

**JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL**

**ORGANIZATIONAL CULTURE CHALLENGES TO INTERAGENCY AND
INTELLIGENCE COMMUNITY COMMUNICATION AND INTERACTION**

by

**Special Agent
Chase H. Boardman
U.S. Department of State**



A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy.

The contents of this paper reflect our own views and are not necessarily endorsed by the Joint Forces Staff College or the Department of State or the Department of Defense.

Signature: _____

Date: May 31, 2006

Thesis Advisory Panel:

Lt Gen (R) Charles Cunningham, JFSC

Dr. Gail Nicula, JFSC

Mr. Stuart Symington, USDoS

Col. Michael Santacroce, USMC

ABSTRACT

A significant factor contributing in many crises of the post-industrial era is the failure by the agencies making up the U.S. Government bureaucracy to communicate with each other. This failure is rooted strongly in the Government's organizational culture. This thesis paper examines the concept of organizational culture and its impact upon how the U.S. Government's Intelligence Community's agencies share information.

It is this author's contention that both the overarching organizational culture of the Intelligence Community (IC) and the internal cultures of the agencies within it keep their members from sharing knowledge. Communication barriers exist because of the nature of the bureaucratic structures that gather, analyze, and distribute intelligence information in our government, and because of how members of the organizations forming the IC interact with one another.

The barriers to cooperation and communication, however, can be torn down through the IC leadership's use of the tools of communication to modify the organizational culture to better coordinate the IC's interagency sharing of the fruits of their intelligence efforts. This exercise of leadership, backed by legislation for restructuring and directing and financing improved systems architecture enabling information sharing in the IC in particular, and the U.S. Government as a whole for that matter, can improve the effectiveness and efficiency of the agencies at the core of the fight in the Global War on Terror.

ORGANIZATIONAL CULTURE CHALLENGES TO INTERAGENCY

COMMUNICATION AND INTERACTION

CONTENTS

I	INTRODUCTION – The Failure to Communicate	1
II	INFORMATION SHARING’S DYSFUNCTIONAL ENVIRONMENT	3
III	THE INTELLIGENCE COMMUNITY AND “THE INTERAGENCY”	8
IV	ORGANIZATIONAL CULTURE INHIBITS COMMUNICATION	13
V	INFORMATION SHARING, TURF, AND THE ZERO-SUM GAME	16
VI	THE ROLE OF THE DIRECTOR OF NATIONAL INTELLIGENCE	30
VII	INTERAGENCY CHANGES IN SYSTEMS AND STRUCTURES	33
VIII	MANAGING ORGANIZATIONAL CULTURAL CHANGE	44
IX	REFORM DEMANDS ARE NOTHING NEW TO THE IC	50
X	TOWARD DEVELOPING ORGANIZATIONAL CULTURE	54
XI	CENTRALIZATION THREATS	56
xii	CONCLUSION – Interagency Cultures Are Changeable	59
	NOTES	62
	BIBLIOGRAPHY	69
	AUTHOR BIOGRAPHY	78

ORGANIZATIONAL CULTURE CHALLENGES TO INTERAGENCY

COMMUNICATION AND INTERACTION

I INTRODUCTION – The Failure to Communicate

In the post-industrial era, the failure of the agencies comprising the U.S. Government to communicate well with each other significantly affects and exacerbates many of the crises facing our nation. That failure to communicate, especially on the part of the agencies in the intelligence community, bears increasingly dangerous implications for our nation's ability to maintain its long-term geopolitical position and status.

In this thesis, this author contends that the overarching organizational culture of the Intelligence Community and the internal cultures of the agencies within it keep their members from communicating with each other. *Communication*, used here, refers to the sharing of intelligence, data, and information, which would increase the capability of an agency's personnel to carry out their mission.

The concept of organizational culture encompasses aspects of management and leadership theory and those patterns of shared assumptions that formal groups use to solve the problems of external adaptation, internal integration, and incorporating changes. An organizational culture is one that is unique to a particular, relatively formal group, agency or organization. Cultures define who is a group member and who is not, and how a member behaves in relation to insiders and outsiders. Using this construct as a basis, this thesis looks at the impact of organizational culture upon communication among members of the agencies that form the U.S. Government's Intelligence Community.

