USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS ROADMAP: ONE RIGHT TURN AND WE'RE THERE

by

Colonel Brian J. McKiernan
United States Army

Colonel David J. Smith
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 MAR 2007	**Strategy Research Project**	**00-00-2006 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Operations Roadmap One Right Turn and We're There	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Brian McKiernan	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**21**	

ABSTRACT

AUTHOR: Colonel Brian J. McKiernan

TITLE: Information Operations Roadmap: One Right Turn and We're There

FORMAT: Strategy Research Project

DATE: 26 March 2007 WORD COUNT: 6,246 PAGES: 21

KEY TERMS: Information Superiority, Information Dominance, Information Age, Third Wave, Principles of War, Wal-Mart, Transformation

CLASSIFICATION: Unclassified

During Secretary Rumsfeld's tenure, the Department of Defense embarked on one of the most far-reaching transformations in the history of the United States military. This transformation is largely driven by the rapid advances in information technology and the belief that information is more critical now to military success and will become even more critical in the foreseeable future. The Department of Defense addressed this assumption by formulating the Information Operations Roadmap with the objective of making information operations a core capability of future forces and a core military competency. The goal of information operations is to gain information superiority – the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting the enemy's ability to do the same. Achieving and sustaining a significant information advantage over the adversary remains problematic, particularly in asymmetric conflicts. This project assesses the Information Operations Roadmap by examining non-military applications of information technology in the Information Age, reviewing current doctrine and assessing information operations during recent United States military operations. This study provides recommended adjustments to the *Information Operations Roadmap* based on this analysis.

INFORMATION OPERATIONS ROADMAP: ONE RIGHT TURN AND WE'RE THERE

During Donald Rumsfeld's tenure as Secretary of Defense, the Department of Defense (DoD) initiated one of the most comprehensive transformations in the history of the United States military. "*The 2001 Quadrennial Defense Review* identified information operations (IO) as one of six critical operational goals that focus transformation efforts within DoD."[1] In October 2003, as a guide for achieving this goal, the DoD published the Information Operations Roadmap. Since its publication, the Roadmap has played a significant role in shaping how DoD, the Services, and Combatant Commands organize, train, equip, plan, and execute information operations. However, based on analysis of non-military applications of information technology, a review of current information operations doctrine, and observations from recent military operations it appears some adjustments to the roadmap are necessary.

The Case for Transformation

"The Administration argues that new technologies make defense transformation possible and that new threats to U.S. security make defense transformation necessary."[2] Among the new technologies profoundly impacting military operations are those in the area of information technology. The Congressional Research Service report on Defense transformation says;

> [t]he Administration's vision for defense transformation calls for shifting the U.S. military away from a reliance on massed forces, sheer quantity of firepower, military services operating in isolation from one another, and attrition-style warfare, and toward a greater reliance on joint (i.e., integrated multi-service) operations, [network centric warfare] NCW, effects-based operations (EBO), speed and agility, and precision application of fire power. Some transformation advocates characterize these changes as shifting from an industrial-age approach to war to an information-age approach.[3]

Presumably, with a transformed military that is "better informed," more agile, and equipped with precision weapons and capabilities, an exponential increase in speed of action more than compensates for the corresponding decrease in mass. This supposes that "…a fundamental law of Newtonian physics applies also to military maneuver: one can achieve overwhelming force by substituting velocity for mass."[4] This increase in velocity relies on the U.S. military's ability to achieve information superiority over its adversaries, which Joint Publication 3-13 *Information Operations*, defines as "… an operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting the enemy's ability to do the same."[5] In large measure, the success of U.S. military transformation rests on the belief that a transformed military can gain and maintain information superiority over its adversaries.

Is the Information Age Really Upon Us?

With so much of the U.S. military transformation resting on the ability to gain and maintain a significant advantage through the application of new technologies, particularly information technologies, it is important to determine if this underlying assumption has merit. In their book, *War and Anti-War, Survival at the Dawn of the 21st Century*, renowned futurists, Alvin and Heidi Toffler assert that "throughout history the way men and women make war has reflected the way they work."[6] The Tofflers' model for the evolution of societies uses the analogy of "waves" to describe the major shifts in civilizations throughout history. Their model includes three waves with the first being the Agrarian Age. They maintain that the Second Wave, known as the Industrial Age, is currently giving way to the Third Wave or Information Age.

