This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

REDEFINING INFORMATION WARFARE BOUNDARIES FOR AN ARMY IN A WIRELESS WORLD

Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held

Prepared for the United States Army

ARROYO CENTER

The research described in this report was sponsored by the United States Army under Contract No. W74V8H-06-C-0001. The findings and views expressed in this report are those of the authors and do not necessarily reflect the views of the Army or the U.S. Department of Defense.

Library of Congress Cataloging-in-Publication Data

Porche, Isaac, 1968-
Redefining information warfare boundaries for an Army in a wireless world / Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held.
pages cm
Includes bibliographical references.
ISBN 978-0-8330-5912-3 (pbk. : alk. paper)
1. Information warfare—United States. 2. Military doctrine—United States. 3. United States. Army—Communication systems. 4. Computer networks—Security measures—United States—Planning. 5. Cyberspace—Security measures—United States. I. Paul, Christopher, 1971- II. Title.

UA23.P58 2013
355.3'43—dc23

2013000702

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Information warfare is not currently defined in U.S. Department of Defense (DoD) or U.S. Army doctrine, but it is a term found in past doctrine.[1] What is in today's DoD lexicon is the term *information environment*, the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (U.S. Joint Chiefs of Staff, 2010b). Joint doctrine (e.g., JP 3-13.1) makes clear that "there is an electromagnetic spectrum portion of the information environment" (U.S. Joint Chiefs of Staff, 2007, p. vii).[2] Thus, wired and wireless technology fit in this landscape.

As a term, *information warfare*, or IW, remains in use worldwide, in the militaries of other countries as well as in some of the U.S. military services. The Navy now has an IW officer position, which it advertises as involving "attacking, defending and exploiting networks to capitalize on vulnerabilities in the information environment" (U.S. Navy, undated). Career paths for these officers are described in Appendix F. We define IW as follows:

> *Information warfare is conflict or struggle between two or more groups in the information environment.*[3]

---

[1] There is no entry in Joint Publication 1-02 (U.S. Joint Chiefs of Staff, 2010b). *Past doctrine* here refers to the mid-1990s. See AFDD 5, 1996, and CJCSI 3201.01, 1996.

[2] Joint doctrine says that a portion of the information environment includes the electromagnetic environment (EME). See U.S. Joint Chiefs of Staff, 2007.

[3] Dan Kuehl of the National Defense University defines IW as "military offensive and defensive actions to control/exploit the environment" (various briefings); U.S. Joint Chiefs

Social networks, as part of the information environment, are also a part of such conflicts or struggles. As noted by LTG Michael Vane, "Army forces operate in and among human populations, facing hybrid threats that are innovative, networked, and technologically-savvy" (TRADOC, 2010a, p. i).[4] Internet-assisted social networking is now a part of the operational environment, as events in Egypt, Moldova, Iran, and even Pittsburgh have made clear.[5] Social networks are a growing and increasingly relevant element of the information environment.

Cyberspace is the technical foundation on which the world is increasingly relying to exchange information (and to facilitate social networking, extend influence from afar, and so on). As a collection of mediums, it is rapidly consuming the information environment's

---

of Staff (1995) notes that "IW focuses on affecting an adversary's information environment while defending our own." CJCSI 3210.01 (1996) defined information warfare as follows: "Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer based networks while defending one's own information, information-based processes, information systems and computer-based networks."

[4] On September 16, 2010, Deputy Secretary of Defense William J. Lynn III signed Directive-Type Memorandum 09-026 establishing Internet-based capabilities as an integral part of DoD operations. Falling under the realm of Internet-based capabilities is social media.

[5] Cell phones and text messaging are believed to have played a crucial role in fostering the so-called Orange Revolution in the Ukraine. Twitter is credited with making these protests widespread and successful (e.g., flash mobs). Ultimately, the protests forced a recount of the general election. See Morozov (2009), Goldstein (2007), and Stack (2009).

