USAWC STRATEGY RESEARCH PROJECT

U.S. STRATEGIC INFORMATION OPERATIONS: THE REQUIREMENT FOR A COMMON DEFINITION AND ORGANIZATIONAL STRUCTURE IN SUPPORT OF THE GLOBAL WAR ON TERRORISM

by

Lieutenant Colonel Andrew B. Seward
United States Army

Mr. William Waddell
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. 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

1. REPORT DATE
03 MAY 2004

2. REPORT TYPE

3. DATES COVERED
-

4. TITLE AND SUBTITLE
U.S. Strategic Information Operations The Requirement for a Common Definition and Organizational Structure in Support of the Global War on Terror

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Andrew Seward

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050

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
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**38**	

ABSTRACT

AUTHOR: Lieutenant Colonel Andrew B. Seward

TITLE: U.S. Strategic Information Operations: The Requirement For A Common Definition And Organizational Structure In Support Of The Global War On Terrorism

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 27 CLASSIFICATION: Unclassified

Despite its lofty title as one of the national elements of power, the informational component is fundamentally misunderstood in concept, diffused in responsibility, and fragmented in application. In American society, the right to free speech has primacy and citizens have a healthy distrust of official government rhetoric. Thus the second tier status of informational power is perhaps unsurprising. But in the war of ideas and ideals that is the current Global War on Terrorism (GWOT), strategic information operations can be neither ignored nor allowed to languish. It is time to re-organize and focus information operations at a national strategic level and harness its potential. Kinetic military power, diplomacy and America’s economic might are critical to the GWOT, but similar success in strategic information operations is essential to creating lasting change.

This paper reviews the current state of strategic information operations, discusses the lack of existing consensus regarding strategic information operations’ definition, scope, and what it might accomplish, suggests a new model for strategic-level information operations, and compares and makes a recommendation from four options for better organizing information operations within the United States Government at the national strategic level in support of GWOT.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The author is pleased to acknowledge the outstanding support he received from his fellow U. S. Army War College Seminar Group 14 classmates and faculty instructors. Without their keen insights, open dialogue and intellectual camaraderie, this paper's content would have been significantly lessened. Within this group of great Americans, I would especially like to extend my deep appreciation to my friend, Mr. Jonathan Haberkern. Jonathan challenged my views and analysis at every step, selflessly giving his time and sharing his experiences in support of improving my work.

The insight and encouragement received from my fellow information operations course classmates and instructors here at the U.S. Army War College Class of 2004 focussed my views and left me with a deeper comprehension of our country's emerging informational capability.

The most important acknowledgement goes to my wonderful wife, Alison. None of this would have been possible without her. Alison's astute, thoughtful comments and her measured reasoning were central to my thesis and the resulting outcome. It is remarkable to have such a talented and supporting friend; to be married to her is just that much better.

LIST OF ILLUSTRATIONS

U.S. STRATEGIC INFORMATION OPERATIONS: THE REQUIREMENT FOR A COMMON DEFINITION AND ORGANIZATIONAL STRUCTURE IN SUPPORT OF THE GLOBAL WAR ON TERRORISM

The Global War on Terrorism (GWOT) is not a war in the traditional sense, but a mixture of kinetic warfare, defense of the homeland, and a war of and about ideas and ideals. This last component – winning the war of ideas and ideals – is proving exceptionally difficult to plan, direct and conduct at the strategic level. The primary reason is simple: the United States Government (USG) is not optimally organized for effective command and control or conduct of information operations[1] at the strategic level.

INFORMATION OPERATIONS AND THE GLOBAL WAR ON TERROR

Owing to the capabilities and far-flung dispersion of the terrorist threat, the Global War on Terrorism requires a national focus and energy equal to or greater than the Cold War of 1945 – 1991. Yet GWOT is fundamentally different from the Cold War in one very important aspect – the enemy this time is not a nation-state. The enemy is terrorism, which is founded in secular or religious ideals and supported by a variety of peoples spread across many different nation-states[2]. These ideals have, at their core, distrust, dislike and even a hatred of western politics, culture and economics. Taken to extremes, these ideals manifest themselves in violent acts. Terrorism against the United States and other western nations has both domestic and international players. At the time of writing and in its present-day Islamic form, this terrorism largely originates from external individuals and groups that share a dislike or hatred of foreign ways and ideas, and who are bolstered by the Mohammedan concept of Jihad taken to extreme measures.

Despite the similarity in terms of the enormity of the threat, the GWOT is fundamentally different from the Cold War. Rather than the bipolar political and military world of the Cold War, we now live in a multi-polar world, where terrorists from a variety of locations pick and choose their targets from a wide array of possibilities flung around the globe. This is no longer strictly “nation state versus nation state” warfare. There was a symmetry to the nation state-based Cold War adversaries that is lacking in GWOT. Terrorism is largely asymmetric in its methods and often operates without borders in the conventional political sense.[3] Our enemies in the war on terror are therefore more difficult to both contain and influence than was the monolithic threat of Soviet Union of the Cold War. The targeted nation states, such as the United States, are like a herd of elephants caught in the open with terrorists hiding behind rocks all around us. They cannot destroy us, but with a few well-placed arrows they certainly might panic us enough to make us change course.

How then can the USG defeat such an asymmetric foe? What tools does the government have at its disposal in the war on terror and how shall they be organized and used? In particular, what role does information play in the GWOT? How is information as a national instrument of power to be employed in that fight?

INFORMATION AS AN ELEMENT OF NATIONAL POWER

Informational power is an essential and recognized element of national power – sort of. On the one hand, the U.S. Government's policy document for the war on terror, *The National Strategy for Combating Terrorism* , formally identifies information as a fundamental tool. In it, President George W. Bush specifically states, "We will not triumph solely or even primarily through military might. We must fight terrorist networks, and all those who support their efforts to spread fear around the world, using every instrument of national power – diplomatic, economic, law enforcement, financial, *information*, intelligence, and the military" (italics added)[4]. On the other hand, however, in *The National Security Strategy of the United States of America* (NSS), published by President Bush in September 2002, the President says, "To defeat this threat [of terror] we must make use of every tool in our arsenal – military power, better homeland defenses, law enforcement, intelligence, and vigorous efforts to cut off terrorist financing."[5] It is instructive that information, diplomatic and economic powers are not specifically mentioned in the context of GWOT in these opening comments.

Although the term "information operations" is mentioned only once *in The National Security Strategy of the United States of America*, different references to informational power and actions occur eight additional times[6]. These occurrences add further understanding to the vital role information operations play in GWOT, with guidance such as "We will also wage a war of ideas to win the battle against international terrorism. This includes using effective public diplomacy to promote the free flow of information and ideas to kindle the hopes and aspirations of freedom of those in societies ruled by the sponsors of global terrorism."[7] Information-based requirements and actions are described in much greater detail, however, in *The National Strategy for Combating Terrorism* . The Intelligence Community is instructed to "acquire new reporting sources, then use those sources to penetrate terrorist organizations to provide information on leadership, plans, intentions, modus operandi, finances, communications and recruitment."[8] Likewise, we will be prepared to act forcefully and unilaterally if necessary to "deny terrorists access to new recruits, financing, equipment, arms, and information."[9] Protection of vital information requires that the United States "continue to pursue an aggressive strategy that identifies sensitive information and technology and outlines appropriate steps to preclude terrorists from obtaining and taking them."[10] In the GWOT, a wide variety of information operations are thus fundamental to our success.