The Tofflers' also observe that, societies from each wave exist simultaneously in today's world, and those reflecting the qualities of the later waves tend to dominate societies from earlier waves. This, along with the Toffler's assertion that the manner in which societies build wealth influences how they make war, means the United States should enjoy distinct advantages over most nations based on its integration of information and information technology in both disciplines. Accepting the Tofflers' views, it seems the Administration's rationale for transformation of the military is on solid ground.

Creating Wealth the "Wal-Mart Way"

The Tofflers explain one of the main distinctions between Second Wave and Third Wave economies this way.

> While land, labor, raw materials, and capital were the main "factors of production" in the Second Wave economy of the past, knowledge – broadly defined here to include data, information, images, symbols, culture, ideology, and values – is the central resource of the Third Wave economy.[7]

Considering the Tofflers' view that the way man wages war largely reflects how he creates wealth, an examination of the largest retail company in the world should reveal some useful insights into how the United States might alter how it wages war in the Information Age.

Thomas Friedman's discussion of Wal-Mart's "supply-chaining" in his book, *The World is Flat: A Brief History of the Twenty-First Century*, details how this small variety store chain became the world's largest retailer through the aggressive and innovative use of information technology (IT) to gain an "information advantage" over its competitors. "By investing early and heavily in cutting-edge technology to identify and track sales on the individual item level, the Bentonville Ark[ansas]-based retail giant made its IT infrastructure a key competitive advantage that has been studied and copied by companies around the world."[8]

Can a Third Wave Military Gain Similar Advantages?

According to the Tofflers, "…a revolution is occurring that places knowledge, in various forms, at the core of military power. In both production and destruction, knowledge reduces the requirement for other inputs."[9] An examination of the DoD transformation confirms the general trend toward "reduced input" based on increased "knowledge." The most obvious and sweeping reduction is found in the U.S. Army. Army transformation replaces the large World War II-style Division with the smaller, more agile Brigade Combat Team (BCT) as the basic war fighting organizational element. According to the Operational and Organizational Plan, the Future Combat System (FCS)-equipped BCT

> … has the wherewithal to develop the situation before, during, and after contact, affording leaders and Soldiers unprecedented situational dominance with revolutionary competencies and capabilities. The BCT operates within a new tactical paradigm based upon the Quality of Firsts–the Ability to See First, Understand First, Act First, and Finish Decisively.[10]

Similarly, Army transformation increases emphasis on Special Operations Forces which will grow by 14,000 personnel and add four battalions to Army Special Forces. The programmed growth in Special Forces is another example of the trend away from mass, attrition-style warfare of the Industrial Age toward reliance on "reduced inputs" in the Information Age.

Similar trends are noticeable in other Services as well. The development of improved sensors, precision guided munitions, and low-observable technology enabled the U.S. Air Force to significantly reduce the number of aircraft and the number of munitions required to destroy tactical and strategic targets. All three of these technological advances provide advantages based on dramatically improved employment of information. Improved sensors provide unprecedented *fidelity of information* concerning the target; precision guided munitions enable unprecedented accuracy by *providing information* directly to the ordnance thereby allowing it to adjust its course; and low-observable technology provides enhanced protection by *denying information* to the enemy about the location of aircraft.

This migration from large inputs to reduced inputs is not merely a matter of new technologies improving the effectiveness of existing weapons and systems. The real driver is technological advances that dramatically increase the quantity and quality of available *information*, help transform this information into *knowledge*, and through network-centric operations rapidly share it vertically and horizontally across the force. In his book, *The Principles of War for the Information Age*, military theorist, Robert Leonhard points out that '[c]urrent military doctrine is "estimate-based."'[11] That is to say, "[w]e are fundamentally ignorant of the enemy's whereabouts and intentions, and so we *estimate* the future."[12] During planning,

staff officers prepare operations estimates, intelligence estimates, logistics estimates, personnel estimates, and various other estimates to inform the commander of the location and status of friendly and enemy forces. During execution, staffs use situation reports to update these estimates. With the proliferation of tactical internet, satellite communications, global positioning systems, and other technologies, the timeliness and fidelity of information concerning enemy and friendly forces has improved dramatically. When a military force with such capabilities is "networked" to the degree of Wal-Mart's business model, warfare approaches a point where Clausewitz's "fog of war" begins to dissipate. In this environment, militaries move away from estimate-based operations toward knowledge-based operations.

