

*United States Marine Corps  
School of Advanced Warfighting  
Marine Corps University  
2076 South Street  
Marine Corps Combat Development Command  
Quantico, Virginia 22134-5068*

# **FUTURE WAR PAPER**

## ***THE FUTURE OF INFORMATION OPERATIONS IN THE UNITED STATES ARMY***

SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS FOR THE DEGREE OF MASTER  
OF OPERATIONAL STUDIES

**Major Walter E. Richter, US Army**

AY 2006-07

Mentor: Col J.E. Driscoll, USMC

Approved: \_\_\_\_\_

Date: \_\_\_\_\_

# 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 <b>2007</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2007 to 00-00-2007</b>	
4. TITLE AND SUBTITLE <b>The Future of Information Operations in the United States Army</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>United States Marine Corps, School of Advanced Warfighting, Marine Corps University, 2076 South Street, Marine Corps Combat Development Command, Quantico, VA, 22134-5068</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
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 <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

## **DISCLAIMER**

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

## ABSTRACT

**Title:** The Future of Information Operations in the US Army.

**Author:** Major Walter E. Richter, United States Army

**Thesis:** The Army's current definition and core capabilities of Information Operations are inadequate to support a national Strategic Communication capability, counter emerging threats to national security, and meet National Defense objectives over the next fifteen years.

**Discussion:** The visibility and significance of Information Operations (IO) and Strategic Communication within United States' national policy has significantly increased in recent years, receiving repeated emphasis in both the National Defense and National Security Strategies. In response to this, the Department of Defense (DOD) has published *Joint Publication 3-13, Information Operations* (13 February 2006), stating that DOD informational efforts must be part of a robust Strategic Communication capability that supports governmental activities to understand, inform, and influence relevant foreign audiences.<sup>i</sup> Within combatant commands, IO then supports national Strategic Communication in order to ensure a unity of themes and messages; emphasize success; accurately confirm or refute civilian reporting of US operations; and reinforce the legitimacy of US goals in the international community.<sup>ii</sup>

### **Recommendations:**

In future operations a reassessment of IO core capabilities should be:

- Public Affairs
- PSYOP
- Combat Camera
- Civil Military Operations

While this may seem a radical departure for some, this actually represents an institutional acknowledgement of what is already reality on the ground for military operations.

---

<sup>i</sup> *JP 3-13, Information Operations*, (US Joint Publication: 13 February 2006): I-10.

<sup>ii</sup> Richard Myers, Gen., USAF, *National Military Strategy: A Strategy for Today; A Vision for Tomorrow*, (Washington DC, 2004): 12.

## ACKNOWLEDGEMENT

As with any military endeavor, this paper represents the contributions and assistance of many people. I would first like to thank my wife, whose enormous support throughout my research for this study, while raising a family and facing the challenges of back-to-back changes of station, allowed me to concentrate on my studies.

These past years have provided me with a wealth of information and appreciation for the challenges and potential of joint and multinational military cooperation. Many professionals have taken considerable amounts of time to aid me in my research and analysis. Tremendous thanks go to Colonel Jerome E. Driscoll and Dr. Gordon W. Rudd for their personal mentorship and for providing me this year to develop my abilities further as a planner and designer while working with some of the brightest minds from the United States Marine Corps, Air Force, United States Army and National Guard. In addition to the outstanding support that I have received from the Marines at Quantico, I must acknowledge the support that I have received from Lieutenant Colonel Charles Eassa and Mr. Paul Tiberi at the United States Army Information Operations proponent at Fort Leavenworth, Kansas, and whose intellectual guidance and mentorship provided the impetus for this paper.

# TABLE OF CONTENTS

	<u>Page</u>
DISCLAIMER.....	ii
ABSTRACT .....	iii
ACKNOWLEDGEMENT .....	iv
TABLE OF CONTENTS .....	v
LIST OF FIGURES .....	vi
THE FUTURE OF INFORMATION OPERATIONS IN THE UNITED STATES ARMY .....	1
INTRODUCTION:.....	1
THE SETTING:.....	2
CONSEQUENCES OF RECENT MILITARY OPERATIONS .....	4
THE BALKANS .....	5
AFGHANISTAN .....	8
IRAQ.....	11
PROPOSED CHANGES .....	14
PUBLIC AFFAIRS VERSES INFORMATION OPERATIONS .....	16
NEW INFORMATION OPERATIONS CONCEPTS .....	17
IO AS MARKETING .....	17
CULTURAL ANTHROPOLOGY .....	18
CHANGE IN DEFINITION .....	19
REASSESSMENT OF CORE CAPABILITIES .....	19
CONCLUSION – IMPLICATIONS FOR FUTURE OPERATIONS.....	20
GLOSSARY .....	24
BIBLIOGRAPHY .....	26

## LIST OF FIGURES

	<u>Page</u>
FIGURE 1 - OLD INFORMATION ENVIRONMENTS .....	14
FIGURE 2 - NEW INFORMATION ENVIRONMENTS.....	15

# **The Future of Information Operations in the United States Army**

## **Introduction:**

The visibility and significance of Information Operations (IO) and Strategic Communication within United States' national policy has significantly increased in recent years, receiving repeated emphasis in both the National Defense and National Security Strategies. In response to this, the Department of Defense (DOD) has published *Joint Publication 3-13, Information Operations (13 February 2006)*, stating that DOD informational efforts must be part of a robust Strategic Communication capability that supports governmental activities to understand, inform, and influence relevant foreign audiences.<sup>iii</sup> Within combatant commands, IO then supports national Strategic Communication in order to ensure a unity of themes and messages; emphasize success; accurately confirm or refute civilian reporting of US operations; and reinforce the legitimacy of US goals in the international community.<sup>iv</sup>

Consequently, the Army is currently revising its *Field Manual 3-13, Information Operations*, further refining the November 2003 edition. Yet, despite IO's recent prominence in national strategies, proposed doctrinal changes are evolutionary rather than revolutionary. They frequently do not reflect commanders' operational experiences and appear reminiscent of a Cold War era threat model. Moreover, the Army's current definition and core capabilities of Information Operations are inadequate to support a national Strategic Communication capability, counter emerging threats to national security, and meet National Defense objectives over the next fifteen years.

## **The Setting:**

Throughout the United States' government, intelligence, and even military communities, the concept of Information Operations as a tool of manipulation has gradually diminished. Instead, IO increasingly seeks to influence attitudes and actions within an area of interest by empowering target audiences with informational tools and access to truthful information. Ideally, this process has the possibility of replacing violence.<sup>v</sup>

The Army has taken a more pragmatic view of IO, focusing on how information can best support leaders in both “kinetic and non-kinetic” operations. This study will evaluate the current five core capabilities of Information Operations. These core capabilities are: Psychological Operations (PSYOP), Electronic Warfare (EW), Computer Network Operations (CNO), Military Deception (MILDEC), and Operational Security (OPSEC), as well as the related activities of Public Affairs (PA) and Civil Military Operations (CMO).