This is our new challenge, then: to defeat, deny, diminish, and defend[11] against terrorism against the United States of America and its citizens, whether at home or abroad. To do this will require our full spectrum of national power: diplomatic, economic, law enforcement, financial, informational, intelligence and military[12]. We are well organized at the strategic level in almost all of these elements, but it is the author's opinion that in a most crucial and relevant area – information power – we are momentarily fractured and marginalized. This must change if we are to expend our national resources more efficiently.

STRATEGIC INFORMATION OPERATIONS CURRENT SITUATION

We currently lack unity of command for information operations at our top level of government. This is because we lack an organization and a leader to take charge of this national tool of power. Consider this: within the cabinets and organizations that comprise the Executive Branch of the United States Government, only one of the seven national elements of power is not represented by a corresponding cabinet-level position.[13] For military operations, the United States has a Secretary of Defense. National diplomatic power is the domain of the Secretary of State. The Secretary of Commerce supervises economic power on behalf of the nation, while the Secretary of the Treasury oversees our financial power. Intelligence is the purview of the Central Intelligence Agency and the Department of Justice heads law enforcement. And national-level informational power is the responsibility of… whom?

There is clearly a major gap here. The United States does not have a "Secretary of Information" or any such similar construct in order to lead, supervise, coordinate and exercise strategic information operations on behalf of the national government. This is perhaps understandable given our national values and culture. Americans traditionally possess a healthy distrust of an overly powerful central government, manifested and regulated through a "checks and balances" federal architecture and enshrined within the Constitution of the United States of America.[14] Providing a formal, legal counterweight to the central government's might, a series of strong individual protections, rights and entitlements are guaranteed to U.S. citizens. These rights both define and reinforce the independence that is so central to the American character and culture. It is not surprising, therefore, that Americans deeply value independence of thought and action, and thus generally dislike being "preached to" by those who govern us. We prefer to choose our own sources of information. Americans dislike propaganda as a rule. The current generation well remembers the evil horrors that can result from information operations controlled and centralized under an unchecked and unprincipled senior leader like Joseph Goebbels of Nazi Germany in the 1930s and 1940s [15]. And we hold the right to free speech and open discussion dear as a nation. Is it any wonder then that we have never created a Department of Information within the United States Government?

Yet these cultural values have positioned us poorly as a nation-state when dealing with a terrorist enemy whose very ability to reconstitute and grow depends upon persuading others to fight against the United States in a war of ideas and ideals. Given this situation, what should we do? First, we must agree on a common definition for information operations at the national strategic level. Secondly, we must then determine the best way to assign the overarching authority and responsibility for strategic information operations within the United States Government.

THE DEFINITION PROBLEM

To begin with, the United States Government must clarify its definition of information operations at all levels – strategic, operational and tactical -- before it can more effectively organize within the political structure and synchronize it with the other national elements of power. In the author's opinion, this is especially important in the area of *strategic* information operations, which is critical for winning the war of ideas and ideals in the Global War on Terrorism. Without common understanding of the definition, synchronization of an overarching national information operations strategy with the other elements of power will be difficult if not impossible. Mutual understanding is required within the entire interagency community of U.S. Government agencies, non-governmental organizations, private voluntary organizations, and regional and international organizations [16] (definition from JSOG) as a whole as to the meaning of "information operations". Yet the definition is not currently agreed upon across the government. For example, the Department of Defense's current publication entitled "*Joint Doctrine for Information Operations*", known as Joint Pub 3-13, states "Information operations are actions taken to affect an adversary's information and information systems, while defending one's own information and information systems."[17]

The actions described in this DOD definition are quite limited in scope. They are tied directly to our own and others' informational elements or the systems that pass those elements. Such a definition does not address the cognitive process of human thoughts, decisions and actions, but is instead oriented at the systems that pass information and the information itself[18]. It therefore fails to include humans and their intellect as things to be acted upon in the context of information operations. It is also instructive that the doctrinal joint military view of information operations is framed in generally offensive and defensive terms, implying a bipolar world consisting only of adversaries and "one's own" friendly forces. It says nothing of third party actors who are neither adversaries nor friendly forces. Such a definition falls short of describing the full information environment[19] of GWOT, where the primary target audiences for a "war of ideas and ideals" clearly includes third parties such as the moderate Muslim world audience or European public opinion. Looking at it strategically, this one-size-fits-all DOD definition also fails to say "why" these operations should occur; it ignores their purpose of supporting the national political interests and objectives.

In Joint Publication 3-13, discussion of war-oriented information operations focuses more at the operational and tactical levels rather than at the strategic level. Generally speaking, strategic information operations focus on human reactions and behaviors. They have a political impetus and goal. They are also longer term. Normally they are grounded in deep-rooted beliefs or philosophies. Information operations at the operational level tend to be more regional or in support of a national campaign. At the tactical level, information operations have greater immediacy and are largely aligned to either technologies or persuasion-oriented tasks. Before a fully encompassing definition of strategic IO may be accepted, it must also interoperable and compatible with operational and tactical IO. Contrast the rather vague definition of Strategic IO with the greater specificity in the operational and tactical definitions:

> "IO and the Strategic Level of War. IO may be included in the spectrum of activities directed by the National Command Authorities (NCA) to achieve national objectives by influencing or affecting all elements (political, military, economic, or informational) of an adversary's or potential adversary's national power while protecting similar elements. There may be a high degree of coordination between the military, other U.S. Government (USG) departments and agencies, and allies/coalition partners to achieve these objectives."[20]

> "IO and the Operational Level of War. IO are conducted to achieve or support campaign or major operation objectives. The focus of IO at this level is on affecting adversary lines of communication (LOCs), logistics, command and control (C2), and related capabilities and activities while protecting similar friendly capabilities and activities. Operational-level IO may contribute to strategic objectives by degrading an adversary's capability to organize, command, deploy, and sustain military forces and capabilities and by allowing the joint force to obtain and maintain the degree of information superiority required to quickly and decisively accomplish the mission."[21]

> "IO and the Tactical Level of War. IO at the tactical level involve achieving specific tactical objectives. The primary focus of these IO is affecting adversary information and information systems relating to C2, intelligence, and other information-based processes directly relating to the conduct of military operations while protecting similar friendly capabilities."[22]

DOD defines the strategic level of war as "the level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) security objectives and guidance, and develops and uses national resources to accomplish these objectives."[23] It goes on to state, "Activities at this level establish national and multinational military objectives; sequence initiatives *; define limits and assess risks for the use of military and other instruments of national powe* r (italics added); develop global plans or theater war plans to achieve these objectives; and provide military forces and other capabilities in accordance with strategic plans."[24] Specific to military information operations at the strategic level, the "*Joint Doctrine for Information Operations"* publication declares "IO support the national military strategy but require support, coordination, and participation by other USG departments and agencies as well as the commercial industry."[25] When discussing offensive information operations, it says "Offensive IO at the strategic level of war will be directed by the National Command Authority and planned in coordination with other agencies or organizations outside the Department of Defense."[26]

This is an accurate portrait of the current state of affairs. Ultimately the President determines if and when strategic information power will be applied in any given situation, especially if IO are to be used offensively, based upon input and recommendations from a wide variety of sources. Yet there is no one point of contact, no singular government entity to task. This is different from the process for applying strategic diplomatic power, for example, where the President turns directly to the Secretary of State in all such matters.