Based on its technological superiority, the U.S. military enjoys a significant advantage over most adversaries that chose to fight symmetrically. However, as the Toffler's observe, societies from all three "waves" exist simultaneously. Therefore, the U.S. military must be prepared to face adversaries that choose to fight asymmetrically. In his book, *Three Cups of Tea*: *One Man's Mission to Fight Terrorism and Build Nations… One School at a Time*, Greg Mortenson, the Director of the Central Asia Institute, described an encounter with suspected Taliban operatives equipped with high-powered binoculars and a satellite phone on an international flight from Afghanistan.

> Down there in the dark, …was the most technologically sophisticated navy strike force in the world, launching fighters and cruise missiles into Afghanistan. I didn't have much sympathy for the Taliban, and I didn't have any for Al Qaeda, but I had to admit that what they were doing was brilliant. Without satellites, without an air force, with even their primitive radar knocked out, they were ingenious enough to use plain old commercial flights to keep track of the Fifth Fleet's positions. I realized that if we were counting on our military technology alone to win the war on terror, we had a lot to learn.[13]

Even Agrarian Age societies can access and employ Information Age technologies such as cellular phones, computers, and the internet, further complicating the task of dealing with opponents that fight asymmetrically.

Another major challenge is gaining an "…understanding of the enemy's intentions, his motivation to fight, and the strength of his will – factors that matter most in war."[14] Determining enemy intent relies heavily on non-technological means like human intelligence (HUMINT) and detailed knowledge of foreign cultures. Achieving information superiority in this environment requires a wide range of capabilities some technological and some not. The IO Roadmap addresses this requirement by emphasizing the need to enhance IO capabilities across the U.S. military.

Key Aspects of the Information Operations Roadmap

Reviewing some key elements of the IO Roadmap establishes an understanding of how the DoD envisions the U.S. military's transition from Industrial Age estimate-based operations to Information Age knowledge-based operations. The IO Roadmap participants believed there were three areas important to making IO a core military capability. First, DoD is building a network-centric force and those networks will increasingly become an operational center of gravity that must be protected.[15] Second, DoD must improve its ability to conduct psychological operations (PSYOP).[16] Third, DoD must improve network and electromagnetic attack capability.[17] The participants also believed that if DoD aggressively implements the recommendations in the Roadmap it will benefit the Department and particularly the Combatant Commanders by providing a common understanding and approach to IO, delegating more authority for IO execution to the Combatant Commanders, creating a trained and educated IO career force, providing a centralized IO planning, integration, and analysis capability in U.S. Strategic Command (USSTRATCOM), and enhancing specific IO capabilities like PSYOP, network protection, electronic and network attack, and improved command and control.[18]

Developing a Common Understanding of Information Operations

Perhaps the most important role of the Roadmap is the establishment of a single, authoritative definition and framework for IO. This is immensely important as it forms the basis for the development of doctrine, organization, training, material, leadership and education, personnel and facilities (DOTMLPF) to support IO as a core military capability. The Roadmap recommended, and DoD later established in DOD Directive O-3600.01, the following definition of information operations.

> 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.[19]

As defined, the purpose of IO is to affect *adversary* decisionmaking in some manner while protecting one's own.

The Roadmap also provides a basic framework for the concept of IO. This framework establishes three broad functions of IO; disrupting the adversary's unity of command while preserving one's own, protecting one's own plans while misdirecting the adversary's, and controlling the adversary's communications and networks while protecting one's own. The framework further describes IO in terms of five core capabilities; electronic warfare (EW),

psychological operations (PSYOP), operational security (OPSEC), military deception (MILDEC), and computer network operations (CNO). Finally, the Roadmap identifies supporting capabilities such as; physical security, information assurance, and counter intelligence, and related activities such as; public affairs and civil military operations, that must be closely coordinated with and integrated to achieve effective information operations. The U.S. military has several years of experience in both conventional and asymmetric conflicts since adopting this definition and framework and it appears they might benefit from further refinement.

Enhancing IO Capabilities

In light of the U.S. military's increased reliance on computer networks, the IO Roadmap places appropriate emphasis on the enhancement of computer network operations (CNO) capabilities. Additionally, the proliferation of computers and computer networks means that both conventional militaries and asymmetric opponents, such as insurgents and terrorists, may use both public and private computer networks to support their operations. In this environment, the U.S. military's ability to achieve information superiority over adversaries relies heavily on its ability to protect its networks through computer network defense (CND) and also to attack an adversaries computer networks through computer network attack (CNA).