Kinetic is defined as an adjective “relating to the motion of material bodies and the forces and energy associated therewith.”<sup>vi</sup> In military usage, kinetic operations involve the application of force in order to achieve a direct effect, such as artillery, infantry, aviation, and armored offensive and defensive operations. Non-kinetic operations are those operations that seek to influence a target audience through electronic or print media, Computer Network Operations, Electronic Warfare, or the targeted administration of humanitarian assistance. It is important to note that many operations will not fall neatly into one category or the other. For example, a security patrol may have the power to apply force (a kinetic operation), but over time their consistently

professional conduct earns the respect of the local populace and is a non-kinetic effect if not a complete operation in and of itself.

Both *JP 3-13* and *FM 3-13* define IO as “the integrated employment of the core capabilities... in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting [friendly] core capabilities.” Here, the difference between kinetic and non-kinetic operations becomes ambiguous. The benefit of this ambiguity is that commanders have the flexibility to concentrate IO on both kinetic and non-kinetic operations. For example, a commander may direct artillery strikes at information nodes and attack command and control through computer network attack, utilizing deceptive tactics that incorporate both electronic and conventional measures to safeguard friendly command and control. Conversely, a commander may direct IO planning efforts toward non-kinetic operations to provide a cultural-anthropological understanding of local leaders as well as public attitudes toward friendly forces and then incorporate that knowledge into kinetic operations.

While commanders must always retain the initiative to incorporate both kinetic and non-kinetic assets to establish information superiority, is it an effective allocation of assets for the IO cell to coordinate such divergent activities, while G3 operations already direct their actions toward many of the same areas? In order to ensure that future commanders do not lose information superiority against enemies unbound by ethics or the truth, it will become necessary for Information Operation officers to develop as resident experts with unique skills in public information, marketing, and cultural anthropology.

## Consequences of Recent Military Operations

Current Army Information Operations doctrine emerged from the 1996 *FM 100-6*, *Information Operations*, which divided IO into five core capabilities (Psychological Operations (PSYOP), Computer Network Operations (CNO), Military Deception (MILDEC), Electronic Warfare (EW), and Operational Security (OPSEC)) that supported the physical destruction of an enemy. Information Operations sought to enhance commanders' ability to ensure the security of friendly information systems and synchronize the application of force throughout hierarchical and nonhierarchical systems, linking sensors, shooters, and commanders while degrading, disrupting, or exploiting the enemy's command and control. While acknowledging the criticality of adapting to the changing information environment, doctrine remained focused, almost exclusively, on defeating a conventional military enemy through support of kinetic operations.

To be fair, the 1996 *FM 100-6* did acknowledge the need to conduct IO across the full spectrum of military operations. Nonetheless, the previous decade's attention to Soviet threat capabilities and the subsequent Gulf War in 1991 against a conventional Soviet-modeled force likely constrained American military thought. Despite the then recent December 1995 Dayton Peace Accords, in response to the ethnic conflict in the former Yugoslavia, *FM 100-6* failed to consider the rise of non-state actors or the emergence of military operations no longer limited to an enemy's physical destruction. Now, rather than only denying, defeating or destroying an enemy, American military leaders worked to create stable and secure environments, promoting the rule of law and respect for human rights among Bosnia's three major ethnic groups.

## The Balkans

Information Operations, as an institutionalized art, showed its potential during NATO-led operations in the former Yugoslavia as US military leaders responded to manipulation of the media by Bosnian, Serb, and Croatian political leaders who were igniting latent ethnic hatreds.<sup>vii</sup> Originally, the Serbs used the government-controlled media to target just its own citizens, rather than the international community with its distorted messages. Governmental leaders sowed fear and paranoia in Bosnian-Serbs, who in-turn developed a violent hatred of Bosniac and Croat ethnicities within Yugoslavia, further convincing the Serbs that they were indeed struggling for their survival as a people. While these messages were highly effective among the Serbs, they found little resonance elsewhere.<sup>viii</sup>

Conversely, Bosnian Muslim (Bosniac) leaders initially had little in the way of media assets. However, since nearly all of the international press correspondents in the former Yugoslavia resided in Sarajevo, a city besieged by Serbs, journalists shared the same hardships as the predominantly Bosniac Sarajevans. As a result, many international reporters gradually succumbed to the Stockholm Syndrome, and being aware of only Bosniac suffering at the hands of the Serbs, the perception of Bosniacs as hapless victims rapidly spread worldwide.<sup>ix</sup>

Following the United States deployment within the Dayton Accord Implementation Force (IFOR) in December 1995 and the publication of *FM 100-6* in 1996, US commanders soon found that IO doctrine failed to recognize adequately the effect of public information (PI) on local populations. PI, in the form of local and international news media, as well as the growing online community, held tremendous

influence among the population that IFOR was attempting to stabilize. Given IFOR's mission to enforce the Dayton Peace Accords and PI's predominance on the populace, it became virtually impossible to separate Public Affairs (PA) completely from IO.<sup>x</sup> With assistance from the Land Information Warfare Agency (LIWA), leaders from the First Armored Division and later the First Infantry Division established an IO council designed to bring together key players for information dissemination from PA, G3, PSYOP, and Civil Affairs.<sup>xi</sup> Both Civil Affairs/ Civil Military Operations and PSYOP played a prominent role in this, acting as an interface between military and civilian organizations, conducting such activities as warning populations about a rabies outbreak, or educating them about the dangers of land mines.<sup>xii</sup>

By obtaining input from the Information Operations council and presenting truthful information to the populace, the multinational division countered enemy propaganda that the local media disseminated. IO was active throughout the planning process, firstly identifying target pressure points of local leaders, secondly identifying objectives for each target, and thirdly preparing IO input for the division synchronization matrix. In order to then convey the division's message to the Bosnian public, the IO council coordinated PSYOP radio messages with military press releases<sup>xiii</sup> in order to avoid conflicting messages or "information fratricide." While information fratricide commonly refers to incidents involving casualties due to conflicts between friendly communication systems, it can also concern PI that compromises OPSEC or the local credibility of a unit's leaders and soldiers. Throughout operations in the Balkans, Combat Camera also emerged as a powerful information tool, documenting activities and events for exploitation by Public Affairs or PSYOP. Additionally, Combat Camera supported

commanders during contentious operations such as cordons and searches as a means to counter enemy propaganda rapidly.<sup>xiv</sup>

Despite these experiences, the ethicality of PA and IO integration remains a contentious debate with military officials firmly entrenched on both sides of the issue. Colonel William M. Darley, a US Army Public Affairs officer, stated in a recent article that “the practical military value of Public Affairs to the operator is neither tactical nor operational, nor is it easily quantifiable. It is strategic, a concept that is difficult to perceive or stomach when one is locked into personal and savage combat at trench-knife level.”<sup>xv</sup> In short, PA service to the Army is an institution with its own code of conduct that supercedes any one command or mission. In contrast to Colonel Darley’s position, Major Todd Sholtis, a US Air Force Public Affairs officer states that while credibility is an unambiguous and inflexible standard of professional conduct, it is neither a center of gravity nor an objective in and of itself.<sup>xvi</sup> Rather, the role of PA is to support the command and its mission through accurate and timely reporting, detailed media analysis, media training and talking points for soldiers throughout all levels of the command.