The State Department does not traditionally use the term "information operations" to describe its missions and actions. Instead, State promotes what it calls "public diplomacy". As defined by the Planning Group for Integration of the United States Information Agency (USIA) into the Department of State, "public diplomacy seeks to promote the national interest of the United States through understanding, informing and influencing foreign audiences."[27] The arm of the State Department responsible for conducting official public diplomacy is the USIA, which was formally merged with the State Department on October 1, 1999 after operating as a separate agency since 1953. The difference between traditional diplomacy and public diplomacy is clearly explained by the USAI Alumni Association, in that "public diplomacy deals not only with governments but primarily with non-governmental individuals and organizations. Furthermore, public diplomacy activities often present many differing views as represented by private American individuals and organizations in addition to official U.S. Government views. Traditional diplomacy actively engages one government with another government. In traditional diplomacy, U.S. Embassy officials represent the U.S. Government in a host country primarily by maintaining relations and conducting official USG business with the officials of the host government whereas public diplomacy primarily engages many diverse non-government elements of a society."[28] Thus although the State Department lacks a specific doctrinal definition for information operations, it actively promotes information sharing and outreach as a means of favorably influencing public opinion in other countries. In the GWOT, public diplomacy is a front line tool in the struggle to win the war of ideas and ideals.[29]

From the State Department's perspective, the Pentagon's "offensive" and "defensive"[30] terms likely are regarded as heavy-handed and pejorative. Describing information operations in these terms runs directly against their organizational culture's code of subtlety. Diplomats operate in an environment of multiple players where precise language and tone are exceedingly important and complexity is a fact of life. The terms "offense" and "defense" are descriptive and starkly opposing, while diplomacy deals in a continuum filled with shades of gray. The State Department's places great emphasis on the human element of information operations Regardless of the definition gap, the State Department is charged by the President to conduct some specific aspects of information operations, although this is not meant to imply that they are assigned overarching responsibility for that function. In *The National Security Strategy of the United States of America*, the President writes, "Just as our diplomatic institutions must adapt so that we can reach out to others, *we also need a different and comprehensive approach to public information efforts* that can help people from around the world learn about and understand America. The war on terrorism is not a clash of civilizations. It does, however, reveal the clash inside a civilization, a battle for the future of the Muslim world. *This is a struggle of ideas and this is an area where America must excel*".[31] As the State Department is the cabinet entity responsible for representing American interests, ideals, and diplomacy abroad, it is therefore a key player in any information operations at the strategic level.

Following from this brief review of DOD and State Department information operations definitions, it is clear we lack consensus at the national level on just exactly what constitutes information operations. Both of these Executive Branch cabinets see IO through their own internal cultural and environmental lens. Hence it is unsurprising that there is disagreement as to information operations' description and scope. Without consensus at the cabinet level, it is difficult – if not impossible – to determine the best organizational structure and responsibility for conducting strategic information operations. Yet it is the author's opinion that it is possible to derive a basic model of information operations from simple observation of the key elements of IO. Following from this, if this model is deemed broad enough to encompass all possible components and sub-disciplines within the current literature, it may serve as a useful frame of reference that could more clearly define the full spectrum of information operations. Any such common definition could prove useful in assessing the best way to assign responsibility for information operations at the strategic level within the United States Government.

THE DOMAIN DEFINITION PROBLEM

To look at information operations at its most basic level, it should be understood in terms of the information environment within which it operates. The DOD defines the Information environment as "the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself."[32] This definition covers the basic components of the information environment, but it does not fully emphasize the important dynamic interactions that take place between these "individuals, organizations, or systems". It may be possible to improve upon this definition. In the author's opinion, there are four basic elements required to describe the underlying Information Environment in the broadest of terms. In short, these are *Humans, Communication, Information, and Process*.

Humans. At the center of the Information Environment are human beings. Although they act both in individual and collective ways, when reduced to the lowest common denominator they are singular in nature, with unique intellectual, psychological, physical and emotional attributes. A Human has a relationship with Information both internally and externally. He internalizes Information as beliefs, memories, values, and facts and figures. This internalized Information is a trusted core that shapes his perceptions and is part of the Human himself, rather than part of the cognitive Process. Externally, all Humans receive Information from outside sources. They then conduct a variety of cognitive functional Processes that result in outcomes ranging from inaction to action.

Communication. A Human requires a method by which he transmits, stores, and receives Information with other human beings. The element of Communication is the means of connection between Humans by which Information in all its forms travels or flows. The means may be electronic or non-electronic, virtual or real, and one-way or two-way. It may involve as few as two discrete individuals or as many as are connected in the broadest of worldwide networks.

Information. The term “Information” actually comprises three basic building blocks that the author will lump together for the purpose of this model, namely “data”, “information” and “intelligence”. These elements are not identical, but rather hierarchical. Data is the lowest common denominator. It consists of the collected words, photos, videos, sounds and other communicative elements. Data is taken at its face value, as a simple discreet item. Next up the scale is information. In this construct, data is combined to produce facts in a meaningful fashion. Information is more highly structured than data, as it communicates facts and ideas, but it is not enlightening in and of itself. For that, something more is required, and this is the application of intellect and the resultant understanding resulting in intelligence. Intelligence denotes awareness. It typically relies upon multiple sources of information, as is required when scrutinizing, comparing and evaluating information and data. The ultimate aim of intelligence is to derive insight or products such as analysis and projection that are synthesized from available data and information.

Process. What Humans do with the information they receive is a complex process, the basic sub-elements of which are: reception, perception, analysis, judgement, and resulting actions. The element of Process in this model describes the cognitive and intellectual component of Human beings. A Human receives Information through Communication Flow, but this Information is then subject to a number of cognitive processes that give or take meaning from that Information. Processing includes perceiving, analyzing, and judging the information received. This is done as a matter of comparison and contrast of this Information with the recipient’s internalized personal values, beliefs, life experiences, personal situation, and a host of environmental factors. Once a Human has judged the Information, he either accepts or rejects this Information. Acceptance outcomes include mental and/or psychological internalization of the Information (storing), an external Communication Flow of this Information to others, or the Human taking follow-on actions resulting from his decisions based upon this Information.