Interagency communication barriers exist, in a large part, because of the bureaucratic

structures in place within each agency that affect how they gather, analyze, and distribute intelligence information. Barriers also exist because members of each bureaucracy forming the IC interact differently with members of their own group than they do with those of other agencies.

Put another way, information sharing among U.S. Government intelligence agencies is affected by organizational cultures and attitudes, chiefly those that call for keeping a close hold on knowledge at all levels of generation and analysis. This author contends that, to the detriment of national security, government agencies operate in an environment not conducive to the sharing of intelligence. This environment results, in part, from regulations, policies and procedures implementing information security laws and executive orders.

The central questions addressed in this paper are essentially these: First, how does organizational culture affect interagency communication? Second, how is organizational cultural change effected so that participants in the interagency process will better communicate with one another? To bring about change, two things are required: leadership in making changes to a culture, and the tools -- in this case information technology architecture -- conducive to organizational intelligence sharing, collaboration and cooperation.

Both leaders and their subordinates need to understand and bridge the cultural divides of and within interagency operations. Essentially, leaders need to remind their people that, with data to pass, they also have the tools and either the direction or permission to do it. It is as if they must say, "We have information. We have a telephone. Use it." At all levels, IC personnel need to understand that the U.S. cannot meet the threats facing our country unless they pass information, without reservation, to those other USG personnel who need it and can

act upon it. This must be done even when those who need the information do not ask for it or when they ask the wrong questions. To achieve this goal requires that personnel in each member agency of the IC know the capabilities and needs of the others. Information needs to be shared, willingly and completely so that timely and effective action can be coordinated.

The methodology of this thesis focuses on a literature review of basic organizational cultural theory and what the theory says about changing cultures within organizations. This is, in significant part, a discussion of what leaders must do to bring about the cultural and structural changes necessary to cause interagency actors to better share information and intelligence in order to ensure the security of the nation's citizens.

II INFORMATION SHARING'S DYSFUNCTIONAL ENVIRONMENT

The United States government muddles through crises fairly effectively¹. It has a long history of doing so, and to some extent that muddling through is reflected in its structure. Many agencies owe their existence in one way or another to national crises, both real and perceived. Some were created to ward off crises or to meet anticipated ones. These include the Departments of State and Defense. Others, such as the Department of Homeland Security and the Central Intelligence Agency as examples, were created in response to events where the needs of the nation had not been met by previously existing agencies or structures.

The U.S. Government responds well, in both the executive and legislative branches. In crises they tend to operate more or less in concert and to come to decisions that meet the needs of the moment and that eventually resolve the emergencies facing the nation in a manner that seems to satisfy the people from whom they derive their powers. However, crisis management and *ad hoc* activity, muddling through, are not what an agency's

personnel want to do. It is not their preferred environment.

Intelligence agencies, and for that matter all United States Government agencies, are charged with serving the American public. In part, this service includes keeping the public safe. In the case of intelligence agencies, carrying out this duty includes getting information about threats to the organizations or people who can analyze and act to neutralize that threat.

Overcoming the problems presented by a dysfunctional bureaucratic environment should be relatively simple and easy. In particular, sharing most information, especially if it is of critical value to the safety of the nation or its people, should be even easier. Information comes to the attention of an agency's personnel. The analysts look it over or pass it to those who can process it if they do not have the expertise or background to do so. They, in turn, pass the results of that analysis to the right people -- those who can operationally act upon it. The intake and passing should be expedient, the analysis hopefully accurate, and the threat neutralization swift.

The problem is that passing that information and the subsequent processed intelligence is not easy, especially if it is of a sensitive nature. This may be that it is potentially embarrassing to the United States, or to the United States Government (which are not necessarily the same thing), or it may have been gathered from a source or in a manner that needs guarding. Then it is, by statute and executive order, to be appropriately safeguarded, to be shared only with those with 'a need to know,' the properly cleared.

The existence of classified information begs questions -- who needs to know?² Who determines that need to know? Can the originating agency trust other agencies, or their people, to take the appropriate care with their sources and methods? Can the originator trust them with the information? How did that *other agency* determine those with access would be

appropriately cleared? What's their clearance process? Does it match or meet the originator's standards?