During Iran's so-called Twitter revolution, it was reported that well-developed Twitter lists showed a constant stream of situational updates and links to photos and videos, all of which painted a portrait of the developing turmoil. According to news reports, when the Iranian regime started taking down these sources, the so-called e-dissidents shifted to email. (See "Iran's Twitter Revolution," 2009.)

During a recent G20 meeting, protesters in Pittsburgh leveraged Twitter. For example, Elliot Madison, an activist in New York City, used Twitter to disseminate information about Pittsburgh police activities and movements during the protests. Reportedly, police raided Madison's hotel room, and, one week later, his home was raided by FBI agents. Police reports claim that Madison and a co-defendant used computers and a radio scanner to track police movements and then passed that information to protesters using cell phones and Twitter. Madison is reportedly being charged with hindering apprehension or prosecution, criminal use of a communication facility, and possession of instruments of crime (Democracy Now! 2009; Electronic Frontier Foundation, 2009; Goodman, 2009).

landscape. Therefore, we conclude that controlling cyberspace (and the intersecting electromagnetic spectrum) could eventually be tantamount to controlling the information environment. The Army must prepare for that possibility.

The Problem with Current Doctrine

Preparation for IW will start with revision of the 2003 Army Field Manual (FM) 3-13, *Information Operations* (IO), which is widely considered antiquated and insufficient for the future. Harkening back to the birth of the information operations concept out of command and control warfare in the late 1990s, this doctrine aggregates the areas of electronic warfare (EW),[6] computer network operations (CNO), psychological operations (PSYOP),[7] military deception (MILDEC), and operations security (OPSEC) as core capabilities, despite the fact that some of these concepts are quite dissimilar. This is shown in Figure S.1.

One conflict that has emerged stems from overlapping doctrine. For example, CNO, historically covered in FM 3-13, is the main component of cyber operations. According to the latest Army operating concept, "Cyberspace operations include computer network operations" (TRADOC, 2010b). Similarly, EW has its own doctrine (FM 3-36) and a growing force structure. Thus, we can say that the growth in size and importance of EW, CNO, and cyber operations as a whole render them too large and fast-moving to fit within this IO doctrine.

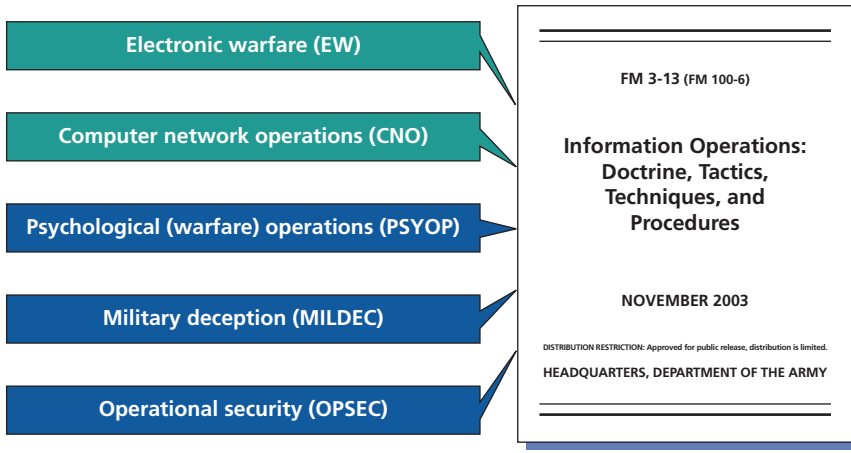
The confusion associated with IO as a term—in the Army and at the joint level—stems from many sources: genuine ambiguity in the lexicon, both willful and unintentional misuse of the term, and both genuine misunderstanding and genuine disagreement about what such operations are and how they ought to be defined.

---

[6] Certain functions in EW can be considered military deception. This includes the use of expendibles (e.g., flares) by vehicles (Hura, 2010). This should be (and likely is already) included in EW doctrine and/or corresponding tactics, techniques, and procedures.

