject-

---

[59] U.S. Joint Chiefs of Staff, 2018, p. v.

[60] U.S. Joint Chiefs of Staff, 2018.

[61] U.S. Army Special Operations Command, *Expanding Maneuver in the Early 21st Century Security Environment*, January 12, 2017.

[62] U.S. Army Special Operations Command, 2016, p. 4.

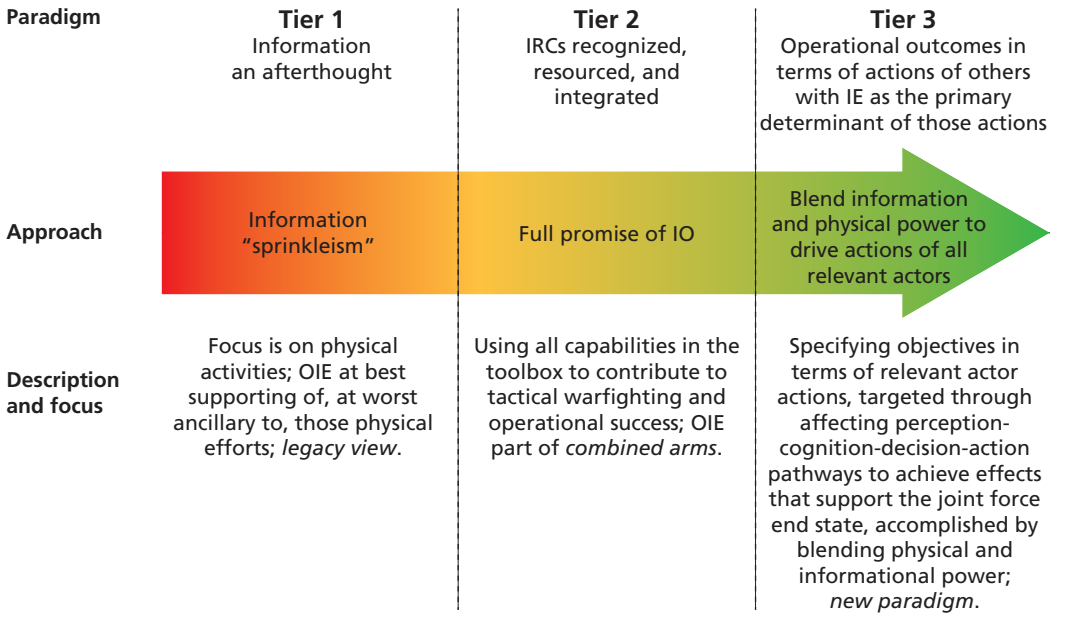
[63] U.S. Army Special Operations Command, 2017, p. 6.

matter experts and stakeholders. Our conclusion is that there are three levels, or tiers, of visions of the future role of information in operations. Each has implications for C2 and situational awareness requirements for operations in and through the IE. The three-tiered framework is shown in Figure 2.5.

The tier 1 vision is the legacy view, the antiquated vision that has dogged IO planners in numerous campaigns and operations. Under this vision, operations in and through the IE are an afterthought. The focus of planning and execution is on physical objectives, physical capabilities, and physical effects. The IE and IRCs are considered only to the extent that they can contribute to or support physical capabilities—for example, using information to increase lethality or to disrupt the adversary so it is easier to achieve a physical advantage. The IE is overlooked and ignored at this tier, and when it is considered, it is considered late. Planners complete their work, then invite an information stakeholder to "sprinkle some of that IO stuff" on the plan.[64] This vision is attractive to no one but serves as a reminder of a prior baseline, something to which DoD could return if attention to the IE wanes.

Tier 2 is the realization of what the IO and IRC communities have aspired to offer and what is implied by several of the concepts described in this report. Under this

Figure 2.5
Three Tiers of Visions of the Role of Information in Operations



RAND *RR2489-2.5*

[64] Dennis M. Murphy, *Talking the Talk: Why Warfighters Don't Understand Information Operations*, Carlisle, Pa.: U.S. Army War College, Center for Strategic Leadership, Issue Paper 4-09, May 2009, p. 2.

vision, capabilities to conduct operations in and through the IE are embraced as valuable military capabilities. IRCs are resourced appropriately and used by commanders and planners just like any other military capability. Information and IRCs become just another tool in the commander's toolbox, seamlessly integrated with the other tools used to accomplish a mission as part of combined arms. Sometimes, information is *supporting* the main effort, but sometimes information is *supported*, and information is the main effort.

This tier 2 vision is strong. If fully realized, it would represent a significant improvement over the tier 1 baseline, in which information is a secondary or tertiary concern and IRCs are poorly understood, mistrusted, and used only hesitantly or when no other capability could deliver the required effect. However, in our discussions and literature review, we identified a third, deeper vision for operations in and through the IE.

Tier 3 represents a true paradigm shift.[65] Tier 3 encompasses all the characteristics of tier 2: Commanders comfortably employ and integrate physical and informational capabilities as part of combined arms as they pursue their objectives. However, under the tier 3 vision, how those objectives are specified is different. In tier 3, all military objectives are phrased in terms of the desired actions and behaviors of relevant actors; then, all military activities seek to drive, lead, push, herd, cajole, coerce, constrain, persuade, or manipulate relevant actors down perception-cognition-decision-action paths that ultimately lead to those objectives.

Getting others to do what one wants is called *influence*, so influence becomes the lingua franca of operational art. Both physical and informational power contribute to influence. (This is not a pacifist vision.) Commanders operating under this vision understand that destruction is a powerful form of influence that deprives actors of alternative courses of action. A relevant actor who has been killed has been successfully influenced from performing any undesired behavior ever again. However, short of this most extreme form of influence, there are a host of ways in which physical and informational power can be used collectively to achieve behavioral objectives that (ideally) accumulate to support enduring strategic end states.

Although DoD has not unambiguously committed to the tier 3 vision, there is enough promise in this vision and enough interest among stakeholders to emphasize it here. In identifying requirements for C2 and situational awareness for operations in the IE (OIE) (discussed in Chapter Four), we sought to identify requirements necessary to support the tier 3 vision, should DoD choose that path. Tier 2 is a wholly included within tier 3, and tier 1 is unattractive to today's military planners. Should DoD's ultimate ambition for operations in and through the IE fall short of tier 3, some of the

[65] Scott K. Thomson and Christopher E. Paul, "Paradigm Change: Operational Art and the Information Joint Function," *Joint Force Quarterly*, Vol. 89, 2nd Quarter 2018.

requirements and criteria discussed in later chapters would see a reduction in relative importance or weight alongside options for meeting those requirements.

Having discussed the IE, shared various emerging visions related to operations in and through the IE, and summarized three tiers of aspirational visions for the future of operations in and through the IE, we now turn to the topic of C2 and situational awareness for those operations, beginning with a review of current practices and processes.

CHAPTER THREE

Current Concepts and Practices for C2 and Situational Awareness

This chapter examines current concepts and practices for C2 and situational awareness to provide a framework for the more ambitious tasks of this report: identifying requirements for C2 and situational awareness for operations in and through the IE and comparing organizational alternatives for meeting those requirements at the geographic combatant commands.

Ubiquitous communication is a defining characteristic of the current IE. Every action (or decision *not* to act) by the joint force conveys a message to multiple audiences, some intended, some not. To better grasp how the concepts of C2 and situation awareness are evolving, it is crucial to look to the foundational principles and practices of traditional C2 and situational awareness.

Command and Control

C2 comprises situational awareness and mission management and is defined as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission."[1] C4ISR is an extension of C2. Now, and in the future, the joint force will rely on C2 spanning echelons, geographic boundaries, and various organizations to "form, dissolve, reform and move" responsive forces to their objective points.[2]

C2 in the spatial domains potentially differs from C2 of the IE in several important ways. First, the IE is not geographically defined or temporally bound: There is no clear beginning or end. Second, conducting C2 in the IE is an inherently complex endeavor. It is far more difficult for all elements of the force (including critical allies) to see the entirety of the IE; it defies the easy graphical representations typical of the spatial domains (i.e., maps). Third, the IE is constantly in flux as new media develop and emerge and as new actors enter the fray, enabled by low barriers to entry and the

[1] JP 1, 2013.

[2] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Force Operations: Joint Force 2030*, Washington, D.C., March 18, 2016a.

distribution of information and communication technology. Fourth, there is a certain *balkanization* effect as entities seek to censor and limit parts of the IE. Near-peer competitors, such as China and Russia, work assiduously to limit their own vulnerabilities through manipulation and censorship while flouting international norms to encroach on other nations in and through the IE—from the theft of intellectual property to meddling in national elections. Fifth, deception is pervasive and much easier to achieve in the IE than in the physical world, as demonstrated by the success of spoofing, bots, fake profiles, and honeypots. Sixth, there is no real "ground truth" in the IE; perception is responsible for shaping attitudes and beliefs. Seventh, and finally, attribution can be difficult to discern, posing a range of problems for forces looking to respond to provocative actions. As witnessed with Russia's use of trolls and freelancers, or in the various cyberattacks thought to emanate from North Korea, nation-states can work through proxies to amplify ambiguity and insulate themselves with an air of plausible deniability.[3]

Situational Awareness

Situational understanding is defined as "the product of applying analysis and judgment to relevant information to determine the relationships among the mission variables to facilitate decisionmaking."[4] Situational awareness leads to situational understanding. Developing and maintaining situational awareness is critical for context, developing plans, assessment, and operational decisionmaking.

With the proliferation of data and noise throughout the IE, identifying *relevant* information and relationships among various operational and mission variables and establishing situational awareness is more challenging than ever. The speed and overall pace of globalization, the cascading effects of the information revolution, a growing need for cooperation with partners, and the pressure to stay out in front of all things "cyber" have vastly increased the complexity of the operational environment.

Increasing volumes and rates of data and the ability of both states and nonstate actors to adapt and evolve have also vastly complicated the IE.[5] Commanders must devote more time to understanding the environment, leaving less time to actually accomplish the mission. Commander's critical information requirements, priority intelligence requirements, and friendly-force information requirements require an intimate level of situational understanding.

---

[3] On Russian use in particular, see Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016.

[4] Army Field Manual 5-0, *The Operations Process*, Washington, D.C., March 2010, p. Glossary-8.

[5] Joint Staff, J7, U.S. Deployable Training Division, Commander's Critical Information Requirements (CCIRs), Suffolk, Va., July 2013, p. 3; Mica Endsley made a similar argument in 1995—that the operational environment has arguably grown appreciably more complex over the past 20 years. See Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, Vol. 37, No. 1, 1995.

To reduce the amount of time that commanders must spend attempting to understand the IE, several requirements are worth noting:[6]

- a detailed knowledge of the processes and procedures necessary to generate and sustain situational awareness
- an understanding of how interactions among various operational and mission variables can degrade situational awareness
- the identification of the commander's critical information requirements needed to support situational awareness in a complex environment
- an appreciation of how various threats adapt and what effect this have on how situational awareness is achieved
- a mechanism that allows commanders to visualize operations, facilitates decision-making, and improves mission command that is resilient in the face of adaptive threats.

DoD must employ an effective means for identifying, acquiring, analyzing, and sharing the data and information that enable situational awareness in a complex operational environment. Another major challenge will be identifying timely and relevant data that are shareable and interoperable, as well as affordable to acquire.[7]

C2 and Situational Awareness in the Spatial Domains

C2 has evolved considerably over the years and is arguably now more complex than ever. Achieving C2 entails a constant quest for certainty while attempting to remove the fog of war. The desire to know more extends across several dimensions, from the state and intentions of the enemy's forces to the myriad variables of the operational environment (and now the IE). In basic terms, C2 is the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. Effective C2 is the net result of the successful interaction of a complex architecture comprising people, procedures, and equipment.

Seemingly limitless information and data sources and the diffusion of communication capabilities have left commanders and decisionmakers with the problem of too much, rather than too little, information.[8] The *sine qua non* of this task is making sense of which information is relevant and discarding that which is not. This separating of

---

6 Joint Staff, J7, 2013.

7 U.S. Defense Information Systems Agency, "Information Volume and Velocity Overview," briefing, June 2015.

8 Isaac R. Porche III, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman, *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information*, Santa Monica, Calif.: RAND Corporation, RR-315-NAVY, 2014.

the "wheat from the chaff" can only be accomplished by using relevant information in the most effective way to make the best possible decisions. Context matters, too, circumstances will affect the outcome.

One way that humans have sought to mitigate the issue of being inundated with information is to rely on technology and promises of big data solutions. Yet, an overreliance on technology to process, filter, and display information has many built-in (and problematic) assumptions. This assumes a sufficient understanding of the commander's responsibilities, circumstances, and decisions to anticipate his or her needs. But it further assumes that the C2 challenges for commanders are acquiring enough information, sorting it, and maintaining connectivity with subordinates so that they may be directed properly. Neither may be the case, especially when it comes to the IE.

Fog of War

Fog of war refers to the uncertainty that comes with battle: uncertainty about the enemy and their actions, uncertainty about the context (e.g., terrain, conditions), and even uncertainty about the location, disposition, and situation of friendly forces. Armed forces collect information in an effort to reduce these uncertainties, but they cannot eliminate them and must accept that decisions in war are often based on incomplete, inaccurate, or even contradictory information.[9]

Efforts to coordinate and conduct military operations in and through the IE are beset with a fog-of-war problem not unlike that experienced in the traditional spatial domains of air, land, and sea. The breadth and depth of information available through all forms of media and the speed with which that information is conveyed has increased exponentially. There has been a proliferation of interoperable digital devices and mobile technology, particularly in the developing world. The result has been lower barriers to entry to the IE; now, almost any individual or small group can participate, observe, or compete.

The IE is further clouded by the fog of war due to the sheer volume of information available at any one time (making finding needed information a constant "needle-in-haystack" challenge), and due to the difficulty of attributing content and actions in the IE to specific actors. U.S. adversaries play by a different set of rules, operating outside customs, societal norms, and unencumbered by international law.

Mission Tactics/Mission Command

According to Army doctrine, "Mission command is the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations."[10] Absent specific orders, mission command allows subordinates to

---

[9] Marine Corps Doctrinal Publication 1, 1997, p. 7.

[10] As defined in Army Doctrine Publication 6-0, *Mission Command*, Washington, D.C., May 2012, p. 1.

continue moving forward in pursuit of the commander's objectives. Mission command is simultaneously a system, a warfighting function, and a philosophy, consisting of two major components: the "art of command" and the "science of control."[11] The art of command is defined as "the creative and skillful exercise of authority through timely decisionmaking and leadership."[12] The science of control consists of "systems and procedures used to improve the commander's understanding and support accomplishing missions."[13] The complexity of this concept and the associated doctrine means that it has not been "fully implemented" across the Army as envisioned in doctrine.[14]

To achieve mission command success, subordinate leaders at all echelons must exercise disciplined initiative and act both aggressively and independently according to the commander's intent. There are several important prerequisites worth highlighting: the use of mission orders; full familiarity with the mission, commander's intent, and concept of operations; and mutual trust and understanding between commanders and subordinates. While Army Field Manual (FM) 5-0 describes the philosophy of mission command as it applies to all activities of the operations process, it is important to understand its more recent doctrinal evolution.

Both FM 3-0 (2001) and FM 6-0 (2003) addressed battle command and the operations process in detail, while FM 5-0 (2005) described the operations process and where planning fits in. Over time, the concept has evolved to emphasize to a far greater extent the commander's role in the conduct of operations. Moreover, there is a focus on the interrelationships between the commander, staff, subordinate commanders, and others in the C2 chain of command. FM 5-0 provides doctrine on the operations process as a whole, along with a chapter on design, a chapter for each activity in the process, and appendixes covering everything from tactics, techniques, and procedures for organizing the headquarters to conducting operations and using the Military Decision Making Process for troop leading.[15]

---

[11] The mission command system consists of people, networks, information systems, processes and procedures, facilities, and equipment (Army Doctrine Publication 6-0, 2012, pp. 11–12).

The mission command warfighting function tasks are as follows: the operations process, knowledge management and information management, inform and influence activities, and cyber electromagnetic activities (Army Doctrine Publication 6-0, 2012, p. 10).

The six principles of mission command are (1) build cohesive teams through mutual trust, (2) create shared understanding, (3) provide a clear commander's intent, (4) exercise disciplined initiative, (5) use mission orders, and (6) accept prudent risk (Army Doctrine Publication 6-0, 2012, p. 2).

[12] Army Doctrine Publication 6-0, 2012, p. 5.

[13] The science of control has four major components: information, communication, structure, and degree of control. *Control* is defined as "the regulation of forces and warfighting functions to accomplish the mission in accordance with the commander's intent" (Army Doctrine Publication 6-0, 2012, p. 5).

[14] Army Doctrine Publication 6-0, 2012, p. 2.

[15] Clinton J. Ancker III and Michael Flynn, "Field Manual 5-0: Exercising Command and Control in an Era of Persistent Conflict," *Military Review*, March–April 2010.

In the 2010 edition of FM 5-0, there was a further evolution of doctrine to focus on the cognitive aspects of C2, including a description of how commanders exercise C2 during full-spectrum operations. In such contexts, commanders face thinking and adaptive enemies, changing civilian perceptions, and the agendas of various organizations in an operational area. Commanders can never predict with certainty how enemies or civilians will act and react or how events may develop. During execution, leaders must continuously anticipate, learn, and adapt to overcome the dynamics of changing circumstances and adaptive adversaries. Because of the complex, uncertain, and ever-changing nature of operations, mission command—as opposed to detailed command—is, doctrinally, the preferred method for exercising C2.[16]

C2 and Situational Awareness of the IE

As James McGrath notes,

> IE situational awareness requires a detailed understanding of individuals, social groups, behavior dynamics, communication architectures, exploitation of narratives, and target audience vulnerabilities, as well as the newly emerging techniques of real-time, live big data analytics, social media scraping, and memetic warfare.[17]

In other words, it requires a significant baseline understanding of human dynamics (psychological and social) and awareness and monitoring of all three of the dimensions of the IE. Each of the three dimensions of the IE is fundamentally distinct and can be conceived of (and perhaps visualized) differently.

Situational Awareness for the Cognitive Dimension of the IE

Most concepts for operating in and through the IE emphasize the cognitive dimension as the clearest path to affecting the actions and behaviors of relevant actors. Sufficient understanding and awareness of the cognitive dimension are paramount. Unfortunately, states and changes in the cognitive dimension are the most difficult to observe. It is much easier to observe an actor's *behavior* than it is to observe the thoughts, feelings, and cognitive processes that produced that behavior. In fact, directly observing the cognitive dimension is all but impossible. Observers are forced to rely on indicators. Action is a good indicator of what someone is thinking and feeling. Another frequently relied-upon indicator is self-report: We know what someone is thinking when they tell us what they are thinking. One way to collect self-reported data is through

---

[16] Ancker and Flynn, 2010.

[17] James R. McGrath, "Twenty-First Century Information Warfare and the Third Offset Strategy," *Joint Force Quarterly*, Vol. 82, 3rd Quarter, 2016, p. 19.

survey research.[18] Another way is to monitor the speech, writings, postings, and other expressions that include self-reports of an individual's cognition or emotional states. If someone posts on social media expressing anger and claiming to be misled by the government, that provides an indicator from which to make reasonable suppositions about the cognitive dimension.

Both survey research and other forms of self-reporting about thoughts and feelings have another virtue: They can be aggregated, and, through aggregation, they can support inferences about groups and thus inferences about a group's shared and collective thoughts, feelings, and perceptions. Groups can be identified and defined in numerous ways. Traditionally, groups or audiences are defined via various demographic characteristics—some intersection of definable characteristics, such as age, gender, nationality, ethnicity or tribal affiliation, education, or religion. A more empirical approach to identifying groups and their members is through social network analysis.[19]

Taking another logical step, it is possible to infer an actor's thoughts or feelings from his or her own statements, even if those statements do not directly include reports of thoughts, perceptions, or feelings. For example, if someone posts about being "angry," that is a direct indicator of anger. However, suppose the person instead uses angry words as part of a discussion; with simple inference, we can still accept that as an indicator of anger. This particular second-order indicator is usually referred to as *sentiment*. For our purposes, sentiment is often characterized by polarity (positive, negative, or neutral to U.S. interests), strength, and emotion (joy-trust, sadness-anger, surprise-fear, and anticipation-disgust).[20] While polarity and emotion are relatively mature concepts within the psychological and behavioral literature, strength of sentiment is more difficult to measure and standardize.[21] Objective measures of frequency and the intensity of specific words used to describe a topic can be a proxy for sentiment strength, but their accuracy is questionable.[22] Automated ways to measure

---

[18] See Christopher Paul, Jessica Yeats, Colin P. Clarke, and Miriam Matthews, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference*, Santa Monica, Calif.: RAND Corporation, RR-809/1-OSD, 2015, chapter 10.

[19] Peter Hedström, Rick Sandell, and Charlotta Stern, "Mesolevel Networks and the Diffusion of Social Movements: The Case of the Swedish Social Democratic Party," *American Journal of Sociology*, Vol. 106, No. 1, July 2000. See also Stephen P. Borgatti, "Centrality and Network Flow," Social Networks, Vol. 27, No. 1, January 2005, and Ronald S. Burt, "Social Contagion and Innovation: Cohesion Versus Structural Equivalence," American Journal of Sociology, Vol. 92, No. 6, May 1987.

[20] Felipe Bravo-Marquez, Marcelo Mendoza, and Barbara Poblete, "Combining Strengths, Emotions And Polarities for Boosting Twitter Sentiment Analysis," *Proceedings of the Second International Workshop on Issues of Sentiment Discovery and Opinion Mining*, New York: Association for Computing Machinery, 2013, article 2, p. 2.

[21] A good overview of the process and challenges of sentiment analysis can be found in Ron Feldman, "Techniques and Applications for Sentiment Analysis," *Communications of the ACM*, Vol. 56, No. 4, April 2013.

[22] Feldman, 2013.

sentiment rely on text analytics, and only the best tools allow for an integrated analysis of spoken words, emoticons, video, and old-fashioned human intelligence.[23]

Sentiment, especially changing sentiment, will rarely be completely homogenous across a group. Because changes in the cognitive dimension of the IE are essential to situational awareness, approaches to understanding and observing the diffusion of sentiment (or other indicators or underlying processes) across a group or population are particularly interesting. Diffusion in international relationships is conceptualized as occurring through one of four possible mechanisms: coercion, competition, learning, and emulation.[24] Recently, analysts have used tools to track sentiment "contagion" on various social media. The evidence from these studies indicates that diffusion patterns differ with network characteristics and emotions.[25]

There is no standard means to visualize the cognitive dimension of the IE. Sentiment polarity is often shown using a meter, but strength and emotion are perhaps better shown with color shading to indicate intensity. Target populations and the spread or diffusion of ideas within those populations can be shown with heat maps on a geographic display or with colors on a social network diagram.

Situational Awareness for the Informational Dimension of the IE

To conduct analyses to describe the cognitive domain, analysts need to understand informational factors that describe the underlying information flows and transmission paths—in a sense, the "infrastructure" of the nonphysical elements of the IE. Specifically, they may need to understand the underlying topology of the social and virtual networks, the impact of temporal effects on information and factors related to the security or trustworthiness of information. In fact, understanding the IE at this informational level is critical to planning future information operations.

Topology relates to how information potentially flows in networks, independent of whether that flow affects perceptions and follow-on cognition. Network analysis techniques to describe and visualize the topology of networks are well established. Such concepts as density and centrality are derived from the number of flows into and out of each entity in the network. Visualizations can be highly effective in com-

---

[23] Mike Thelwall, "The Heart and Soul of the Web? Sentiment Strength Detection in the Social Web with SentiStrength," in Janusz A. Holyst, ed., *Cyberemotions: Cognitive Emotions in Cyberspace*, Basel, Switzerland: Springer, 2017.