Electronic warfare (EW), another IO core capability, is essential to achieving information superiority in the contemporary operating environment. The Roadmap states that EW remains too focused on defensive activities such as electronic protection (EP) and suppression of enemy air defenses (SEAD). DoD's vision for EW is to develop a more robust offensive EW capability that will "…deny adversary situational awareness, disrupt command and control, and develop targeting solutions to defeat weapons while protecting [one's own] against the same."[20] This enhanced capability will be critical across the entire range of military operations from stability, security, transition, and reconstruction (SSTR) operations, to counterinsurgency, to major combat operations.

The Roadmap also recommends that DoD enhance and refocus PSYOP capability. This recommendation was based on the assessment that PSYOP forces lacked the ability to rapidly develop and disseminate high quality products targeted at diverse audiences, sufficient numbers of fully qualified and equipped personnel with diverse linguistic capability, and the ability to disseminate PSYOP products in denied areas. Recent experience in Operation Iraqi Freedom confirms that these capabilities are some of the most important for effective IO. DoD's goal is to create " [a] PSYOP force ready to conduct sophisticated target-audience analysis and

modify behavior with multi-media PSYOP campaigns featuring commercial-quality products that can be rapidly disseminated throughout the Combatant Commander's area of operations."[21]

Trained and Ready IO Career Force

A major challenge in moving IO from concept to capability is the development of a trained career force. The Roadmap participants assessed that the five core capabilities were not well understood across the Services. Further complicating matters, each Service tended to train their specialists based on service specific requirements each emphasizing elements that had the most impact in their particular medium. Developing a trained and educated IO career force is also difficult because of the growing complexity and rapid technological changes in specialty areas such as EW, PSYOP, and CNO.

The solution described in the Roadmap includes the development of a core cadre of professionals capable of planning and executing fully integrated IO. This cadre will consist of IO planners that come from the mainstream of each Service and IO specialists who are functional experts in one or more of the core IO capabilities; EW, CNO, or PSYOP. IO planners would serve in assignments that alternate between their basic branch and IO planning positions. Similarly, IO specialists would serve in assignments that alternate between their specialty areas and general IO planning positions.

Developing a robust training and education program for IO is another critical requirement for creating a trained and ready IO career field. The Roadmap asserts that programs of instruction for joint IO planners and specialists must be standardized. The Roadmap also emphasizes the need to develop a greater appreciation for IO in the general military population. This would be accomplished by standardizing the IO curriculum at intermediate level education (ILE) for majors, and at senior service college (SSC) for lieutenant colonels and colonels. The Roadmap also calls for DoD to coordinate across the Service schools to integrate IO training into early military education as well.

These concepts and recommendations made in the IO Roadmap establish a solid foundation for the process of moving IO from idea to operational capability. The U.S. military transformation is well underway, and developing IO as a core military capability continues to gain momentum. There seems to be little debate whether or not the U.S. military should pursue information operations as a core capability. However, there is still much debate among the Services, in the classrooms at Service Colleges, and at Military Training Centers about how best to plan and integrate IO into military operations. An examination of information operations

in some recent military operations provides some insight into U.S. military successes and challenges and leads to some recommended adjustments to the IO Roadmap.

Information Superiority in Recent Military Operations

"Information Warfare" in Operation Desert Storm

The term information operations had not been coined when the United States led a coalition in the 1991 war to eject Iraqi forces from Kuwait. Even so, Coalition Forces under command of General Norman Schwarzkopf, developed a campaign plan that foreshadowed current information operations doctrinal concepts. Key components of the strategy to defeat the Iraqi forces in Kuwait and restore Kuwaiti sovereignty relied on integrating four of the five core capabilities of today's information operations; operations security (OPSEC), military deception (MILDEC), psychological operations (PSYOP), and electronic warfare (EW).

Coalition success relied on OPSEC of the grandest scale. Essential to a successful flanking attack, the coalition surreptitiously moved the entire XVIIIth Airborne Corps from the vicinity of Dhahran, Saudi Arabia, to tactical assembly areas hundreds of miles to the west just prior to initiating ground combat operations. Another key element of Schwarzkopf's operational design were deception operations aimed at tying Iraqi forces to the defense of areas not essential to coalition success. Schwarzkopf positioned the 82nd Airborne Division near major airfields and retained the 4th and 5th Marine Expeditionary Brigades (MEB) afloat in the Persian Gulf to convince the Iraqi leadership there was a threat of both an airborne operation and an amphibious assault. Coalition forces also employed large scale psychological operations coupled with B-52 strikes on frontline units to undermine the will of individual soldiers and whole units to fight. Disruption of enemy command, control, communications, intelligence, surveillance, and reconnaissance (C4ISR) was also essential to gaining an informational advantage over the enemy. Upon gaining air superiority, coalition Air Forces, relying heavily on EW capabilities, systematically attacked key command and control (C2) nodes and infrastructure to degrade Iraqi leaders' ability to "see" what was in front of their forces; make decisions about the orientation of their forces; and command and control the withdrawal of those forces once the decision was made to quit Kuwait.