This integration of public information with IO developed more refinement in the war against Serbia and subsequent stability and support operations in Kosovo. Following a bombing campaign against the Serbian Capital, attention centered on a refugee convoy that USAF F16s mistakenly targeted. Reluctance by the command to confront the issue openly further fueled local media speculation. Furthermore, the lack of a common PA theme among commanders led to conflicting statements by NATO leaders that Serbs were responsible for the attack. Later statements were that NATO had indeed fired on the convoy, but only targeted military vehicles. Following a week without a clear military

message, NATO belatedly acknowledged through a press release that it had mistakenly targeted humanitarian vehicles. This honest assessment of issues leading to the attack did much to quell the issue, but the initial lack of a coherent response had seriously damaged the credibility of peacekeeping forces in Kosovo.<sup>xvii</sup>

Published accounts of commanders in the Balkans repeatedly emphasize the criticality of information dominance. While one cannot ignore the role of technology, these lessons are squarely centered on the human dimension and the need to develop an understanding of social and cultural structures through communication, both formal and informal. The irony is that the Army has yet to adjust its doctrinal IO core capabilities, especially the incorporation of PA and CMO into IO.

### Afghanistan

Operations in Afghanistan further demonstrated the need to integrate Public Affairs and Civil Military Operations into Information Operations. In response to the terrorist attacks of 11 September 2001 against the World Trade Center and the Pentagon, the United States initiated military actions in Afghanistan under the name, Operation Enduring Freedom (OEF). Early operations utilized land-based B-1, B-2 and B-52 bombers in addition to carrier-based F-14 and F/A-18 fighters and Tomahawk cruise missiles launched into Afghanistan from both U.S. and British ships and submarines. Special Operations Forces provided ground coordination and worked closely with local Afghan militias opposed to the Taliban regime.<sup>xviii</sup> Initial military objectives were the destruction of terrorist training camps and infrastructure within Afghanistan, the capture of Al Qaeda leaders, and the cessation of terrorist activities in Afghanistan.<sup>xix</sup>

EW predominated these early IO efforts, targeting enemy communication and air-defense-artillery (ADA) assets. Psychological or influence operations were limited to convincing enemy combatants to surrender. Only later did commanders work to convince Afghans that attacks on Taliban fighters were not attacks on the Afghan populace; thus laying the groundwork for a democratic Afghan government opposed to terror and respectful of human rights. Lastly, influence operations had the objective to convince world audiences that despite violent attacks on the Taliban and Al Qaeda, the coalition was doing everything possible to minimize the loss of life and property of Afghan civilians.<sup>xx</sup>

While these initial kinetic operations were successful, due in no small part to the coalition's overwhelming military strength, they did not fully address larger cultural issues essential to stable democracy in Afghanistan. The tendency of commanders to place IO almost exclusively in support of kinetic operations is understandable, since gauging the success of an influence operation promoting a democratic government is inherently more complex than tallying a battle damage assessment following an air strike. Not surprisingly, IO lacked the doctrinal structure to address these issues. It had remained fixated on physical systems and not understanding the operational significance of Afghan culture, thus limiting the coalition's ability to influence it. In short, the exclusive use of IO to support short-range kinetic objectives is redundant at best, and it ultimately fails to support a commander's long-range objectives.

The skills necessary for influence operations supporting the creation of a stable government are markedly different than those needed to destroy a combatant's information capabilities. Moreover, IO planners must ensure that stability will endure

long after coalition forces have left. In preparation for OEF, military planners either overlooked long-term informational consequences, or became subsumed by the immediacy of their kinetic operations, giving insufficient attention to the mission's message and its effect on long term objectives.

In order for an IO theme to be successful, it must fulfill three criteria. It must first recast the perception of the enemy, both locally and internationally, from that of a freedom fighter or even a rebel, to an illegitimate militant force or something that the local culture finds unacceptable. Secondly, it must recast the perceived nature of conflict, both nationally and internationally so that coalition forces are seen as liberators and not a conquering army. Finally, IO must have the ability to recast the ultimate goals of the operation, as conditions on the ground fit or do not fit planning expectations.<sup>xxi</sup> In all this, it is critical when confronting numerous threats across vastly different cultures that planners recognize that one solution will not fit every situation. In other words, a particular projected image of an effective military may be acceptable to one society and wholly unacceptable to another.

The recent resurgence in militant and criminal activity by the Taliban may very well be due to IO planning oversights, such as eradicating poppy production without providing poppy farmers profitable alternatives. Nonetheless, prior to this resurgence, IO underwent refinements in planning and execution to include the interaction of Civil Affairs units and PSYOP, as well as increased interagency integration. PSYOP provided support to the Interim Afghan Administration as well as humanitarian de-mining operations. Additionally, CA soldiers coordinated with Non-Governmental Organizations as part of the State Department's Overseas Humanitarian Disaster and Civic Aid

(OHDACA) program. This highlighted the ability of Civil Military Operations to influence the populace and demonstrated the need for a fully equipped Civil Military Operations Center (CMOC), capable of entering a theater with little logistical support from theater level special operations forces.<sup>xxii</sup> The potential of this integration is not “winning hearts and minds,” but rather building relationships of mutual trust and respect based on an understanding of the long-term benefits of cooperating with coalition forces.<sup>xxiii</sup>

### Iraq

In early 2003, the United States prepared to lead an international coalition to oust the regime of Saddam Hussein. As forces invaded Iraq and the Baathist leadership fled, military leaders had leveraged Information Operations overwhelmingly in support of kinetic operations. While initially successful, IO did not support the establishment of a stable environment or lasting peace. Technologically oriented IO planners had concentrated efforts on tracking computer networks and integrating EW and CNO into division operations rather than understanding regional social and cultural dynamics and their consequences for coalition operations.