These four basic elements are constantly changing and interacting. Seen as a system, the basic Information Environment may be graphically rendered as follows, with all four of the elements shown here:

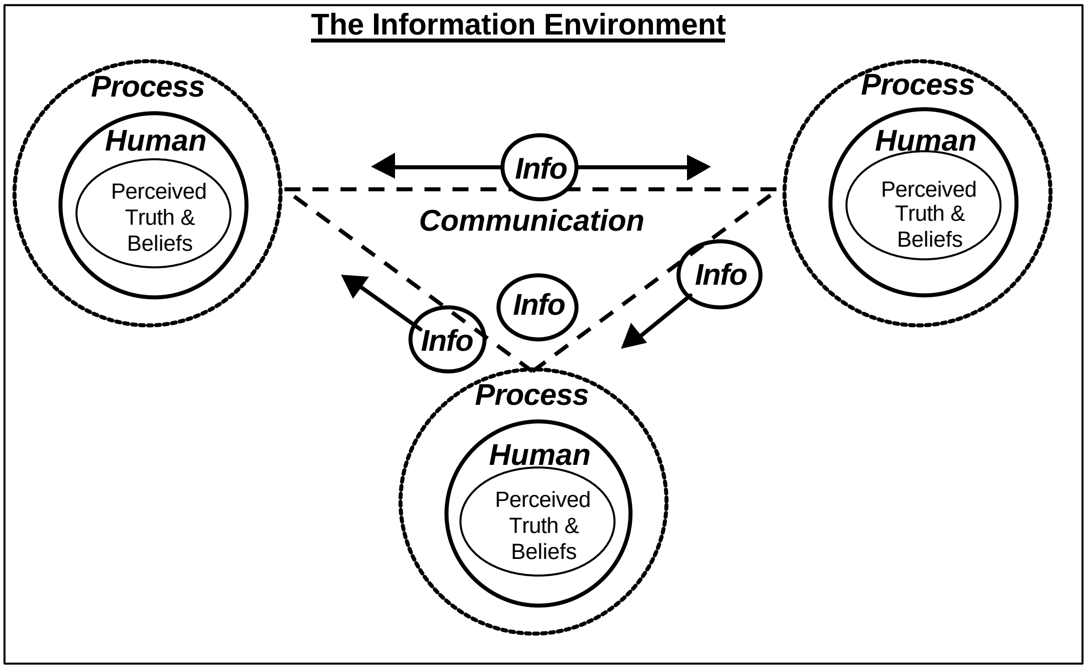
The Information Environment
Process
Human
Perceived Truth & Beliefs
Process
Human
Perceived Truth & Beliefs
Info
Communication
Info
Info
Info
Process
Human
Perceived Truth & Beliefs

FIGURE 1. THE INFORMATION ENVIRONMENT

Humans are both central to and at the periphery of this diagram. Each Human being possesses cognitive and intellectual functions, which they apply as a Process to Information. This Information resides both within and outside of each Human within the Information Environment. Each Human is connected to other human beings through Communication, which allows Information to pass between them or stores Info inside systems within Communication. The overall Information Environment is defined by these four elements and is limited by the natural boundaries presented by time and space.

A REFINED DEFINITION OF INFORMATION OPERATIONS

This basic model of the Information Environment is intentionally broad. The author proposes a possible definition for describing the Information Environment as “the entire set of conditions under which humans relate to, communicate and process information.” Unlike the definition of the Information Environment given in Joint Pub 3-13, which describes the environment as an “aggregate” wherein “individuals, organizations, and systems” “collect, process, or disseminate information"[33], this definition centers on human beings and their relationship with information. If the reader can accept this proposed definition as a universal description of the information environment, then it may be sufficient to serve as a starting point for deriving a common definition of information operations. Information operations might therefore be defined as "actions taken that are specifically calculated to affect the information environment 's human, information, communication, and process elements in order to achieve desired goals and objectives."

This new definition adds the concept of deliberateness, implying that information operations are calculated with a specific intention in mind, and that their idealistic goals or attainable objectives are pre-determined. Information operations defined in this way would encompass the entire range of how information interacts with humans both internally and externally, within the process of communication, and simply as an element with value unto itself: information for information's sake. The scope of this proposed definition exceeds that of DOD's official definition, which says, "information operations are actions taken to affect an adversary's information and information systems, while defending one's own information and information systems."[34]

As such, this proposed definition might be better suited as a basis for defining the full spectrum of strategic-level information operations for the United States Government as well. By replacing the somewhat cumbersome term "Information Environment" with a brief definitive phrase, and by reflecting the strategic IO's wide scope, a revised definition might read "U.S. Government strategic information operations are actions specifically calculated to affect the conditions under which humans relate to, communicate, and process information, taken in order to achieve desired national strategic goals and objectives."

This definition is built upon the underlying concepts implicit within the full range of elements within the Information Environment. It is bounded by the term "strategic", which serves to denote the essential importance of such operations in pursuit of national goals and objectives, and the term "United States Government", which defines the authority for their undertaking. It also answers the specific questions of "who" and "why" related to strategic IO. In the author's opinion, it is also sufficiently broad to serve as a basis for all U. S. strategic-level information operations, encompassing their full range and scope regardless of which arm of the Executive Branch (or Congress, for that matter) is conducting them.

To further develop this issue, the realm of strategic information operations could be divided into operational domains that promote better understanding and common definitions. Since the terms "offensive" and "defensive" as used by DOD are limited by virtue of their essentially bipolar --rather than multi-polar -- nature and whereas the term “offensive” is not conducive to representing diplomatic niceties in international statesmanship, new categories are required. By defining these categories based upon their operational domains, information operations might be divided by a flexible boundary into “External Information Operations” and “Internal Information Operations”.

The terms “external” and “internal” in this context would be defined relative to the boundary of U.S. Government authority, actors, organizations and infrastructure. The edges of this USG boundary could be logically extended to incorporate non-USG actors, organizations and infrastructure that directly support the government’s goals and objectives, including such things as privately-owned national telecommunications systems, Non-Governmental Organizations (NGOs) supplying much-needed services in humanitarian missions when USG assets are unavailable, or United Kingdom classified information shared with the USG. “External” and “internal” are not meant to describe a domestic versus foreign delineation, although those terms were considered. Ultimately, however, any term suggesting that the U.S. Government would conduct domestic information operations upon its populace would certainly result in a vigorous and resistive legal challenge from many quarters, not to mention the potential for highly critical and negative press coverage. Even if a hypothetical construct such as “Domestic IO” were specifically and legally limited to encompass only protective IO measures, the resulting definition would fall short of the aggressive IO measures required when dealing with domestic terrorists in the GWOT.

The domain of External Information Operations would contain both friendly and adversarial actors. It would also comprise a wide range of IO measures spanning the full spectrum from protective IO intended to protect our allies through aggressive IO designed to physically destroy an enemy’s information or communications. Internal Information Operations’ domain would by default contain only friendly actors and be largely defensive in nature. These two operational domains would define the limits of information operations. Within the boundaries of External and Internal IO, the full spectrum of possible actions may be described as categories known as “measures” to be taken. How do these action-based terms differ from the existing DOD “offensive” and “defensive” IO terms? There is an important difference. The greatest conceptual change is the substantive widening of “Offensive IO” into the much broader “External IO”. “External” does not necessarily mean “offensive” operations, but may instead include IO such as public affairs relations with the foreign press or civil affairs assistance to third party nations. By contrast, there is admittedly less difference between “Defensive IO” and “Internal IO”, since internal measures overall are inherently defensive in nature. Yet, what a thing is called matters greatly at the strategic diplomatic and political level, especially when the subject at hand directly concerns information itself.[35] It is not simply the conceptual differences that are important. Choosing the name of these categories with skill and care might make the difference between general acceptability and condemnation.