Using improved intelligence, surveillance, and reconnaissance (ISR) capabilities like the Joint Surveillance Target Attack and Radar System (JSTARS), space-based systems, precision guided weapons, and low-observable technology, coalition forces attacked throughout the depth of the Theater of Operations to isolate, and then defeat the Iraqi forces in Kuwait and Southern Iraq. Coalition forces attained their military objectives and created the conditions required for

terminating major combat after thirty-seven days of air combat operations and only one hundred hours of ground combat. This remarkable victory was achieved at a much smaller cost in manpower and material than experts predicted largely due to the coalition's ability to "blind" the enemy while maintaining its own ability to see the enemy and the environment. However, even though coalition forces enjoyed information superiority and used it to great advantage, the U.S. military had not yet parted with the Industrial Age approach of massive forces using "attrition-style warfare."

Information Operations in Operation Iraqi Freedom

As the prospect of a new war against Iraq grew throughout the early months of 2003, many "military analysts" were astonished that the United States was prepared to initiate war with Iraq, and "regime removal" was its military objective. More surprising was the prospect of achieving this much broader objective with only a fraction of the forces used to eject Iraqi forces from Kuwait in 1991. Many wondered if the degradation of Iraqi military capability through a decade of sanctions was sufficient to make such a ratio feasible. Actually, a combination of the degradation of Iraqi military strength, coupled with the U.S military's improved ability to gain information superiority based on advances in information technology, made this plausible.

The Coalition's advantages in sensors, precision guided weapons, and improved command and control systems like tactical internet, global positioning systems, and satellite communications, provided unprecedented information superiority over the adversary in a conventional fight. Increased certainty about the location, disposition, and status of both one's own forces as well as the enemy's gave commanders greater confidence in directing the actions of their forces and resulted in a dramatic increase in the tempo of operations. With only 183,000 ground forces at the outset of Operation Iraqi Freedom (OIF), a fraction of the forces available at the start of Desert Storm, the Coalition penetrated two hundred and fifty miles into enemy territory. In less than three weeks, a bold Coalition offensive reached the enemy capital, toppled the regime, and achieved the initial military objectives of the campaign. As Leonhard predicted, "knowledge-based" operations dramatically changed the way the U.S. military waged war and resulted in a significant increase in the tempo of operations. Similarly, the Toffler's predicted "reduction of inputs to destruction" in warfare was realized in OIF.

However, with the Iraqi military defeated and Saddam removed from power, the operational environment changed dramatically. The center of gravity in this new environment shifted from Saddam and his regime to the country's population. The Coalition's considerable advantages in major combat operations seemed to carry less significance in this new conflict

where a stubborn insurgency had taken root. In this conflict, the range of activities Coalition forces engage in, and the manner in which they apply military resources, changed drastically. The nature of the information required to accomplish its tasks differs from the information required to conduct operations against a conventional military force. Still, gathering that information and gaining information superiority over the adversary remain central to success. However, this superiority rests not on the ability to "see enemy formations" over the next ridge but to understand where, when, and how the adversary will attempt to influence the population to support their cause rather than that of the Iraqi Government and the Coalition.

One U.S. Brigade Commander responsible for an area of operations in Central Baghdad at the outset of SSTR operations noted, "… I quickly discovered that IO was going to be one of the two most vital tools (along with human intelligence) I would need to be successful in a counterinsurgency (COIN) campaign."[22] However, upon examination of this commander's information operations, it is clear the primary focus of the brigade's information operations was on influencing the behavior of the neutral population rather than adversary decisionmaking. This commander describes his concept for IO in the following way.

> Our overall target audience was clearly the silent majority. However, to reach them and to ensure that our messages and themes would resonate with them, we determined that we needed to use mainly Iraqi proxies to convey our messages. We therefore, identified five groups of Iraqis that had significant influence among the population: local imams and priests, local and district council members, staff and faculty from the universities, Arab and international media and local sheiks and tribal leaders.[23]

Consistent with the preponderance of tactical commanders and many operational commanders in OIF, this commander views PSYOP, civil military operations, and public affairs as the central efforts of information operations in COIN and SSTR operations. This highlights an inconsistency between the current definition of IO and how most commanders view IO. The current definition *does not include operations intended to influence the behavior or decisionmaking of foreign neutral or friendly populations*.