Potentially as a result of this near exclusive IO emphasis on technology, commanders soon found themselves struggling to understand social structures, ethnic and tribal divisions, as well as historical factors that fed into the emerging intra-Iraqi conflict.<sup>xxiv</sup> Practices such as occupying former Baathist party palaces and infrequently mingling with the local populace<sup>xxv</sup> may have prevented Iraqis from seeing coalition forces as anything more than a follow-on regime to the Baathists. Inexperienced soldiers frequently found themselves in dangerous situations where enemies were hard to identify,

leading some to “humiliate the men, offend the women, and alienate the very people who are supposed to be providing [the coalition] intelligence about terrorists and Baathists.”<sup>xxvi</sup>

Fortunately, IO has received every increasing consideration as the conflict has progressed. Commanders, who by their own admission originally saw IO as no more than a distraction, soon sought to understand the ethnically diverse sectors that they controlled. As commanders have further developed their own understanding of IO, they have also created organizations at the brigade, division, and corps level that endeavor to address the human dimension of the conflict. Colonel Ralph O. Baker, a brigade commander in Iraq discovered, as did previous commanders in the Balkans and Afghanistan, the operational significance of public information and the subsequent need for PA and IO integration. He realized that press releases, whether Iraqi or international have immediate effects on popular attitudes and can counter enemy propaganda. To assist Colonel Baker’s IO planning, PA provided him with media analysis on popular perceptions in sector.<sup>xxvii</sup> Additionally, humanitarian assistance coordinated through CA teams in conjunction with the brigade’s own medical, engineer, and maneuver units helped establish relationships of “trust and respect” among community leaders and members.

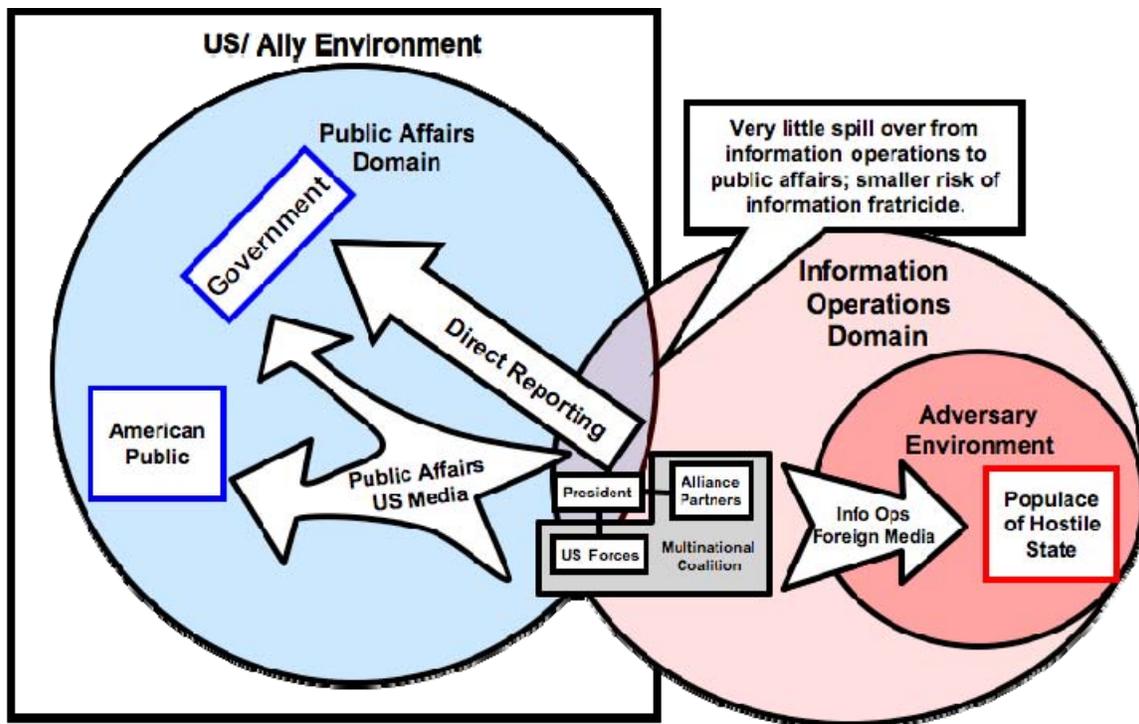
While the integration of IO and PA remains a contentious issue, leaders at the most senior levels of the military have acknowledged the need for it. Joseph Collins, a former Deputy Assistant Secretary of Defense for Stability Operations in Bush’s administration stated the need for improvement in Strategic Communication on Iraq, stating that if they do not improve, we will fail. He went on to add “We are not achieving synergy and mass in our Strategic Communication (consisting of IO, PI, diplomacy (both

public and military).<sup>xxviii</sup> Finally, Lieutenant General Thomas Metz, after a tour as III Corps commander in Iraq, declared that the Army needed a “broader and more aggressive, comprehensive, and holistic approach to IO – an approach that recognizes the challenges of the global information environment and seamlessly integrates the functions of traditional IO and PA.”<sup>xxix</sup>

In these after action reviews, the need for leaders to understand complex social networks, and not just computer or electronic networks is a constant theme. While mediums such as radio, television, and the Internet are invaluable in delivering messages, the need for greater understanding is in creating those messages that will find cultural and social resonance among target audiences.

## Proposed Changes

In discussing changes, it is helpful to consider how the flow of information has evolved and changed. Figure 1 below demonstrates how the United States traditionally viewed the flow of information in and out of theater, to and from the military to the US government, the American public, and a foreign audience. It is important to note that while information flow has become more complex and erratic, it was never simplistic or entirely precise in nature.