[24] Fabrizio Gilardi, "Transnational Diffusion: Norms, Ideas and Policies," in Walter Carlsnaes, Thomas Risse, and Beth A. Simmons, eds., *Handbook of International Relations*, 2nd ed., Thousand Oaks, Calif.: Sage Publications, 2012.

[25] A fascinating look at how disruptions of network characteristics might influence the effectiveness of a terrorist organization can be found in Maksim Tsvetovat and Kathleen M. Carley, "Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence," *Journal of Social Structure*, Vol. 6, No. 2, 2005.

Also see Rui Fan, Jichang Zhao, Yan Chen, and Ke Xu, "Anger Is More Influential Than Joy: Sentiment Correlation in Weibo," *PLoS ONE*, Vol. 9, No. 10, 2014.

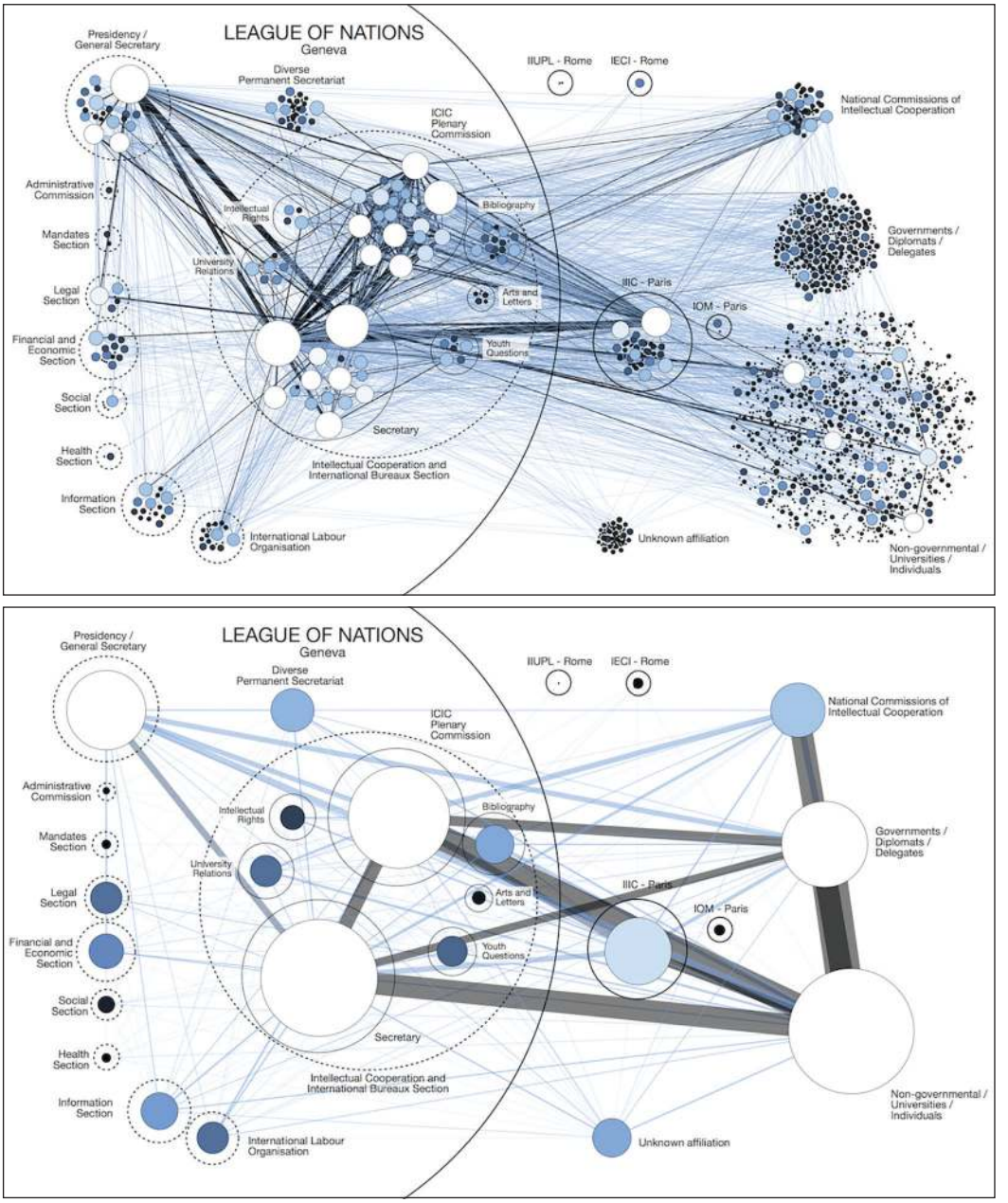
municating situational awareness of the potential ways those networks could support OIE. For example, Figure 3.1 shows two flow diagrams for a small, multilevel social network derived from archival records of the correspondence of the League of Nations International Committee on Intellectual Cooperation after World War I.[26] The size of the circle depicting a given network entity is scaled to represent an objective measure of that entity's potential influence within the network. Similarly, the width of each line in the diagram represents an objective measure of the strength of the tie between any two entities. "Distance" in networks is measured by the number of nodes on the path between any two entities in the network and is usually unrelated to spatial distance on diagrams. We chose the network diagrams in Figure 3.1 as our example because they show an interesting use of the spatial dimension and how choices made in a visualization can change the impression created and the meaning conveyed. The figure shows different views of the network at different levels of granularity, and the spatial layout facilitates understanding by organizing entities according to group affiliation. Individual players that might be dismissed as inconsequential in the view on the top appear highly influential when shown banded together by a common cause on the bottom. Both views of the network are socially and mathematically valid. Tools that allow analysts to switch between levels of granularity in this manner enhance situational awareness.

Temporal perspectives on the IE are concerned with the timing of decisionmaking processes. For example, behavioral analysts and planners may be interested in exploring whether or for how long individuals in the target audience cling to old beliefs. They may also be interested in whether a lack of change indicates that (1) no new information has entered the system or (2) new information is present and being circulated but has been rejected. Timelines are a common means of displaying situational awareness of temporal aspects of the IE.

The security and trustworthiness of information flows are determined by the integrity, credibility, and number of both human messengers and electronic information systems involved in the transmission. How information is filtered, aggregated, and synthesized to produce knowledge affects the integrity of the information and is highly influenced by social factors. Perceptions of credibility can be a factor of not simply the source of information but also the path or process by which the information was obtained. For instance, information that is gained by eavesdropping is often perceived as more credible than that provided by more formal means of communication, especially if the source is perceived to be untrustworthy. Likewise, information gleaned from multiple sources is often deemed more credible than information obtained from

[26] This particular analysis was conducted to explore how international norms spread after World War I under the auspices of the League of Nations. See Martin Grandjean, "Intellectual Cooperation: Multi-Level Network Analysis of an International Organization," blog post, December 15, 2014.

Figure 3.1
Examples of Visualization of International and Multilevel Social Networks



SOURCE: Grandjean, 2014 (CC BY 3.0).

NOTE: Based on an analysis of tens of thousands of documents, the top diagram shows relationships among the approximately 1,700 individuals in the League of Nations and distinctions between groups. The bottom diagram shows a simplified version with correspondents grouped by affiliation, making it easier to trace influence.

RAND *RR2489-3.1*

a single source.[27] A replicable scale for measuring source reliability (or information believability) in traditional media and human interactions asks whether the source is fair and unbiased, tells the whole story, is accurate, and can be trusted.[28] In 2002, the Stanford Persuasive Technology Lab generated a set of ten guidelines associated with perceptions of website credibility, and researchers have proposed methods for automatically assessing the credibility of tweets.[29] However, credibility is intertwined with notions of both cognitive authority (i.e., those who exert influence are recognized as credible sources) and information quality, a subjective judgement of the goodness, usefulness, and relevance of information.[30] As such, measuring and communicating credibility for situational awareness remains highly subjective, and automated "credibility" metrics used to provide situational awareness of the IE must be approached with this understanding.[31]

Situational Awareness for the Physical Dimension of the IE

Situational awareness of the IE, including the temporal and security/trustworthiness aspects of communication, is also derived from the physical dimension of the IE. In the physical dimension, information sources and receivers can be mapped geographically and on a timeline. Information flows can be described in concrete terms, such as frequency, duration, and data rate. While the challenge in creating situational awareness from the cognitive and informational dimensions of the IE is to make abstract concepts

---

[27] Bill Hilligoss and Soo Young Rieh, "Developing A Unifying Framework of Credibility Assessment: Construct, Heuristics, and Interaction in Context," *Information Processing and Management*, Vol. 44, No. 4, July 2008.

[28] Philip Meyer, "Defining and Measuring Credibility of Newspapers: Developing an Index," *Journalism Quarterly*, Vol. 65, No. 3, 1988.

[29] B. J. Fogg, "Stanford Guidelines for Web Credibility," Stanford Persuasive Technology Lab, Stanford University, May 2002; Carlos Castillo, Marcelo Mendoza, and Barbara Poblete, "Information Credibility on Twitter," *Proceedings of the 20th International Conference on World Wide Web*, New York: Association for Computing Machinery, 2011; Byungkyu Kang, John O'Donovan, and Tobias Höllerer, "Modeling Topic Specific Credibility on Twitter," *Proceedings of the 2012 ACM International Conference on Intelligent User Interfaces*, New York: Association for Computing Machinery, 2012.

[30] Hilligoss and Rieh, 2008.

[31] In developing a typology of credibility, Rieh proposes distinguishing among source credibility (the believability of the communicator), message credibility (the resonance of the message among the target audience), and media credibility (including web-based media). As noted earlier, how information is processed affects credibility. Rieh distinguishes among conferred credibility (based on reputation), tabulated credibility (based on peer ratings), and emergent credibility (that which arises from pooling multiple sources). She also notes that while all cognitive authorities are credible, not all credible sources have cognitive authority. Therefore, a reasonable requirement for a situational awareness display of the IE might be to distinguish cognitive authorities from those that are merely credible and to determine whether source, message, or media credibility is at work. An additional drill to distinguish among conferred, tabulated, and emergent credibility may also be useful. See Soo Young Rieh, "Credibility and Cognitive Authority of Information," in Marcia J. Bates and Mary Niles Maack, eds., *Encyclopedia of Library Information Sciences*, 3rd ed., Boca Raton, Fla.: CRC Press, 2009.

clear, objective, and standardized, the challenge in the physical dimension is to ensure that concrete measures are not overemphasized in ways that detract from understanding the dynamics of the IE. For instance, frequent communication between geographically close participants may simply be routine correspondence with little influence, yet it could be misjudged as highly influential if it is shown as a thick line connecting two close dots on a geographic map.

The physical dimension of the IE is conceptually straightforward, but it is not always easy to accurately observe. For example, there are reasonably good national-level data on the use and penetration of the internet and other information and communication technologies. It is much harder to find reliable subnational-level data on communication technology penetration, but some scholars have used georeferenced surveys to produce better estimates and inform useful analysis.[32]

The physical dimension of the IE, especially the temporal dimension, is a valuable contributor to situational awareness. For instance, it is sometimes possible to detect "operations" in or from the IE by observing the physical patterns of routine correspondence and highlighting departures from that routine. Changes in both the frequency and duration of communications can be indicators of operations, but so can changes in the routing of information. Even attempts to obscure changes in communication by generating noise or spam can sometimes be detected, highlighting the criticality of extending operational security measures to the IE.

Current State of Situational Awareness of the IE: The Combined Information Overlay

JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment* provides guidance on the preparation of the combined information overlay (CIO), the current default approach to providing situational awareness of the IE.[33] Figure 3.2 shows an example of a CIO.

The CIO was first articulated by Marc Romanych in the early 2000s and represents one of the earliest efforts to visualize the IE.[34] The premise of the CIO is that it is sometimes useful to relate activities in the IE to activities in the spatial domains of warfare. Knowing the physical location of prominent individuals or groups within the IE and the time and physical place of their communications can be the difference between winning and losing. In these cases, it is useful to overlay information about the IE onto geographical maps used for planning operations in the physical domain.

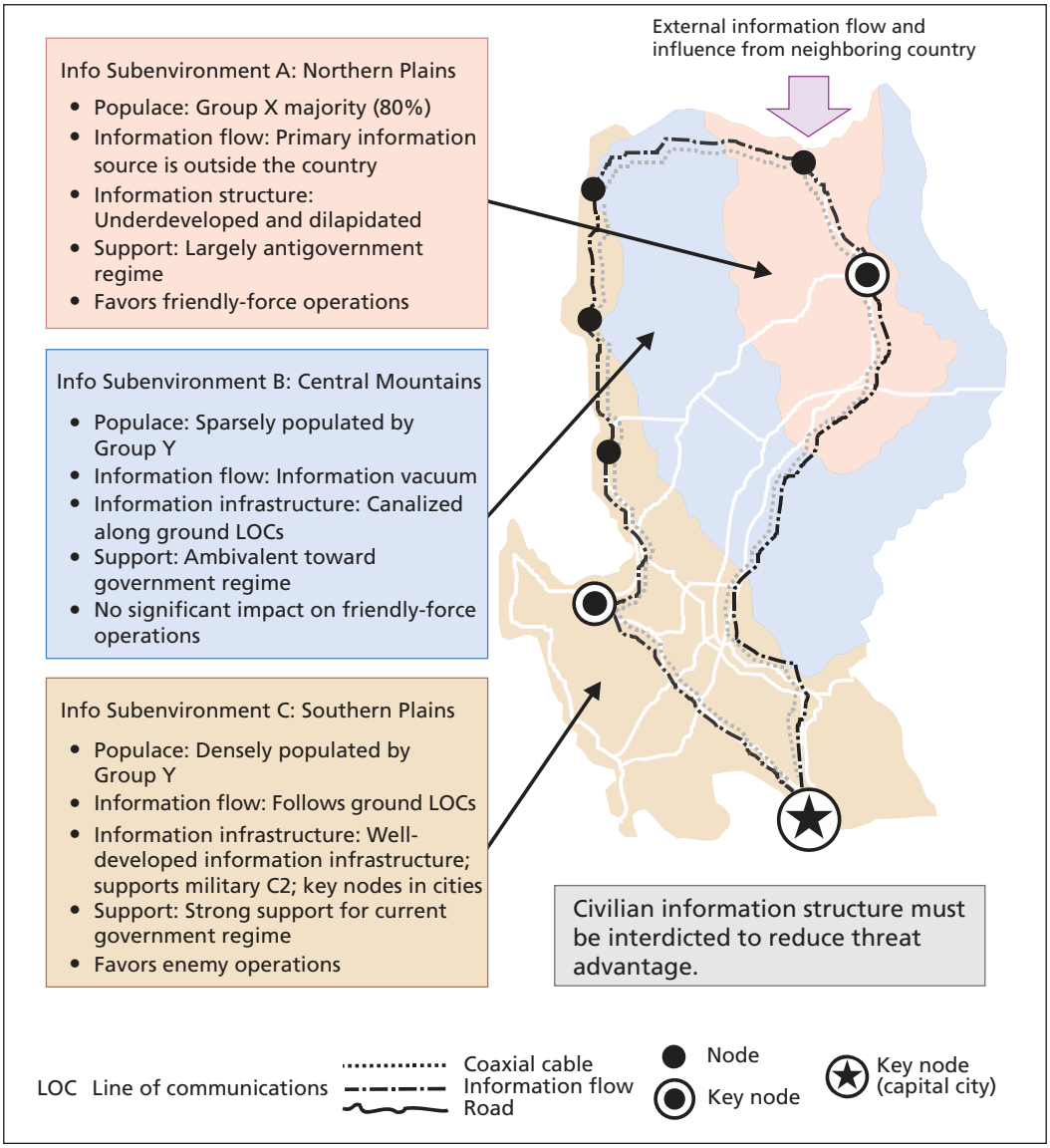
---

[32] See, for example, T. Camber Warren, "Explosive Connections? Mass Media, Social Media, and the Geography of Collective Violence in African States," *Journal of Peace Research*, Vol. 52, No. 3, 2015.

[33] Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, Washington, D.C.: U.S. Joint Chiefs of Staff, May 21, 2014, p. III-24.

[34] Marc J. Romanych, "Visualizing the Information Environment," *Military Intelligence Professional Bulletin*, Vol. 29, No. 3, 2003.

Figure 3.2
Combined Information Overlay as Depicted in JP 2-01.3



SOURCE: JP 2-01.3, 2014, Figure III-9.
RAND *RR2489-3.2*

The approach also fits the existing paradigm for situational awareness: Fundamentally, tools for situational awareness are based on maps and overlaid layers with additional geolocated features and information. These overlays can cover myriad topics (e.g., weather forecasts, soil density, terrain elevation, projected enemy force move-

ments). Maps and overlays could be physical (paper maps, acetate overlays) or digital, but the formats are conceptually the same. DoD concepts for visualizing situational awareness have not changed much since World War II, when paper maps and acetate overlays were used in much the same way in major headquarters. Note that the CIO has also not changed much since Romanych proposed it. Figure 3.2 showed the 2014 concept of the CIO as articulated in JP 2-01.3; it is virtually unchanged from Cordray and Romanych's 2005 version.

Not all information belongs on a geographic map, and too much information can degrade the commander's situational awareness through information overload (see the discussion later in this chapter). Knowing what to edit out of the overlay may be as critical as knowing what to put on it. Perhaps Cordray and Romanych said it best:

> The information included in the graphic can quickly become overwhelming if not presented in a concise manner. A refined and clearly presented CIO will usually have a greater effect on the commander than an overly complex graphic.[35]

New and Emerging Tools for Visualizing the IE

In the mid-2010s, work began on an integrated tool suite for C2 of the IE under the auspices of DoD's Strategic Capabilities Office. The tool suite includes an integrated common operational picture (iCOP) for displaying situational awareness. Early depictions of this display showed a variety of tailorable visualizations, including meters to display sentiments, map overlays to show where certain topics were trending, and social network diagrams. The types of displays and ability to tailor them are what we would expect to find in an iCOP; however, users should remember that simpler is often better. As with the CIO, knowing what to edit out may be the most critical skill in using the iCOP.

As part of other RAND research in support of the Strategic Capabilities Office, we compiled a list of tools related to situational awareness and C2 of the IE. We found approximately 70 tools either in use or in development across DoD, and we were able to gather sufficient information to characterize 64 of them. Project Noor was one of the most promising tools designed to enable situational awareness and assessment of the IE while also including key C2 concepts. Project Noor aims to provide USCENTCOM commanders with population-based and regional expertise in Syria or Iraq so they can interactively query social media and other data resources. It is meant to help commanders understand how to maneuver in the cognitive space. The goal as of May 2017 was to develop this interactive capability and create a proof-of-concept operational tool for early June demonstrations. Project Noor combines a number of existing tools and techniques from DoD and the wider U.S. government, including Athena. Athena is a decision support tool developed by Pacific Northwest National Labs to help the

[35] Cordray and Romanych, 2005.

commanders and their staffs understand the consequences of proposed actions in the operational environment as a function of political, military, economic, social, information, and infrastructure variables.

"As-Is" C2 and Situational Awareness at GCCs and Other Major Headquarters

In our interviews with stakeholders, we asked how C2 and situational awareness of the IE have been handled by staffs. This summary review of the "as-is" state focuses on conditions that predominate across the commands we considered. In speaking with stakeholders, we heard about temporary practices that were more successful than those that currently predominate—for example, a single-unit rotation or a specific commander's temporary staff organization and approach to achieving C2 and situational awareness. However, these pockets of excellence drifted back to baseline at the conclusion of the rotation or when that specific commander transitioned to a new assignment.

We drew these observations about the current state of C2 and situational awareness from interviews with personnel at a number of GCCs with perspectives spanning a range of staffing and other arrangements. We also spoke with individuals familiar with efforts at several joint task forces and service components. The current state of C2 and situational awareness of the IE as reported in these interviews was underwhelming.

Although many respected military theorists elevate the moral, the mental, the cognitive, or stratagem, the joint force has fallen into the habit of emphasizing the use of physical force against adversary capabilities at the expense of all other aspects of warfighting. Therefore, the IE is often an afterthought and not given significant attention for the purposes of C2, situational awareness, and intelligence collection. When it is considered, the emphasis on the IE defaults to "green" in operations: efforts aimed at indigenous publics rather than adversary forces or leaders. This is due, in part, to a failure to appreciate the potential of information and IRCs across the full spectrum of military operations—and this is reinforced by the heavy classification of the content and capabilities of some IRCs. When information efforts are focused exclusively on noncombatant populations, they end up being excluded from battle-oriented processes and procedures. Situational awareness of the IE is secondary to the situational awareness of friendly forces and enemy forces when the IE is viewed as only secondary or tangential to warfighting.

Because of the low level of priority and attention that it receives and because of the inherent difficulty in offering an effective display of the IE, the presence of the IE-related displays on most commands' watch floors is virtually negligible. The watch floor may include one or more televisions showing area of responsibility (AOR)–relevant news programs, but often not even that much.

The IE and operations in and through the IE are lucky to have a slide in the commander's update briefing, and the presence, style, and format of such a slide are not standardized, even though much of the other content of an update briefing *is*. Use of a CIO is fairly common. However, such an approach pretends that what is relevant

and significant about the IE can be sufficiently captured in the equivalent of a layer of acetate on a map. Current tools for presenting information for situational awareness are map-based. While they are technologically sophisticated in their ability to update in real time, rapidly change scales, and display numerous filtered layers of iconography, the fundamental principles are unchanged from World War II–era map boards with acetates and grease pencils. Some aspects of the IE can be meaningfully geolocated, but others cannot. Even those that can be meaningfully located lack a familiar and well-understood set of map icons akin to those used to denote military formations and features of terrain.

One of the reasons OIE are often excluded from displays and processes is their comparatively slow operational tempo. Physical maneuver and fires occur on much shorter timelines and are subject to C2 and situational awareness with rapid battle rhythms. OIE, by contrast, often have lengthy (and poorly understood) timelines, both for the preparation, authorization, and delivery of efforts and for the time they require to take effect. Thus, OIE are often crowded out by busy physical capability–oriented battle rhythms.

When IRCs are amenable to integration with air forces and fires (such as for electronic warfare or suppression of enemy air defenses), staffs effectively integrate these capabilities with existing C2 processes. However, absent a forcing function, staffs tend to default to emphasizing traditional physical capabilities and their effects in planning and execution.

Commanders typically organize for the IE in one of two ways: within a traditional staff structure (commonly J39) or as a separate directorate.[36] Whichever form they take, these structures commonly manage C2 and situational awareness for OIE in a piecemeal fashion, out of sight of the command and the rest of the staff and away from the watch floor. This is often sufficient when a command is operating under steady-state conditions and OIE are predominantly light-footprint, low-intensity efforts to set conditions or shape perceptions and preferences. However, such structures would be totally inadequate to support C2 and situational awareness of the IE as an integrated and integral part of a command's warfighting activities. While commands without areas of active hostility routinely exercise their warfighting staff processes, the IE rarely plays much of a role in those exercises, and most information-related staff have limited or no experience with OIE under wartime conditions. This lack of experience exercising OIE as part of broader operations extends beyond command staffs to training for the broader IRC community.[37]

---

[36] U.S. Joint Staff, J7, Deployable Training Division, *Communication Strategy and Synchronization*, Washington, D.C., May 2016a.

[37] One of the findings of Unified Quest in 2016 was a limited ability to demonstrate the effects of IRC operations when it came to combat training center rotations (U.S. Army, 2016, p. 12).

Insights on Doctrine and Practice, Roles and Responsibilities, and Solutions to Improve C2 and Situational Awareness of the IE

Doctrine Can Support Improved Practice

There is a gap between the emerging concepts for operations in and through the IE discussed in Chapter Two and current prevalent practice at the GCCs and other commands. As noted earlier, emerging concepts are not part of routine processes in these commands. However, our review of relevant doctrine finds that many existing processes could easily accommodate a greater focus on the IE.