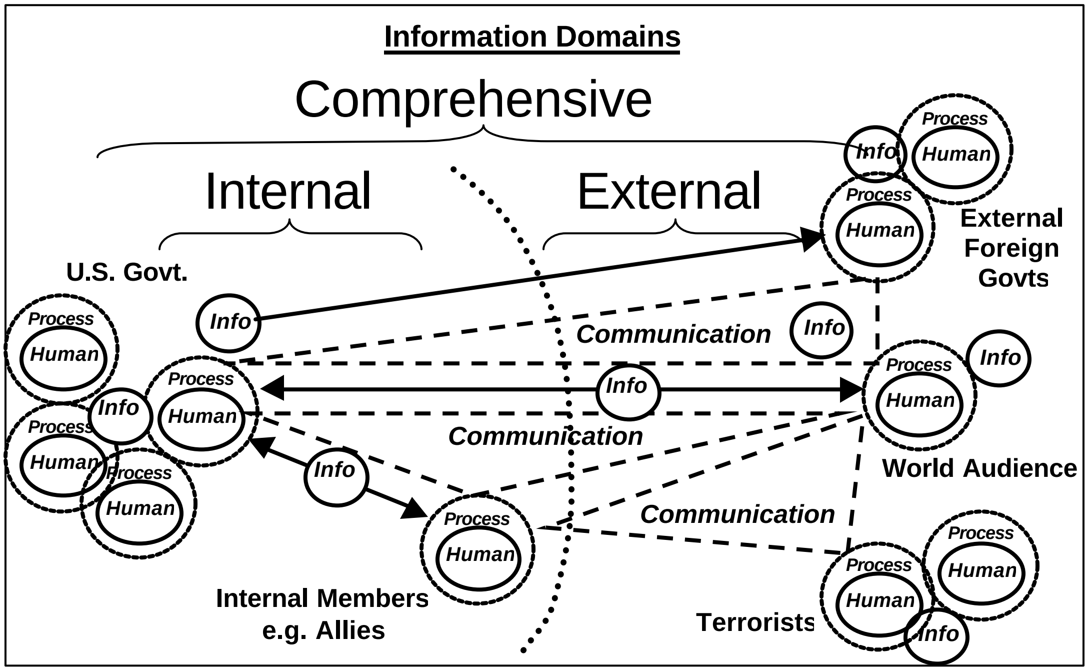

FIGURE 2. INFORMATION DOMAINS

Given this internal-external boundary defining the Information Environment into domains, conclusions may be drawn. Of the four Information Environment elements, there are some that are discretely separated by the internal-external boundary, and others that move across the boundary between domains. Human beings and their closely related cognitive Processes exist discretely within either the external or internal domain. Conversely, Information and the Communications means that supports Information are not necessarily confined by the external-internal boundary.

Since the Human and Process elements when combined are either external or internal domain members, any IO measures they take may be described in relation to their internal or external orientation, or both. From the U.S. Government's point of view, Information Operation measures would normally be addressed from the perspective of the Internal IO members, namely the U.S. Government and other trusted internal members or allies. This allows IO measures to be broken into three fundamental major categories:

External Measures. Actions (by Internal Members) that actively apply information operations capabilities to affect the external Information Environment in order to achieve desired goals and objectives.

Internal Measures. Actions (by Internal Members) that actively apply information operations capabilities to affect the internal Information Environment in order to achieve desired goals and objectives.

Comprehensive Measures. Actions (by Internal Members) that actively apply information operations capabilities to affect the full internal and external combined Information Environment in order to achieve desired goals and objectives.

More specific IO measures are then categorical subsets of External, Internal, or Comprehensive measures. Here is a proposed list of these subcategories and their definitions:

External Measures.

- *Physical Effects Measures*. Actions designed to have a physical effect upon elements of the external Information Environment.
- *Persuasion Measures*. Actions designed to persuade, affect perceptions and influence the actions of external Information Environment members.
- *Exploitation Measures*. Actions designed to give an advantage to Internal Members by affecting elements of the external Information Environment.

Internal Measures[36].

- *Protective Measures*. Actions designed to protect internal Information Environment elements from unwanted effects.
- *Resistive Measures*. Actions designed to resist unwanted effects within the internal Information Environment.
- *Restorative Measures*. Actions designed to reestablish internal Information Environment elements to their former desired state following undesired changes.

Comprehensive Measures.

- *Dissemination Measures*. Actions designed to disseminate information, both declarative and perceptive, to both internal and external Information Environment elements.
- *Acquisition Measures*. Actions designed to gather desired information from across the full Information Environment.
- *Assessment Measures*. Actions designed to assess and evaluate information and information operations across the full Information Environment.

The relationship of these measures to IO capabilities must now be determined. To be a satisfactory semantic construct, these proposed IO measures must be able to encompass all of our current IO capabilities. How will those capabilities be determined?

In a perfect world, a superior method for determining IO capabilities would be to conduct a visionary approach by answering the basic question, "what do we want to accomplish using IO?" Once that question is answered, the next logical question would be, "what capabilities will we need to accomplish this?" This method is euphemistically referred to as the "Eve" method, thus called because the biblical character Eve was created out of Adam's rib bone based upon God's vision of what was required for Adam.[37] An "Eve"-based model of IO would develop capabilities that could best directly accomplish the desired IO endstate.

However, a more apt analogy for describing the reality of IO capabilities today might be "Frankenstein" rather than "Eve". Whereas Frankenstein the monster was created by stitching together available body parts to form a whole body, we are striving to achieve our desired IO endstate using a stitched-together amalgamation of IO capabilities currently at hand. The "Frankenstein" model is reality. A cursory review of joint military suggests that a combining of existing military capabilities or related activities forms the current doctrinal basis of IO capabilities. What are these IO capabilities and related activities to be applied? According to Joint Pub 3-13, they comprise the existing functions known as Operations Security (OPSEC), Military Deception, Psychological Operations (PSYOPS), Electronic Warfare (EW), Physical Attack/Destruction, Computer Network Attack, Civil Affairs (CA), Special Information Operations (SIO), Information Assurance (IA), Education, Training, and Awareness, Intelligence Support, Physical Security, Counterdeception, Counter-Propaganda, Counterintelligence (CI), Public Affairs (PA), Command Information, and Offensive IO Support.[38] Some of these functions, notably OPSEC and EW, are found in both the existing categories of "Offensive IO" and "Defensive IO".

This Frankenstein-like group of disparate capabilities may be grouped and organized in an orderly fashion under the nine subcategories of External, Internal, and Comprehensive Measures. If this construct is therefore sufficiently broad and flexible enough to describe the existing array of DOD's IO capabilities, it may be similarly broad enough to serve as a useful construct for IO at the national strategic level.