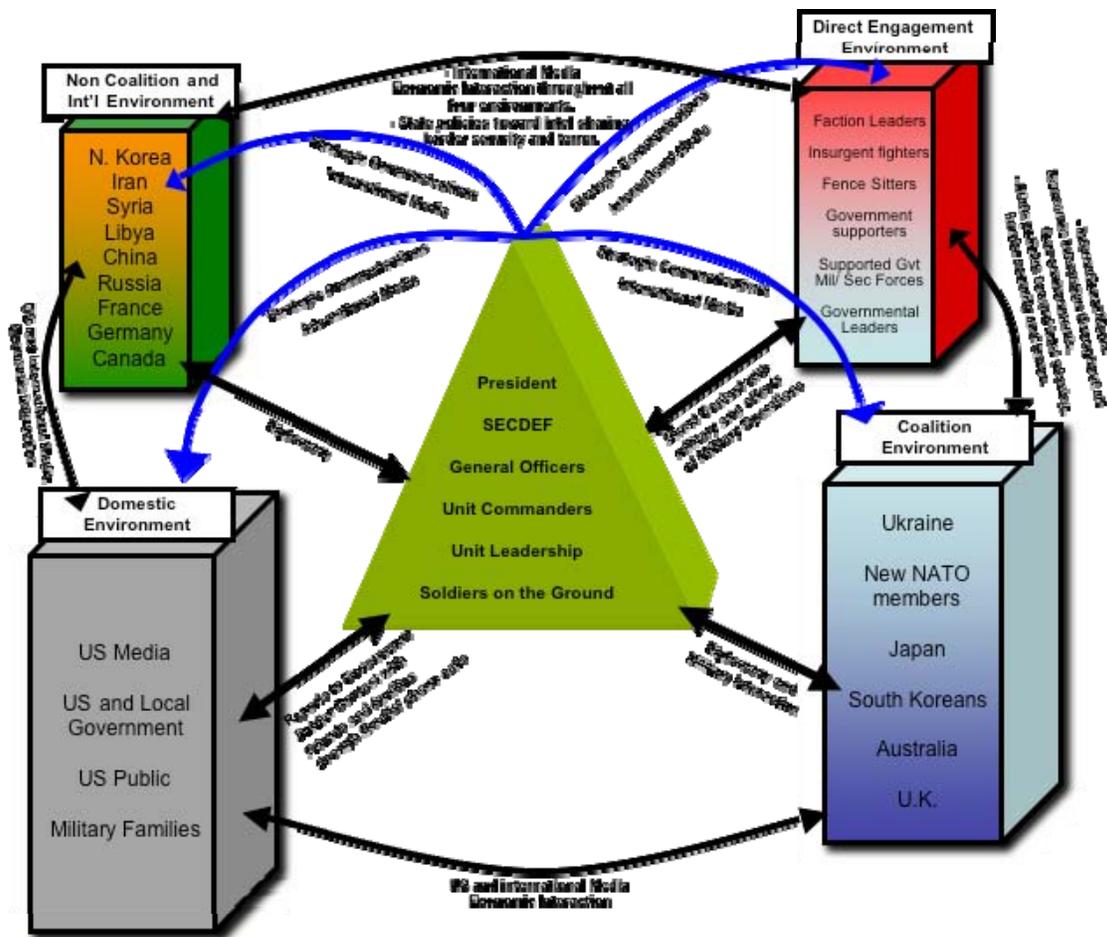


**Figure 1 - Old Information Environments**

As technology has allowed a faster and unregulated exchange of information, the domains of Public Affairs and Information Operations have become virtually indistinguishable. Whereas IO previously remained predominantly in an “adversary environment” and PA in a “US/ ally environment”, information now readily flows across four different environments, which are: the “direct engagement environment”; the

“domestic environment”; the “allied environment” and the “non-coalition/ international environment”. While each environment has its own characteristics, IO can no longer consider these environments as simply friend or foe. Within each environment, there are varying degrees of trust and commonality with or in opposition to US goals and objectives. The most significant difference between these environments is how the same information will have vastly different effects from one environment to the next.

**Figure 2 - New Information Environments**



In analyzing the emergent effects of the New Information Environments (depicted in Figure 2), it may be tempting to concentrate exclusively on the technology that is transmitting the data. However, based on observations of commanders, controlling or

stopping information flow is virtually impossible. The value of IO lays not in the technology that transmits information, but rather in understanding and eventually influencing how that information affects each environment. Moreover, in response to any concerns of IO not providing support to technical capabilities, expertise resident in the G6 has the ability to provide far more comprehensive support than IO. More importantly, the incorporation of these assets into G2 for collection and G3 for offensive electronic measures would allow IO to concentrate on influence operations.

#### Public Affairs versus Information Operations

Throughout numerous after action reviews by military leaders, the integration of PA and IO is a continual theme. Recent incidents regarding the Lincoln Group's placement of positive stories in Iraqi newspapers<sup>xxx</sup> demonstrated how readily information now crosses environments and raised concerns over the prospect of IO controlling PA. The issue here was that the stories, while factual, were deceitful in that they concealed their source and appeared to reflect the interests of the editorial staff of an Iraqi newspaper.<sup>xxxi</sup>

Stories, such as these, undermine the credibility of any positive coverage the military receives. Proper coordination of PA with IO never deceives the populace as to the origin of the information that they are receiving. Rather, this coordination ensures that press releases: do counter enemy propaganda; do not violate OPSEC; and minimize information fratricide. In time, if commanders are consistent in their press releases and avoid information fratricide, they may have greater success establishing trust and respect with the populace. Additionally, PA should provide units media analysis and media

training, enabling commanders, soldiers and staffs to engage the media effectively, further establishing and maintaining credibility.

### New Information Operations Concepts

Beyond PA integration, how can IO further enhance influence capabilities of a supported command? Persistence of current conditions in future operations could provide the Army with the incentive to provide extensive training and graduate schooling to IO officers in the studies of both marketing and cultural anthropology.

### IO as Marketing

Marketing tools and concepts could generate support for coalition military operations just as an advertiser promoting a commercial product. Similar to commercial products, local support for coalition operations has costs and benefits. Benefits for citizens supporting coalition operations may be the receipt of humanitarian assistance, as well as stability and security for their areas. Costs could be the loss of black market wealth and possibly the appearance of collaboration, placing lives of coalition supporters and their families in peril. While applying commercial concepts to military operations may appear unorthodox, this construct could help IO planners present commanders with a clear cost benefit analysis of the conditions that commanders are influencing the local populace to accept.<sup>xxxii</sup>

While it is difficult to predict future areas of operation for the US military, the advanced application of marketing tools to leverage humanitarian assistance and public affairs within an Information Operations plan targeting a global audience has tremendous possibilities.

## Cultural Anthropology

In conjunction with marketing, the study of cultural anthropology seeks to understand motivations and desires of actors within the context of a foreign culture and society. Cultural anthropology is defined as the “scientific study of human culture based on archaeological, ethnological, ethnographic, linguistic, social, and psychological data and methods of analysis.”<sup>xxxiii</sup> It is a social science discipline, traditionally focused on non-western, tribal societies; many of which we are now confronting in our current operations. Anthropological methodologies include participant observation, fieldwork, and historical research and endeavor to understand societies from their own perspective, rather than personal experiences, beliefs, and values.<sup>xxxiv</sup>

Within the military, a primary task of cultural anthropology would be translating knowledge gained from operational knowledge into doctrine, an obvious benefit for military leaders seeking to understand and even predict behavior in non-western societies. Despite such benefits, there has been little movement to incorporate anthropology into military leader training.<sup>xxxv</sup> In military terms, understanding cultural anthropology is an important step toward enabling better human intelligence. Understanding cultures through training, increased interaction with the local population during operations, and ideally living amongst them may help local civilians understand a unit’s values and the importance of its mission for the area’s welfare. While there is an inherent security risk in this, increased public access may create commonality between both military units and local populaces.