For example, the joint operation planning process (JOPP) described in JP 5-0 provides ample opportunity to consider the IE and plan for operations in and through it.[38] JOPP also provides the opportunity to completely ignore the IE. However, if the commander's guidance to initiate planning at the beginning of the operational design process includes an interest in the IE, then everything that follows (including problem framing, specification of objectives and military end state, and courses of action developed) can also be mindful of the IE and its role in the planned effort. With the simple addition of the IE as a consideration, the other elements of the planning process can accommodate it.

Similarly, while numerous stakeholders reported to us that intelligence support for planning and operations in and through the IE is inadequate, it is our view that this is due to practice (especially habit and priorities) rather than a lack of opportunity in doctrine. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, includes numerous hooks amenable to greater inclusion of the IE and OIE-relevant considerations. Right in the summary, the document describes how one aspect of this preparation is the development of "a detailed understanding of adversary and other relevant actors' probable intent and future strategy."[39] Such an understanding is foundational to planning and executing operations designed to affect the behavior of relevant actors, and the development of such an understanding is already called for in doctrine. JP 2-01.3 has numerous other hooks for the inclusion of the IE in the form of explicit calls and general guidance. Examples include the discussion of defining the operational environment, evaluating the adversary and other relevant actors, determining the likely courses of action of those actors, and supporting JOPP. In fact, this latter discussion connects to the JOPP hooks in JP 5-0. If planners emphasize the IE to a greater extent as they work through that process, intelligence analysts preparing the operational environment to support JOPP should follow with increased emphasis on the IE. The actual detailed requirements and supporting analytic practices for intelligence support for operations in and through the IE is an area ripe for further research.

---

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

[39] JP 2-01.3, 2014, p. xi.

Other aspects of doctrinal processes may need some adjustment. Consider, for example, doctrine for targeting in JP 3-09, *Joint Fire Support*.[40] While the process does provide some possible opportunities for greater focus on the IE, effects are described only in terms of lethal and nonlethal (which is too limiting), and the time horizons discussed are often too narrow for efforts to persuade or influence targets. Target acquisition is described only as the detection, identification, and location of the target.[41] This is an insufficient number of layers for many OIE scenarios, in which greater understanding of possible targets is necessary to choose the right ones, and more detail about their disposition and proclivities is necessary to identify the right actions to take to drive them toward desired behaviors.

C2 and Situational Awareness of the IE Face Huge Seams

Both C2 and situational awareness of the IE face significant seams—areas that either overlap with or fail to cover the roles and responsibilities of those tasked with conducting operations in and through the IE. First, there is the issue of whether C2 and situational awareness staffs are functionally aligned to operate in the IE by themselves or as part of broader (and more kinetic) operations. Second, there is a substantial difference between undertaking steady-state OIE as opposed to OIE in a crisis or contingency. Third, there are differences between integrating the IE in deliberate planning and integrating the IE in rapid-reaction planning. Fourth, C2 and situational awareness approaches for OIE need to be able to handle and move between operating against a nation-state and against violent nonstate actors, and they entail collaboration with non-adversaries in a range of situations and scenarios. As the world moves further into the information age, the capabilities of both state and nonstate actors to operate in and through the IE will only continue to grow.[42] Finally, there are seams in operating with interorganizational, interagency, international, and multinational partners.

Situational Awareness Solutions for the IE Are Not One-Size-Fits-All

In reviewing the literature and discussing with stakeholders current and possible practice for situational awareness of the IE, we were struck by the diversity of possibly useful information about the IE. Not only does the IE have three dimensions (the cognitive, the informational, and the physical), but there is also considerable variation in context (the IE as relevant to a specific geographic area or region or for a specific actor or audience of interest). There was also considerable variation in interest, depending on the types of missions, operations, or activities on which a specific command might focus. For example, one command might be interested in monitoring networks

---

[40] Joint Publication 3-09, *Joint Fire Support*, Washington, D.C.: U.S. Joint Chiefs of Staff, December 12, 2014.

[41] JP 3-09, 2014, p. xiv.

[42] William R. Gery, SeYoung Lee, and Jacob Ninas, "Information Warfare in an Information Age," *Joint Force Quarterly*, Vol. 85, 2nd Quarter, 2017, p. 24.

for expressions of support for violent extremists (as indicators of supportive behavior toward terrorist organizations or as possible routes to radicalization or recruitment). Another might be interested in aggressor nation propaganda and its impact on democratic participation and perceptions of government legitimacy among citizens in an allied nation. Yet a third command may be watching potential aggressor command networks for indications that deterrence is failing and the aggressor intends to launch an invasion. A fourth command may be interested in permutations of all three of the previous examples.

Supporting this insight is the observation that a commander cannot know everything about the IE. There is simply too much that could be known. Any design for situational awareness that aspires to track and present everything about the IE will collapse under its own weight. Instead, command staffs must identify the elements of the IE that are relevant to their missions and responsibilities, then tailor the presentations and visualizations (and supporting data collection and analyses) accordingly.

Any given command staff must identify which actors in or associated with the AOR are relevant, what aspects of which dimensions of the IE that pertain to those actors they wish to monitor or understand, what observations or measurements can capture or approximate the needed information, how those observations can be presented and summarized, what level of detail or aggregation is appropriate to those presentations, and how frequently the underlying data and the resulting presentations can and should be updated. Since all of those elements potentially vary by context, by requirements of the command, or by the preference of the commander (or other senior staff), exactly how a given command maintains situational awareness of the IE must also vary.

Situational awareness becomes much more tractable when considering specific operational goals or effects. Rather than asking a very general and broad question—for example, "What could happen in the IE that would affect the security environment in our area of responsibility?"—staffs will find a more specific question a much better starting place to identify where the actors and the range of effects are constrained: "What might a specific terrorist organization do in or through the IE that would prevent us from achieving operational objective 2.1?"

Situational Awareness is Subject to Human Limitations and Information Overload

There was another challenge we observed that relates to situational awareness more generally but is particularly salient in the context of the IE: information overload. A great deal of information could be generated from or about the IE, but how would a staff make sense of it? One possible answer involves the use of automated processes to help reduce information overload, but the joint force must also be aware of the use of automation by other actors in an attempt to cause information overload.

Automation can be used to interact with the environment, with other systems, or with humans. The latter case is particularly important in the midterm because

automation assists in exploiting human limitations and is becoming more capable of doing so independently. These types of automation can be simple or complex and multifaceted. In either case, mitigating the propaganda effects of advancing automation is important.

A simple example is how automation is used to overload audiences by employing what other RAND research has called a *firehose of falsehood*.[43] Some suggestions for defense discussed in that research, such as forewarning, may be useful, but there is no panacea. Other methods of exploitation are more complex, such as exploiting decision timing and creating many alternatives to force decisionmakers to revert to inappropriate heuristics. Speier, Valacich, and Vessey show that interruptions can enhance performance of simple tasks but degrade performance of complex tasks.[44] This is relevant for real-time decisions and inputs; such techniques as minimizing unneeded interruptions may be important for countering the problem. Whether simple or complex, there is a need for research is needed on preventing the exploitation of these human biases, especially when interacting with disinformation and propaganda systems.

Human Limitations

In practice, humans suffer from several burdens of deficient decisionmaking, a product of incorrect understanding or deficient information processing systems. Heuristics and biases research, pioneered by Kahneman and Tversky, shows that people make decisions in predictably incorrect ways. Later research has shown that these heuristics are adaptive in some contexts but not in others. The implication is twofold: There is a need to understand how to enable better decisions in isolation and how systems could be built to mislead decisionmakers.

Preexisting beliefs and anchors can bias decisionmakers, and people tend to become more certain in the presence of more data, even when the additional data are not informative. Kahneman discusses systems designed with these limitations in mind, which can "nudge" better decisions.[45] Extending this concept to the current discussion, because these biases are known and partially understood, they can reduce the negative impact of the heuristic instead of just nudging. Two examples illustrate this point more clearly.

Because we know that people overestimate the importance of information, we can consistently frame evidence in context. For example, instead of saying, "The target has a threat score of 7," we might say that it is "in the top 23 percent of locations in the system," so it is clear where on the threat spectrum the target lies. Similarly, when presenting raw numbers, it is important to give context so that the evidence is not

---

[43] Paul and Matthews, 2016.

[44] Cheri Speier, Joseph S. Valacich, and Iris Vessey, "The Influence of Task Interruption on Individual Decision Making: An Information Overload Perspective," *Decision Sciences*, Vol. 30, No. 2, March 1999.

[45] Daniel Kahneman, *Thinking, Fast and Slow*, London: Macmillan, 2011.

overinterpreted: "There were 700 occurrences of threat-relevant phrases in online discussions in the past week, which is 3-percent higher than normal." Or "The difference is 0.1 standard deviations above the mean amount—and an increase but not a statistically insignificant one.

Another known bias in evaluating evidence is that people frequently double-count or "rehearse evidence" when presented with counter arguments.[46] For example, an initial report suggests there is an issue that a decisionmaker may take seriously. Over the next number of months, several other reports suggest it is not a problem. Despite this, as each new report is presented, the decisionmaker reconsiders the initial report as evidence of a problem. To combat this, each time a report is presented, it may be useful to explicitly mention all prior evidence relevant to the question. This way, when a question is reevaluated, the decisionmaker can ensure that the evaluation does not consider evidence that unreasonably favors the initial conclusion.

Reducing Information Overload

Clay Shirky put the challenge to human information processing simply: "It's not information overload, it's filter failure."[47] There are various methods for approaching the challenges of reducing and summarizing information, but the difficulties of considering, observing, and orienting are critical.[48]

Approaches for dealing with the problem of information overload are instructive but cannot resolve this central tension. Shirky himself suggests that "the older pattern of professional filtering of the good from the mediocre before publication [is broken]; now such filtering is increasingly social and happens after the fact."[49] By leveraging filtering, social media platforms are able to bring the most interesting (i.e., viral) content to the fore. Unfortunately, this approach is not a panacea, as "popular" and "useful" or "true" are not synonymous. Some level of automation is needed to process information, especially for making nonpublic decisions.

Opportunities to Better Incorporate IE Considerations in C2

Based on our review of current C2 and situational awareness practices, we identified four categories of opportunities to better incorporate consideration of the IE in future initiatives. Some of these opportunities are relevant to the requirements and organiza-

---

[46] Eliezer Yudkowsky, *Rationality: From AI to Zombies*, Berkeley, Calif.: Machine Intelligence Research Institute, 2015.

[47] Clay Shirky, "It's Not Information Overload, It's Filter Failure," keynote address, Web2.0 Expo, September 18, 2008b; O'Reilly Media, "Clay Shirky," keynote speaker bio, Web 2.0 Expo, 2008.

[48] Paul Rogers, Rudy Puryear, and James Root, "Infobesity: The Enemy of Good Decisions," *Bain Insights*, June 11, 2013.

[49] Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations*, London: Penguin, 2008a.

tional analyses presented in Chapters Four and Five, but others represent continuing opportunities for future improvement (and possibly further research).

First, there are huge opportunities related to *operational needs framing*. The IE is not sufficiently present in C2 and situational awareness activities, nor is it sufficiently prominent in commanders' thinking. C2 or situational awareness processes, structures, tools, and other capabilities that help increase commanders' awareness of events in the IE and how the IE might affect operations could help close this gap.

Second, there is an opportunity to improve *decisionmaking support* related to the IE. Not only is awareness of the IE lacking, but so too are tools and concepts to help visualize the IE. Commanders and planners could be better supported in visualizing and understanding the IE. They could be better connected to IE-related data and analysis—especially for warnings and indicators of activity or changes in the IE—and models to predict the impact in and through the IE of various course of action.

Third, there are opportunities to improve *information sharing* about the IE. These opportunities include better collection of intelligence, surveillance, and reconnaissance (ISR) of the IE, as well as concepts for sharing and accessing information both vertically across echelons and horizontally within DoD and across partner organizations.

Finally, it is possible to improve *analytical processes* related to the IE—not only the underlying models and analysis to support monitoring and forecasting (as noted earlier) but also concepts for machine indexing information about the IE to increase accessibility and enable analysis. These analytical processes could promote better understanding of human dynamics, including culture, narrative, and other relevant insights from the behavioral and social sciences. There is a need for better analyses of human decisionmaking, and the increase of autonomy creates similar opportunities to incorporate understanding of automated decisionmaking processes and AI in these analytical processes, too.

CHAPTER FOUR

Identifying Requirements for Effective C2 and Situational Awareness of the IE

This chapter enumerates requirements for effective C2 and situational awareness of the IE at a GCC or other major headquarters. Per request of the sponsor, the paramount focus here (and the subsequent analysis in Chapter Five) is on organizational requirements, though we also identify broader and more general requirements.

One of the challenges facing this effort to identify requirements for C2 and situational awareness of the IE was the fact that DoD OIE are a moving target. As noted in Chapter Two, there have been many new developments in concepts related to the IE. Many of these new concepts emerged or were published during the study period, and other efforts remained under way at the time of this writing in early 2018. Thus, the requirements we enumerate straddle a line between existing requirements for OIE as practiced and conceived during the 2017 research period and emerging requirements for how OIE are likely to be conceived in the near future. We identified both current and possible future requirements through a review of the literature and interviews with practitioners and stakeholders. While our questions for practitioners emphasized current requirements, these conversations unavoidably turned to future requirements or acknowledged the expanding role of information in operations and the changes and improvements in C2 and situational awareness that would be needed to support that growth. Where a requirement is discussed without citation, assume that the input comes either directly from a not-for-attribution interview with a stakeholder or from the research team's synthesis of stakeholder input and existing studies and documents.

Three Examples of OIE

To identify some of the challenges inherent in conducting C2 for OIE and to begin distilling additional requirements for effectiveness in this area, we considered the challenges and requirements inherent in specific missions across the range of military operations. We examined three mission areas in the abstract: humanitarian assistance and disaster relief (HA/DR), the purpose of which is to assist host-nation forces affected by tragedy (e.g., famine, drought, earthquake, tsunami); countering violent extremism (CVE), a catchall phrase for various forms of engagement focused on diminishing the

appeal of violent extremist ideologies and disrupting paths to radicalization with an ultimate goal of reducing terrorist violence; and major combat operations (MCO), specifically focused on ISR/strike operations, in which combat power is applied to delay, impede, halt, or dislodge the adversary, as well as to gain access to theater infrastructure and enhance friendly freedom of action. Although these three mission areas are not exhaustive of the range of military operations, they are broadly representative, with variation in intensity of operations, the presence of an adversary, and the nature of the adversary, and whether they are steady-state operations or operations conducted as part of declared hostilities.

A Selection of IE-Related Issues that Vary Across the Range of Military Operations

For the commander, there are several important priorities when considering the IE, many of which remain constant across the range of military operations. These issues include

- ensuring compliance
- force protection
- indications and warnings
- damage control/consequence mitigation
- support to strategic goals
- key leader engagement
- reassurance
- synchronization
- countering adversary ideology.

The remainder of this section describes each of these issues in the context of generic operations in each of the three categories (HA/DR, CVE, and MCO). It then turns to a more detailed examination using examples from specific cases.

In a HA/DR setting, ensuring compliance requires clearly communicating where citizens should go, what areas citizens should avoid, and how to behave at evacuation sites and aid depots to prevent overcrowding, rioting, or other dangerous situations. Force protection in HA/DR is geared toward striking the right balance between operations security accounting for possible threat actors in the vicinity and disclosure of pertinent information to partners, aid organizations, and aid recipients. For example, militant groups may monitor the timing of aid distribution and plan attacks on forces involved in distributing aid or protecting aid organizations. IE indications and warnings in a HA/DR situation prioritize finding out where militants are mobilizing in the IE and whether, for example, demonstrations are planned or forming, protests are mounting, or resistance or dissatisfaction is growing.

The IE can also be an avenue for damage control or consequence mitigation during HA/DR operations. If something goes awry during the operation, the joint

force could employ a range of response actions in and through the IE to mitigate fallout. The joint force can also work in and through the IE to contribute to strategic objectives by demonstrating and enhancing legitimacy, showcasing effective partnership, and increasing support both internationally and within the partner nation. Finally, key leader engagement with partner representatives and forces means working effectively with the partner nation to promote certain themes or actions, ensure that goals and objectives align, and avoid misleading or contradictory statements while also listening to leaders' concerns and preferences about the operation and its aftermath. HA/DR might also require reassurance, calming anxieties about the U.S. presence, U.S. objectives, and how long U.S. forces will remain. The joint force should promulgate a clear and consistent narrative regarding the HA/DR mission, its purpose, its scope, and its duration. To support this narrative, the operation must include efforts synchronize words and deeds—efforts to inject content into the IE through messaging and physical activities. To the extent that the mission context includes a threat actor, or even just an opposed counternarrative, the joint force would need to be prepared to counter adversary ideology by offering more positive and plausible explanations for U.S. presence and actions and by portraying the HA/DR operation as being in everyone's interests, including those of the threat actor's supporters).

CVE is an increasingly important policy goal for the West, especially as the Islamic State caliphate collapses, and the same lines of effort are relevant. Efforts to seek compliance should be focused, explaining and ensuring adherence to the terms of amnesty or disarmament procedures. Compliance enforcement might also be directed at partner-nation forces, promoting professionalism and respect for human rights to minimize the chance of catalyzing further resistance or radicalization. Force protection, especially operations security, is central to the counterterrorism portion of CVE. Compliance and force protection intersect when efforts in and through the IE seek to ensure noninterference with U.S. forces during infiltration or exfiltration. Indications and warnings in and through the IE help identify targets for counter-radicalization and may also indicate when CVE has failed and an attack by extremists is eminent. IE damage control or consequence mitigation plans should be in place in case there is backlash against the U.S. role or counterterrorism activities produce (or are said to produce) collateral damage. CVE largely takes place through the IE, so OIE will of course support strategic goals: delegitimizing violence and violence-promoting groups, providing alternatives for at-risk individuals, providing paths to deradicalization, and promoting alternative views and voices. Key leader engagement is important to sustaining the cooperation of partners in CVE efforts. In terms of reassurance, it is crucial to let broader audiences know that CVE efforts are not profiling specific communities and to explain that the point of working in specific communities is to help, not necessarily engage in punitive measures. Another important issue is synchronization and working to ensure that a CVE strategy is compatible with ongoing kinetic operations (if they are occurring in tandem). Moreover, discerning whether there is any attempt

to bring both approaches together under a more comprehensive plan to counter violent extremism could greatly enhance the long-term effectiveness of such programs.

Operations in and through the IE can simultaneously prevent panic and provide guidance, including on how to communicate with the public to inform people and communities of possible outlets available to them if they are suspicious of radicalizing behaviors among friends, family, or neighbors. At some level, there should be an effort to point out the bankruptcy and hypocrisy of violent extremist organizations' ideology and propaganda, something that can be done in and through the IE. Countering adversary ideology is one of the central focal points of CVE.

For MCO, there are myriad issues directly related to operating in and through the IE. Compliance could include providing directions to noncombatants on how to avoid being caught in the crossfire and which evacuation routes will lead them out of harm's way. Compliance could also be sought from adversary forces through instructions on safe ways to surrender when in untenable situations. Compliance could also be sought from adversary forces by pressuring, deceiving, or manipulating them to move (or not move) in certain ways. Force protection includes attempting to ensure that actions in and through the IE do not expose troop movements, operations, or elements of a campaign plan to the adversary or populations supporting the adversary. Against a near-peer adversary, operations security indiscretions (such as inadvertently revealing one's location through social media) could invite adversary indirect fires. Indications and warnings would focus on what is occurring in the IE that might give the U.S. military and coalition partners clues to ongoing or emerging issues with respect to adversary movement and maneuver, as well as help piece adversary efforts at deception.

A very real consideration related to damage control is how the United States might respond in and through the IE to reports of civilian casualties, both real and falsified, as well as those responsible for specific actions or negative consequences. IE support to strategic goals is potentially diverse and could include maintaining support for allied coalitions, seeking to undermine the legitimacy of continued adversary aggression among the adversary populations and stakeholders, or pushing adversary senior leadership toward perspectives and decisions that are consistent with strategic end states. Key leader engagement might focus on allies and partners, working with them to maintain unity of effort, avoid conflicting messages and clearly explain to populations in the area of conflict what is happening, where, and why. Local and international populations would need to be reassured about the legitimacy of the U.S. response, as well as the intended scope of hostilities and broader U.S. intentions. Synchronization of operations in and through the IE with all lines of effort is critical in MCO because all military activities have inherent informational characteristics. Failure to take them into account and synchronize them with other OIE could jeopardize the mission or prospects for achieving strategic outcomes. Countering adversary ideology may not seem like a primary emphasis in MCO, but as thoughts turn from not just

winning the war but to winning the peace, thoughts should also turn to the narratives and prevailing ideologies among the population and adversary forces.

Humanitarian Assistance/Disaster Relief

From the outset, the commander must have a clear understanding of the HA/DR mission and how the military, host nation, and other participants in the operation fit together. To be sure, it takes a considerable amount of time and information to stand up a headquarters, and short-notice requirements for assessment or delivery are common in HA/DR operations. Initial steps include reviewing the superior commander's guidance and direction, conducting mission analysis, preparing intelligence, and reviewing lessons learned and developing a battle rhythm. The United States has conducted HA/DR operations around the globe but especially in the U.S. Pacific Command AOR, providing relief in the aftermath of such natural disasters and extreme weather-related events as Cyclone Nargis (Burma, 2008), the Padang earthquake (West Sumatra, Indonesia, 2009), monsoon floods (Pakistan, 2010), and the Great East Japan Earthquake/Operation Tomodachi (Japan, 2011).[1]

Developing situational awareness and a common operating picture are keys to ensuring effective delivery of aid and assistance, tasks that are complicated during crisis events. Sufficient forces need to be assigned or tasked to develop and maintain a robust awareness of the situation to allow the commander to determine what information is necessary to reach a decision. Immediate tasks include determining safety concerns, such as navigation safety, air traffic control, and force protection. Robust situational awareness can help with the assessment of progress, including the disposition of friendly and enemy forces. In these scenarios, it soon becomes a prerequisite to determine what other elements are "on the ground" (e.g., host-nation government officials, nongovernmental organizations, allies).[2]

In Pakistan, Jamaat-ud-Dawa volunteers routinely assist in providing supplies and relief following natural disasters. Jamaat-ud-Dawa is a front for the militant group Lashkar-e-Taiba and uses its social service outreach to help "win hearts and minds" and influence the perceptions of local victims.[3] Other violent nonstate actors, such as Hezbollah in Lebanon and the Liberation Tigers of Tamil Eelam in Sri Lanka, have also historically benefited from similar activities.[4]

---

[1] Jennifer D. P. Moroney, Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom, and Abby Doll, *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region*, Santa Monica, Calif.: RAND Corporation, RR-146-OSD, 2013.

[2] Moroney et al., 2013.

[3] "Militant-Linked Muslim Charity on Front Line of Pakistan Quake Aid," Reuters, October 30, 2015.

[4] Shawn Teresa Flanigan, "Nonprofit Service Provision by Insurgent Organizations: The Cases of Hizballah and the Tamil Tigers," *Studies in Conflict and Terrorism*, Vol. 31, No. 6, 2008.