Furthermore, both the current definition and the framework described in the IO Roadmap cause many to view information operations as separate operations which must be synchronized and coordinated with the overall operations. In an effort to provide some theoretical underpinnings for IO, Colonel William Darley, the V Corps Public Affairs Officer during Operation Iraqi Freedom, wrote an article entitled *Clausewitz's Theory of War and Information Operations*. In it, he describes the relationship between IO and kinetic operations this way.

> IO and kinetic operations are inseparably linked, like strands of a DNA molecule in a gene, and in the same way have a dominant/recessive relationship (for

> example, one exercising dominance over the other depending on where the conflict falls on the continuum relative to the polar extremes).[24]

While this is a step in the right direction, it might be further improved by viewing IO as an integral part of all operations both kinetic and non-kinetic. Colonel Darley maintains that information operations are dominant at the lower end of a continuum of violence in "The Universe of Political Conflict" while "kinetic operations" are more dominant at the higher end of this spectrum. This is a common conclusion many make because they tend to equate IO core capabilities and supporting activities like psychological operations and civil military operations, which have become euphemistically known as "non-kinetic" operations, with information operations as a whole.

The contrast between the two I Marine Expeditionary Force (MEF) operations in 2004 to gain control of Fallujah, a key insurgent stronghold, provides important lessons about dominating the information environment and integrating information operations into operations. The first operation, Operation Vigilant Resolve, ended almost before it began when the "U.S. forces unilaterally halted combat operations after a few days due to lack of support from the Interim Iraqi Government and international pressures amid media focus on unsubstantiated enemy reports of collateral damage and excessive force."[25] According to LTG Metz, the Commander of Multinational Corps Iraq (MNCI),

> … the operation failed because operations in the information domain were not integrated into the battle plan… Steps to prepare the information battlefield, including engaging numerous and varied Iraqi leaders, removing enemy information centers, and rapidly disseminating information from the battlefield to worldwide media were not woven into the plan.[26]

I MEF had all of the required resources to dominate the enemy tactically and would certainly have succeeded if they had not been forced to unilaterally cease operations. Unfortunately, they failed to properly consider the information environment and the potential impacts that failing to dominate that portion of the operational environment would have on their operations.

The outcome of I MEF's second operation, Operation Al-Fajr, in November 2004, was significantly different. "A key task for the MNC-I planners was to ensure that the information defeat of Vigilant Resolve was not repeated in Operation Al-Fajr."[27] The success of the operation relied on OPSEC and MILDEC to conceal the build-up of forces north of Fallujah; effective PSYOP to encourage noncombatants to leave the city and insurgents to surrender; and electronic warfare to control the enemy's communication. Other keys to the success of the operation were the early seizure of Fallujah Hospital, the insurgent's propaganda facility, and a deliberate plan for forces to document evidence of insurgent atrocities and quickly share the

information with international media outlets. All of these actions were essential in the Coalition's effort to control the information environment and ultimately to accomplish its military objective of seizing control of Fallujah from the insurgents. Operation Al-Fajr was not really a case of information operations tightly woven into the operational plan. It was more a case of planners developing a comprehensive understanding of the operational environment, particularly the informational realm, and developing a plan to effectively employ *all* available capabilities to dominate the adversary across every part of the operational environment – informational included.

This review of information operations in recent military operations confirms that the U.S. military continues to progress toward making information operations a core military capability. This progress actually builds on initial successes in Desert Storm even before the current concept for IO was established by the IO Roadmap. Observations from Desert Storm and OIF I also demonstrate that the U.S. military has and continues to improve its significant advantage in information superiority when fighting symmetric wars against conventional militaries. Observations from later stages of OIF suggest that more effort is required to achieve the same advantages when fighting asymmetric warfare during counterinsurgency or SSTR operations.

Recommended Adjustments to the Information Operations Roadmap

The IO Roadmap is a good guide for expanding the U.S. military's information operations capability as a critical goal of transformation. The Roadmap places appropriate emphasis on developing a common understanding of IO across the military, enhancing key IO capabilities, and developing a trained IO career force. However, the process could be improved by making some adjustments to the Roadmap.