For future operations, soldiers will require a greater appreciation of the culture in which they operate. Knowledge about customs and courtesies is valuable, but only a

beginning. Leaders, planners, and soldiers must understand how a culture will affect operations. Forcing IO officers to understand human, rather than technical aspects of information environments, will better enable IO to leverage influence and provide combat leaders, planners, and soldiers the tools necessary for future deployments.

#### Change in definition

The current definition of IO listed in the November 2003 FM 3-13 is:

*The 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 affect or defend information and information systems, and to influence decision making.*

The US Army recently approved an updated definition that replaces the previous purpose "... to affect..." with an expanded one that reads:

*... to influence, disrupt, corrupt or usurp adversarial human and automated decision making, while protecting our own. It includes the use of these capabilities to influence the perceptions of foreign friendly and neutral audiences.*

#### Reassessment of core capabilities

While this revised purpose acknowledges the ramifications of incorporating IO into planning, it does nothing to reassess its core capabilities, and may give commanders, who have only used IO in support of kinetic operations, the false impression that technology remains the key to information dominance. On the contrary, capabilities that have historically been associated with successful IO are: Public Affairs, PSYOP, Combat Camera, and Civil Affairs/ Civil Military Operations.

If current trends persist, operations seeking only the destruction of an enemy, an objective, or a capability will occur with decreasing frequency, while those enabling a foreign security force or empowering a local civil administration will become

increasingly frequent. Beyond accomplishing complex missions, the ability to project successful accomplishments, either locally, internationally, or both, may well determine overall mission success.

A reassessment of IO core capabilities that can effectively address future operations should be:

- Public Affairs
- PSYOP
- Combat Camera
- Civil Military Operations

Current IO core capabilities of OPSEC and MILDEC would fall under G3 operations, while EW and CNO would fall under the G6 for support, under the G2 for collection of intelligence, and the G3 for offensive electronic measures. While this may seem a radical departure for some, it represents an institutional acknowledgement of what is already reality on the ground for military operations.

### **Conclusion – Implications for Future Operations**

As the US National Security Strategy calls for a “future force that will provide tailored deterrence of both state and non-state threats (including WMD employment, terrorist attacks in the physical and information domains, and opportunistic aggression) while assuring allies and dissuading potential competitors,”<sup>xxxvi</sup> the lines between information environments will continue to blur. It is distressing that lessons have repeatedly presented themselves during operations in the Balkans, Afghanistan, and Iraq, with little change to the doctrine. Given the Army’s continual self-assessment and published reports, commanders in Afghanistan and Iraq must have been aware of the

challenges faced in Balkan operations. The reluctance to modify doctrine may have been an unwillingness to accept the risk of diverting limited assets and personnel from the initial mission of destroying the enemy. However, a more likely explanation was that planners viewed lessons learned from a declared peacekeeping mission invalid during a high intensity conflict.

In order for Information Operations to address these threats adequately and support a national Strategic Communication capability, the Army must ensure that its IO officers have both the skills and assets necessary to provide commanders with an in-depth understanding of cultural and societal factors within any given environment. IO officers must further assess how those factors will affect operations, further enabling commanders to influence local populaces, establish relationships of trust and respect, and ultimately create legacies of stability and security.

---

<sup>iii</sup> *JP 3-13, Information Operations*, (US Joint Publication: 13 February 2006): I-10.

<sup>iv</sup> Richard Myers, Gen., USAF, *National Military Strategy: A Strategy for Today; A Vision for Tomorrow*, (Washington DC, 2004): 12.

<sup>v</sup> Robert David Steele, "Information Operations" Putting the 'I' back into DIME," (Washington, DC: Government Printing Office, February 2006): 3.

<sup>vi</sup> "Kinetic," *Merriam-Webster Online*, (2007) [database on-line]; available from <http://www.m-w.com/dictionary/kinetic>; Internet; accessed 4 February 2007.

<sup>vii</sup> Steven Collins, "Army PSYOP in Bosnia: Capabilities and Constraints," *Parameters, US Army War College Quarterly*, (Carlisle, PA: US Army War College, Summer 1999): 57-73.

<sup>viii</sup> *Ibid.*

<sup>ix</sup> *Ibid.*

<sup>x</sup> *Ibid.*

<sup>xi</sup> Pascale Combelles Siegel, "VII. Information Activities," *Lesson from Bosnia: The IFOR Experience* (1997) [ASAF Air War College database on-line]; available from [http://www.au.af.mil/au/awc/awcgate/ccrp/wentz\\_bosnia.pdf](http://www.au.af.mil/au/awc/awcgate/ccrp/wentz_bosnia.pdf); Internet; accessed 20 February 2007.

<sup>xii</sup> Pascales Combelles Siegel, "Target Bosnia: Integrating Information Activities in Peace Operations: NATO-Led Operations in Bosnia-Herzegovina, December 1995-1997", (Washington, DC: National Defense University, 1998): 42.