[7] Now referred to as military information support operations (MISO). See Chapter Two.

Figure S.1
IO Doctrine



RAND *MG1113-S.1*

As reflected in Figure S.1, at the time of this research, joint doctrine defined IO as follows:

> The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (U.S. Joint Chiefs of Staff, 2007, p. G-10)

This definition does little to clear up the confusion, both because of ambiguities in the definition itself—because soldiers imagine it to (or want it to) mean something else—and because IO, as actually practiced, deviates from that definition.[8]

[8] This alone demands new doctrinal writings. As Maj Gen I. B. Holley (1983) said, "What is doctrine? Simply this: doctrine is officially approved prescriptions of the best way to do a job. Doctrine is, or should be, the product of experience. Doctrine is what experience has shown usually works best."

In January, 2011, Secretary of Defense Robert Gates issues a memorandum outlining a revised definition of IO, with a greater focus on integration. He stated that the definition in effect when this research was conducted placed "too much emphasis on core capabilities" and supported the "notion that the core capabilities must be overseen by one entity. Joint doctrine now defines IO as

> the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries while protecting our own. (Gates, 2011)

There are genuine disputes regarding both the terminology and the concepts of IO, so resolution cannot be had with simple clarification. There are decisions to be made.

Information Operations as a Moving Target

Further complicating the situation is that the need for change in IO is recognized, and progress is under way as of this writing in both the joint community and the Army toward improving definitions, revising doctrine, clarifying concepts, and adjusting organizations. The 2011 Gates memo is an example of the progress made between the time that this monograph was first drafted and the time of its publication. The authors have endeavored to stay abreast of such movement, but other changes and advances have taken or are taking place at the time of publication. Undoubtedly, some important decisions will have been made, other important progress will have occurred, and some of the recommendations presented here will have been overtaken by events.

However, challenges will remain. Debate within and surrounding the information operations community runs hot and fierce, and progress is often delayed by disagreements (such as the 2009 attempt to revise FM 3-13, described in Appendix B). The information environment continues to evolve, adding new challenges. If we believed that all the issues facing information operations would be resolved by the time this monograph was released, we would not have published it. As

the doctrine and practice of IO continue to evolve, this monograph will remain useful when further changes are considered or when past changes are revisited, reviewed, and debated again.

Resolving the Problems by Redefining Doctrinal Terms

More clarity can be provided by separating the functional areas currently defined in the IO definition into two realms: the more technical functional areas and the other functional areas associated with PSYOP/MISO.

Information content (e.g., the message) is key for the psychological part; the means to deliver content (or prevent delivery) is key for the technical part. Ultimately, it makes sense that most of what falls into the psychological realm (shown in Table S.1) be redefined as inform and influence operations (IIO) and that most of what falls into the technical realm be considered information technical operations (ITO).

Essentially, we suggest that the doctrine be split to reflect how the expertise has been divided today, as illustrated in Figure S.2. The table does not account for the integrating function; integration of these areas belongs with the commander. Revisions to the mission command doctrine should reflect this.

Network operations fall clearly within the technical realm. While we include them in the table for completeness, we do not foresee any practical benefit in merging network doctrine and personnel with the other areas. This is because network operations are large, long-standing efforts in the Army that should remain focused (Porche et al., 2010). However, this issue requires more study and was outside the scope of our research.