In HA/DR operations, the starting point is typically steady-state or low-intensity operations, in the sense that the mission is to deliver assistance, not to engage an adversary kinetically. The initial concern in these operations is the long-term narrative and influence—conveying to the local population who the force is, what it is doing, and exactly what aid it is distributing. There may be specific directions that need to be relayed, including where affected civilians should go (e.g., shelters) and other precautions that should be taken to avoid follow-on risks (from aftershocks, tenuously constructed buildings, and other hazards)

The major transition in steady-state operations is that there is either no baseline activity or the shaping effort has broader or different purposes. When a disaster occurs, the lack of baseline activity means that the operational tempo quickly shifts to "all systems go." This suggests the need for baseline shaping and preparation with a partner nation that has regularly occurring, somewhat predictable natural disasters or weather-related events. The situation on the ground can change rapidly, necessitating an ability to alter the narrative.

In Padang, Indonesia, there was no joint task force for C2 when the 353rd Special Operations Group set up a C2 center at Ta Bing Airfield to coordinate the U.S. military effort in the aftermath of the 2009 earthquake. Indeed, a joint task force (JTF) would have been useful to assist with the facilitation and overall coordination of U.S. assistance. The chief of staff of Combined Task Force–76, which oversaw these functions, stated that "the command and control of multiple service components was done informally. It worked because of the people involved, but a JTF would have provided clear-cut command and-control relationships."[5]

During Operation Tomodachi in Japan, there was friction between the decentralized U.S. approach to C2 and the centralized Japanese approach. There were also a number of issues related to tactical control versus operational control. In terms of C2, one of the most significant issues on the U.S. side was that while U.S. Forces Japan retained tactical control over forces, it did not have operational control. In addition, the United States and Japan did not have a shared common operating picture; both sides worked from different systems and processes until a new C2 structure could be put into place. The new C2 structure worked to streamline and facilitate communication between the United States and Japan, including videoconferences, liaisons, and coordination structures, but the main issue was that no one was really "in charge" of U.S. government assets. As a result, the response process was slow and redundant in some areas.[6]

[5] Moroney et al., 2013, p. 48.

[6] Moroney et al., 2013, pp. 85–102.

Countering Violent Extremism

CVE is a nascent field, and there are difficulties in both defining and measuring the progress of these efforts. Some critics believe that "violent extremism" is too broad a category to be useful, while others point out that the United States might not care equally about all kinds or typologies of violent extremism.[7] There has also been increased concerns over privacy, social network monitoring, and the narratives of long-term influence campaigns. Furthermore, measuring effectiveness of programs remains a major point of contention.[8]

Persuasive appeals can be delivered through a range of channels, from interpersonal (family, friends, other interlocutors) to media and direct communication with those considered vulnerable, as well as actual group members. Part of the mission is reaching individuals *before* the radicalization process ever begins, rather than reaching them in the midst of the process or once they are "past the point of no return."[9] Maintaining situational awareness is difficult because CVE is not simply the domain of the United States; it is being undertaken by multiple countries, agencies, and jurisdictions around the world—and in various ways, using myriad methods.

Clusters of activity might be apparent, but so much of the radicalization process takes place online that geography is far less important than the concept of the IE.[10] A CVE case can go from steady state to "on" the moment an individual moves from expressing thoughts, support, or sympathy for violent extremists to actually being a participant in violent actions.

Another way to conceptualize this shift juxtaposes the status quo of terrorist activity and propaganda in and through the IE with a period similar to the Islamic State's declaration of a caliphate in June 2014. It can be difficult to differentiate between steady state versus "on" because a continuous stream of terrorist propaganda may make it seem as though "on" has become steady state or vice versa. Simply reducing the volume of the messages could be an important indicator of success in limiting the exposure of broader populations to terrorist groups' appeal.[11]

---

[7] For a useful literature review, see Alex P. Schmid, *Radicalisation, de-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review*, The Hague, Netherlands: International Centre for Counter-Terrorism, 2013.

[8] Seamus Hughes, deputy director, Program on Extremism, George Washington University, "Combating Homegrown Terrorism," written testimony submitted to the U.S. House of Representatives Oversight and Government Reform, July 27, 2017.

[9] On various stages, including intermediate stages of radicalization efforts, see Christopher Paul and Elizabeth L. Petrun Sayers, "Assessing Against and Moving Past the "Funnel" Model of Counterterrorism Communication," *Defence Strategic Communications*, Vol. 1, No. 1, Winter 2015.

[10] This is not to say that face-to-face or in-person radicalization is unimportant. See Seamus Hughes, "To Stop ISIS Recruitment, Focus Offline," *Lawfare Blog*, August 7, 2016.

[11] Charlie Winter and Colin P. Clarke, "Is ISIS Breaking Apart?" *Foreign Affairs*, January 31, 2017.

There will be peaks and troughs when undertaking CVE efforts, as there are when dealing with the threat of returning foreign fighters. It is difficult to *prove* that CVE is working. There is the question of how CVE programs can measure whether individuals are dissuaded from engaging in terrorism, something that is necessary to evaluate which programs have worked and which have been unsuccessful as the academic and policy communities build a body of best practices and lessons learned from which to glean evidence to inform future CVE efforts.

Major Combat Operations

Conducting a mission ISR/strike and similar missions, especially against a near-peer adversary, means preparing to engage fully in the IE. The adversary will certainly be active in this space as well. This particular mission entails high-intensity, high-demand planning, with a focus on addressing short-term corruption, disruption, and usurpation and influence. In general, the targets are more likely to be state-owned military systems and professional troops. OIE are important not just for delivering effects on enemy targets but also because there is a need to maintain legitimacy domestically and internationally by explaining and justifying the overall operation and associated activities and events.

It is important to take into account a range of actors, including the adversary and host-nation leadership and populations. The commander will need situational awareness of the IE to determine what information is needed to achieve objectives and how the information can best be communicated. One particularly crucial step is figuring out whether existing data sources and tools can help and, if so, how they might best be applied. Commanders will need to know a great deal about enemy commanders to anticipate their likely actions and drive them toward courses of action that serve friendly objectives.

If there are visual tools that might to contribute to the commander's overall level of situational awareness, including what the adversary is doing in the IE, they may be instrumental to operating in an MCO. In this scenario, a commander seeks to create effects in and through the IE that provide a decisive advantage over adversaries. This means preserving and facilitating decisionmaking and the impact of decisionmaking while influencing, disrupting, or degrading adversary decisionmaking, and it will be complicated by the likely lack of air superiority and the adversary's ability to jam, disrupt, or disable friendly communication systems, satellites, and networks.

This scenario features a race to see which side can access, utilize, and project required information faster and with greater accuracy and clarity. Another goal is to influence the attitudes and behaviors of relevant audiences that will have an impact on operations and decisionmaking.

The United States must be able to operate in a degraded C4ISR environment where an adversary engages in cyber operations, electronic warfare, and other means to disrupt C2 and position, navigation, timing capabilities. Russia is a near peer in with

the ability to escalate through numerous options, as well as disrupt or interfere with ISR satellites. In the "on" state, C4ISR in and through the IE needs to be mutually supporting and, to the extent possible, able to operate effectively in a degraded environment. This stresses IO forces that are integrated and interoperable, including special operations and conventional forces in the area of operations.

The Russian armed forces and the militaries of many other near-peer competitors are capable of rapid, integrated employment of conventional kinetic and nonkinetic assets and can bring to bear air, missile, cyber, special operations, and electronic attack capabilities. The transition from steady state to "on" would be rather abrupt in this case, with steady-state activity, including exercises or training events. Once the conflict begins in earnest, the IE becomes highly chaotic, and clarity is difficult to achieve. However, communicating intentions still matters a great deal, especially when confronted by a truly multivector hybrid force.

A major challenge in such a highly kinetic fight against a capable adversary in a denied environment would be the patience required for OIE to work (and for a commander to "see" these operations working). The commander must recognize the importance of IE in a conflict with Russia before it is too late. By phase 2 (and before if possible), successful forces will have incorporated IE-related issues into the commander's planning process and raised awareness of IE considerations

Is this something that can be addressed by a change in organizational structure? One possibility is to make the IE the equivalent of a component (e.g., an information warfare command), but that would likely be a short-term solution at best. Because no single entity "owns" the IE, there is a dire need for cross-staff coordination and deconfliction (as well as cross-echelon coordination and deconfliction).

Requirements for Effective C2 and Situational Awareness in the IE

Drawing from considerations identified in these three examples of OIE, our extensive literature review, and interviews with stakeholders at GCCs, other major headquarters, and various IE-, IO-, and IRC-related offices in DoD, we distilled a set of summary requirements for effective C2 and situational awareness. We list and discuss those requirements here, beginning with requirements specific to effective C2 of the IE.

Understanding is foundational to C2 of the IE—both for formulating and choosing options and for sharing the concept of the problem and the proposed operational solution with subordinates.[12] Army doctrine for mission command notes that a commander's tasks include "understanding, visualizing, describing, directing, leading, and

[12] Joint Staff, J7, U.S. Deployable Training Division, *Geographic Combatant Commander (GCC) Command and Control Organizational Options*, Suffolk, Va., 2nd ed., August 2016b, p2.

assessing operations."[13] The general requirement for understanding includes knowing what motivates situational awareness, and this is why situational awareness is considered part of C2.

Beyond a general requirement for understanding, there are several specific levels of understanding required for effective C2 of OIE. Commanders and staffs must know what forces and capabilities are available that can affect the IE. This includes all of the traditional IRCs, especially those that are held at high levels of classification, such as military deception, special technical operations, and various special access programs. Commanders and staffs must not only be aware of these capabilities, but they must truly understand them to be comfortable calling for their use (and controlling them). This can be challenging because many in the joint force are not as familiar with IRCs as they are with the application of physical military force. Furthermore, many of the IRCs are inherently less predictable in their effects than other military capabilities precisely because they are not governed by physics.[14] Deception, for example, hinges on whether or not the target of deception actually observes the deceptive actions, whether or not the target "sees through" the deception, and how these perceptions actually affect the target's actions. Influence (through military information support operations or other means) depends on a host of factors, can take an uncertain amount of time, and can achieve uncertain levels of success.

Commanders and staffs that wish to achieve effective C2 for OIE must understand both the traditional IRCs available to them and the inherent informational potential of all available capabilities. Movement, maneuver, and fires can all contribute to deterrence or intimidation. Physical destruction can affect information flows by damaging communication and broadcast networks; cognitive effects are also possible for witnesses of destruction (whether direct witnesses or secondhand observers of audio, video, or even written or spoken accounts). The presence, posture, and profile of joint forces send messages that are often much more powerful than broadcast communications.

Commanders and staffs must understand not only how all of these capabilities can affect the IE (or deliver effects through the IE) but also the authorities, permissions, and procedures enabling their use. Effective C2 requires determining the processes and timelines required to employ certain capabilities, as along with an ability to track progress toward execution or delivery. Too often, opportunities to employ certain capabilities are missed because of a failure to allow sufficient time to attend to the necessary preparations and permissions.

Once the commander and staff understand what capabilities they can contribute to OIE and how to use them, they need to determine the objectives for their use. Clear goals or objectives are a critical requirement for effective C2 in the IE. They are also

---

[13] Army Doctrine Reference Publication 6-0, *Mission Command*, Washington, D.C., March 28, 2014, p. v.

[14] Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly*, Spring 2017, p. 55.

foundational for assessment.[15] Assessment is the means by which a commander or staff will measure progress toward those goals. Assessment is essential to C2 because it helps ensure continued progress and facilitates course correction by pointing out where progress has fallen short. Many stakeholders we interviewed emphasized the importance of assessment, noting requirements to report on status and the progress of efforts in and through the IE, plan ahead and measure baselines, consider how desired effects can be observed and measured, and support assessment design and planning, including directories or repositories of measures of performance and measures of effectiveness that have been used successfully in the past.

The requirement for clear goals and the ability to assess against those goals leads to the requirement to specify how the efforts of the command will lead to those objectives. Meeting this requirement demands understanding of human dynamics and the various processes and levers that drive behavior. With this information, planners can design a sequence of joint force actions that will plausibly lead to the specified outcomes.[16] According to JC-HAMO, "The Joint Force must analyze and understand the social, cultural, physical, informational, and psychological elements that influence behavior."[17]

Meeting these requirements is nontrivial, especially with regard to the iterative process of planning, designing, and assessing OIE. This leads to another C2 requirement: the need for sufficient capacity to staff OIE. This includes sufficient staff (and staff expertise) to plan, monitor, and assess OIE, as well as sufficient staff to ensure the horizontal integration of the various IRCs and other functional communities that contribute to OIE.[18]

Of course, OIE are not just about IRCs and the IE. Effects in the IE echo through the spatial domains, and physical actions generate or alter information. Thus, OIE need to be considered in all staff sections and all staff processes.[19] Because other operations will affect the IE, OIE must be integrated with other operations, and effects in and through the IE should always be able to contribute to other operations. OIE should be planned and integrated to support other operations, but staff structures and processes must also allow OIE to be supported by other efforts. There is a pressing requirement for the vertical integration of operations across the spatial domains, cyberspace, and the IE.[20] COL Tim Huening of the Army and Col. John Atkinson of the Marine Corps caution,

---

15 Paul, Yeats, et al., 2015.

16 Williams, 2017.

17 U.S. Joint Chiefs of Staff, 2016b, p. 1.

18 Dave Goldfein, "War in the Information Age," *Defense One*, November 16, 2016.

19 This point was raised in numerous interviews but is also documented in U.S. Army, 2016.

20 Goldfein, 2016.

> This reliance on technology and other processes [in support of conventional warfare], when combined with other shortfalls in Strategic Art, has typically resulted in insufficient strategic guidance, a misalignment of ends, ways, and means, wholly military solutions, fleeting military successes, and a consistent failure to deliver favorable political outcomes.[21]

The final but certainly not least important requirement for effective C2 for IE is the commander's interest in and attention to OIE. In the words of one stakeholder interviewed for this project, "The commanding general and key staff members must take ownership." If the commander ignores or just fails to emphasize OIE, the rest of the staff will likely choose to do so, too. The staff's priorities are the commander's priorities. Given the number of seams that OIE can fall into (as discussed in Chapter Three), these operations are very vulnerable when commanders fail to make the IE a point of emphasis or contribute sufficient time and attention to the subject.

We now turn to the requirements specific to effective situational awareness of the IE. The first and broadest requirement is for a responsive and capable ISR apparatus that is willing to observe and collect intelligence from the IE. One stakeholder pointed out "a very discernable gap of intelligence support" for IO and the IRCs. Other observers have noted that the "focus on 'enemy-centric' intelligence leaves U.S. forces vulnerable to manipulation and less attuned to drivers of conflict."[22] The commands' ISR resources and broader support from the intelligence community must be responsive to a wider range of collection requirements—and may well need new assets, tools, and analytical approaches.

A responsive and robust ISR apparatus could support the requirement for adequate observation and intelligence collection. The requirement is for "adequate" collection, not comprehensive or complete observation; as noted in Chapter Three, the IE is too vast and complicated to be wholly comprehended. Still, the requirement can be further specified, as there are certain areas of emphasis required in GCC or major headquarters operations.

One of these areas of emphasis must be observations focused on the IE and the context of the command's AOR, as well as identifying the relevant actors, determining courses of action available to relevant actors, and identifying which of those possible courses of action are likely.[23] The requirement includes the need to "collect and analyze the political, economic, social, and cultural dynamics" in the AOR.[24] Also included

---

[21] Tim Huening and John Atkinson, "Operationalizing Cyberspace to Prevail in the Competition of Wills," *Special Warfare*, July–December 20, 2016, p. 1.

[22] Christopher D. Kolenda, Rachel Reid, Chris Rogers, and Marte Retzius, *The Strategic Costs of Civilian Harm*, New York: Open Society Foundations, June 2016.

[23] U.S. Joint Chiefs of Staff, 2016b.

[24] Kolenda et al., 2016, p. 13.

are the various audiences, their beliefs and relationships, adversary supporters (and how to influence them), and adversaries' critical capabilities and vulnerabilities in the IE.[25] Numerous interviewees emphasized the importance of collecting data on adversary thought and decision processes and on their likely courses of action. A briefing we received captured a list of factors to understand about a relevant actor: values, beliefs, worldview, operational behavioral history and organizational dynamics, perceptions, motivations (needs and objectives), current capabilities, situational factors, decision processes, probable intent, likely behaviors or courses of action, vulnerabilities, influence susceptibilities, and accessibility.[26]

A second area of emphasis considers threats and possible adversary action in the IE. While the first point of emphasis focused on what the joint force needs to know about relevant actors' general intentions (and, if necessary, how to change them), this second area is more defensive in nature, seeking indications and warnings of how adversaries and others might be trying to affect the joint force in and through the IE.

Collection and observation alone are not sufficient; presentation, display, and visualization of observations and analyses are also part of this requirement. Unfortunately, according to Cordray and Romanych, "graphic representation of the information environment remains a challenge for IO staffs."[27]

Again, the IE is too vast and complicated to generate or sustain meaningful situational awareness, but effective situational awareness can be achieved through careful prioritization. What actors or aspects of the IE are of greatest relevance to the command? What command objectives can be supported (or thwarted) through the IE? Commands and staffs need to scale, scope, and prioritize aspects of the IE as priorities for ISR.

Finally, effective situational awareness of the IE requires commander interest and attention. Scarce ISR assets follow commander priorities, and if the commander deemphasizes the IE, so will ISR. If the IE is a point of emphasis, then that should be reflected in the commander's critical information requirements: priority intelligence requirements and friendly-force information requirements.

There are additional organizational requirements for effectiveness in the IE. The structure responsible for C2 and situational awareness of the IE must be sustained in low-demand, steady-state operations; that is, that structure must continue to function when the commands' OIE are at a very low level. This is a consideration for organizational alternatives that place OIE responsibilities in a separate structure with few other obligations. If such a structure were employed in a context with limited steady-state

---

[25] U.S. Joint Staff, J7, Deployable Training Division, *Communication Strategy and Synchronization*, Washington, D.C., May 2016a.

[26] Greg Jannarone, "Behavioral Influences Analysis Workflow Example," briefing slides, Maxwell Air Force Base, Ala.: Air University, undated.

[27] Cordray and Romanych, 2005, p. 7.

OIE, that structure might be (or just appear to be) predominantly idle, which would likely result in its rapid cannibalization by other (busier) structures.

Furthermore, whatever structure is responsible for OIE must be able to handle steady-state OIE and crisis or contingency OIE, as well as manage the transition between the two. These two conditions (steady state and contingency) might foster very different relationships with other structures within a command and thus deserve additional attention and consideration.

Finally, the structure responsible for OIE must have an understood place in the overall organizational structure and a clear place in the hierarchy and chain of command. If OIE C2 responsibility falls to a specific group, that responsibility must be clear to the rest of the staff. If OIE responsibility lies in a separate structure, the organizations within the command must understand how to relate to and interact with that structure. This would be easiest if the OIE structure were like some other existing entity, so a direct analogy could be made: "like a theater special operations command (TSOC)" or "like a service component command." If responsibility for OIE resides in some unique and separate position within a staff or structure within the command, there is a risk of constant organizational friction as personnel negotiate and renegotiate their interactions and relationships with that unique structure. This would likely be suboptimal.

We identified 17 summary requirements for effective C2 and situational awareness for operations in and through the IE.

Effective C2 for OIE requires

1. understanding the capabilities available to affect the IE (not just IRCs), as well as the inherent informational aspects of operations
2. understanding authorities and procedures
3. understanding what you want in the IE (clear goals)
4. knowing what progress toward those goals will look like (assessment)
5. having some concept of how you will get there (logic of the effort)
6. sufficient capacity to staff OIE
7. that OIE are considered in all staff sections and processes
8. that OIE are included/integrated with other operations
9. being able to staff OIE as supported or supporting
10. commander interest in OIE.

Effective situational awareness of the IE requires

11. a responsive and capable ISR apparatus
12. adequate observation and collection of intelligence on the IE
13. points of focus narrower than the entire IE
14. commander interest.

Additional organizational requirements for C2 and situational awareness of the IE include

15. the ability to sustain activities under low-demand, steady-state conditions
16. the ability to handle steady and contingency states and the ability to transition between the two
17. understanding of the place of IE-related staffs, structures, and organizations in the chain of command/organizational hierarchy.

Most of These Requirements Do Not Depend on Organizational Structure

Most of these requirements are independent of organizational structure. That is, they are no easier or harder to satisfy under different organizational structures. Because the analysis requested by sponsor focused on the ability of different organizational structures to meet C2 and situational awareness requirements for OIE, we reduced the list of requirements under consideration before moving to that analysis. Removing requirements that do not depend on organizational structure left us with the following list:

- The commander is attentive to OIE.
- There is sufficient capacity to staff OIE functions.
- OIE are considered in all staff sections and processes.
- OIE are included or integrated with other operations.
- The command is able to staff OIE as either supported or supporting.
- The command is able to handle both steady-state and contingency operations tempos (as well as the transition between the two).
- The command is able to sustain capabilities under low-demand, steady-state conditions.
- The place of OIE is understood in the chain of command/organizational hierarchy.

Chapter Five compares seven organizational alternatives for C2 of the IE against these eight requirements.

CHAPTER FIVE

Provisional Evaluation of Organizational Alternatives for C2

We evaluated seven organizational alternatives for OIE at the GCC level that emerged from the interviews, literature review, and related discussion: as is (in the staff), in the staff but more prominent, in the staff but with an element in each directorate, the equivalent of a domain component command, a subunified command (e.g., TSOC), a JTF, and a standing JTF or joint interagency task force (JIATF). We weighed each organizational option against eight criteria:

- the extent to which the structure would promote commander attention to OIE
- whether the new organizational structure would provide sufficient capacity to staff OIE
- the extent to which the IE would be considered in all staff sections and processes
- whether OIE would be included in or integrated with other operations
- the ability to staff OIE in either a supported or supporting
- the organizational option's ability to handle both steady-state and contingency operations (and transition between the two)
- the ability to sit idle (low-demand, steady-state operations)
- whether the considered organization would occupy an understood and accepted place in the chain of command and broader organizational hierarchy.

The analysis presented here should be considered provisional for at least two reasons. First, as noted in Chapter Four, the shape and role of OIE in the joint force is undergoing transformation and being reconceived; OIE and, thus, the requirements for C2 and situational awareness of the IE are moving targets. Provisional analysis is all that is possible until concepts have been settled and requirements stabilize. Second, the assessments informing this analysis are good-faith assessments based on the study team's subject-matter expertise. Although we are confident in the general direction of the assessments (whether an organizational alternative would represent improvement over baseline, for example), determining the relative magnitude of those improvements across alternatives is more speculative. Furthermore, we present the various requirements considered in an unweighted and unprioritized format. We believe that all the requirements identified are important, but we do not believe that they are all *equally*

important. How these requirements are prioritized in practice will depend on the specifics of the command. So, any effort to move these evaluations beyond provisional would need to confirm the salience of the identified requirements and the evolving demand for OIE and prioritize requirements to match the specific intended command context.

Descriptions of the Organizational Alternatives Considered

Our provisional analysis considered seven organizational alternatives for C2 and situational awareness for OIE. In this section, we briefly discuss each.[1]

As Is (in the Staff)

The as-is organizational option leaves responsibility for C2 for OIE in the GCC staff. C2 is ordinarily handled by the operations directorate (J3), usually in an IO staff section (J39). This option has the virtue of requiring no change whatsoever, but it would also likely preserve all the weaknesses noted in the section "'As-Is' C2 and Situational Awareness at GCCs and Other Major Headquarters" in Chapter Three.

In the Staff but More Prominent

In this organizational alternative, C2 for OIE remains in the GCC staff, but the responsible staff section is both more robust and more prominent—robust in that it has more personnel and more prominent in that it has a higher position in the staff hierarchy. In considering this alternative, we do not specify the manning level or a precise location in internal wire-and-block diagrams. We assumed that manning for this alternative would be adequate to the task (whereas many respondents reported that J39 sections are thin relative to their workloads). We also assumed that the section's position in the GCC staff put it at the full J-code level; that is, rather than housing OIE responsibility in J39 and subordinate to the J3, a more prominent role would be JX: The staff officer responsible for OIE is ostensibly co-equal with the other J-codes and reports directly to the commander (or chief of staff) rather than through a senior staff officer. This could be akin to experiments in the U.S. Army with G-7 as the "engagement" staff, or it could follow some other J-code designation or functional form.