Developing a Common Understanding of IO

Based on observations of recent United States military operations it appears that the definition and framework require further refinement. The DoD should consider refining the definition that was promulgated by DoD Instruction O-3600.01. The review of recent operations indicates that most of the "information operations" executed in COIN and SSTR are largely focused on neutral-party behavior and decisionmaking. The current definition of IO is too narrowly focused on *adversary decisionmaking* and doesn't address operations and activities that most commanders, in practice, view as critical to success in COIN and SSTR operations – influencing and affecting foreign population behavior.

The analysis of the two Fallujah operations suggests another potential improvement to the definition and the framework for IO. Currently, the term IO is used to describe the

employment of several disparate capabilities (core and supporting) and related activities. The rationale for this, according to the IO Roadmap, is that "[l]ike all core competencies, information operations can not be successfully executed without diverse supporting capabilities."[28] Rather than focusing the definition on the capabilities and activities associated with IO, it may be more useful to define IO in terms of the information environment.

Joint Publication 1-02 defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[29] This might lead to an alternate definition for information operations such as;

> Operations conducted in the information environment to affect foreign populations, and adversary behavior and decisionmaking processes while protecting friendly decisionmaking.

This definition, while much broader, focuses on the medium in which information operations take place and the purpose of those operations, rather than a set of capabilities that may be employed. This change would cause commanders and staffs to view information operations more as a fundamental of operational design and the information environment as a dimension of the operational environment that must be analyzed and understood in the same way as other components of the operational environment such as the political, social, economic, and military systems.

This approach is consistent with the model described by LTG Metz when he highlighted the differences between the first and second battles for Fallujah in 2004. Additionally, for the United States military to gain an advantage over its competitors similar to Wal-Mart's advantage over its competitors, it should view information in much the same way that Wal-Mart does, as the central resource in the business. "Any military – like any company or corporation – has to perform at least four key functions with respect to knowledge. It must acquire, process, distribute, and protect information, while selectively denying or distributing it to its adversaries or allies."[30]

Wal-Mart leveraged the latest innovations in information technology to reengineer their business process across every element of the organization including; marketing, sales, and distribution. Fundamentally, the business units perform the same functions but in a vastly different manner, a manner that streamlines virtually every aspect of the company's core processes and functions. Similarly, using the IO Roadmap as the guide, DoD should focus the *entire* organization on information as fundamental to operations. This requires a revision of the roles, responsibilities, and capabilities of the existing functional elements of the force so they

best accomplish the four functions with respect to knowledge; acquire, process, distribute, and protect information.

Trained Career Force

Next to establishing a common understanding of IO, the Roadmap's second most significant contribution is building and maintaining a trained and educated IO career force. While on the surface it seems that an Information Age military has a distinct advantage over military or paramilitary forces of a first or second wave society, the differences between the Operation Vigilant Resolve and Operation Al Fajr indicate the importance of appropriate emphasis on the information component of warfare when designing and executing military operations on today's battlefield. The United States military must build a core cadre of personnel that are knowledgeable and experienced in planning and conducting integrated operations that fully consider the informational element of the operational environment and maximize the contributions of all the available resources and capabilities.

The Roadmap lays out a logical approach to this problem but DoD may need to adjust its emphasis on different aspects of this plan. First, DoD should place the greatest emphasis on training the general military population on the analysis of the information environment and the implications for each functional element of the force. The program of instruction for every level of professional military education must include appropriate instruction on information as a fundamental of operations and how it pertains to that particular military occupational specialty. Second, the services must enhance the proficiency and capability of what are currently called information operation specialists like electronic warfare, computer network attack, computer network defense, psychological operations, and other technical specialists. Third, the services should train *all* of their planners to be experts in planning operations which take all aspects of the information environment in to consideration. Integrating information operations should not be viewed as a "mystical task" whose secrets can only be carried out by an "IO wizard." Every commander, chief of operations, and chief of plans at every level must be completely conversant and adept at integrating information operations into the plans and operations.

This is somewhat different from the current approach of establishing a separate career force of Information Operations personnel that are responsible for planning and integrating IO into operations. The U.S military must not allow IO to become a "sideshow" rather than an essential part of the "main event." This will likely happen if Combatant Commanders and Joint Force Commanders maintain the approach of integrating the information component into operations by first separating out something that is fundamental to operations and crosses

every functional element of warfighting. This separation of an integral element of operations is accentuated when the services create a separate career force with functional responsibility for integrating a core capability into operations.