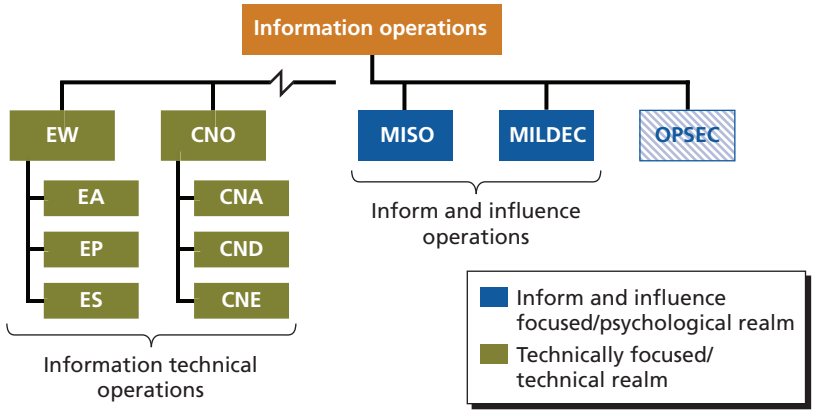
We offer the following definition of IIO. It integrates features of three different visions of what IO could be (these different visions are described in Chapter Three): an integrating function, an influence capability, and an advisory capability.

> *Inform and influence operations are efforts to inform, influence, or persuade selected audiences through actions, utterances, signals, or messages.*

Table S.1
Information Warfare: Realms of the Possible

Category	Psychological Realm	Technical Realm
Functional areas, subareas, defined in existing doctrine	MISO, public affairs (PA), aspects of MILDEC	Electronic attack (EA), electronic protect (EP), electronic support (ES), computer network attack (CNA), computer network exploit (CNE), signals intelligence, electromagnetic spectrum operations (EMSO), information assurance, operating and maintaining networks (network operations), aspects of MILDEC, aspects of OPSEC
Target	People	Machines
Alternate name	Inform and influence operations (IIO)	Information technical operations (ITO) or cyber-electronic operations or cyber-electromagnetic operations

Figure S.2
The Dividing Line That Should Be Sharpened: Technical Operations Versus Inform and Influence Operations



NOTE: CND = computer network defense.

RAND *MG1113-S.2*

We offer the following definition of ITO. We do not mean to imply that all or most of the areas are covered under signals intelligence. It is a combination of electronic warfare, computer network operations, and other functions.

> *Information technical operations are efforts to protect and/or coordinate U.S. and allied technical means and mediums (e.g., the EMS) that facilitate command-and-control and, perhaps, certain intelligence activities and to deny the means and mediums used by adversaries.*

This definition and the associated vision have several notable characteristics. First, this definition separates the "apples" of information content from the "apple carts" of information systems (e.g., information technology and electronics) and retains the term *information operations* to refer to the former exclusively (see Paul, 2008). Under this vision, IIO include only efforts to inform, influence, or persuade.

Advantages of Revising Doctrinal Definitions

These separated definitions make clear the distinctions between the functional area groupings (i.e., the psychological and technical realms) shown in Table S.1. More distinction helps lessen the confusion that exists today regarding who executes the missions shown in Figure S.1. The personnel in these areas might be more focused and better able to develop concentrated expertise. Finally, separating these areas could translate into more opportunity to consolidate within them.

Consolidation in the Technical Realm

Consolidation in the technical realm is possible and advisable. The boundary between CNO over wireless networks and EW is blurring. At a minimum, the impact of the convergence trend is that EW (electronic attack [EA], electronic protect [EP], and electronic support [ES]) and CNO (computer network attack [CNA], computer network defense [CND], and computer network exploitation [CNE]) are becoming increasingly comingled.

On the materiel side, the convergence of wired and wireless mediums suggests that there might be circumstances in which the functional requirements of these currently separate areas can be met by the same device that combines technologies to yield the best system solution. Advanced electronic steerable array (AESA) radars might fall into the EW and the CNO areas because they can sense and transmit in both analog and digital formats.

As a result, we conclude that EW and CNO could—and perhaps should—share the same people, process, and technologies to carry out these operations to avoid duplication of effort or working at cross-purposes. We understand that the Army has already begun to make some moves toward aggregation in this area.