In the Staff but with an Element in Each Directorate

In this alternative, C2 for OIE remains in the GCC staff. Additional personnel are assigned OIE responsibilities, but rather than residing in a single division, they are spread across the directorates so that each J-code has a division with OIE responsibili-

[1] The draft of this report included six alternatives, but a reviewer made a compelling argument for including a seventh, "in the staff, with an element in each directorate," based on his experience in J39 at a GCC in the early 2000s. We expanded the analysis to include that additional alternative.

ties. Thus, instead of just having a J39 IO division, the GCCs would have a J29, J39, J49, J59, J69, and so on. During steady-state operations, these divisions would both support their directorate and attend regular working group meetings chaired by the J39. During a crisis or conflict, these division staffs would all work directly under the J3 (or a deputy) on crisis action planning and execution, but they would still support integration and connectedness with their "home" directorates, where they would retain working and reachback relationships with other directorate personnel.

Equivalent of Domain Component Command for the IE

A series of more radical organizational alternatives would remove primary responsibility for OIE from the GCC staff and place it in a different structure. The first of these would assign responsibility to the equivalent of a domain component command for the IE.

Currently, each GCC is supported by a service component commander with primary responsibility for operations conducted by that service. These theater service component commands are "permanent organizations with responsibility for Service-specific functions including administration, personnel support, training, logistics, and Service intelligence operations" which retain their service responsibilities and authorities along with any additional authorities delegated or assigned by the GCC.[2]

Sometimes one in the same are functional component commands, where a command accepts responsibility for unity of operations within a domain. This typically follows the service component command assignments, with each responsible for its respective domain: Army (land), Navy (sea), and Air Force (air). This is most often necessary when there is significant involvement by more than one service in given operation, such as large numbers of both Air Force and Navy air assets. A functional component command is typically just an extra designation of an existing service component command and not actually a new or different organization (but it certainly could be).

Noteworthy for a domain component command is that it does not necessarily correspond to a service component command. For example, a GCC could have a cyber functional command, but there is no service-designated cyber force. Also noteworthy is that functional component commands can have oversight and responsibility for the operations of forces from multiple services.

These points both become relevant when considering OIE and the IE. Currently, the IE is not acknowledged as a warfighting domain, and it does not have its own service- or domain-specific forces. However, a functional component command does not have to correspond directly with a domain or service, nor is its responsibility confined to forces and capabilities from a single service. While it would certainly be *easier* to assemble and operate IE-specific functional component commands based on preexisting (notional) IE service-specific component commands, one can at least imagine (and

[2] Joint Staff, J7, U.S. Deployable Training Division, 2016b, p. 6.

consider as an organizational alternative) something like an IE functional component command.

Subunified Command for OIE

Another organizational alternative would remove primary OIE responsibility from the GCC staff and create a subordinate unified command (also called a subunified command) for OIE. A subunified command is a structure subordinate to a GCC that also employs (joint) forces. According to the J7's U.S. Deployable Training Division, "GCCs may establish subunified commands to conduct operations on a continuing basis when authorized by [the Secretary of Defense] through the Chairman of the Joint Chiefs of Staff." It adds that these subunified commands may be geographical (giving the example of U.S. Forces Korea and U.S. Forces Japan) or functional basis (similar to TSOCs and U.S. Cyber Command).[3] Clearly, a subunified command for OIE would be functional rather than geographic.

When considering this organizational alternative, we envisioned something like a TSOC for OIE. TSOCs are staffed primarily by special operations personnel and have all of the knowledge, understanding, and capability needed to plan, conduct, and perform C2 functions for special operations on behalf of the GCC. An equivalent structure for OIE is a sufficiently clear notion, but there is currently no arrangement for an OIE subunified command that is equivalent to the relationship between TSOCs and U.S. Special Operations Command.

JTF for the IE

Another organizational option would be a JTF for the IE. JTFs are typically stood up for a single, specific mission or operation and delegated significant authority to execute that mission.[4] JTF commanders still report to the GCC, but they have wide latitude and can draw on considerable support from other organizations and commands as they execute their mission.

JTFs are traditionally transitory in nature, being assembled and employed for a specific mission and then disbanding when that mission is complete. *Transitory* does not necessarily imply *short*. While some JTFs operate for months, others have lasted decades, such as JTF–Southwest Asia, which began in 1992 and remained active into 2003.

Standing JTF or JIATF for the IE

Like a JTF but more enduring is the organizational alternative of a standing JTF or JIATF. A JIATF includes direct participation by departments outside of DoD, but this does not imply any kind of authority or command relationship with DoD or other

[3] Joint Staff, J7, U.S. Deployable Training Division, 2016b, p. 8.

[4] Joint Staff, J7, U.S. Deployable Training Division, 2016b, p. 9.

departments. A JIATF does not even necessarily need to have a military commander. Given the number of other U.S. departments and agencies that also pursue and generate effects in and through the IE, a JIATF for OIE could certainly make sense.

The principal difference for this organizational option is the enduring nature implied by *standing*. JIATFs tend to be more enduring than JTFs, established to confront long-term mission needs. Participants also have shared authorities, processes, and procedures that can take years to formalize and finalize.[5] A standing JTF or JIATF would be very much like the previous organizational alternative but more enduring.

A good example is JIATF-South, headquartered in Key West, Florida. JIATF-South coordinates national and international efforts to stem the flow of drugs through the Caribbean and into the United States. It was established in 1999 and has grown and evolved considerably since that time.[6]

Provisional Analysis of the Organizational Alternatives

Table 5.1 presents a summary of our provisional analysis of the seven organizational alternatives against the eight requirements identified and described in Chapter Four. In keeping with the provisional nature of the analysis, the extent to which each organizational alternative satisfies each requirement is somewhat provisional as well. In the table, where an organizational alternative appears to wholly or sufficiently satisfy a requirement, a cell contains a check mark (√). Where an organizational alternative appears significantly lacking or likely to fail to meet the criterion, the cell contains an X. Where the organizational alternative partially satisfies the criterion, the cell is marked with a ½. These three scoring levels are always ordinal to each other; that is, a check is always better than a ½, which is always better than an X. However, we acknowledge the potential for unscored variation within the categories: Some halves may be better than others but still fall short of wholly meeting the requirement, and some Xs may be worse than others, with some being merely inadequate while others are complete failures. Fine-grained comparison within a level requires care or, perhaps, additional analysis. Finally, a question mark (?) indicates "it depends." This score appears only in the column for the requirement "Commander attentive to OIE," which under three of the alternatives is wholly dependent on the proclivities of the individual commander; under the four other alternatives, the commander is exclusively and specifically responsible for the OIE and so is organizationally constrained to be attentive to it. In the remainder of this chapter, we evaluate each of the organizational alternatives.

---

[5] Joint Staff, J7, U.S. Deployable Training Division, 2016b, p. 10.

[6] For more on the history and organizational effectiveness of JIATF-S, see Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, Calif.: RAND Corporation, RR-1600-A, 2017, chapter 2.

Table 5.1
Summary of Provisional Organizational Analysis

	Alternatives						
Criteria	**As is**	**In the staff but more prominent**	**In the staff, with an element in each directorate**	**Equivalent of domain component command**	**Subunified command**	**JTF**	**Standing JTF or JIATF**
Commander attentive to OIE	?	?	?	√	√	√	√
Sufficient capacity to staff OIE	X	½	½	√	√	√	√
OIE considered in all staff sections and processes	X	½	√	√	√	√	√
OIE included/ integrated with other operations	½	√	√	√	½	√	X
Able to staff OIE as supported or supporting operations	X	½	√	√	√	√	X
Able to handle steady-state and contingency operations	X	½	√	√	√	X	X
Able to function in low-demand steady state	√	½	√	X	X	X	X
Understood/ accepted place in chain of command/ organizational hierarchy	√	√	½	X	½	½	X

NOTE: √ indicates that the organizational alternative wholly or sufficiently satisfy the requirement. X indicates that the organizational alternative is significantly lacking or likely to fail to sufficiently meet the requirement. ½ indicates that the organizational alternative partially satisfies the requirement criteria. ? indicates that the ability to meet the requirement depends on any of a number of factors.

As Is

Keeping the organizational structure as is means that effectiveness would wholly depend on the interest of the commander. In short, the result remains unknown, but the status quo might not be enough to garner adequate attention from the commander. Other negative aspects of this arrangement include an insufficient capacity to staff OIE and an inability to staff OIE as either supported or supporting operations. Furthermore, while this structure pairs well with an ability to sit idle, it leaves much to be

desired in terms of handling steady-state and contingency operations and transitioning between them.

Positive characteristics are that staff functions could be responsive as needed, with no organizational overhauls. Readiness would be less of an issue because this option does not involve establishing a large and possibly cumbersome headquarters. This arrangement might provide decision space for combatant commanders to interact with host-nation leaders and focus on the broader AOR, but, ultimately, it would not succeed in affording more resources and garnering greater attention from the commander. It was the least attractive option of all the alternative organizational structures that we assessed.

In the Staff but More Prominent

More robust and prominent OIE staffing would be better than the baseline but still highly dependent on the commander's emphasis. Accordingly, this option would only go partway toward achieving sufficient capacity to staff OIE and to ensuring that the IE considered in all staff selections and processes. Moreover, it remains unclear just how effective this organizational structure would be in staffing OIE as either supported or supporting operations. Also unclear is its ability to handle steady-state and contingency operations or the transition between them. Finally, it may lack the reach that a higher-level command structure could afford.

This option would help significantly with ensuring that the IE is included and integrated with other operations and would foster greater acceptance and understanding of the IE in the chain of command and organizational hierarchy. A more prominent role in the staff could empower subordinate commands to conduct operational-level missions, while supporting elements could focus on a return to steady-state AOR-wide operations in the longer term.

In the Staff but with an Element in Each Directorate

This option has a lot to recommended it. Though it is still sensitive to variations in focus and attention from the commander, it ensures the presence of IE-conscious staff across all directorates and institutionalizes processes for integration across the staff. A particular strength of this organizational alternative is its flexibility. Staff from the various X9 divisions can align and aggregate as needed during a crisis or contingency, but their dispersion during periods of low IE-related demand supports the development of habitual relationships and the possibility of additional support for other directorate-level tasks as ancillary duties.[7] Under this design, it is still possible that demand for OIE staffing and expertise could overwhelm capacity—perhaps drawing personnel

[7] Currently, J39 is the the only Joint Staff IO directorate/division; it is the information division (9) within the operations directorate (3). This alternative proposes a "9" division in each J-code. Thus, J29 would be the IO division (9) within the intelligence staff (2), J59 would be the IO division in plans (5), and so on. Here, X9 stands in for the directorate and its "9" division.

from the other directorates' divisions (e.g., J29, J49) into more routine support of J39 and thus diminishing their connectedness to their "home" directorate. This is also not a typical or traditional staffing relationship, something that could result in friction or misuse due to a misunderstanding of the roles of X9 divisions within their staff directorate.

Equivalent of Domain Component Command for the IE

Supporting the equivalent of a domain component command for the IE was one of the most highly rated alternatives. However, with no service responsibilities and no clear force provider role, there are some cons to this organizational structure. Other negatives include a questionable ability to sit idle or find an accepted place in the chain of command the lag time needed to establish a new domain component command, and the likely a struggle to acquire resources (perhaps not initially but over time). This option would necessarily involve establishing a large and possibly cumbersome headquarters and bureaucracy, which could have a deleterious effect on agility in the IE.

On balance, the positives outweighed the negatives. This alternative scored high marks on commander attention, providing sufficient capacity to staff OIE, ensuring that the IE is considered in all staff sections and processes while also being included and integrated with other operations, and being able to staff OIE as supported or supporting operations, as well as on its ability to handle steady-state and contingency operations. The need for a global common operating picture and the dynamic prioritization and allocation process should be enabled by this structure, coupled with an ability to provide robust support to subordinates' requirements and increased commander involvement with component input.

Subunified Command for OIE

The option of a subunified command for OIE also received an overall positive assessment, with shortcomings in some specific areas. Like other alternative organizational structures, it would not fare well sitting idle in low-demand, steady-state scenarios. And it might not be as strong as other organizational arrangements in facilitating the inclusion and integration of OIE with other operations, nor would it find itself as comfortably placed within the organizational hierarchy. In terms of readiness, there is the potential for significant capacity shortfalls in directing a non–warfighting-focused response to a crisis under this arrangement. In short, it could lead to good internal integration but possibly poor upward or lateral integration.

Overall, however, this structure would include a commander who is attentive to the IE, provide sufficient capacity to staff OIE, and ensure that the IE is considered in all staff sections and processes. A subunified command would increase the prospects of staffing OIE as supported or supporting operations while also handling steady-state and contingency operations and the transition between them. Other benefits to this structure include resident regional and functional expertise and personnel who have

experience planning military information support operations in peacetime and during limited crisis-response events. Indeed, it is common for TSOCs to focus on broad and continuous missions, and this arrangement offers multiple options for tasking and deploying C2 elements to match special operations capabilities and meet GCC requirements. Through experience and familiarity with geographic AORs, this arrangement would leverage the global special operations network to complement other means for maintaining global and situational awareness.

JTF for the IE

A JTF for the IE could have trouble "turning on and off" and thus might not be ideally suited to either sit idle or to handle both steady-state and contingency operations and the transition between them. Responsibility for transregional and multidomain operations could be challenging, and time and resources will be required for the JTF to form, receive personnel, and achieve operational capacity. This structure could place limits on a GCC's agility to rapidly shift forces to other emergent challenges in the AOR.

The single-mission focus and ability to closely integrate forces in the objective area would be a benefit, as would relying on the existing organizational structure, developed understanding of the AOR, and preestablished relationships. This structure would limit disruption to the theater C2 architecture, and, like the fourth alternative structure (equivalent of a domain component command for the IE), this option was positively assessed in terms of commander attention, providing sufficient capacity to staff OIE, ensuring that the IE is considered in all staff selections and processes, being included and integrated with other operations, and being able to staff OIE as supported or supporting operations.

Standing JTF or JIATF for the IE

The final alternative organizational structure that we considered was a standing JTF or JIATF. This option could be a strong performer in busy steady-state operations. It could also be good on the joint, interagency, intergovernmental, and multinational problem. However, it could struggle to mount a surge in a crisis or contingency. In short, it would likely prove difficult to have a JTF for steady-state operations—unless it was an extremely busy steady state. Other important factors to consider are the time delays and risks associated with JIATF headquarters activation even under the best of circumstances. This is in addition to challenges of coordination, synchronization and information sharing with interagency and multinational partners. Interagency partners could have primacy and legal authority, while a JIATF-type organization could provide a wide range of supporting capabilities for multiple contingencies. That said, as discussed earlier, successful JIATFs can take years to develop.

Pros of this arrangement are that a JIATF often includes a wide array of specialized experts, including those with law enforcement, military, and intelligence backgrounds. It is one way to use a complex organization to counter a complex problem—

operating in and through the IE. Indeed, under a single command, streamlined processes improve unity of effort. This structure could also make the commander more attentive to the IE, and it could have sufficient capacity to staff OIE and ensure that the IE is considered in all staff sections and processes.

CHAPTER SIX

Conclusions and Recommendations

The IE is growing in importance, and the extent to which operations in and through the IE are acknowledged as important within DoD is growing, too. There have been numerous conceptual advances related to operations in and through the IE in recent years. All of this means that requirements for these operations remain a moving target; subsequent research on optimal organization may need to consider revised and expanded requirements drawn from revised and expanding concepts related to operating in the IE.

The current state of C2 and situational awareness of the IE at the GCCs and other major headquarters is underwhelming. Our interviews revealed that the IE is predominantly an afterthought; when it is considered, the emphasis tends to fall on noncombatant populations rather than threats or adversarial actors. Commanders and staffs often fail to appreciate the potential of OIE, IO and the IRCs are largely excluded from battle-oriented processes and procedures, and IE-related displays are virtually negligible on the watch floor and all but absent from the commander's update briefing. OIE are often crowded out by busy (and faster) physical capability–oriented battle rhythms. C2 and situational awareness for OIE are handled in a piecemeal fashion, out of sight of the commander. The IE rarely plays much of a role in exercises, and most staff have limited or no experience with OIE under wartime conditions (even exercises).

Our research on existing concepts and practices highlights a number of insights that, while tangential to the primary inquiry, are still worth noting:

- There are hooks in much existing doctrine for improved practice and an increased emphasis on the IE.
- C2 and situational awareness of the IE face significant seams, including their roles and responsibilities in separate OIE versus OIE as part of larger operations; steady-state OIE versus OIE in a contingency; baseline steady-state OIE versus those that set the conditions for a possible future contingency; integrating the IE into deliberate versus rapid planning; OIE against state actors, nonstate actors, or non-adversaries; and integration with interagency and international partners.

- Situational awareness solutions for the IE are not one-size-fits-all; different commands will be concerned with different actors, different types of actors, different aspects of the IE, and different contexts.
- Information overload and other human vulnerabilities create possible weaknesses that the joint force will need to guard against.

We identified 17 summary requirements for effective C2 and situational awareness for operations in and through the IE. Effective C2 for OIE requires

1. understanding the capabilities available to affect the IE (not just IRCs), as well as inherent informational aspects of operations
2. understanding authorities and procedures
3. understanding what you want in the IE (clear goals)
4. knowing what progress toward those goals will look like (assessment)
5. having some concept of how you will get there (logic of the effort)
6. sufficient capacity to staff OIE
7. that OIE are considered in all staff sections and processes
8. that OIE are included/integrated with other operations
9. being able to staff OIE as supported or supporting operations
10. commander interest in OIE.

Effective situational awareness of the IE requires

11. a responsive and capable ISR apparatus
12. adequate observation and collection of intelligence on the IE
13. points of focus narrower than the entire IE
14. commander interest.

Additional organizational requirements for C2 and situational awareness of the IE include

15. ability to sustain activities under low-demand, steady-state conditions
16. the ability to handle steady and contingency states and the ability to transition between the two
17. understanding of the place of IE-related staffs, structures, and organizations in the chain of command/organizational hierarchy.

Starting with the requirements that depend in whole or in part on a given organizational arrangement, we conducted a provisional analysis of seven organizational alternatives: "as is" (in the staff), in the staff but more prominent, in the staff but with an element in each directorate, the equivalent of a domain component command for IE, a subunified command for IE (e.g., TSOC), a JTF for the IE, and a standing JTF or JIATF for the IE.

Comparing the seven organizational alternatives, we found that each has different strengths and weaknesses. The provisional analysis here does not unambiguously endorse any of the alternatives as the obvious solution for every GCC. It does, however, provide useful decision support for any GCC. Any GCC considering how to organize for C2 of OIE should first consider the relative importance of the eight requirement criteria within its context and command. An organizational alternative that satisfies the most important of those criteria (recognizing that priorities may vary across GCCs)—and satisfies other organizational criteria (such as cost-efficiency, organizational consistency, or commander preference)—should be strongly considered.

Recommendations

Based on these conclusions and the findings of this research, we make the following recommendations:

First, *DoD should make changes across doctrine, processes, education and training, and tactics, techniques, and procedures to appropriately emphasize the importance of OIE and the role of OIE in combined-arms and multidomain operations*. Addressing many of the gaps, shortfalls, and requirements that we have identified demands a greater understanding of the IE, new concepts for OIE, and details of IRCs across the joint force. This understanding must be inculcated in junior and noncommissioned officers as they progress through their careers to senior staff and command positions. These processes and the necessary appreciation and understanding must be introduced in training and education, and they should be routinized and standardized in doctrine and procedures.

Second, building on the first point, *DoD should make OIE an integral part of joint force staffing and operations—always*. If DoD aspires to the tier 3 vision shown in Figure 2.5 in Chapter Two, under which all operations are conceived of as seeking to shape the behaviors of relevant actors to achieve enduring strategic outcomes, then influence must become the lingua franca of operational art. Existing doctrine and practice include *opportunities* to consider the IE, should the commander and staff be so inclined. We recommend changes to doctrine and processes that make consideration of the IE and articulation of problems and objectives in terms of relevant actor behavior *compulsory*.

Third, when GCCs decide how to staff and organize for C2 of the IE, they should *choose C2 structures that align with priorities in the specific theater*.

Fourth, when preparing presentations or visualizations of the IE, *match visualizations to specific situations or operations and specific commanders*. Do not expect one-size-fits-all situational awareness or presentational solutions for the IE; it is too complex, diverse, and extensive.

Related to the fourth point, we recommend that *visualization tools offer a host of default options to help ensure that at least one meets any given contextual need*. No single combined information overlay or display of the IE will be sufficient for all areas of operations and all types of missions. Instead, where possible, display and visualization designers should offer numerous customizable layouts so that end users do not have to start from scratch and can easily consider a range of possible displays, select the visualization that best meets their needs, and then refine or customize it as required.

Finally, we recommend that the DoD intelligence apparatus and the supporting intelligence community *refocus existing capabilities and develop new capabilities to better observe the IE, with a particular emphasis on the proclivities, intentions, and decisionmaking processes of relevant actors*. New ways of operating and a new emphasis on operating in and through the IE require a new understanding of the operational context. The exact details of the changes and improvements required will need further research or experimentation.

For Further Research

The findings from this project suggest several possibilities for further research:

- Advance the provisional organizational analysis presented here by refining requirements in light of emerging concepts; exploring practical considerations under different scenarios, either the three addressed here or other scenarios that capture different operations or contexts; conducting organizational analysis specific to specific GCC contexts, with stakeholder input to prioritize evaluation criteria; and capturing the details of organizational alternatives with greater granularity.
- Extend consideration of C2 and situational awareness of the IE to lower echelons, from operational to tactical formations.
- Explore the requirements for intelligence support to OIE, including approaches to reporting and displaying data and analyses.

There are other relevant research opportunities that extend beyond the topic of C2 and situational awareness for operations in and through the IE. Given the requirement for greater understanding of IRCs and OIE among staffs and commanders, research on the content and extent of training and education on OIE and the IRCs available to the force could be rewarding. Similarly, there is room for research on defensive OIE. While joint concepts related to OIE mention the protection of joint force decisions and forces, actual processes and practices for doing so are lagging and could be more extensively developed. This could include further research into countering misinformation and strengthening weaknesses or vulnerabilities created by human, cultural, and organizational biases unavoidably present within the joint force.

APPENDIX

Automation, Machine Learning, and Computational Propaganda

The prospect of autonomous warfare has been discussed for decades, but most of these discussions focused on the physical domain. Crude automation has long existed in the form of digital communication networks that are programmed, but modern automation has gone much further and is poised for continue advancing. DoD is actively looking to leverage these capabilities in support of C4ISR,[1] but it needs a fuller understanding of what is and is not possible to determine where different approaches to automation, AI, and machine learning may be viable.

Types of Automation

The spectrum from early automation to future systems is one of degree and one of fundamental changes in systems. Depending on the applications being discussed, the terms *automation*, *machine learning*, and *AI* can refer to different types of systems, or they can be synonymous. In this discussion, we use these terms to refer to different types of systems. Understanding these differences is important to understanding how these terms can and cannot be used. In the context of OIE, automation is relevant in at least two ways: first, for supporting the refinement of information as part of situational awareness (to avoid or reduce information overload) and, second, as an element of influence or propaganda campaigns for automated content generation and refinement.

Direct automation is a program that executes prespecified actions chosen on the basis of experts' understanding. This could include anything from a simple program with no conditional logic that automates a single, repetitive task to an "expert system" that is programmed to evaluate complex questions and recommend actions or responses according to a preprogrammed logic tree. This range captured almost all computer programs until recently. These systems can be incredibly complex—but their complexity derives from programmed behavior.