Then other more troubling questions begin to surface, some not even acknowledged or articulated. For instance, will sharing the information allow someone else to advance him or herself? At the expense of the person or organization sharing that information? Will appropriate credit be given? Or will the action taken on it be used to illustrate the other agency's superiority? Will it be used for justification to receive a better budget at the expense of the originator? Will it be used at 'my' expense? The questions may even be, 'did they ask for it?' or 'what did they ask for?' The answer to this last question may well miss the point, or fail to have what was wanted or needed passed on if the answer is simply, 'Answer the mail, no more, no less.' What may be useful or critical information, that last piece of the puzzle to put it all together, may not be obvious or may even appear trivial to the person or the analyst who comes across it, and so the information is not passed on.

This all leads to a culture, or a series of organizational cultures, discouraging information sharing. In the past, information sharing has been, or has developed into a sort of 'pull' process -- that is, someone needs to ask for the information. There are exceptions that push or distribute information or intelligence to users who do not ask for it. For example, the terrorist report (TERREP) has been around for some time in the cable and reporting system. Cable messages with this heading receive fairly wide distribution throughout the defense, intelligence and law enforcement counterterrorism communities. But this appears to be more of an exception than the rule.

This author offers that the system must, of necessity, become one of a 'push' of information, including raw intelligence information with its traps and problems, such as

information overload and source reliability and credibility. To do this, one must overcome the tendency and organizational cultures of intelligence generating and using agencies, to include law enforcement agencies, to exclude others from receiving, to not share or publish the information that comes to them. In broad terms, this paper examines that organizational culture and presents some possible solutions. In recent years, the United States' intelligence community has been accused of some fairly spectacular failures -- to include nations' development of nuclear weapons, the September 11, 2001, terrorist attacks, or of a nation *not* having the weapons of mass destruction it was believed to have or be developing.³

The causes of intelligence failures do not revolve around the issue of whether U.S. intelligence is doing its job right. Rather they can be found in all aspects of intelligence, from how the public perceives intelligence to how intelligence agencies perform their specialized tasks, all the way to the specific steps in the intelligence process and how the policy makers use intelligence information.⁴

Critical in this perceived failure are the organizational arrangements and communication processes throughout the Intelligence Community (IC) that appear to account for many of the problems associated with its failures.⁵

This thesis, set as it is against the backdrop of the Global War on Terror (GWOT)⁶, ultimately illustrates that although we have legal structures to enable interagency communication, the structures are not necessarily working the way they are meant to work. For the most part, they are not overcoming the problems they were formed to overcome. Serious barriers to interagency communication are created by both the bureaucracy of gathering, analyzing, and distributing intelligence information in our government, and how members of the agencies forming the IC interact with each other.

Solutions to the communication and information sharing problems *are* out there -- in theory, law, doctrine, and technology.

Procedurally meeting this challenge may be not so easy. How the various agencies go about their business, even in areas where there might be duplication of process if not of work or activity or effort, depends on which agencies are involved. Each has its own processes, practices, rules, regulations, and data bases. For example, most Federal law enforcement agencies conduct training at a single facility, usually in classes where their agents mingle, get to know one another and even live together. However, after they depart the Federal Law Enforcement Training Center, they may never cross paths again. For example, Diplomatic Security Special Agents conduct investigations with different needs and particular data bases than do those in the Treasury Department or the Federal Bureau of Investigation (FBI). Some data bases overlap or are used by multiple agencies. Others do not. Common training and databases notwithstanding, the agencies barely interact at the information-sharing level even yet.

Overcoming the organizational cultures of multiple, disparate agencies, departments and organizations is critical to solving the problem of sharing information and intelligence such that it may be analyzed and utilized by the people who need it. Without changes across a wide range of organizations and their information dissemination policies, the U.S. Government will continue to face problems and needless internal challenges among the agencies that are jointly charged with responsibility for national security.

However, these changes are manageable. They can be effected through direction from the upper echelons of the nation's leadership, aimed at both the willing and the unwilling, to initiate and maintain the structural and cultural alterations to improve the Intelligence Community's interagency interactions to ensure its long-term effectiveness.