- 
- <sup>xiii</sup> Ibid, 56.
- <sup>xiv</sup> Marc J. Romanych, USA Retired, and Kenneth Krumm, LTC, USA, “Tactical Information Operations in Kosovo,” *Military Review*, (September-October 2004): 59.
- <sup>xv</sup> William M. Darley, COL, USA, “Why Public Affairs is not Information Operations,” *Army Magazine*. 55, no. 1 (January 2005): [journal on-line]; available from <http://www.ansa.org/webpub/DeptArmyMagazine.nsf/byid/CCRN-6CCSFV>; Internet; accessed 20 February 2007.
- <sup>xvi</sup> Todd Sholtis, Maj., USAF, “Planning for Legitimacy: a Joint Operational Approach to Public Affairs,” *Air & Space Power Journal*, (8 June 2005) [journal on-line]; available from <http://www.airpower.maxwell.af.mil/airchronicles/cc/sholtis.html>; Internet; Accessed 20 February 2007.
- <sup>xvii</sup> Gary Pounder, Maj., USAF, “Opportunity Lost: Public Affairs Information Operations, and the Air War against Serbia,” *Aerospace Power Journal*, (Maxwell Air Force Base: Air Force University, Summer 2000): 1-2.
- <sup>xviii</sup> “Operation Enduring Freedom – Afghanistan,” *Global Security Website*, [database on-line]; available from <http://www.globalsecurity.org/military/ops/enduring-freedom.htm>; Internet; accessed 19 February 2007.
- <sup>xix</sup> George W. Bush, “September 20<sup>th</sup> Address to a Joint Session of Congress” and “October 7<sup>th</sup> Address to the Country,” *Global Security website* [database on-line]; available from <http://www.globalsecurity.org/military/ops/enduring-freedom.htm>; Internet; accessed on 19 February 2007.
- <sup>xx</sup> Joseph Cox, MAJ, USA. “Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?” (Forth Leavenworth, KS: School of Advanced Military Studies, 2006): 57.
- <sup>xxi</sup> Peter W. Singer, “Winning the War of Words: Information Warfare in Afghanistan, America’s response to Terrorism Analysis Paper #5, (23 October 2001). [Brookings Institute database on-line]; available from <http://www.brookings.edu/views/papers/psinger/20011023.htm>; Internet; accessed 30 November 2006.
- <sup>xxii</sup> Pat Maney, BG, USA, Deputy Commander, USACAPOC (A). “Lessons learned in Afghanistan Slideshow” *National Defense Industrial Association-SO/LIC Symposium* (11 February 2003) [USAF Air War College database on-line]; available from <http://www.au.af.mil/au/awc/awcgate/ndia/maney.pdf>; Internet; accessed 19 February 2007.
- <sup>xxiii</sup> Charles Eassa, LTC USA, Deputy Director US Army Information Operations, source Michael Schrage, “Use Every Article in the Arsenal,” *Washington Post*, (15 January 2006).
- <sup>xxiv</sup> Based on personal interview with Charles Eassa, LTC, USA, Deputy Director, US Army Information Operations Proponent (Alexandria, VA, 2 November 2006).
- <sup>xxv</sup> Norman Emery, MAJ, USA, “Information Operations in Iraq,” *Military Review* (May-June 2004): 11-14.
- <sup>xxvi</sup> Evan Thomas, “Groping in the Dark,” *Newsweek* (1 September 2003): 30.
- <sup>xxvii</sup> Ralph O. Baker, COL, USA, “The Decisive Weapon,” *Military Review*, (May-June 2006): 13-32.

- 
- <sup>xxviii</sup> Joseph Collins, former Deputy Assistant Secretary of Defense quoted in *Military Review* article, source: Thomas Metz, Lieutenant General, USA, "Massing Effects in the Information Domain," *Military Review* (May – June 2006): 4.
- <sup>xxix</sup> Metz: 5.
- <sup>xxx</sup> Josh White, "Military Planting Articles in Iraq Papers," *Washington Post* (1 December 2005): A18.
- <sup>xxxi</sup> Ibid.
- <sup>xxxii</sup> Stoney Trent, CPT, USA, "Marketing: An Overlooked Aspect of Information Operations," *Military Review* (July – August 2006): 70-74.
- <sup>xxxiii</sup> Soukhanov, Anne H. *WEBSTER'S II, New Riverside University Dictionary* (The Riverside Publishing Company: Boston, MA, 1994): 335.
- <sup>xxxiv</sup> Montgomery McFate, J.D., Ph.D., "Anthropology and Counterinsurgency: The Strange Story of their Curious Relationship," *Military Review* (March – April 2005) [database on-line]; available from [http://www.army.mil/professionalwriting/volumes/volume3/august\\_2005/7\\_05\\_2.html](http://www.army.mil/professionalwriting/volumes/volume3/august_2005/7_05_2.html); Internet; accessed 20 February 2007.
- <sup>xxxv</sup> Ibid.
- <sup>xxxvi</sup> George Bush, *National Security Strategy 2006* (Washington, DC, March 2006): 43.

## Glossary

**Bosniac:** A Bosnian of Muslim origin, but not necessarily active in that faith. It is a secular term used to differentiate them from Bosnian-Serbs and Bosnian-Croats, who traditionally are Orthodox Christian and Catholics, respectively. Typically, a person's name and family ancestry will dictate these distinctions, which endure regardless of whether an individual continues to practice that faith or even converts to another faith.

**CA – Civil Affairs:** Designated Active and Reserve component forces and units organized, trained, and **equipped** specifically to conduct Civil Affairs activities and to support civil-military operations.<sup>xxxvii</sup>

**Combat Camera:** The acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services.<sup>xxxviii</sup>

**CMOC – (Civil Military Operations Center):** The operations center is formed from CA assets and serves as the primary interface between the U.S. armed forces and the local population, humanitarian organizations, nongovernmental agencies, international organizations, the United Nations, multinational forces, and other agencies of the U.S. Government. The CMOC is not generally established and run by the military. If not, the military plays a supporting role.<sup>xxxix</sup>

**Cultural Anthropology:** The scientific study of human culture based on archaeological, ethnological, ethnographic, linguistic, social, and psychological data, as well as methods of analysis.<sup>xl</sup>

**EW – (Electronic Warfare):** Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within Electronic Warfare are: electronic attack, electronic protection, and Electronic Warfare support.<sup>xli</sup>

**Information Fratricide:** The result of employing Information Operations elements in such a way that that openly contradicts other information elements, impedes the conduct of friendly operations, or adversely affects the morale of friendly forces.

**IO – (Information Operations):** The 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 that of its own command. It includes the use of these capabilities to influence the perceptions of foreign friendly and neutral audiences.<sup>xlii</sup>

**Information Environment:** The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.<sup>xliii</sup>

**Kinetic Operations:** Military operations involving the application of force in order to achieve a direct effect. Examples include, but are not limited to, artillery, infantry, and aviation offensive and defensive operations.

**Non-Kinetic Operations:** Operations that seek to influence actions of a target audience through, but not limited to, the employment of electronic or print media, computer-network operations, Electronic Warfare, and the targeted administration of humanitarian assistance.

**PA – Public Affairs:** Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense.<sup>xliv</sup>

**PI – Public Information:** Information of a military nature, the dissemination of which through public news media is not inconsistent with security, and the release of which is considered desirable or non-objectionable to the responsible releasing agency.<sup>xlv</sup>

---

<sup>xxxvii</sup> Department of Defense, *JP 1-02: Department of Defense Dictionary of Military and Associated Terms*, (12 April 2001): 87.

<sup>xxxviii</sup> Department of Defense: 97.

<sup>xxxix</sup> FM 41-10 *Civil Military Operations*, (14 February 2000): H-1.

<sup>xl</sup> Anne H Soukhanov, *WEBSTER'S II, New Riverside University Dictionary*, (The Riverside Publishing Company: Boston, MA, 1994): 335.

<sup>xli</sup> Department of Defense, *JP 3-13 Information Operations*, (13 February 2006): GL 7.