[1] Office of the Secretary of Defense, Rapid Reaction Technology Office, "Cyber S&T COI Needs Statement, Solicitation RRTO-20170710-W-CyberCOI, July 10, 2017.

Machine-learning systems differ from direct automation in that they "learn" from data provided instead of being directly programmed. This means that the system can determine the relationship between an input and the appropriate output based on previous validated decisions.

For example, if most pictures with a specific pattern and a particular range of colors depict cats, a machine-learning system will assume that future pictures of this sort are also cats. Depending on the data chosen as inputs, there can be two notable consequences. First, typical machine-learning systems are vulnerable to specific types of manipulation of their inputs (sometimes termed *adversarial examples*). This means that these systems may be relatively easy to fool. Second, a system's performance can degrade rapidly when the input data differ from the data set used for training. This topic has been discussed extensively in the literature.[2]

Finally, AI, for the purpose of this discussion, is a system that reacts to novel situations in ways similar to humans. Artificial narrow intelligence (ANI) models are used by the game-playing systems Deep Blue and AlphaGo. Artificial general intelligence (AGI) systems are still in development but, in concept, they allow the general application of intelligence to different classes of problems. The demands of the IE are less structured than the current applications for ANI systems, and those systems' success is far more limited when the rules are less clearly defined.

Requirements for Automation

Direct automation requires specifying a response or action in every case considered. This can require specifying a large number of responses, especially when there are significant numbers of conditionals and possible cases for the system to consider. Machine learning and AI do not require directly specifying the responses; instead, these systems respond based on training and learned cues. This process requires a data set from which to learn, and the data set must therefore cover enough cases to allow the system to be trained.

Machine-learning and AI systems can take several forms, principally categorized as supervised or unsupervised learning. *Unsupervised learning* occurs when the system is trained to categorize data into groups or to detect outliers and anomalies. For the purposes of this discussion of automation, we are more concerned with *supervised learning*, when algorithms receive or generate input data with known correct responses.

Machine-driven communication (MADCOM) occurs when automatic systems interact with each other and with humans—and it is not always readily apparent to a human user whether a given interaction is with a human or with an automated system. These systems are potentially important both for automating tasks typically performed by humans and for interfering with or manipulating other systems.

---

[2] See Osonde A. Osoba and William Welser IV, *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017.

Using these definitions, we discuss how these types of systems can be applied to C4ISR in and through the IE. However, before discussing applications, we address the specific challenge of propaganda, then provide a specific example of how these three classes of techniques are used in other settings.

Example: Levels of Automation and Autonomy

Automation in vehicle operation is less structured than most current domains for machine learning and ANI. It has already advanced through the early stages of ANI, so less speculation is necessary to explore its potential. Another advantage is the existence of a clear six-level taxonomy for vehicle automation, which aligns with our characterization, albeit limited to this specific domain.[3] This taxonomy starts with level 0, which is complete human control, and progresses to level 5, full automation.

Level 0: Full Human Control

Level 0 is the baseline, with an unassisted human performing tasks and functions. In the automobile analogy, this is akin to driving an early-model car: All mechanical functions are a direct translation of the decisions and actions of the driver (in concert, of course, with exogenous conditions, such as traffic, weather, and road surface).

Level 1: Direct Automation

Level 1 automation is automation of an individual driving task, either steering or speed control. An early form of direct automation in cars was cruise control, which automates the manual process of monitoring the car's speed. This accomplishes something humans can do well but relieves them of the need to do so. Antilock brake systems are a bit more complex and automatically control braking to prevent skidding. This automates a response to nonconstant conditions and replaces the need for a human to pump the brakes at the appropriate time while monitoring individual wheel speed and reacting when each wheel begins locking. Even though people are theoretically able to do this, given additional controls and information, the direct automation of the process makes it much more practical; the standard calls this "driver assistance."

Level 2: From Direct Automation to Machine Learning

Level 2 automation is a system that controls both steering and speed. Some newer cars have automatic lane following, which uses sensors to feed data to a machine-learning system and steer the car. For humans, this form of control is fairly easy, but it requires an in-depth understanding of what lanes are and what actions are required to keep the

[3] SAE International, On-Road Automated Vehicle Standards Committee, "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," SAE Standard J3016, September 30, 2016.

car in the lane. Lane following algorithms do not have the same level of understanding as human drivers, but they can replace this knowledge with feedback from data-driven systems.

Lane following is not something that humans generally have trouble with, but it is something that direct automation is likely incapable of doing. This illustrates an important point about such systems: The degree of difficulty for humans is only loosely correlated with the degree of difficulty in automating a system.

Levels 3 and 4: From Machine Learning to ANI

Self-driving is a more complete automation of the system—one that integrates machine learning to fully automate the process under some or all conditions. This is effectively domain-specific AI. Such cars are either level 3, if they rely on having a driver available to take over, or level 4, if they only occasionally request to revert to driver control but are able to maintain safe conditions if a driver is not available. A level 3 car might need a user to realize that it began raining and make a decision to take control. A level 4 car could suggest that human control is needed but would be able to pull over and wait if the driver does not respond.

As envisioned, these systems allow cars to integrate route planning, similar to GPS-guided systems, with full control of the car, effectively replacing human drivers completely. Some of the challenges in building full automation are dealing with unusual cases that human drivers can easily manage. For example, if a ball bounces into the street, a human driver understands why a ball would emerge, is prepared to slow down, and knows that there might be a need to brake abruptly if someone chases the ball. A level 3 automated car might need driver intervention to prevent the car from needing to stop abruptly or swerve or perhaps to prevent it from crashing. However, because the domain of "driving" can be connected to many other types of understanding, the limits of machine learning–based systems emerge when training data do not anticipate the need for a particular case. In our taxonomy, this is where AGI could be used.

Level 5: Advancing ANI and the Potential for AGI

Level 5 is full automation. The car can be told to drive itself, and human control is optional or even disabled by default. This is the limit of the current taxonomy, but greater degrees of autonomy are possible. Capabilities beyond those of near-term ANI blur the line between automation and MADCOM.

We can imagine a more complete system that integrates decisions across more domains—combining and enhancing the current abilities of several disparate systems. For example, suppose you tell a MADCOM system to find a good Italian restaurant for dinner with a business client. It would connect to the client's MADCOM system and decide which restaurant to recommend based on the client's past preferences and descriptions and ratings of various restaurants, perhaps allowing you to approve the

decision. The system would then coordinate timing, make a reservation, and forward the information to your calendar, instructing it to remind you when you need to leave (accounting for the current drive time), and your car would then drive you to the meeting. Many of these capabilities are already available or will be in the near term.

However, to be trusted to make arbitrary decisions, a system needs a more complete understanding of what is desired when you make a request. For example, it would need to understand that the client's restaurant preference needs to be prioritized, but it would also need to know to downgrade this preference in favor of other factors if it is arranging a different sort of meeting—say, with a subordinate.

This hypothetical example shows that when automation goes far enough, it can act independently, without a human in the loop. This is what science fiction has billed as an AI assistant; it can follow complex direct commands, as well as interpret a situation and make appropriate suggestions. It can even act accordingly without further supervision. This may be desirable for arranging a meeting, but it could be problematic when making more consequential decisions, military or otherwise. For some systems, it is necessary to make moral or judgement calls, and, even when a system's judgment is better than human decisionmaking, people may not trust the system.

The mechanism—automation, machine learning, or AI—can be less critical than the type of decision being made and the degree to which it replaces human judgment. In some cases, as in a car's automatic transmission, direct automation is sufficient to fully replace human decisionmaking. In other cases, such as driving in unusual weather conditions, very capable AI is required.

In the following discussion of the C4ISR domain, we will examine where automation is and is not viable. Clearly, some tasks are already fully automated, while others may be assisted by automation. Other parts of the process will continue to require extensive human judgment, at least in the near future, and attempts at automation should be approached cautiously or not at all.

Framework for the Analysis

In this discussion, we use John Boyd's OODA framework to consider how traditional C4ISR can be supported or replaced by various levels of automation. This is not the only way to frame the discussion, but it is a useful construct that is familiar in C4ISR domain. In fact, because OODA describes "ideal" decisionmaking, it better characterizes approaches that could replace current C4ISR systems than it does the current systems.[4]

[4] Interestingly, this makes OODA useful for determining how to do things but much less useful for understanding the foibles of humans who are the subjects of the analysis, for creating information to deploy, or for exploiting an opponent's likely reactions.

Before discussing the OODA framework's application to C4ISR, we review the different types of automation that can be used for C4ISR. Our discussion characterizes levels of automation possible in the past, present, near future, and slightly beyond: direct automation, machine learning, ANI, and potential AGI.

The Past: Direct Automation

Over the past 50 years, computerized systems have become integral to a wide variety of processes. Templates, automated calculations, and quicker access to data have all contributed to a significant shift in how processes are designed and carried out and made simple, partial automation possible. Recently, as processes themselves became more computerized, many or most routine parts of these processes became fully automated.

It is relatively easy to automate processes that are based on a clear, fully understood workflow. Such processes, which require knowing everything and conveying that to a system, are candidates for automation only if the "business logic" is known and the relevant inputs are available. As noted throughout this report, it is not possible to fully know the IE.

Specific portions of C2 can be automated, with an attendant loss of flexibility. If a system has a built-in set of commands to choose from, going outside that anticipated set will necessarily involve either further automation to include the new command or side-stepping the built-in options to revert to a manual process. Direct automation is therefore helpful but cannot replace a human in the loop unless the system is completely understood.

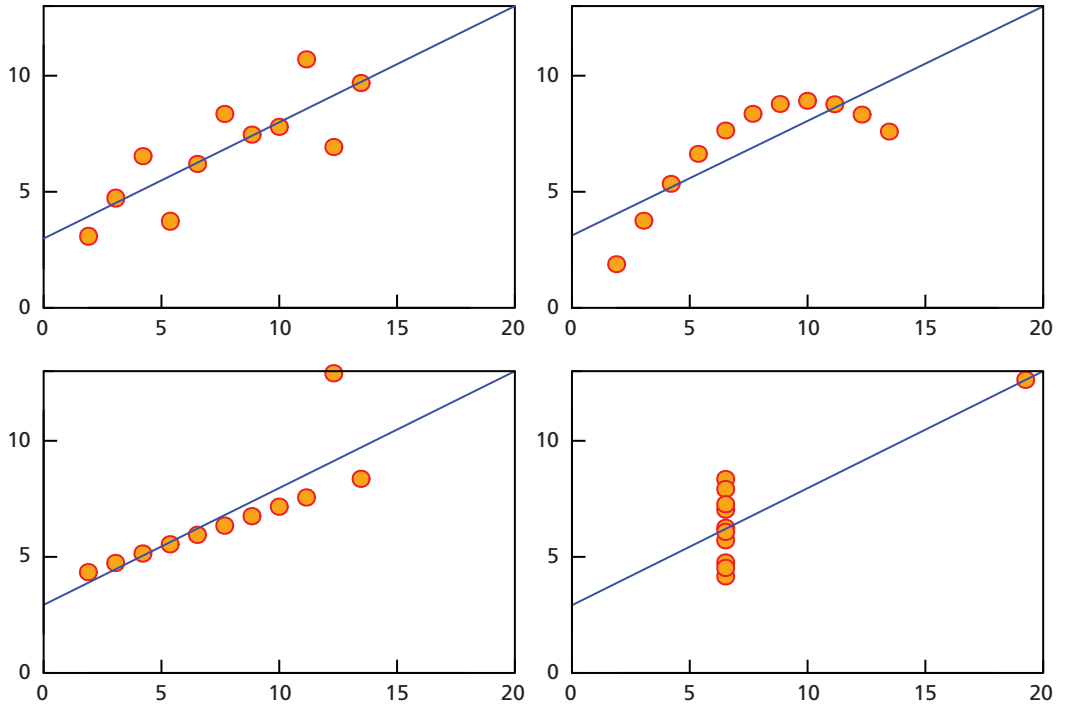
In C4ISR, the purpose of many automated processes is to distill or present information. These processes can significantly reduce the complexity of information analysis, but simplification necessarily involves *removing* information. Critically, any simplification presumes that a human can fully characterize what is relevant on behalf of an automated system. Alternatively, automated systems can organize information without removing any, but this approach requires the same assumption.

For example, statistical analysis involves summarizing data—and this can lead to misunderstanding of the phenomena being summarized. One famous example is Anscombe's quartet (see Figure A.1), in which the visualizations have almost identical means and variances. Furthermore, each linear regression produces the same predicted line. This example shows how summaries can accidentally mislead.[5]

However, this example also differs somewhat from the type of deception that might concern C4ISR efforts. For instance, the Datasaurus Dozen is a playful example of how information could be engineered in an adversarial setting, showing how the

[5] Francis J. Anscombe, "Graphs in Statistical Analysis," *American Statistician*, Vol. 27, No. 1, 1973.

Figure A.1
Anscombe's Quartet



SOURCE: Anscombe, 1973, pp. 19–20, Figures 1–4. Used with permission.
RAND *RR2489-A.1*

same data (resembling a dinosaur when plotted) take on four increasingly different visualizations when summarized to two decimal places.[6]

These processes can be automated or draw on more modern techniques, but the same types of problems can apply in either case. Deep dives and reviews (which are manual processes) can mitigate these problems, at the expense of reducing the extent to which the process can be automated.

The Present: Machine Learning

More automation can be achieved with currently available machine learning and related techniques. Machine learning is a way to train a system to evaluate future data on the basis of available past data. The ability of a machine to learn and apply heuristics is a strength of such systems; the exact inputs that lead to a particular response do not need to be exactly known. A less desired consequence is that, in many domains,

[6] Justin Matejka and George Fitzmaurice, "Same Stats, Different Graphs: Generating Datasets with Varied Appearance and Identical Statistics Through Simulated Annealing," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York: Association of Computing Machinery, 2017.

even a well-trained system is likely to have less-than-perfect success; the heuristics that these systems develop are limited.

The complexity of these systems can vary widely, but advances in computing power available are making it relatively easy to build and train even complex machine-learning systems. Unlike traditional automation, the outputs of a machine-learning system are not dictated directly. A principal challenge is choosing or generating the data used to train the system in a way that does not create biases and systemic mistakes in how the system operates. Where so-called Big Data are available, training can be accomplished with these data, but care must be taken to ensure that any available data are representative and sufficient in quantity.

Based on the provided or generated data, the system builds an algorithm to decide how to respond in similar cases. This works as long as the system can efficiently learn an approximately correct response algorithm and has enough training data to do so. The complexity of the resulting algorithm depends on the complexity of what is being learned. A principle drawback is that the input data are not always unbiased, and, as a consequence, the resulting system can have inbuilt flaws and biases that are hard to detect. The process for generating the output is not necessarily interpretable in human-understandable terms, even by those who develop it.

Data Availability and Bias

One important application of machine learning is image recognition. The standard test of image recognition capability uses ImageNet, a collection of 14 million images organized into 1,000 distinct categories. (For example, there are almost 1,500 images of cinnamon buns.) Despite huge advances in this capability, the best techniques still have an error rate of several percentage points. The top-5 error rate, or the percentage of the time that the true answer is not one of the AI image classifier's top five suggestions, improved from 17 percent in 2012 to 4.97 percent in 2015.[7] At the same time, the average top-5 error rate for humans was 5.1 percent.[8]

As this example shows, machines can achieve near- or better-than-human performance on well-structured tasks with clear outcomes, and they can complete these tasks faster than humans in most cases. As mentioned, less-structured domains, domains with larger potential decision spaces, and situations in which outcomes are unclear are more challenging. Even where these algorithms perform well, accuracy relies on clear

---

[7] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei, "ImageNet Large Scale Visual Recognition Challenge," arXiv, Cornell University Library, paper1409.0575, revised January 30, 2015.

[8] Based on a two-person test that involved classifying 1,758 images. This almost certainly overstates what we would normally think of as the human error rate. The best human performance was by a team from China at the 2017 annual competition, which managed to achieve an error rate under 3 percent (Xiaoteng Zhang, Zhengyan Ding, Jianying Zhou, Jie Shao, Lin Mei, *The Third Research Institute of the Ministry of Public Security*, P.R. China, undated).

categorization of data. Success rates depend on the relative strengths of humans and algorithms, and system performance depends heavily on the class of problems being addressed. The differences between a computer system's mistakes and human mistakes clearly show this.[9]

For machine learning, mistakes involved difficulty identifying the most central or important object in a set (24 percent of errors), recognizing small objects (21 percent of errors), and an inability to deal with contrast and color variations in images (13 percent of errors). Mistakes by humans mostly concerned issues with the data set and categorization. For example, most human errors (37 percent) involved incorrectly distinguishing fine details, such as among 120 dog breeds. A large portion of the remaining errors (25 percent) were due to class unawareness—that is, not realizing that a class existed in the list of 1,000 options.

Dealing with Change

A general issue with machine-learning systems is that they are almost invariably trained using data that differ from the data they need to interpret. This is sometimes called *out-of-sample prediction*, by analogy with statistics. It can occur in many forms: when data from the past and present are used to train a system that will be used in the future, when data from one region or condition are used to train a system for application elsewhere, or when data from one group of people are used to train a model that is applied to other populations. This can be mitigated by careful planning and by identifying changes to allow the system to adapt to new contexts. However, in an adversarial domain, shortcomings like this can be exploited.

Another general challenge is understanding and interpreting outputs and determining how they can be changed. It can be difficult to interpret why these methods predict or return the results they do. Additionally, biases in the model are often hard to identify, and even identified biases or mistakes can be hard to remedy. This is both because of the internal complexity of the model and because the details of the model structure and the data used to train the model can create complex biases that are hard to predict or correct.

Ensuring that the input data are unbiased can be more difficult than it seems. In looking at the 2009 Iran election, tweets tagged #IranElection were not exclusively supportive of any particular side or position; therefore, it was hard to determine whether the hashtag was representative of those tweeting about the election, and further care needed to be taken because the discussion was not exclusively domestic.[10] When collecting opinions about a trending issue, such as an election, it is easy to accidentally introduce bias into the data. Comparing support of the two candidates

---

[9] Russakovsky et al., 2015.

[10] Sara Beth Elson, Douglas Yeung, Parisa Roshan, S. R. Bohandy, and Alireza Nader, *Using Social Media to Gauge Iranian Public Opinion and Mood After the 2009 Election*, Santa Monica, Calif.: RAND Corporation, TR-1161-RC, 2012.

in the 2016 U.S. election by looking at tweets tagged #MAGA or #Trump versus #ImWithHer or #Hillary may seem like a balanced approach, but shorter hashtags are used more easily and more often than longer ones. Additionally, social media platforms were infiltrated by foreign bots and automated retweets. An analysis that fails to account for these facts would have negative value: It would mislead instead of inform. Machine-learning methods are not able to deal with these issues independently, and because their output relies on input, care is needed when selecting the data used for training.

Accidental Confusion and Adversarial Attacks

One specific class of problems is similar to the previously discussed Anscombe's quartet and Datasaurus examples: Machine-learning systems are vulnerable to being fooled. For example, sentiment analysis of Twitter data replaces the text of the tweets with numeric scores on various scales. If information is not captured by the sentiment analysis, or if it is not captured well, this summary process can eliminate important data points. Alternatively, it may categorize the data into topics for human analysis. This process does not remove information, but it can obscure it through mistaken categorization. To the extent that an adversary decides to create misinformation, that campaign can be targeted against known analytic techniques and machine-learning models.

An active area of research in machine learning is adversarial examples. In 2014, researchers noticed that neural networks can be fooled using nearly imperceptible changes to inputs.[11] Similar adversarial examples have been found to target other machine-learning models. For example, research has demonstrated the ability to maliciously manipulate a system's perceptions of 3D objects, such as by physically modifying stop signs so that self-driving cars no longer recognize them.[12] More generally, there is an area of research into adversarial learning that has already made important contributions to applications supporting spam filtering and game playing. Techniques from this area of research are potentially useful in many other adversarial situations.

It is unclear whether machine-learning algorithms can be secured against adversarial attacks in general.[13] It is also unclear how easily or effectively individual systems can be fooled or avoid being fooled.[14] Further research on the possibility of adversarial

---

[11] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus, "Intriguing Properties of Neural Networks," arXiv, Cornell University Library, paper 1312.6199, revised February 19, 2014.

[12] Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, and Dawn Song, "Robust Physical-World Attacks on Deep Learning Models," paper presented at the Conference on Computer Vision and Pattern Recognition, June 2018.

[13] Marco Barreno, Blaine Nelson, Russell Sears, Anthony D. Joseph, and J. D. Tygar, "Can Machine Learning be Secure?" *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, New York: Association for Computing Machinery, 2006.

[14] Anish Athalye, "Robust Adversarial Examples," OpenAI blog post, OpenAI, July 17, 2017.

attacks on machine learning is critical; in the interim, human involvement in the process is necessary if the types of adversarial attacks anticipated could compromise the system.

For both these reasons, machine-learning and autonomous systems should be designed to notice unusual patterns or examples to flag for human review. They should also be built to rapidly adapt to changes, and they should be used interactively by decisionmakers, who should have the ability to perform routine deep dives and provide feedback on performance. These are departures from typical design goals of systems, which are meant to require minimal human guidance and to be finalized, then deployed. In this context, routine changes are disruptive and seen as problematic.

Collaborative Use of Systems

Most systems in use today involve close interaction with a human decisionmaker. A simple example is a smartphone with predictive text; typing becomes an interaction between the machine-learning system and the user, the system can greatly improve the human user's speed and accuracy. Similarly, modern chess engines have outperformed humans since Gary Kasparov's loss to Deep Blue two decades ago, but they could not compete independently in what Kasparov called *advanced chess*. In this game, humans consult chess engines and human and machine play as a hybrid team. Such hybrid teams had an advantage over pure chess engines for several years, a state that lasted until chess engines improved to the point that human involvement became a hindrance rather than a help.[15]

Not all uses of a system call for such close collaboration. The difference lies in the user's familiarity with and reliance on the system. Until more-sophisticated systems are able to reliably and fully replace human decisionmaking in a given situation, close human collaboration and familiarity with systems can greatly improve human and system performance. This already occurs in many domains. For example, many drivers now rely on GPS devices to assist their navigation. Such a system may or may not plan a route based on traffic conditions, or it may only consider traffic on roads for which data are available. In these cases, users can learn when to ignore the system's suggestions.

When there are concerns about adversarial action, human decisionmaking is particularly important, but it can benefit from automated assistance. For example, developing secure software for military systems involves automated tasks, such as static testing, dynamic analysis, and other processes to check code.[16] Similar tools are not yet routine in machine learning, but at least one project at Google has developed tools for

---

[15] Tyler Cowen, "What Are Humans Still Good for? The Turning Point in Freestyle Chess May Be Approaching," *Marginal Revolution*, November 5, 2013.

[16] Raymond Richards, "High-Assurance Cyber Military Systems (HACMS)," webpage, Defense Advanced Research Projects Agency, undated.

diagnosing issues with a training set, which is a start in facilitating greater understanding of the systems.[17]

Close collaborative interaction between users and systems allows greater trust in the system and allows people to compensate for known (or discovered) biases and problems with the system. As mentioned earlier, the abilities of computer systems and humans differ, and strategically using them in combination can amplify their strengths. We speculate that this form of engaged interaction with automated systems should be able to compensate for many adversarial attacks against systems, especially in the near term.

The Near Future: Artificial Narrow Intelligence

Many types of automation that involve machine learning are now considered AI.[18] Our initial definition of *AI* was "a system that reacts to novel situations in ways similar to humans," which is not quite sufficient to differentiate AI from machine-learning systems in general. The key characteristic differentiating AI and machine learning is potential autonomy. A system could be considered ANI if it can perform a single task at a human level without monitoring or supervision, even when it encounters novel situations.