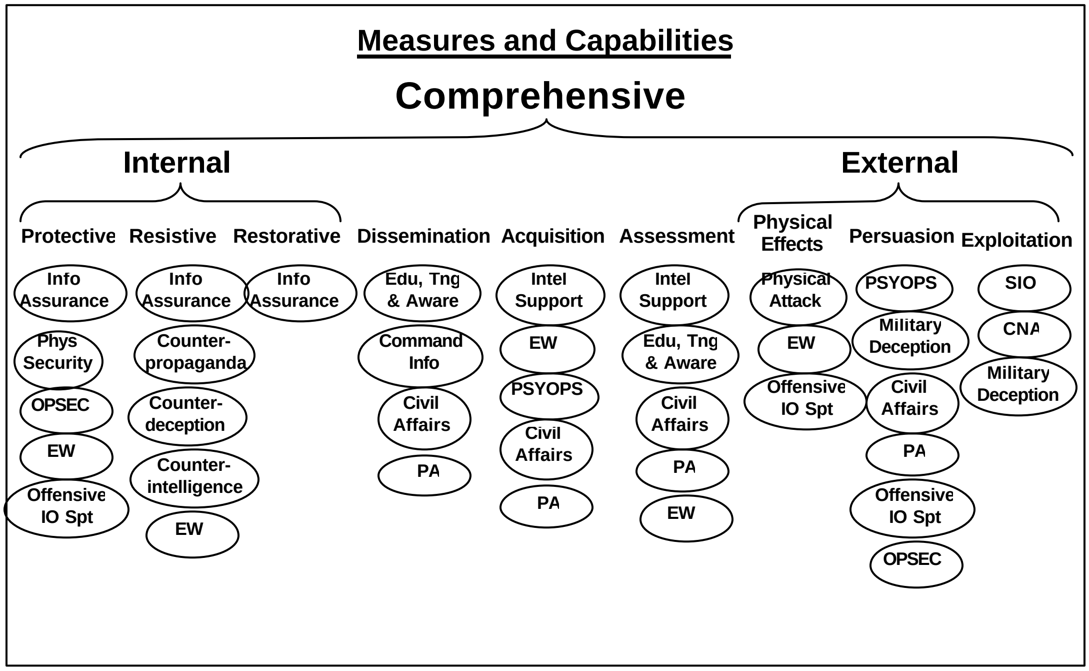

FIGURE 3. MEASURES AND CAPABILITIES

THE ORGANIZATIONAL PROBLEM

United States Government decisionmakers operate within limited dimensions and parameters. Political and diplomatic leaders are concerned with the parameters of domestic and international policies, political parties, finance bases and constituents. Economic leaders are concerned with markets, regulations, currencies and businesses. American military leaders are traditionally oriented towards the application of military capabilities[39] in physical, geospatial regions, including land, sea, air and space. This requires superior technologies and highly trained personnel. But the application of informational power requires additional elements, such as ideas, ideals and beliefs. These are fundamentally human-oriented, and they can only be measured through the words or actions of human beings. Historically, the United States has primarily exercised strategic power through its military and diplomatic corps. Information was not seen as a major national element of power in its own right, but rather as a tool to serve diplomacy and warfighting. The world has changed considerably through the rapid advances made in technology over the past 50 years, especially in computing and telecommunications. Data, information and intelligence now have a real, significant and pervasive capability to influence political will, direction and national strategy, owing to their widespread availability, portability, dispersion and transparence.

PROPOSALS FOR ORGANIZING U.S. STRATEGIC INFORMATION OPERATIONS

There are at least four possibilities for exercising the informational element of national power within the United States Government at the strategic level:

- Create a new Department or Agency within the Executive Branch.
- Assign executive agency responsibility for information operations to an existing Department Secretary or Agency.
- Create a National Security Council Policy Coordination Committee specifically for strategic information operations.
- Status Quo.

This list of options is likely not exhaustive, but rather serves as logical proposals providing instructive insight to the issue at hand. These possibilities will be discussed regarding their feasibility, suitability and acceptability within a political and operational context. What are the advantages and disadvantages of each of these ideas? Which option(s) offer superior ability to plan, control and conduct strategic information operations over the long term?

Proposal 1: Create A New Department Of Information Within The Executive Branch

Despite declaring information to be one of our primary national elements of power, there is currently no single Executive Branch cabinet-level organization responsible for information operations at the strategic level. Given the cultural American resistance to government-sponsored propaganda and the realistic political and resource constraints associated with creating such an entity, it is unlikely that a “Secretary of Information” cabinet post will be created. This does not mean the leadership and oversight authority for U.S. strategic information operations should remain as disjointed as it currently finds itself.

A consequence of not assigning responsibility for information operations to a single cabinet is a reduced sense of competition for preeminence within the Executive Branch. Historically, the Departments of Defense, State, and Commerce have competed for primacy as the preferred “tool of choice” when implementing national foreign and security policy. The Department of Justice, Central Intelligence Agency, and Department of Treasury have tended to play supporting rather than primary roles compared to Defense, State and Commerce. Of these, the Department of Commerce has been a specialized player owing to its market-driven outlook. The Departments of State and Defense have been cast in supporting roles with respect to Commerce, ensuring diplomacy and, if necessary, military power is made available to ensure economic growth and stability. Informational power, much like military and diplomatic power, occupies something of a second tier position relative to national economic power. To elevate it to cabinet-level status would likely result in additional competition for primacy, which would be dysfunctional, and thus undesirable from a national perspective. However, if information operations were viewed more in view of a supporting role to existing cabinet and Interagency organizations, similar to the roles played by Defense and State enabling the economic power provided by Commerce, this sense of competition would likely be lessened.

Unfortunately, regardless of how the three primary cabinets of Commerce, State and Defense might view a Department of Information Management cast in a supporting role, they would certainly view its very existence as competitive, and find its potential for competition over scarce budget dollars and resources quite threatening. The entire Executive Branch is in competition for limited resources. Elevating information operations to cabinet-level status would divert resources from existing organizations, who would resist any such new organization, regardless of whether it was viewed as a peer-competitor or supporting actor. This fact alone makes it unlikely that a separate cabinet level might be created.

An additional consideration is Congress, whose support for creating any new cabinet within the Executive is crucial. The Congress is typically supportive of the Executive in these matters, but the response and opinion of their constituents would drive their acceptance. Given the historical U.S. trend to dislike and distrust anything smacking of propaganda. It is highly unlikely that constituent response would be favorable. It is much more likely that the mainstream media would receive the proposal of such a new Executive cabinet entity very unfavorably. Without grassroots and popular media support, this proposal would be a non-starter with Congress.