III THE INTELLIGENCE COMMUNITY AND “THE INTERAGENCY”

“Intelligence can be defined as the ‘product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas.’”⁷ With the onset of the Global War on Terror, and even prior to it, that definition can be expanded to include information on domestic organizations or individuals that pose some threat to the nation, whether it is terrorist or criminal or counterintelligence. *Information* itself is what is sometimes called *raw intelligence*, the basic data that comes to the attention of a person involved in intelligence gathering or analysis. *Finished intelligence* is that same information after it has been viewed by people who can make an analysis of it, compare it with or add it to other bits of information and intelligence, and use it to make a prediction or add it to the whole of the knowledge on a particular subject.

To conduct intelligence activities -- collection, analysis and dissemination, the United States government has a variety of agencies which, collectively, are known as the Intelligence Community or IC. This Intelligence Community currently consists of 16 major organizations: the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial Intelligence Agency, the National Reconnaissance Office, the Army, Navy, Air Force, Marine Corps and Coast Guard intelligence elements, the Departments of State (DoS), Energy (DoE), Homeland Security (DHS), and Treasury intelligence offices, and the Federal Bureau of Investigation (FBI)⁸ and the Drug Enforcement Agency (DEA). Three of these, the CIA, DIA and State Department’s Bureau of Intelligence and Research (INR) produce all-source, finished intelligence products. The others are primarily concerned with collection or processing more

limited reports within their respective departments.

In the Intelligence Community, in addition to the nation's political leadership, one can clearly identify the needs for analysis by at least three other different types of consumers, sometimes referred to as cops, spies, and soldiers. Their needs produce at least three distinct types of intelligence: investigative or operational, strategic, and tactical.⁹

As such, all government is, to some degree, a collector and user of information or some sort of intelligence. Of the other agencies, some are more overt collectors, analyzers, and users of intelligence than others. Those outside the formal Intelligence Community, such as the Centers for Disease Control, collect information and conduct their analyses on a relatively narrow scale both in use and application, though not necessarily in implication. But of the IC, some eighty percent of the intelligence collection and analysis resources reside within the Department of Defense.¹⁰

The Defense Department's holding of the lion's share of the IC assets creates its own set of problems with regard to coordination and communication. The Secretary of Defense can be viewed as the proverbial '800-lb gorilla' in the community, with power and agency management authority rivaling or even exceeding that of the statutory leader of the community, once the Director of Central Intelligence but now the Director of National Intelligence. Authority issues will be discussed in more detail later in this paper.

Because of this level of authority, a significant portion, if not the majority, of the intelligence information gathered by the United States has military application or implication. Thus, the focus is on a particular type of threat, policy or application and on a relatively narrow area of interest compared to what is available in the world so far as the resources and volume of collection goes. Further, although the uniformed military services (the Army,

Navy, Marine Corps, and Air Force) may not themselves be directly involved in the collection or action taken pursuant to a particular piece of information or analysis, some intelligence the Department of Defense collects may be perceived as having *posse comitatus*¹¹ implications. That is the general prohibition on using the military for domestic law enforcement purposes. Some people may see the application of Defense Department assets to domestic problems as a violation of that law. For example, the National Security Agency, which falls primarily under the Secretary of Defense, has historically been banned from spying or directly collecting information on U.S. citizens and U.S. persons. With the advent of the Global War on Terror, this prohibition has been loosened both in law and in practice.

The agencies in the Intelligence Community interact within the framework of the government. Interactions between two or more agencies are described as “interagency.” The process, relationships, and interplay among the various executive agencies of the United States Government, a sometimes seemingly fragmented conglomeration that has developed over two-and-a-quarter centuries, has contemporarily come to be called ‘*the Interagency*’ as if the adjective were sufficient as a noun to describe it. Perhaps this is a reflection of reality as, with the globalization of the information age and the post-industrial era, once clear lines between economics and politics, government and private sectors, the military and non-military realms of study and operation have become increasingly blurred. “If the interagency process is to be successful, it should bring together the interests of multiple agencies, departments and organizations.... The essence of interagency coordination is the interplay of multiple agencies with individual agendas.”¹² Further, “each agency, department, and organization has different access and a different perspective on the international scene. This

difference can result in a dysfunctional approach to security issues.”¹³ However, there are processes in place to overcome that dysfunctionality, and there have been such processes for some time.