<sup>xlii</sup> US Army Information Operations Proponent, briefed to Information Operations Qualification Course (Fort Leavenworth, KS: US Army Combined Arms Center, May-June 2006).

<sup>xliii</sup> Department of Defense, *JP 3-13*: GL 9.

<sup>xliv</sup> Department of Defense, *JP 1-02*: 433.

<sup>xlv</sup> Department of Defense, *JP 1-02*: 434.

## Bibliography

- Baker, Ralph O., COL, USA. "The Decisive Weapon." *Military Review* (May-June 2006): 13-32.
- Bush, George W. *National Security Strategy 2006*. (Washington, DC, March 2006): 43.
- \_\_\_\_\_. "October 7<sup>th</sup> (2001) Address to the Country" *Global Security Website*. Available from <http://www.globalsecurity.org/military/ops/enduring-freedom.htm>. Internet. Accessed on 19 February 2007.
- \_\_\_\_\_. "September 20<sup>th</sup> (2001) Address to a Joint Session of Congress" *Global Security Website*. Available from <http://www.globalsecurity.org/military/ops/enduring-freedom.htm>. Internet. Accessed on 19 February 2007.
- Collins, Steven. "Army PSYOP in Bosnia: Capabilities and Constraints." *Parameters, US Army War College Quarterly*. (Summer 1999): 57-73.
- Cox, Joseph, MAJ, USA. "Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?" Forth Leavenworth, KS: School of Advanced Military Studies, 2006: 1-127.
- Darley, William M., COL, USA. "Why Public Affairs is not Information Operations." *Army Magazine*. 55, no. 1 (January 2005): Available from <http://www.ausa.org/webpub/DeptArmyMagazine.nsf/byid/CCRN-6CCSFV>; Internet. Accessed 20 February 2007.
- Eassa, Charles, LTC USA, Deputy Director US Army Information Operations. Quoted in Schrage, Michael. "Use Every Article in the Arsenal." *Washington Post*. 15 January 2006.
- \_\_\_\_\_. Interview by author, 2 November 2006.
- Emery, Norman, MAJ, USA. "Information Operations in Iraq." *Military Review* (May-June 2004): 11-14.
- FM 3-13: Information Operations*, US Army Field Manual: 28 November 2003.
- Global Security. "Operation Enduring Freedom – Afghanistan." *Global Security Website*. Available from <http://www.globalsecurity.org/military/ops/enduring-freedom.htm>. Internet. Accessed 19 February 2007.
- JP 3-13: Information Operations*, US Joint Publication: 13 February 2006.
- Josten, Richard J., "Strategic Communication, Key Enabler for Elements of National Power," *IO Sphere* (Summer 2006)16-20. Available from [http://www.au.af.mil/info-ops/iosphere/iosphere\\_summer06\\_josten.pdf](http://www.au.af.mil/info-ops/iosphere/iosphere_summer06_josten.pdf). Internet. Accessed 1 October 2006.

- Maney, Pat, BG, USA, Deputy Commander, USACAPOC (A). “Lessons learned in Afghanistan Slideshow.” *National Defense Industrial Association-SO/LIC Symposium*. 11 February 2003. Available from <http://www.au.af.mil/au/awc/awcgate/ndia/maney.pdf>. Internet. Accessed 19 February 2007.
- McFate, Montgomery, J.D., Ph.D., “Anthropology and Counterinsurgency: The Strange Story of their Curious Relationship.” *Military Review* (March – April 2005). Available from [http://www.army.mil/professionalwriting/volumes/volume3/august\\_2005/7\\_05\\_2.html](http://www.army.mil/professionalwriting/volumes/volume3/august_2005/7_05_2.html). Internet. Accessed 20 February 2007.
- Metz, Thomas F., Lieutenant General, USA. “Massing Effects in the Information Domain.” *Military Review* (May – June 2006): 2-12.
- Myers, Richard, Gen., USAF. *National Military Strategy: A Strategy for Today; A Vision for Tomorrow*. Washington, DC: Government Printing Office, 2004.
- Pounder, Gary, Maj., USAF. “Opportunity Lost: Public Affairs Information Operations, and the Air War against Serbia.” *Aerospace Power Journal*. (Summer 2000): 1-2.
- Romanych, Marc J., USA, Retired and Kenneth Krumm, LTC, USA. “Tactical Information Operations in Kosovo.” *Military Review* (September-October 2004): 59.
- Rumsfeld, Donald. *National Defense Strategy 2005*. Washington, DC, March 2005.
- Schneider, William Jr., *Report of the Defense Science Board Task Force on Strategic Communication*, Report prepared by the office of the Under Secretary of Defense for Acquisition. Washington, DC, September 2004.
- Sholtis, Todd, Maj., USAF. “Planning for Legitimacy: a Joint Operational Approach to Public Affairs.” *Air & Space Power Journal*. (8 June 2005) Available from <http://www.airpower.maxwell.af.mil/airchronicles/cc/sholtis.html>. Internet. Accessed 20 February 2007.
- Siegel, Pascale Combelles. *Target Bosnia: Integrating Information Activities in Peace Operations: NATO-Led Operations in Bosnia-Herzegovina, December 1995-1997*. Washington, DC: National Defense University, 1998: 42.
- \_\_\_\_\_. “VII. Information Activities.” *Lesson from Bosnia: The IFOR Experience* (1997) Available from [http://www.au.af.mil/au/awc/awcgate/ccrp/wentz\\_bosnia.pdf](http://www.au.af.mil/au/awc/awcgate/ccrp/wentz_bosnia.pdf). Internet. Accessed 20 February 2007.
- Singer, Peter W. “Winning the War of Words: Information Warfare in Afghanistan, America’s response to Terrorism Analysis Paper #5, (23 October 2001). Available from <http://www.brookings.edu/views/papers/psinger/20011023.htm>. Internet. Accessed 30 November 2006.

Soukhanov, Anne H. *WEBSTER'S II, New Riverside University Dictionary*. (The Riverside Publishing Company: Boston, MA, 1994): 335.

Steele, Robert David. "Information Operations: Putting the 'I' back into DIME." Washington, DC: Strategic Studies Institute, February 2006.

Stoney Trent, CPT, USA, "Marketing: An Overlooked Aspect of Information Operations," *Military Review* (July – August 2006): 70-74.

Thomas, Evan. "Groping in the Dark." *Newsweek*, 1 September 2003: 30.

US Army. *JP 3-13, Information Operations*. US Joint Publication: 13 February 2006: I-10.

White, Josh. "Military Planting Articles in Iraq Papers." *Washington Post*, 1 December 2005: A18.