Improve PSYOP Capability

While it seems the U.S. military is far down the path in gaining a sustainable technical advantage over its adversaries which results in information superiority in conventional warfare, it does not appear the same is true for COIN and SSTR operations. The IO Roadmap identifies the requirement to improve the PSYOP capability in the U.S. military. Recent experience in Operation Iraqi Freedom indicates that psychological operations are extremely important in COIN and SSTR operations thus confirming this requirement. This capability is not well understood by the general military population. There is also a pervasive perception across the conventional force that IO is nothing more than the coordinated application of PSYOP, CMO, and PA. DoD should develop a program to educate the force on the proper integration of PSYOP into operations and clarify its role. All military planners, not just a special subset called IO planners, must understand the organization, capability, and principles of employment of PSYOP forces

Conclusion

Overall, the Information Operations Roadmap serves a very important purpose throughout DoD. The Roadmap provides a forcing function for leaders in every Service to move the process of transformation forward with respect to warfare in the Information Age. It correctly recognizes the increased advantage a military force gains over the adversary through the ability to “see first,” “decide first,” “act first,” and “act more effectively.” This advantage is equally important throughout the entire range of military operations from SSTR to major combat operations. The difference lies in the kind of information required, the methods and capabilities used to collect that information, and methods and capabilities used to affect decisionmaking and behavior.

The Roadmap forces the Services to move beyond concepts and experimentation to developing policy, doctrine, tactics, techniques, and procedures for integrating information and advances in information technology into military operations. There remains a wide range of opinions and understandings of what constitute information operations and how they should be integrated into operations. DoD should continue its emphasis on information superiority and the establishment of common understanding of IO across the DoD if the United States is to remain peerless in its ability to project and successfully employ the military as an element of national

power far into the 21st Century. However, it should consider some adjustments to the Roadmap in order for the United States military to successfully integrate the information component in operations and garner a significant and lasting advantage over its potential adversaries.

Endnotes

[1] U.S. Department of Defense, *Information Operations Roadmap*, redacted ver., (Washington, D.C.: U.S. Department of Defense, 30 October 2003), 2.

[2] Congressional Research Service Report for Congress, *Defense Transformation: Background and Oversight Issues for Congress*, (Washington, D.C.: The Library of Congress, Updated November 9, 2006).

[3] Ibid.

[4] Williamson Murray and Robert H. Scales, Jr., *The Iraq War*, (Cambridge, MA: The Belknap Press of Harvard University Press, 2003), 245.

[5] U.S. Department of Defense, *Information Operations*, Joint Publication 3-13, 13 February 2006, GL 9.

[6] Alvin Toffler and Heidi Toffler, *War and Anti-War: Surviving at the Dawn of the 21st Century*, (Boston: Little, Brown and Company, 1993), 33.

[7] Ibid., 58.

[8] Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-first Century*, (New York: Farrar, Straus and Giroux, 2005), 133.

[9] Toffler, 67.

[10] U.S. Army Training and Doctrine Command, Change 3 to TRADOC Pam 525-3-90, *Operational and Organizational Plan for the Future Combat Systems Brigade Combat Team* (Ft Knox, KY: Unit of Action Maneuver Battle Lab, 16 December, 2005), 4-4.

[11] Robert R. Leonhard, *The Principles of War for the Information Age*, 2nd ed. (Novato, CA: Presidio Press, 2000), 19.

[12] Ibid., 18.

[13] Greg Mortenson and David Oliver Relin, *Three Cups of Tea: One Man's Mission to Fight Terrorism and Build Nations … One School at a Time*, (New York, NY: Viking Penguin, 2006), 274.

[14] Murray and Scales, 240.

[15] U.S. Department of Defense, *Information Operations Roadmap*, redacted ver., 6.

[16] Ibid.

[17] Ibid.

[18] Ibid., 7.

[19] Ibid., 22.

[20] Ibid., 60.

[21] Ibid., 63.

[22] Ralph O. Baker, “The Decisive Weapon: A Brigade Combat Team Commander’s Perspective on Information Operations,” *Military Review* (May-Jun 2006): 13.

[23] Ibid., 21.

[24] William M. Darley, “Clausewitz’s Theory of War and Information Operations,” *Joint Force Quarterly*, issue 40, (1st Quarter 2006): 79.

[25] Thomas F. Metz et al., Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations,” *Military Review* (May-June 2006): 5.

[26] Ibid.

[27] Ibid., 6.

[28] U.S. Department of Defense, *Information Operations Roadmap*, 23.

[29] U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, amended 1 March 2007, 259.

[30] Toffler, 141-2.