Changing geopolitical priorities, social and governmental shifts, and private and economic developments have nibbled away at the historical decentralization of the U.S. Government as a whole and the IC in its microcosm of that government. Most organizations in the government display both centralized and decentralized structures and administration, somewhat dependent upon what particular activities are involved. The shifts in organizational demands and requirements have multiplied coordination and communication problems within agencies as well as within their interagency activities.¹⁴

“The interagency process at the national level is grounded within the Constitution and established by law in the National Security Act of 1947.”¹⁵ A product of that act, the National Security Council (NSC) “provides the foundation for interagency coordination.”¹⁶ Other statutes govern how sensitive information is classified, handled and disseminated within the government. Among these are the Freedom of Information Act which allows not only public access to U.S. Government data and information, but requires its release under many circumstances, and the Privacy Act of 1974 which governs personal information that may be released to the public or collected and used by the U.S. Government. Over the years since World War II, presidents have issued a series of executive orders to clarify what information is to be classified, how it is to be classified, and who has the authority to classify and declassify information. Additionally, a part of the law known as the *Third Agency Rule*, which states, in effect, that information obtained from a second agency may not be shared with a third agency unless or until cleared by the originating agency, has grown out of these

statutes. This rule, as much as any other, presents a barrier to effective intelligence sharing. Because of this, post September 11, 2001, legislation, such as the USA PATRIOT ACT of 2001¹⁷, weakened *legal* barriers to information and intelligence sharing among intelligence and law enforcement agencies.¹⁸

But this is a recent shift in the workings of the Intelligence Community. History, culture, both at the national and organizational levels, and the way agencies are and were structured have tended to produce patterns of conduct that have ill-served the IC at times. For example, the strict lines of separation drawn between intelligence and law enforcement, even within individual agencies such as the FBI, were put in place to prevent intelligence services from overstepping their bounds. However, the line also inhibited cooperation in investigating terrorism.¹⁹

Terrorist activity, when it occurs within the U.S., has generally been treated as a law enforcement matter rather than a military one. This author believes terrorism that should continue to be a law enforcement matter. Law enforcement officers are often among the very first responders. Additionally, law enforcement agencies have the expertise, background, and *authority* to conduct investigations and inquiries that the military and IC agencies do not. Empowering intelligence or military agents to conduct investigations both diverts them from their primary constitutional purpose and focus -- to defend against the nation's enemies. It would be necessary to form domestic intelligence and investigatory arms to carry out terrorist-tracking and investigation processes. Besides, even in the case of terrorist incidents, empowering the military or the non-law enforcement intelligence agencies as the police force runs against some very deep-set American traditions and beliefs against their use for domestic, internal purposes. The military, in particular, probably has some role in the

apprehension of terrorist suspects, but it has only a supporting role in investigating incidents and in the actual domestic hunt for the nation's enemies off the external battlefield.

IV ORGANIZATIONAL CULTURE INHIBITS COMMUNICATION

The organizational culture school came to be recognized as a legitimate, significant branch of organizational study and theory in the late 1970s and 1980s. It offers a basis from which to begin to understand the inner workings of agencies in the government and how they operate both internally and in their external interactions with each other. *Organizational culture* can be defined as a pattern of shared basic assumptions that a formal group learns as it solves its problems of external adaptation and internal integration. This pattern is one that has been validated over time and, therefore, is taught to new members as the correct way to perceive, think, and feel in relation to those problems.

“[I]t is the culture that exists in an organization, something akin to a societal culture. It is comprised of many intangible things such as values, beliefs, assumptions, perceptions, behavioral norms, artifacts and patterns of behavior. It is the unseen and unobservable force that is always behind organizational activities that can be seen and observed.... [O]rganizational culture is a social energy that moves people to act.”²⁰

In the study of organizations and organizational theory, the word *organization* itself describes an institution “whose primary purpose is to accomplish established goals. Those goals are set by people in positions of formal authority.”²¹

[O]rganizations [may] be viewed as culture-bearing milieux...shared social ideals, frames of reference and symbols for conveying them are indigenous to social systems in organizations, as elsewhere; and ... these aid members in interpreting experience and that they facilitate expression and guide behavior.²²