In competitive contexts, not only can ANI now defeat the best human players of chess and the strategy-based board game Go, but it is well on the way to beating humans at almost any formally defined game. The OpenAI Universe platform is designed to apply machine learning to almost any computer game, and there has been similar work to develop ANI that can win at strategy games as well.

However, these systems are domain-specific and much less effective when the number of possible decisions is larger. The relative complexity of chess and Go meant that decades passed between when Deep Blue defeated Gary Kasparov and when AlphaGo was able to challenge and defeat human champions. This shows the evolving complexity of domains where AI can fully outcompete humans. Many AI experts have suggested that the next step is to create ANI that can compete with human players at Starcraft, a real-time computer-based strategy game.[19] Despite this evolution, human-

---

[17] James Wexler, "Facets: An Open Source Visualization Tool for Machine Learning Training Data," *Google Open Source Blog*, July 17, 2017; GitHub, "PAIR-Code/Facets," webpage, last updated April 30, 2018.

[18] The flippant comment supposedly made by Stanford University's John McCarthy in the late 1980s was that "AI is everything we can't do with today's computers," a characterization that could be applied to the current taxonomy.

[19] Will Knight, "StarCraft Will Become the Next Big Playground for AI," *MIT Technology Review*, November 4, 2016. StarCraft competitions have been held at, the IEEE annual Conference on Computational Intelligence in Games and the Association for the Advancement of Artificial Intelligence annual Conference on Artificial Intelligence and Interactive Digital Entertainment. Many early entries were direct automation, but more sophisticated methods have been developed in the past several years. arXiv papers about Starcraft are an indication of research into these methods. As of May 2018, there were 32 papers mentioning StarCraft, seven of which had been posted in the first months of 2018.

level performance by AI systems is limited to contexts with clear and measurable victory conditions.[20]

Autonomy

Returning to the earlier discussion of autonomous cars, level 3 would qualify as a machine-learning system, with an inability to react in certain situations and, therefore, a requirement for human supervision. This is a central point about ANI: It will be autonomous in domains in which direct automation or basic machine-learning systems cannot be. The central characteristic of automation in general is to free humans from needing to be involved. As automation becomes more sophisticated, it leads to less involvement of humans in ever-higher levels of systems.

In the extreme, MADCOM replaces not only human interaction with the environment but also human interaction with other humans or human interaction with systems. It does so by substituting for both parties in an interaction. Ceding control of parts of a system requires trust in automation, MADCOM or otherwise. In adversarial situations, this requires trusting both the normal performance of a system and its ability to avoid subversion and misdirection. The ability to perform at that level is somewhat domain-specific and requires a much broader set of abilities than what is anticipated to be possible for most presently envisioned systems.

The Future: Complete Automation

Complete automation, which would require replacing human judgment, involves more-capable general intelligence. These systems would begin to have the capabilities that we suggested were beyond those of the domain-specific ANI systems that are currently available. For example, our earlier characterization of ANI would suggest that chess systems have long since reached the point of "AI" and that cars are not far behind. However, these systems fall far short of humans' cross-domain intelligence. For this reason, it is important to differentiate between ANI and artificial general intelligence (AGI).

In the first case, ANI is limited to controlling systems and interacting only within well-defined boundaries. In the second, AGI must be capable of much more general decisionmaking. AGI might involve domains other than the expected ones, which involves a level of creativity. The resulting MADCOM would need to serve as a full proxy for a human decisionmaker. Perhaps more importantly from the perspective of developing such systems, the definitions of success are much harder to quantify.

These challenges are some of the most active areas of AI and AI safety research. It is unclear how effective the current tools are in addressing these challenges, and it

[20] The reason for this limitation is the set of methods used by machine-learning and AI researchers, such as neural networks and adversarial self-play, which require evaluating success as feedback to improve the system. See Johannes Heinrich and David Silver, "Deep Reinforcement Learning from Self-Play in Imperfect-Information Games," arXiv, Cornell University Library, paper 1603.01121, revised June 28, 2016.

is difficult to predict when near-human level AGI will be possible. Perhaps more critically, it is unclear how complex the methods for success in creating AGI will be or how much further progress can be expected from these methods. These questions are central to understanding both how safe the systems are and the risks of developing and using them.

Unclear Risks

There has been much speculation and argument about the risks and potential harms of AI. The gap between the near-human cross-domain abilities of an early AGI and AI systems with human-equivalent or superhuman general intelligence is unclear. It could be decades of progress, or advances will be rapid once the necessary breakthroughs occur.[21]

If such advances were possible, unaided machines with human-level general intelligence would be able to accomplish every task as well as human workers.[22] Again, the development timeline is unclear, but the potential for AI to achieve human intelligence and capability—and for technology to make possible self-improving AGI systems—will inevitably give rise to a variety of concerns about safety and controllability. A combination of above-human abilities and cascading improvements (and self-improvements) to AI technology call into question humans' ability to mitigate the attendant risks.[23]

Even if machine intelligence cannot surpass human-level intelligence, if these systems can run relatively inexpensively, their effects are likely to be catastrophic because they could outcompete or displace humans from almost all parts of the economy.[24] It is still unclear when and if such technologies will be developed, but they are hardly in the far future; one survey of experts found a median estimate of 50-percent confidence that AI development would reach this stage by 2050.[25]

---

[21] The argument that general intelligence is not exactly defined or has multiple dimensions is largely irrelevant to whether an AI system exceeds human intelligence in a particular domain. If an AI system is cross-domain–capable and adaptive, it can perform similarly to (or better than) humans across relevant domains. For our purposes, it does not matter whether humans have a higher emotional IQ or superior creative thinking capabilities. See AI Impacts, "The Range of Human Intelligence," blog post, January 18, 2015.

[22] This differs from AI Impacts' use of *high-level machine intelligence to refer to what we call human-level general intelligence*. This intelligence is also less expensive than human workers.

[23] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford, UK: Oxford University Press, 2014; Roman Yampolskiy and Joshua Fox, "Safety Engineering for Artificial General Intelligence," *Topoi*, Vol. 32, No. 2, October 2013.

[24] Robin Hanson, *The Age of Em: Work, Love, and Life When Robots Rule the Earth*, Oxford, UK: Oxford University Press, 2016.

[25] Luke Muehlhauser, "When Will AI Be Created?" Berkeley, Calif.: Machine Intelligence Research Institute, May 15, 2013, footnote 1.

Automation for Assisting OODA

Given the overview of what automation means and what is—or can become—possible, we turn to applications relevant to C4ISR, focusing on how they could affect operations in and through the IE.

Observe

The initial point of iterative OODA processes is data gathering, which is particularly challenging when there is a rapidly expanding amount of available data. The difficulty that emerges from this expansion has been called *information overload*. Speier, Valacich, and Vessey, discussing the relevant literature, explain, "Information overload occurs when the amount of input to a system exceeds its processing capacity. Decision makers have fairly limited cognitive processing capacity."[26] Automation can assist with data processing, subject to the limitations of the systems being used.

Early Automation

Direct automation for coping with information overload includes a variety of tool types and interfaces. Examples include basic approaches for detecting viruses using signatures, most statistical methods and their applications to automated summaries and reports, and databases with interfaces for querying gathered data directly.

These direct automation methods have the limitations, as discussed earlier. They are susceptible to accidental oversimplification, which can mislead, and they are very susceptible to adversarial manipulation. Because of this, they need close supervision and routine deep dives by human users to be reliable methods of ingesting information for digestion and orientation. Despite these drawbacks, these systems' ability to reduce information overload is a significant advance.

Present and Near-Future Automation

More recent approaches involve automatic classification, summary generation, or identification of unusual activity using machine learning. These are significant advances in all of these areas, and it is likely possible to minimize—but not eliminate—accidental oversimplification with further development. The more problematic areas for application are those with adversarial components; significant human involvement will be needed to routinely investigate and update any automation used to assist with data observation.

Limits to Automation

It is possible that domain-specific AI will mitigate some or even many of the challenges discussed here, but the manner in which it would do so is not straightforward. The primary barrier is that human decisionmakers have a limited ability to verify the

[26] Speier, Valacich, and Vessey, 1999, p. 338.

competence of a system. Potentially rapid changes in the data being observed make any assurance based on current performance unhelpful in evaluating future capability.

The more critical challenges here relate to moving from observe to orient; systems need to be able to recognize anomalies of types that are not obvious in advance and then provide cogent summaries for decisionmakers—a task that requires some degree of orienting and recognizing which anomalies and trends are important.

Orient

John Boyd described *orienting* as "an interactive process of many-sided implicit cross-referencing projections, empathies, correlations, and rejections."[27] What the process of orientation accomplishes is somewhat simpler to describe. It is what Peirce characterized as abduction, or inference from data to create a set of reasonable explanations.[28] For decisionmaking, hypotheses about how potential actions would help or hurt desired outcomes are the critical output of orienting, and Boyd's explanation makes it clear why this is difficult to accomplish at all, much less automate.[29]

The Complexity of Orienting

Boyd clearly saw orienting as by far the most complex part of the OODA process. (See Figure 2.4 in Chapter Two.) Later explanations have sometimes failed to appreciate how and why it is so complex. The lack of nuance is perhaps understandable in the domains in which it was applied. For instance, in tactical warfare, it can be interpreted as knowing the terrain, the positions of enemy and allied fighting units, and the capabilities of each. Although it remains difficult to accomplish in practice, this is a very domain-limited type of orienting, and the set of facts that might be relevant is assumed to be fully known.

As an example of why orientation is complex and difficult to automate, we note that the interpretation of domain-limited orientation for tactical warfare is insufficient in practice, especially given the complexity of the IE. The need to orient to a larger set of considerations is discussed extensively in Krulak's example of the "strategic corporal," in which the local and tactical decisions of a very junior leader can have strategic impact because of how actions are perceived and potentially amplified in the global

---

[27] John R. Boyd, *Organic Design for Command and Control*, Washington, D.C.: Project on Government Oversight, February 2005. Boyd developed the briefing in 1987.

[28] Robert Burch, "Charles Sanders Peirce: Deduction, Induction, and Abduction," in Edward N. Zalta, ed., Stanford Encyclopedia of Philosophy, Stanford, Calif.: Center for the Study of Language and Information, Stanford University, November 12, 2014.

[29] Humans, in fact, largely avoid this difficult step when they have familiarity with a situation, especially when performing tasks under time pressure. Klein's work on recognition-primed decisions found that the typical procedure for decisions is to pattern match to previous situations and decisions, as well as to accept the first action that comes to mind and has been correct in the past. Perhaps unsurprisingly, this resembles supervised machine learning, which chooses outputs based on similarity to previously seen cases. See Gary Klein, *Sources of Power: How People Make Decisions*, Cambridge, Mass.: MIT Press, 1998.

IE.[30] As Kozloski explains, in the IE, there are significantly broader and less clear questions needed to orient for basic tactical purposes.[31]

More generally, we can use our earlier example of autonomous vehicles to consider what is required to automate orientation. In driving, orienting is not just about being aware of where the car is and what surrounds it. Full automation requires recognizing relationships between the car's location and the rules of the road, rules that change dynamically based on the situation, and novel or unexpected inputs. A car does not need to stop when it encounters a person walking on the sidewalk wearing a shirt with a picture of a stop sign, but it does need to stop when it encounters a police officer holding a stop sign—and it needs to know what to do when a police officer is waving cars through a red light, overriding the normal rules of the road.

Bypassing Orientation for Automation

It has been simpler to integrate observe, orient, and decide than to require a system to explain how it would evaluate various decisions. We see this not only for self-driving cars but also for many other systems that use direct automation and machine learning to suggest or initiate actions. Google sees an email with flight information or hotel reservations and adds it to your calendar; this combines several steps, with the implicit ability for the user to veto the action—in this case, by declining to add the calendar entry.

Early approaches to direct automation for decisionmaking assumed that orientation occurred elsewhere, or, at most, attempted to distill relevant observations into decision trees. Even more recent systems usually move directly from observation to suggested or default actions, instead of observing and acting directly. This process implicitly relies on the humans to provide needed orientation and identification capabilities of when different options are or are not appropriate. This is not to say that automated recommendations are not helpful, but they rely on humans remaining in the loop, and they usually elide orientation rather than assisting it.

One reason that integrated systems are easier than orientation alone is because abduction, described earlier, is central to the process of decisionmaking. Automating orientation requires this step, and while it is possible to translate such hypotheses into human-digestible forms, it requires a level of self-reflection that is only beginning to be developed in AI.[32] However, integrating the process is possible with direct automa-

---

[30] Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999.

[31] Robert Kozloski, "Creating Cognitive Warriors," blog post, U.S. Department of the Navy, Office of Strategy and Innovation, August 2015; Alexander Kott, David Alberts, Amy Zalman, Paulo Shakarian, Fernando Maymi, Cliff Wang, and Gang Qu, *Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report*, Adelphi, Md.: U.S. Army Research Lab, June 2015.

[32] Sven Tomforde, Jörg Hähner, Sebastian von Mammen, Christian Gruhl, Bernhard Sick, and Kurt Geihs, "'Know Thyself': Computational Self-Reflection in Intelligent Technical Systems," *2014 IEEE Eighth International Conference on Self-Adaptive and Self-Organizing Systems Workshops*, Piscataway, N.J.: IEEE, 2014.

tion and machine learning, at least in non-adversarial domains, as the example of automated vehicles shows.

In the near future, ANI may be able to accomplish parts of orientation, such as summarizing and analyzing the basic implications of data. For example, "automated journalism" is already able to write articles in a human-like manner about events based on clear and unambiguous data, such as sports games and the weather.[33] Expanding this approach to less quantitative domains is a challenge but seems possible with current technologies and sufficient investment. Investigation into these possibilities by the private sector and academia has already started.

More complete automation would require AGI, which requires trustworthy and capable systems. As noted earlier, it is unclear when this could be developed, and such advances pose significant risks.

(Failures of) Automating Orientation

Succeeding in automating orientation non-adversarial domains would be helpful and may be possible using extant techniques. In adversarial contexts, deceptive inputs become much more problematic, because a system may be purposely misled into recommending actions that are unhelpful or actively counterproductive.

Reflexive control is already an increasingly effective and well-developed technique for manipulating human decisionmakers. The deleterious effects of this manipulation could be significantly worse if adversaries can exploit automated systems.

The ability to build systems to accomplish a task requires the ability to define success. Generally speaking, the task of ensuring that AGI will pursue the intended goals is an unsolved and potentially unsolvable problem.[34] Given that humans have a limited ability to understand deception and predict what will happen in complex domains, it seems likely that even human-level AGI would not solve this problem.

Decide

Deciding in the OODA model consists of two steps: generating useful options and suggesting or recommending which to act on. Without some degree of orientation, which provides hypotheses for evaluating possible actions, full automation for decisions is impossible. However, partial automation *is* possible to assist human decisionmakers. As suggested earlier, lacking orientation, any decisions made would implicitly rely on human judgment and human understanding of a problem. This is true whether the human directly makes the decisions or whether the human directly automates the decision process.

---

[33] Konstantin Nicholas Dörr, "Mapping the Field of Algorithmic Journalism," *Digital Journalism*, Vol. 4, No. 6, 2016.

[34] Nate Soares and Benya Fallenstein, "Agent Foundations for Aligning Machine Intelligence with Human Interests: A Technical Research Agenda," in Victor Callaghan, James Miller, and Roman Yampolskiy, and Stuart Armstrong, eds., *The Technological Singularity: Managing the Journey*, New York: Springer, 2017.

Direct automation in a decision system relies on the equivalent to military standard operating procedures. Even when a decision is complex, requiring the evaluation of many conditional branches of a decision tree, the decisions are made by people. The more flexible approach, required for domains with many dimensions and choices, direct automation provides a list of default reactions from which a decisionmaker can choose. In this way, the decisionmaker can choose among the automatic suggestions or go outside the system to act differently. A common example is a word processor's suggested corrections for spelling and grammar mistakes. In the context of C4ISR, this would include suggesting preprogrammed surveillance patterns or C2 systems providing options for action.

Modern systems go beyond direct automation of the decision process and instead make suggestions based on the understood context. These systems can learn from user behavior, and sophisticated systems can be remarkably accurate. Modern search engines are a hybrid decision system, in which the search engine delivers results based on a complex ranking and suggestion system, as well as previously suggested and accessed links. The list of recommended actions are the links returned, and while they are frequently very helpful, the ability to infer context is limited, which can result in suggestions that are off-target or even offensive.

Future systems can continue to improve on these forms of automation using more accurate heuristics, but only integration across the full decision process will limit the need for human supervision.

Act

The final stage of the OODA cycle is acting, carrying out the decision made. In the IE, some parts of an action are inevitably automated; the systems do not use human guidance to execute a chosen decision. The degree of automation is almost always a question of the scope of the decision being implemented and the time frame necessary for decisions. When decisions are routine, systems are able to automate them completely. Antivirus software and firewalls constantly and automatically make decisions and acting on them. In some cases, these decisions can be countermanded by the user, but the initial decisions require real-time reactions.

Direct Automation

A critical purpose of direct automation is as a force multiplier: It allows quicker reactions or more reactions. The utility of using automation can be seen in Russian factories of people overseeing propaganda and trolling bots, running many accounts that are nearly identical or use slight variations on the same message, perhaps via automated rephrasing. The sheer volume of content posted on social media sites is possible only via automation, with reactions and responses to the posts controlled manually. These are near-MADCOM processes, and they suggest how hard it would be to distinguish

sophisticated, fully automated propaganda from human-generated propaganda if it is deployed in large volumes.

Another purpose for direct automation of actions is programming specified reactions to certain events. Most alarms operate on direct-automation principles; instead of waiting for someone to pull the fire alarm, they detect a condition and automatically activate the alarm and sprinklers. The drawback is the complete inability to detect or react to anything not exactly matching the programmed triggers, or to avoid reacting when triggered by false alarms. This makes them relatively easy for adversaries to exploit.

Machine Learning and Automating Interactive Systems

Machine learning has become more and more common for automated systems to use as heuristics for acting directly, especially for alarms. Machine learning allows flexible automation, but it does not materially change how automation is used, unless the system is allowed to react autonomously, as is the case with firewalls, for example. Due to the need for immediate reaction, automation is needed, and because false positives can be reported and rectified, automating firewall rules is relatively low-risk.

In other applications, sophisticated automation allows systems to respond immediately. The critical change required to allow immediate response is that the system becomes largely autonomous. Given the speed of interaction in the IE, this provides a limited window for decisionmaker intervention. MADCOM systems are already being used to automate customer support, albeit not at the level of ANI, because they not are capable of resolving large classes of issues and thus almost universally allow navigation to talk to a human. Again, this type of application is limited to domains in which the cost of mistakes is low or the automation is not allowed to make decisions.

There is discussion of creating "adaptive defenses and self-securing systems," which would use machine learning and ANI to automatically react to prevent attacks.[35] When restricted to risk mitigation, this only increases the defensive capabilities of the system.

Full Automation of OODA

Other similar requests, however, such as "cueing and orchestration of defenses and remediation" or "automated obfuscation, deception, [and] resource reallocation" are potentially vulnerable to exploitation.[36] Because these systems are not purely defensive and have limited domain understanding, they could be used by adversaries to manipulate behaviors in ways that could be damaging.

While systems can automate certain portions of a decision process, more fully automating the process to eliminate the need for human involvement requires either accepting a high level of risk of manipulation by adversaries or ensuring that systems

---

[35] Office of the Secretary of Defense, Rapid Reaction Technology Office, 2017.

[36] Office of the Secretary of Defense, Rapid Reaction Technology Office, 2017.

are trustworthy and that the possibility of manipulation is mitigated or not damaging. In the first case, it may not be possible to diagnose or fix such systems within a reasonable time frame. If a customer service system were autonomous and allowed to issue refunds or credit, for example, it might be possible to exploit the system to issue large credits inappropriately. Unless used collaboratively, with an expectation of iterative development and adaptation to new circumstances, these risks are usually unacceptable. In the second case, as discussed earlier, it is difficult to build very trustworthy ANI systems.

Machine learning and ANI may still be useful for full automation when some mistakes are acceptable or when problematic manipulation is unlikely or inconsequential—for example, due to risk mitigation or limited scope of action. Any processes for analyzing these systems and evaluating their safety and security should explicitly include these concerns.

Looking Forward: Risks of Future Machine Learning and Automation in the IE

As the capabilities of these systems advance, they become ever more critical to adversarial decisions. Understanding and responding to adversary systems may require embracing these technologies. Regardless of the exact capabilities and limitations of automated systems, they will be necessary to maintain a competitive advantage, or even parity, if adversaries begin to use them in critical domains. If a MADCOM system can coordinate and respond an order of magnitude faster than human systems, these systems will magnify both the risk of exploitation and the benefits of using them.

For MADCOM systems that interact with humans, there is at least an inherent limit on the speed and volume of interactions. Propaganda and information overload will become more and more critical components of domestic and international communication as systems operate with more autonomy.

For machine-to-machine interaction, even in the near term, there is a further risk that exploitation and subversion of a system could occur faster than humans can react, and control could be ceded nearly completely to the systems. The possibility of exploitation and counterexploitation of these systems is a critical concern, and escalating capabilities are likely to make certain types of exploitation ever more dangerous. Because formally verifying and securing complex systems would be nearly or completely impossible, if these systems continue to advance, the choices would be to accept the risks of exploitation, allow a competitive gap to emerge, or coordinate with adversaries to reduce risks to both sides. Without some limitations, this multiparty arms race in the domain of machine learning and AI will continue to pose risks to all sides—and it is unclear how to mitigate them.

References

AI Impacts, "The Range of Human Intelligence," blog post, January 18, 2015. As of May 2, 2018: http://aiimpacts.org/is-the-range-of-human-intelligence-small

Alexander, Jandria S., "Achieving Mission Resilience for Space Systems," *Crosslink Magazine*, Spring 2012. As of May 2, 2018: http://www.aerospace.org/crosslinkmag/spring2012/achieving-mission-resilience-for-space-systems

Ancker, Clinton J. III, and Michael Flynn, "Field Manual 5-0: Exercising Command and Control in an Era of Persistent Conflict," *Military Review*, March–April 2010, pp. 13–19. As of May 2, 2018: http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20120630MC_art009.pdf

Anscombe, Francis J., "Graphs in Statistical Analysis," *American Statistician*, Vol. 27, No. 1, 1973, pp. 17–21.

Army Doctrine Publication 6-0, *Mission Command*, Washington, D.C., May 2012.

Army Doctrine Reference Publication 6-0, *Mission Command*, Washington, D.C., March 28, 2014.

Army Field Manual 5-0, *The Operations Process*, Washington, D.C., March 2010.

Army Techniques Publication 6-01.1, *Techniques for Effective Knowledge Management*, Washington D.C., March 2015.

Athalye, Anish, "Robust Adversarial Examples," blog post, OpenAI, July 17, 2017. As of July 27, 2017: https://blog.openai.com/robust-adversarial-inputs

Avidor, Gideon, and Russell W. Glenn, "Information and Warfare: The Israeli Case," *Parameters*, Vol. 46, No. 3, Autumn 2016, pp. 99–107.

Barreno, Marco, Blaine Nelson, Russell Sears, Anthony D. Joseph, and J. D. Tygar, "Can Machine Learning be Secure?" *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, New York: Association for Computing Machinery, 2006, pp. 16–25.

Borgatti, Stephen P., "Centrality and Network Flow," *Social Networks*, Vol. 27, No. 1, January 2005, pp. 55–71.

Bostrom, Nick, *Superintelligence: Paths, Dangers, Strategies*, Oxford, UK: Oxford University Press, 2014.