Proposal 2: Assign Executive Agency Responsibility For Strategic Information Operations To An Existing Department Secretary Or Agency

A second option would be to assign primary responsibility for strategic information operations to one of the Executive Branch's organizations. By delegating the responsibility for IO to one cabinet, the ambiguities and difficulties inherent in creating a new Executive-level cabinet would be avoided. The resource scarcities would remain, but rather than be divided amongst a larger total number of organizations, it would simply be shifted as required between them. If history is any judge, the organization shouldered with this new responsibility would be forced to fund this capability primarily within their existing budgets. The A-list candidates for this mission would be the Department of Defense, Department of State, and the CIA. All of these organizations are already heavily involved in the daily conduct of international actions on behalf of the United States. They are also well organized, well established and in possession of significant budgets for promulgating information operations programs. Of these candidates, the Department of Defense has the greatest number of IO personnel, the widest range of IO capabilities, a worldwide focus and dispersion of personnel, and has made a great effort to document the use of informational power in support of national goals and objectives. It also receives a large proportion of the national budget, and so can better afford to absorb the associated costs than most of the others. Defense acts and applies its power at all levels, from strategic through operational and down to tactical. The Secretary of Defense also serves as a permanent member of the Principals Committee -- the highest level of the National Security Council.[40] By comparison, the State Department is probably best designed to conduct "hearts and mind" IO through its public diplomacy program, but is poorly trained or untrained and equipped to conduct physical effects measures or many of the more hard-hitting aspects of IO. The Secretary of State is a member of the NSC Principals Committee, but his cabinet is significantly smaller in size than DOD, lacking Defense's personnel and resource depth. The other top candidate, the CIA, similarly lacks personnel resources.[41] CIA would likely be impeded by its cloak and dagger reputation when operating in the relative openness and veracity required for an effective GWOT "hearts and minds" campaign. Thus the Department of Defense is best suited to assume national responsibility for information operations in general and specifically Strategic IO.

Proposal 3: Create A National Security Council Policy Coordination Committee Specifically For Information Operations

Both the Department of Defense and the State Department recognize the value of information operations and have developed various internal organizations with some degree of capability. However, in each case, these sub-organizations are specifically designed to enable and support the greater overall mission of the Department in which they find themselves; they are neither autonomous nor broad-based in a strategic sense. Where is the person or organization charged with developing, planning, supervising and analyzing the overarching strategic information operations of the United States Government? Perhaps the question might better be phrased in this manner: where is national political will translated into strategy, and the national elements of power assigned to support that strategy? The responsibility for that mission falls upon the National Security Council in the Executive Branch. President Bush's National Security Policy Directive #1, dated 13 February 2001, states, "The National Security Council functions through a series of functional and regional Policy Coordination Committees, or PCCs, which are chaired by an Undersecretary or Assistant Secretary appointed by the Secretary of Defense, Secretary of State, or the Assistant to the President for National Security Affairs, commonly known as the National Security Advisor. NSC/PCCs shall be the main day-to-day fora for interagency coordination[42] of national security policy. They shall provide policy analysis for consideration by the more senior committees of the NSC system and ensure timely responses to decisions made by the President."[43]

At this time, there is no functional PCC assigned responsibility for strategic information operations policy development, planning, guidance and oversight. As a result, information operations undertaken by the United States tend to be unsynchronized and sub-efficient. The organizations responsible for exercising the other elements of national power – diplomatic, economic, law enforcement, financial, intelligence, and military – develop internal information operations supporting their element of power rather than as a tool of national power in its own right. This is sub-optimal. A new Information PCC could provide a forum wherein all of the interagency might find representation and thus interact to develop information operations policy and national IO direction.

It should be noted that the NSC and its PCCs are primarily concerned with developing policy – not conducting planning and operations. They are therefore the organization best suited to develop the national strategic vision, themes and synchronization with the other national elements of power. They are not, however, even remotely capable of conducting a continuous information operation. Yet the creation of a separate information operations PCC would greatly improve our nation's ability to form strategic information operations policy and develop strategic themes that are synchronized with the national political will and the other three elements of national power. The greatest improvement would be in the leadership this PCC would provide during "hearts and minds" operations.

Proposal 4: Status Quo

Are there advantages to maintaining the status quo? Currently, information operations are widely distributed across our government. The U.S. government thus lacks a single focal point for coordinating information operations. Instead, it takes direction from variety of sources according to the situation at hand. The NSC diffuses politically-led strategic messages amongst its eleven functional PCCs. This allows the White House Office of the Press Secretary great latitude to develop messages of strategic informational importance that may be chiefly of short-term political design and intent. Such messages may be a short-term reaction to media-raised issues of the moment, and may not necessarily support long-term national strategic information needs. Maintaining the status quo condemns the USG to sub-optimal implementation of information operations within the interagency and risks conducting unsynchronized and possibly conflicting information measures with resulting negative effects. Given the importance of IO in the war on terror, the status quo is not acceptable.

SUMMARY AND RECOMMENDATIONS

The United States Government must use information operations in the most effective manner possible if we are to triumph in the Global War On Terror. Our current organization and application of the informational element of national power is disjointed at the strategic level. There are many IO capabilities extant within the interagency, but they lack the strong central focus and synchronization required to create synergy and obtain the best possible results. There is no designated organization responsible for leading IO within the government. Without this appointed leadership, strategic information operations are neither optimally organized nor coordinated for truly effective application in the war on terror. Of the four proposals examined in this paper, the author concludes that two of them hold merit. First, the NSC should create a Policy Coordination Committee expressly charged with developing and promulgating strategic-level information operations policy and national political IO direction. Secondly, one of the Executive Branch's organizations should be assigned as the executive agent for conducting and resourcing information operations. Given the candidates available, the author recommends the Department of Defense as best postured and equipped to assume this responsibility.

Exacerbating the current situation is a fundamental lack of agreement as to the definition and meaning of IO. Until concurrence is attained within the Interagency and a shared opinion harmonizes around a common understanding of IO and its elements, measures, capabilities and focus between the internal elements of the USG and its allies, the growth of IO as a discipline will be found wanting. This paper suggests a possible IO model that might serve as a possible starting point for a broad-based definition of IO. After being rigorously reviewed, tested, and improved, the author hopes a common set of IO definitions and constructs will result throughout the Interagency, eventually leading to improved application of information operations at the national strategic level.

WORD COUNT= 7,906

ENDNOTES

[1] Department of Defense, “Joint Publication 1-02, DOD Dictionary of Military and Associated Terms,“ n.d.; available from <http://www.dtic.mil/doctrine/jel/doddict/data/i/02606.html>; Internet; accessed 4 March 2004.

[2] George W. Bush, *National Strategy for Combating Terrorism* ; Washington, D.C.: The White House; February 2003, 1.

[3] Donald H. Rumsfeld, *Quadrennial Defense Review Report*; Washington, D.C.: U.S. Department of Defense; 30 September 2001, 3.

[4] Bush,1.

[5] George W. Bush, *The National Security Strategy of the United States of America*; Washington, D.C.: The White House; September 2002, 1.

[6] Ibid, pages 6, 16, 23, 30, and 31.

[7] Ibid, 6.

[8] Bush, *National Strategy for Combating Terrorism* , 16.

[9] Ibid, 21.

[10] Ibid, 22.

[11] Ibid, 15.

[12] Ibid.

[13] The White House, “President Bush’s Cabinet,” n.d.; available from <http://www.whitehouse.gov/government/cabinet.html>; Internet; accessed 16 February 2004.

[14] Gerhard Casper, *Separating Power: Essays on the Founding Period*; Cambridge, MA: Harvard University Press; 1997.

[15] Calvin College, “German Propaganda Archive: Nazi Propaganda by Joseph Goebbels 1933-1945,” 16 February 2004; available from <http://www.calvin.edu/academic/cas/gpa/goebmain.htm >; Internet; accessed 15 February 2004.