Proposals already exist to merge existing EW and emerging cyber operations doctrine, and they appear to be advantageous; progress is being made in this direction. However, there are cautions. Today, the authorities required to conduct offensive EW are more clearly understood and more permissive than the authorities that exist for offensive CNO. In addition, the clearance levels required for offensive EW differ from those required for offensive CNO.[9] Doctrine for EMSO and spectrum managers themselves (e.g., personnel with the 25E military occupational specialty [MOS])[10] should be part of this consolida-

---

[9] For example, generally, electronic attack operations are planned at the secret level, and authority to plan and execute operations resides with tactical- and operational-level commanders. On the other hand, CNA operations are often conducted at higher security levels (Hura, 2010).

[10] The signal corps' MOS 25E enlisted specialty for spectrum management was created a number of years ago. Prior to the creation of this specialty, noncommissioned officer spectrum managers were tracked only with a skill identifier attached to a preexisting MOS. The skill identifier for enlisted personnel (for spectrum managers) was not found to be satisfactory because these spectrum managers were often retasked outside of the spectrum specialty. There is a skill identifier for commissioned officers, but it is dormant.

In the case of EW, the Army recently created a new career management field that provides a new MOS for officers, warrant officers, and enlisted personnel. Hundreds of billets (greater than 3,000 personnel) have been created, although not all have been filled. The specific career management field identifiers for EW are to be FA29 for officers, MOS 290A for warrant officers, and MOS 29E for enlisted personnel.

tion. We illustrate this proposal in Figure S.3. Also, technical aspects of OPSEC and MILDEC fall here.

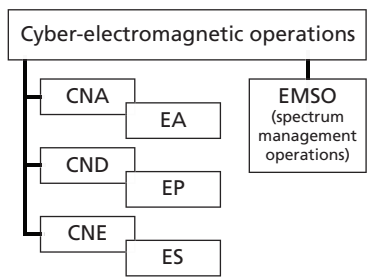
The Army eventually needs to either create a new "cyber-electronic" or "cyber-electromagnetic" career management field or transform an existing one (e.g., CMF 29) to provide dedicated support to all or most of the technical realm of IW. This would serve as a first step toward a new branch for cyber-electromagnetic warriors for the far future who can be utilized to cover the areas discussed here. This group includes EW and spectrum managers.

Consolidation in the Psychological Realm

A similar argument can be made for the psychological realm, where there is just as much opportunity for consolidation. Specifically, PA and MISO (formerly PSYOP) have ample reason to become better integrated.

Currently, there is a "firewall" between PA and MISO. The concern that has kept PA and MISO separate is the commitment to use (or not use) truthful information. However, the lack of PA-MISO coordination has resulted in repeated instances of "information fratricide," in which the separate capabilities provide conflicting information. The fear is that MISO could contain less-than-truthful information and thus jeopardize the credibility of PA efforts. However, almost all conventional MISO use truthful information (and sometimes the only dif-

Figure S.3
Potential Consolidation in the Technical Realm



RAND *MG1113-S.3*

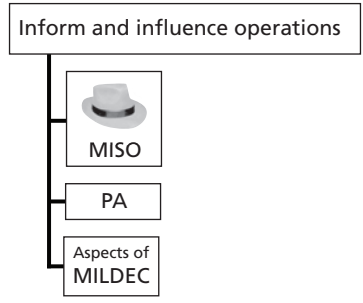
ference is the audience). A commitment to the truth is a reasonable approach. A bridge between the two seems possible with the approach suggested here.[11] Thus, beneficial integration and perhaps even consolidation (organizationally and/or with respect to personnel) is conceivable as envisioned in Figure S.4. At minimum, the firewall between inform and influence should be removed and placed at the bounds of truth and good intention. All communications seek to influence, and that is OK. Where the line should be drawn is between truthful efforts at virtuous persuasion (wholly acceptable) and deceptive manipulation.

Courses of Action

We see three courses of action for revising Army doctrine, addressing needs of FM 3-13 and the use of information operations officers.