The organizational culture school of study believes that many organizational behaviors and decisions are virtually ‘predetermined’ by the patterns of basic, almost

unconscious assumptions and beliefs held by the members of an organization. Certain patterns of activities reflecting those assumptions continue to exist and to influence individual and organizational behaviors because they lead to decisions that have usually ‘worked’ for the organization. Some of the agency’s deeply held assumptions continue to influence organizational decisions and behaviors even if the organization’s environment changes. They are the almost forgotten reasons for ‘the way we do things here.’ “Thus a strong organizational culture controls organizational behavior; for example, it can block an organization from making changes needed to adapt to a changing environment.”²³

The members of organizations, like those in more generalized cultures, exhibit characteristics that indicate that, within the milieu of their employment, they are members of a culture. The first component of an organizational culture includes its *core values*. These values, which define the organization at its most basic with regard to mission and internal philosophy, may concern technical issues of its creation. They may be more humanistic, emphasizing the importance or role of the people or the customers it serves.²⁴

Cultural forms, another component of a culture include the various, sometimes unconscious and subtle means of value transmission to both employees and customers or clients. Forms, in its use here, include its special language, jargon, organizational stories, rituals and ceremonies, and physical arrangements such as dress and décor, and help communicate and inculcate the culture, especially to its members. How these are used by the group depends upon, and may be mirrored by the location, employment environment, layout of the site, cohesiveness, and hierarchy, among other things. These forms are not directly or even consciously applied.²⁵

The third component of an organizational culture, and what differentiates it from a

broader study of a societal culture, is the existence of formal management structures, policies and strategies. Through these, managers reinforce the culture's content and underlying values. Strategies, as used here, include overt tools for teaching, supporting, and demonstrating behaviors and attitudes appropriate to the organizations members within both its cultural and statutory contexts. These include recruitment policies, training, compensation, promotion practices, and other management activities.²⁶

Organizations and their cultures serve purposes beneficial to the overall operation of the government and the interagency. For instance, the organizational culture helps pass along the core values of an agency and lays down which ones may not be willfully compromised or violated. Cultures are essential in the training of agencies' employees.

Taking a cultural view of organizational systems and activities serves to solve a practical problem faced by a seemingly ever-increasing number of agencies, both in and out of the government: a rising rate of voluntary turnover at all levels as the overall society becomes more mobile. Organizational theorists recognize the need of new employees to become acculturated, to 'pay their dues,' and in doing so, to 'learn the ropes,' when they enter and establish themselves in unfamiliar organizational settings. This recognition "suggests that some cultural strata is present in any organization, and that its mastery is critical for the well-functioning of new organizational members."²⁷

The importance of organizational culture will come into play again in this paper as it is viewed as an element of reform within the interagency and the intelligence community. With the attacks on the United States on September 11, 2001 (commonly abbreviated as *9/11*), the Intelligence Community has been viewed as having failed the nation. There are those who would argue otherwise. Legitimately they can say that intelligence is not

necessarily a good predictor of a specific event. However, others can counter with the argument that the magnitude of an event such as 9/11 should have made it foreseeable and that, if the information existed and was available, the various members of the IC in particular, if not the interagency as a whole, should have had the awareness to see it coming and even apprehend some if not all of the perpetrators.

In reaction to the 2001 attacks, the structure of the intelligence community itself was cited by the joint congressional investigation into the attacks and by the independent 9/11 Commission as a significant reason for the failure to predict and prevent the incidents. Some people studying the problem and threat of terrorism recommended that the U.S. should have a robust, separate office for homeland security (which came to pass with Congress creating of the Department of Homeland Security). Others said what was needed was a new cabinet-level head of the IC.