[16] Edward L. LaFountaine, *The Joint Staff Officer’s Guide* (Norfolk, VA: Nation Defense University Joint Staff Forces College, 2000), G-41.

[17] Henry H. Shelton, *Joint Pub 3-13: Joint Doctrine for Information Operations* (Washington, D.C.: U.S. Government Printing Office, 9 October 1998), I-9.

[18] George W. Bush, *National Strategy for Homeland Security*; (Washington, D.C.: The White House; 16 July 2002), 55-61. The government’s emphasis on technical issues such as

information systems and sharing of information is clearly demonstrated in this chapter, which deals exclusively with these topics and does not address other areas of IO.

[19] Department of Defense, Internet; available from <http://www.dtic.mil/doctrine/jel/doddict/data/i/02605.html>.

[20] Shelton, I-2.

[21] Ibid.

[22] Ibid, I-3.

[23] Department of Defense, Internet; available from <http://www.dtic.mil/doctrine/jel/doddict/data/s/05072.html>.

[24] Ibid.

[25] Shelton, I-11.

[26] Ibid, II-10.

[27] USIA Alumni Association, "Public Diplomacy Website," 1 September 2002; available from <http://www.publicdiplomacy.org/1.htm >; Internet; accessed 3 March 2004.

[28] Ibid.

[29] Margaret DeBardeleben Tutwiler, *Opening Statement regarding Public Diplomacy Programs to the House Appropriations Subcommittee on Commerce, Justice, State and the Judiciary*, 4 February 2004; available from <http://appropriations.house.gov/index.cfm?Fuseaction=Hearings.Testimony&HearingID=284&WitnessID=441>; Internet; accessed 5 March 2004. Under Secretary Tutwiler calls for additional funding for public diplomacy programs with emphasis on public diplomacy's role in the GWOT.

[30] Shelton, I-10.

[31] Bush, *The National Security Strategy of the United States of America*, 31.

[32] Shelton, GL-7.

[33] Ibid.

[34] Ibid.

[35] Ronal A. Samuelson, *The Great Conversation: The Origins and Development of the National Operations Security Program* ; (Greenbelt, MD: Interagency OPSEC Support Staff Publications Department, April 1991), 2-4. Samuelson relates just how very important names can be as he relates how the title "Operations Security" was chosen ahead of several other possibilities in order to generate interest in this new field and garner funding. It is Samuelson's

contention that, had OPSEC been named something less interesting, it would not have survived as a discipline.

[36] David S. Alberts, *Defensive Information Warfare*; (Washington, D.C.: National Defense University; August 1996), 55-58. Alberts uses slightly different terms to describe his vision of the USG's measure, namely "collection", "deterrence", "protecting", and "reconstitution". He also stresses the requirement for the government to work hand-in-hand with private industry.

[37] COL David J. Smith, "Information Operations," lecture, Carlisle Barracks, PA, U.S. Army War College, 6 February 2004. Cited with permission of COL Smith. COL Smith's analogy is apt: the current DoD definition of IO capabilities appears to be derived from status quo military capabilities rather than from any vision of what IO capabilities DoD might require to perform its missions.

[38] Shelton, II-2 – II-7 and III-4 – III-7.

[39] Department of Defense, Internet; available from <http://www.dtic.mil/doctrine/jel/doddict/data/m/03309.html>.

[40] Federation of American Scientists Intelligence Resource Program, "National Security Presidential Directive 1," 13 February 2001; available from <http://fas.org/irp/offdocs/nspd/nspd-1.htm >; Internet, accessed 5 March 2004.

[41] Ibid, Internet; available from <http://www.fas.org/irp/cia/ciastaff.htm >. CIA personnel staff strength is currently estimated to be between 15,000 – 20,000; the actual numbers remain officially unavailable.

[42] Department of Defense, Internet; available from <http://www.dtic.mil/doctrine/jel/doddict/data/i/02698.html>.

[43] Federation of American Scientists Intelligence Resource Program, Internet; available from <http://fas.org/irp/offdocs/nspd/nspd-1.htm >.

BIBLIOGRAPHY

Alberts, David S. *Defensive Information Warfare*. Washington, D.C.: National Defense University, August 1996.

________, John W. Gartska, Richard E. Hayes, and David Signori*. Understanding Information Age Warfare*. Washington D.C.: CCRP Publications Series, August 2001.

Bush, George W. *National Strategy for Combating Terrorism* . Washington, D.C.: The White House, February 2003.

________. *National* Strategy *for Homeland Security*. Washington, D.C.: The White House, 16 July 2002.

________. *The* National *Security Strategy of the United States of America.* Washington, D.C.: The White House, September 2002.

Calvin College. "German Propaganda Archive: Nazi Propaganda by Joseph Goebbels 1933-1945." 16 February 2004. Available from <http://www.calvin.edu/academic/cas/gpa/goebmain.htm >; Internet. Accessed 15 February 2004.

Casper, Gerhard. *Separating Power: Essays on the Founding Period* . Cambridge, MA: Harvard University Press, 1997.

Federation of American Scientists Intelligence Resource Program. "National Security Presidential Directive – 1." 13 February 2001; available from <http://fas.org/irp/offdocs/nspd/nspd-1.htm >; Internet. Accessed 5 March 2004.

LaFountaine, Edward L. *The Joint Staff Officer's Guide*. Norfolk, VA: National Defense University Joint Forces Staff College, 2000.

Marsh, Robert T. Critical Foundations: Protecting America's Infrastructures – The President's Commission *on Critical Infrastructure Protection* . Washington, D.C.: U.S. Government Printing Office, October 1997.

Rumsfeld, Donald H. *Quadrennial Defense Review Report*. Washington, D.C.: U.S. Department of Defense, 30 September 2001.

Samuelson, Ronald A. *The Great Conversation: The Origins and Development of the National Operations Security Program* . Greenbelt, MD: Interagency OPSEC Support Staff Publications Department, April 1991.

Shelton, Henry H*. Joint Pub 3-13: Joint Doctrine for Information Operations*. Washington, D.C.: U.S. Government Printing Office, 9 October 1998.

Smith, COL David J. "Information Operations." Lecture. Carlisle Barracks, PA, U.S. Army War College, 6 February 2004. Cited with permission of COL Smith.

The White House. "President Bush's Cabinet." n.d. Available from <http://www.whitehouse.gov/government/cabinet.html>; Internet. Accessed 16 February 2004.

Tutwiler, Margaret DeBardeleben. *Opening Statement regarding Public Diplomacy Programs to the House Appropriations Subcommittee on Commerce, Justice, State and the Judiciary*. 4 February 2004. Available from <http://appropriations.house.gov/index.cfm?Fuseaction=Hearings.Testimony&HearingID=284&WitnessID=441>; Internet. Accessed 5 March 2004.

USIA Alumni Association. "Public Diplomacy Website." 28 February 2004. Available from <http://www.publicdiplomacy.org>; Internet. Accessed 3 March 2004.

Waltz, Edward. *Information Warfare: Principles and Operations*. Norwood, MA: Artech House, 1998.