Boyd, Curtis D., "Army IO Is PSYOP: Influencing More with Less," *Military Review*, May–June 2007, pp 67–75. As of May 2, 2018: http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20070630_art012.pdf

Boyd, John R., *Organic Design for Command and Control*, Washington, D.C.: Project on Government Oversight, February 2005. As of May 2, 2018:
http://www.dnipogo.org/boyd/organic_design.pdf

———, *The Essense of Winning and Losing*, Washington, D.C.: Project on Government Oversight, August 2010. As of May 2, 2018:
http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf

———, *Conceptual Spiral*, Washington, D.C.: Project on Government Oversight, November 2011. As of May 2, 2018:
http://pogoarchives.org/m/dni/john_boyd_compendium/conceptual-spiral-20111100.pdf

Bravo-Marquez, Felipe, Marcelo Mendoza, and Barbara Poblete, "Combining Strengths, Emotions And Polarities for Boosting Twitter Sentiment Analysis," *Proceedings of the Second International Workshop on Issues of Sentiment Discovery and Opinion Mining*, New York: Association for Computing Machinery, 2013, article 2.

Burch, Robert, "Charles Sanders Peirce: Deduction, Induction, and Abduction," in Edward N. Zalta, ed., *Stanford Encyclopedia of Philosophy*, Stanford, Calif.: Center for the Study of Language and Information, Stanford University, November 12, 2014. As of May 2, 2018:
https://plato.stanford.edu/archives/fall2017/entries/peirce

Burt, Ronald S., "Social Contagion and Innovation: Cohesion Versus Structural Equivalence," *American Journal of Sociology*, Vol. 92, No. 6, May 1987, pp. 1287–1335.

Castillo, Carlos, Marcelo Mendoza, and Barbara Poblete, "Information Credibility on Twitter," *Proceedings of the 20th International Conference on World Wide Web*, New York: Association for Computing Machinery, 2011, pp. 675–684.

Chairman of the Joint Chiefs of Staff Instruction 3201.01, *Joint Information Warfare Policy*, January 2, 1996.

Cordray, Robert III, and Marc J. Romanych, "Mapping the Information Environment," *IO Sphere*, Summer 2005, pp. 7–10. As of May 2, 2018:
http://www.au.af.mil/info-ops/iosphere/iosphere_summer05_cordray.pdf

Cowen, Tyler, "What Are Humans Still Good for? The Turning Point in Freestyle Chess May Be Approaching," *Marginal Revolution*, November 5, 2013. As of May 2, 2018:
http://marginalrevolution.com/marginalrevolution/2013/11/what-are-humans-still-good-for-the-turning-point-in-freestyle-chess-may-be-approaching.html

Davenport, Thomas H., and Laurence Prusak, *Information Ecology: Mastering the Information and Knowledge Environment*, Oxford, UK: Oxford University Press, 1997.

DoD—*See* U.S. Department of Defense.

Dörr, Konstantin Nicholas, "Mapping the Field of Algorithmic Journalism," *Digital Journalism*, Vol. 4, No. 6, 2016, pp. 700–722.

Elson, Sara Beth, Douglas Yeung, Parisa Roshan, S. R. Bohandy, and Alireza Nader, *Using Social Media to Gauge Iranian Public Opinion and Mood After the 2009 Election*, Santa Monica, Calif.: RAND Corporation, TR-1161-RC, 2012. As of May 2, 2018:
https://www.rand.org/pubs/technical_reports/TR1161.html

Endsley, Mica R., "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, Vol. 37, No. 1, 1995, pp. 32–64.

Eykholt, Kevin, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, and Dawn Song, "Robust Physical-World Attacks on Deep Learning Models," paper presented at the Conference on Computer Vision and Pattern Recognition, June 2018.

Fan, Rui, Jichang Zhao, Yan Chen, and Ke Xu, "Anger Is More Influential Than Joy: Sentiment Correlation in Weibo," *PLoS ONE*, Vol. 9, No. 10, 2014, e110184.

Feldman, Ron, "Techniques and Applications for Sentiment Analysis," *Communications of the ACM*, Vol. 56, No. 4, April 2013, pp. 82–89.

Flanigan, Shawn Teresa, "Nonprofit Service Provision by Insurgent Organizations: The Cases of Hizballah and the Tamil Tigers," *Studies in Conflict and Terrorism*, Vol. 31, No. 6, 2008, pp. 499–519.

Fogg, B. J., "Stanford Guidelines for Web Credibility," Stanford Persuasive Technology Lab, Stanford University, May 2002. As of May 2, 2018: https://credibility.stanford.edu/guidelines

Gery, William R., SeYoung Lee, and Jacob Ninas, "Information Warfare in an Information Age," *Joint Force Quarterly*, Vol. 85, 2nd Quarter 2017.

Gilardi, Fabrizio, "Transnational Diffusion: Norms, Ideas and Policies," in Walter Carlsnaes, Thomas Risse, and Beth A. Simmons, eds., *Handbook of International Relations*, 2nd ed., Thousand Oaks, Calif.: Sage Publications, 2012, pp. 453–477.

GitHub, "PAIR-Code/Facets," webpage, last updated April 30, 2018. As of May 2, 2018: https://github.com/PAIR-code/facets

Goldfein, Dave, "War in the Information Age," *Defense One*, November 16, 2016. As of May 2, 2018: https://www.defenseone.com/ideas/2016/11/war-information-age/133193

Grandjean, Martin, "Intellectual Cooperation: Multi-Level Network Analysis of an International Organization," blog post, December 15, 2014. As of May 2, 2018: http://www.martingrandjean.ch/intellectual-cooperation-multi-level-network-analysis/

Hanson, Robin, *The Age of Em: Work, Love, and Life When Robots Rule the Earth*, Oxford, UK: Oxford University Press, 2016.

Hedström, Peter, Rick Sandell, and Charlotta Stern, "Mesolevel Networks and the Diffusion of Social Movements: The Case of the Swedish Social Democratic Party," *American Journal of Sociology*, Vol. 106, No. 1, July 2000, pp. 145–172.

Heinrich, Johannes, and David Silver, "Deep Reinforcement Learning from Self-Play in Imperfect-Information Games," arXiv, Cornell University Library, paper 1603.01121, revised June 28, 2016. As of May 2, 2018: https://arxiv.org/abs/1603.01121

Hilligoss, Bill, and Soo Young Rieh, "Developing A Unifying Framework of Credibility Assessment: Construct, Heuristics, and Interaction in Context," *Information Processing and Management*, Vol. 44, No. 4, July 2008, pp. 1467–1484.

Huening, Tim, and John Atkinson, "Operationalizing Cyberspace to Prevail in the Competition of Wills," *Special Warfare*, July–December 20, 2016, pp. 38–42. As of May 2, 2018: http://www.soc.mil/SWCS/SWmag/archive/SW2902/JUL-Dec_2016.pdf

Hughes, Seamus, "To Stop ISIS Recruitment, Focus Offline," *Lawfare Blog*, August 7, 2016. As of May 2, 2018: https://www.lawfareblog.com/stop-isis-recruitment-focus-offline

———, deputy director, Program on Extremism, George Washington University, "Combating Homegrown Terrorism," written testimony submitted to the U.S. House of Representatives Oversight and Government Reform, July 27, 2017.

Jannarone, Greg, "Behavioral Influences Analysis: Workflow Example," briefing slides, Maxwell Air Force Base, Ala.: Air University, undated. As of May 2, 2018: http://www.au.af.mil/bia/events/conf-mar08/bia_workflow_and_tools.pdf

Joint Publication 1, *Doctrine for the Armed Forces of the United States*, Washington, D.C.: U.S. Joint Chiefs of Staff, March 25, 2013.

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

Joint Publication 3-09, *Joint Fire Support*, Washington, D.C.: U.S. Joint Chiefs of Staff, December 12, 2014.

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

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

Joint Staff, J7, Deployable Training Division, *Commander's Critical Information Requirements (CCIRs)*, Suffolk, Va., July 2013.

———, *Communication Strategy and Synchronization*, Washington, D.C., May 2016a.

———, *Geographic Combatant Commander (GCC) Command and Control Organizational Options*, Suffolk, Va., 2nd ed., August 2016b.

JP—*See* Joint Publication.

Kahneman, Daniel, *Thinking, Fast and Slow*, London: Macmillan, 2011.

Kang, Byungkyu, John O'Donovan, and Tobias Höllerer, "Modeling Topic Specific Credibility on Twitter," *Proceedings of the 2012 ACM International Conference on Intelligent User Interfaces*, New York: Association for Computing Machinery, 2012, pp. 179–188.

Klein, Gary, *Sources of Power: How People Make Decisions*, Cambridge, Mass.: MIT Press, 1998.

Knight, Will, "StarCraft Will Become the Next Big Playground for AI," *MIT Technology Review*, November 4, 2016. As of May 2, 2018: https://www.technologyreview.com/s/602796/starcraft-will-become-the-next-big-playground-for-ai

Kolenda, Christopher D., Rachel Reid, Chris Rogers, and Marte Retzius, *The Strategic Costs of Civilian Harm*, New York: Open Society Foundations, June 2016. As of May 2, 2018: https://www.opensocietyfoundations.org/reports/strategic-costs-civilian-harm

Kott, Alexander, David Alberts, Amy Zalman, Paulo Shakarian, Fernando Maymi, Cliff Wang, and Gang Qu, *Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report*, Adelphi, Md.: U.S. Army Research Lab, June 2015. As of May 2, 2018: http://www.arl.army.mil/arlreports/2015/ARL-SR-0327.pdf

Kozloski, Robert, "Creating Cognitive Warriors," blog post, U.S. Department of the Navy, Office of Strategy and Innovation, August 2015. As of May 2, 2018: http://www.secnav.navy.mil/innovation/HTML_Pages/2015/08/CreatingCognitiveWarriors.htm

Krulak, Charles C., "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999.

Kuehl, Dan, National Defense University, "Information Warfare," briefing, undated.

Libicki, Martin C., *What Is Information Warfare?* Washington, D.C.: National Defense University, August 1995.

———, "The Convergence of Information Warfare," *Strategic Studies Quarterly*, Spring 2017, pp. 49–65.

Marine Corps Doctrinal Publication 1, *Warfighting*, Washington, D.C., June 20, 1997.

Matejka, Justin, and George Fitzmaurice, "Same Stats, Different Graphs: Generating Datasets with Varied Appearance and Identical Statistics Through Simulated Annealing," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York: Association of Computing Machinery, 2017, pp. 1290–1294.

McGrath, James R., "Twenty-First Century Information Warfare and the Third Offset Strategy," *Joint Force Quarterly*, Vol. 82, 3rd Quarter 2016, pp. 16–23.

Meyer, Philip, "Defining and Measuring Credibility of Newspapers: Developing an Index," *Journalism Quarterly*, Vol. 65, No. 3, 1988, pp. 567–574.

"Militant-Linked Muslim Charity on Front Line of Pakistan Quake Aid," Reuters, October 30, 2015.

Moroney, Jennifer D. P., Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom, and Abby Doll, *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region*, Santa Monica, Calif.: RAND Corporation, RR-146-OSD, 2013. As of May 2, 2018: https://www.rand.org/pubs/research_reports/RR146.html

Muehlhauser, Luke, "When Will AI Be Created?" Berkeley, Calif.: Machine Intelligence Research Institute, May 15, 2013. As of May 2, 2018: https://intelligence.org/2013/05/15/when-will-ai-be-created

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

Nicholas, James, "Australia: Current Developments in Australian Army Information Operations," *IO Sphere*, Special Edition, 2008, pp. 38–43.

Odierno, Raymond T., James F. Amos, and William H. McRaven, *Strategic Landpower: Winning the Clash of Wills*, white paper, U.S. Army, U.S. Marine Corps, and U.S. Special Operations Command, October 28, 2013. As of May 2, 2018: http://www.tradoc.army.mil/frontpagecontent/docs/strategic%20landpower%20white%20paper.pdf

Office of the Secretary of Defense, Rapid Reaction Technology Office, "Cyber S&T COI Needs Statement," Solicitation RRTO-20170710-W-CyberCOI, July 10, 2017. As of May 2, 2018: https://www.fbo.gov/?s=opportunity&mode=form&id=23babdb83e3dca29ff5360ff8d2aff0f

O'Reilly Media, "Clay Shirky," keynote speaker bio, Web 2.0 Expo, 2008. As of May 2, 2018: http://www.web2expo.com/webexny2008/public/schedule/detail/4817

Osoba, Osonde A., and William Welser IV, *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017. As of May 2, 2018: https://www.rand.org/pubs/research_reports/RR1744.html

Oxford Dictionaries, *Orient*, webpage, Oxford University Press, undated. As of May 2, 2018: https://en.oxforddictionaries.com/definition/orient

Paul, Christopher, *Information Operations Doctrine and Practice: A Reference Handbook*, Westport, Conn.: Praeger, 2008.

———, *Strategic Communication: Origins, Concepts, and Current Debates*, Santa Barbara, Calif.: Praeger, 2011.

———, "Confessions of a Hybrid Warfare Skeptic," *Small Wars Journal*, May 3, 2016. As of May 2, 2018:
http://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic

Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub 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 May 15, 2018:
https://www.rand.org/pubs/research_reports/RR1925z1.html

Paul, Christopher, and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of May 2, 2018:
https://www.rand.org/pubs/perspectives/PE198.html

Paul, Christopher, and Elizabeth L. Petrun Sayers, "Assessing Against and Moving Past the 'Funnel' Model of Counterterrorism Communication," *Defence Strategic Communications*, Vol. 1, No. 1, Winter 2015, pp. 27–41.

Paul, Christopher, Jessica Yeats, Colin P. Clarke, and Miriam Matthews, *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference*, Santa Monica, Calif.: RAND Corporation, RR-809/1-OSD, 2015. As of May 2, 2018:
https://www.rand.org/pubs/research_reports/RR809z1.html

Poisel, Richard A., *Information Environment and Electronic Warfare*, Norwood, Mass.: Artech House, 2013.

Pomerleau, Mark, "Marines Look to Dominate in Information Environment," *C4ISRNET*, April 5, 2017. As of May 2, 2018:
https://www.c4isrnet.com/c2-comms/2017/04/05/marines-look-to-dominate-in-information-environment

Porche, Isaac R. III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, Calif.: RAND Corporation, RR-1600-A, 2017. As of May 2, 2018:
https://www.rand.org/pubs/research_reports/RR1600.html

Porche, Isaac R. III, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman, *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information*, Santa Monica, Calif.: RAND Corporation, RR-315-NAVY, 2014. As of May 2, 2018:
https://www.rand.org/pubs/research_reports/RR315.html

Richards, Raymond, "High-Assurance Cyber Military Systems (HACMS)," webpage, Defense Advanced Research Projects Agency, undated. As of May 2, 2018:
https://www.darpa.mil/program/high-assurance-cyber-military-systems

Rieh, Soo Young, "Credibility and Cognitive Authority of Information," in Marcia J. Bates and Mary Niles Maack, eds., *Encyclopedia of Library Information Sciences*, 3rd ed., Boca Raton, Fla.: CRC Press, 2009, pp. 1337–1344.

Rogers, Paul, Rudy Puryear, and James Root, "Infobesity: The Enemy of Good Decisions," *Bain Insights*, June 11, 2013. As of May 2, 2018:
http://www.bain.com/publications/articles/infobesity-the-enemy-of-good-decisions.aspx

Romanych, Marc J., "Visualizing the Information Environment," *Military Intelligence Professional Bulletin*, Vol. 29, No. 3, 2003.

———, "A Theory-Based View of Information Operations," *IO Sphere*, Spring 2005, pp. 14–18. As of May 2, 2018:
http://www.au.af.mil/au/awc/info-Ops/iosphere/iosphere_spring05_romanych.pdf

Rosen, Rebecca, "Clouds: The Most Useful Metaphor of All Time?" *The Atlantic*, September 30, 2011. As of May 2, 2018:
https://www.theatlantic.com/technology/archive/2011/09/clouds-the-most-useful-metaphor-of-all-time/245851

Russakovsky, Olga, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei, "ImageNet Large Scale Visual Recognition Challenge," arXiv, Cornell University Library, paper 1409.0575, revised January 30, 2015. As of May 2, 2018:
https://arxiv.org/abs/1409.0575

SAE International, On-Road Automated Vehicle Standards Committee, "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," SAE Standard J3016, September 30, 2016. As of May 2, 2018:
http://standards.sae.org/j3016_201609

Schmid, Alex P., *Radicalisation, de-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review*, The Hague, Netherlands: International Centre for Counter-Terrorism, 2013. As of May 2, 2018:
https://icct.nl/publication/radicalisation-de-radicalisation-counter-radicalisation-a-conceptual-discussion-and-literature-review

Shirky, Clay, *Here Comes Everybody: The Power of Organizing Without Organizations*, London: Penguin, 2008a.

———, "It's Not Information Overload, It's Filter Failure," keynote address, Web 2.0 Expo, September 18, 2008b. As of May 2, 2018:
https://www.youtube.com/watch?v=LabqeJEOQyI

Soares, Nate, and Benya Fallenstein, "Agent Foundations for Aligning Machine Intelligence with Human Interests: A Technical Research Agenda," in Victor Callaghan, James Miller, Roman Yampolskiy, and Stuart Armstrong, eds., *The Technological Singularity: Managing the Journey*, New York: Springer, 2017, pp. 103–125.

Speier, Cheri, Joseph S. Valacich, and Iris Vessey, "The Influence of Task Interruption on Individual Decision Making: An Information Overload Perspective," *Decision Sciences*, Vol. 30, No. 2, March 1999, pp. 337–360.

Szegedy, Christian, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus, "Intriguing Properties of Neural Networks," arXiv, Cornell University Library, paper 1312.6199, revised February 19, 2014. As of May 2, 2018:
https://arxiv.org/abs/1312.6199

Thelwall, Mike, "The Heart and Soul of the Web? Sentiment Strength Detection in the Social Web with SentiStrength," in Janusz A. Holyst, ed., *Cyberemotions: Cognitive Emotions in Cyberspace*, Basel, Switzerland: Springer, 2017, pp. 119–136.

Thomson, Scott K., and Christopher E. Paul, "Paradigm Change: Operational Art and the Information Joint Function," *Joint Force Quarterly*, Vol. 89, 2nd Quarter 2018, pp. 8–14.

Tomforde, Sven, Jörg Hähner, Sebastian von Mammen, Christian Gruhl, Bernhard Sick, and Kurt Geihs, "'Know Thyself': Computational Self-Reflection in Intelligent Technical Systems," *2014 IEEE Eighth International Conference on Self-Adaptive and Self-Organizing Systems Workshop*s, Piscataway, N.J.: IEEE, 2014, pp. 150–159.

Tsvetovat, Maksim, and Kathleen M. Carley, "Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence," *Journal of Social Structure*, Vol. 6, No. 2, 2005. As of May 2, 2018:
http://repository.cmu.edu/isr/43

U.S. Army, *Unified Quest: Fighting on the Battleground of Perception*, Washington, D.C., October 4, 2016. As of May 2, 2018:
http://www.arcic.army.mil/App_Documents/UQ/UQ-Fighting-on-the-Battleground-of-Perception.pdf

U.S. Army Special Operations Command, *Cognitive Maneuver for the Contemporary and Future Strategic Operating Environment*, white paper, May 13, 2016.

———, *Expanding Maneuver in the Early 21st Century Security Environment*, January 12, 2017. As of May 2, 2018:
http://www.soc.mil/Files/ExpandingManeuvers21Century.pdf

U.S. Defense Information Systems Agency, "Information Volume and Velocity Overview," briefing, June 2015.

U.S. Department of Defense, *Strategy for Operations in the Information Environment*, Washington, D.C., June 2016. As of May 2, 2018:
https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Force Operations: Joint Force 2030*, Washington, D.C., March 18, 2016a.

———, *Joint Concept for Human Aspects of Military Operations*, Washington, D.C., October 19, 2016b.

———, *Joint Concept for Integrated Campaigning*, Washington, D.C., March 16, 2018. As of May 2, 2018:
http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

U.S. Marine Corps, *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, Washington, D.C., September 2016.

———, *Information Warfare Concept of Employment*, Washington, D.C., May 10, 2017a.

———, *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, Washington, D.C., July 6, 2017b.

von Clausewitz, Carl, *On War*, J. J. Graham, trans., London: Wm. Clowes and Sons, 1909.

Waina, Beth, National Air and Space Intelligence Center, "Behavioral Influences: Mission, Methodology and Analysis," presentation at the RAND Corporation, Santa Monica, Calif., October 7, 2016.

Warren, T. Camber, "Explosive Connections? Mass Media, Social Media, and the Geography of Collective Violence in African States," *Journal of Peace Research*, Vol. 52, No. 3, 2015, pp. 297–311.

Watzlawick, Paul, Janet Beavin Bavelas, and Don D. Jackson, *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes*, New York: W. W. Norton and Company, 2014.

Weedon, Jen, William Nuland, and Alex Stamos, *Information Operations and Facebook*, version 1.0, Menlo Park, Calif.: Facebook, 2017.

Wexler, James, "Facets: An Open Source Visualization Tool for Machine Learning Training Data," *Google Open Source Blog*, July 17, 2017. As of May 2, 2018:
https://research.googleblog.com/2017/07/facets-open-source-visualization-tool.html

Williams, Michael, "Speed, Volume, and Ubiquity: Forget Information Operations and Focus on the Information Environment," *Strategy Bridge*, July 26, 2017. As of May 2, 2018:
https://thestrategybridge.org/the-bridge/2017/7/26/
speed-volume-and-ubiquity-forget-information-operations-focus-on-the-information-environment

Winter, Charlie, and Colin P. Clarke, "Is ISIS Breaking Apart?" *Foreign Affairs*, January 31, 2017. As of May 2, 2018:
https://www.foreignaffairs.com/articles/2017-01-31/isis-breaking-apart

Yampolskiy, Roman, and Joshua Fox, "Safety Engineering for Artificial General Intelligence," *Topoi*, Vol. 32, No. 2, October 2013, pp. 217–226.

Yudkowsky, Eliezer, *Rationality: From AI to Zombies*, Berkeley, Calif.: Machine Intelligence Research Institute, 2015.

Zeleny, Milan, *Human Systems Management: Integrating Knowledge, Management and Systems*, Hackensack, N.J.: World Scientific, 2005.

Zhang, Xiaoteng, Zhengyan Ding, Jianying Zhou, Jie Shao, and Lin Mei, *The Third Research Institute of the Ministry of Public Security*, Beijing, undated.

The information environment (IE) is not a physical place and has not yet been defined as a warfighting domain in U.S. military doctrine. Targets of operations in and through the IE include human perceptions or behaviors: Weapons are ideas, and defenses are norms, beliefs, and traditions.

Adding to the complexity of achieving command and control (C2) and situational awareness of the IE is the fact that the U.S. Department of Defense has not effectively integrated the IE into operational planning, doctrine, or processes, instead considering traditional land, air, and sea operations separately from operations in the information space. However, every military activity has inherent informational aspects, and adversaries are increasingly using propaganda, misinformation, and other means to influence public perceptions, alliances, and decisions.

Drawing on a review of doctrine and processes, the history of information operations and information-related capabilities, and interviews with subject-matter experts and stakeholders, this report presents a three-tiered vision for the role of information in U.S. military operations. It also identifies requirements for achieving effective C2 and situational awareness of the IE and presents a detailed analysis of seven ways to organize for this objective. Ultimately, addressing the gaps and shortfalls identified in this report will require a much stronger understanding of the IE, associated concepts and capabilities, and roles and responsibilities across the joint force.

NATIONAL DEFENSE RESEARCH INSTITUTE

www.rand.org

$29.00

ISBN-10 1-9774-0131-7
ISBN-13 978-1-9774-0131-1

RR-2489-OSD