1. The first course of action is to maintain the status quo (nearly). Maintain a broad definition of IO that involves integration of the five key functional areas listed in Figure S.1. This course of action includes continued reliance on FM 3-13 nearly as is;

Figure S.4
Potential Consolidation in the Psychological Realm



RAND *MG1113-S.4*

[11] NATO tried unsuccessfully to merge IO and PA but without making a clear commitment to use the truth only.

it would perhaps need an update to accommodate the expected revision to the joint definition of IO (when it becomes official).

2. Course of action two is to develop new doctrine that divides current doctrine (FM 3-13, as shown in Figure S.1) into IIO and ITO, as suggested in Figures S.2, S.3, and S.4. Integration functions would explicitly become the task of commanders, and this role and task will have documented in the corresponding doctrine (mission command). As such, FM 3-13 would be obviated, as would the role of IO officers as integrators. Doctrinally, ITO would fall under cyber-electronic operations or cyber-electromagnetic operations, which could be addressed in a revised FM 3-36 (currently titled *Electronic Warfare*).
3. Course of action three is to limit the scope of IO and IO officers to IIO as we define it here. This would essentially involve redefining IO to include only the functional areas we list in the psychological realm and the integration role of IO officers to be one of integrating MISO, PA, MILDEC, and similar functional areas.[12] To be clear, this would involve redefining IO *as efforts to inform, influence, or persuade selected audiences through actions, utterances, signals, or messages*. Doctrinally, ITO would fall under cyber-electronic operations or cyber-electromagnetic operations, which could be addressed in a revised FM 3-36 (currently titled *Electronic Warfare*).

Recommendations

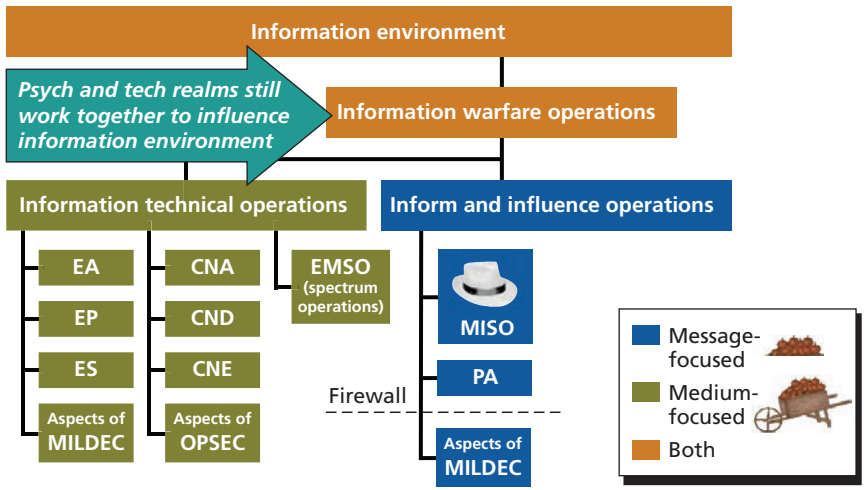
Based on our review of the literature and analysis of overlapping tasks in some of these functional areas, we recommend course of action two. This is illustrated in Figure S.5.

Not addressed explicitly by the listed courses of action but certainly important to the discussion is the relationship of OPSEC as a

[12] For example, revise FM 3-13 to cover the need to integrate only MISO, PA, MILDEC, and other capabilities contributing to informing and influencing. Retain FA30s to integrate inform and influence. Certain aspects of MILDEC fall under EW (e.g., use of expendables and flares).

capability area to the new structure. We believe that OPSEC is everyone's responsibility. Aspects of it certainly fall under technical operations, but it could also be covered in the mission command doctrine that is currently under revision.

Figure S.5
Recommended Course of Action: Redefine Information Warfare Operations



RAND *MG1113-S.5*