However, underlying this discussion is a prevailing cynicism about any real possibility for change. Between the fall of the Berlin Wall and the time the 9/11 Commission issued its final report in the summer of 2004, the Intelligence Community had been subject to no fewer than sixteen federal studies, many of which called for major structural reforms. But the fundamental characteristics of the community had weathered the scrutiny and remained basically unaltered. Part of what makes institutions institutions, after all, is precisely their unwillingness -- or inability -- to change.²⁸

V INFORMATION SHARING, TURF, AND THE ZERO-SUM GAME

“Information is the coin of the realm in interagency operations, as it provides those who possess it a decided advantage in the decision-making process.”²⁹ Theoretically, the accurate exchange of information is a purpose of communication. Distortion or withholding information is dysfunctional to this purpose. However, in organizations, especially government agencies, information may pose a threat or give an advantage, and

communication often has purposes other than just passing information: to influence, especially in the policy realm. Information handling and transfer, rather than dysfunctional, becomes a tool or method for influence. Whether distortion and withholding is intentional or unintentional, and it may be both, it has the potential to affect or even set policy in motion.³⁰

A challenge in effecting interagency organizational change and cooperation is that bureaucratic insecurity and uncertainty result in an intense, and often unseen-to-the-public, competition among agencies to place their concerns as high as possible in policy makers' intelligence requirements lists. Agencies that are outmaneuvered have the potential "to see their requirements either ignored or given short shrift."³¹

"Fragmentation [of the intelligence community] creates competition; competition creates bureaucratic glitches; and bureaucratic impediments lead to communication problems. In fact, communication difficulties are probably the most direct and important result of a culture of competition."³²

As a result, members of the various organizations making up the Intelligence community become part of an 'us-them' process wherein 'they' -- the outsiders -- are not just enemies of the nation, but those outside the individual agencies themselves. 'They' are not to be entirely trusted and so are not given the 'owning' agency's information or the fruits of its labor, or at least not without some sort of payback or *quid pro quo*.

Interagency competition has had considerable almost corrosive effects on intelligence. Intelligence agencies use competitive intelligence gathering, processing, analysis, sharing and release to promote their own agendas, effectively undermining other intelligence agencies and IC members as they seek money, resources, or political face time at the expense of the others. This subverts and corrodes cooperation. "While there is some

utility to competitive intelligence as a variation of ‘peer review,’ the net result more often than not is to stymie a unified intelligence effort.”³³

Members of U.S. Government agencies perceive themselves to be caught in a zero-sum game. That is, in garnering funding and resources, often they are told to organize or reorganize in a resource-neutral environment. They are told to make changes using existing structures, personnel, and funds. Should one need more funding or resources, either these are not forthcoming or they are perceived to be gained by taking money or resources from another organization. Agency personnel worry that theirs might be the agency raided for the resources. Competition can be good or it can be crippling. When it creates an environment where an organization must shine or stand out in the crowd in order to continue to survive or improve itself, it can and does mean that information becomes a commodity in and of itself. If information is shared with another, and that agency acts upon that information and takes sole credit for its use, that using agency may and can gain resources at the expense of the originating agency. Those resources may or may not be used for the purposes that the information, and actions it made possible, were originally intended.

The intelligence process, in its perfect, theoretical form, puts data into an orderly, factual report. The report is then delivered to policy-makers and politicians for their action and use. In this simplified view of the process, the intelligence analyst delivers a flat, factual report to the policy makers and leaders whose job and position and authority lets them sell the action they want or need to take to the public.³⁴

But sometimes between the source and the analyst, or between the analyst and the consumers of that finished intelligence are one or more *gatekeepers* through whom it must pass in order for the agency itself, or other agencies’ members or their clients to access and

use it. The term *gatekeeper* is a term used in journalism studies to describe those who “control the flow of communication through a given channel or network. Any individual in a position through which messages must pass plays the role of gatekeeper to some extent.”³⁵ The control may be formal or informal, statutory or stated by agency policy, practice or operation. Acting as a filter for the information flow, a gatekeeper helps reduce information overload. Thus, not all gatekeeping is negative. However, bureau responsiveness and the policy process as well as the public at large are “poorly served when gatekeepers impede needed access to important policy figures in the bureau or give clientele the runaround.”³⁶ The same is true if, instead of the runaround, those in the gatekeeper role twist how or what information is released.

Consider the following scenario. One agency might develop information on the whereabouts of a high-profile terrorist target. That information is passed to the second agency because it has jurisdiction over the target. The capture of the target is determined to be efficacious to the Global War on Terror. The originating agency’s agents coordinate the take-down of the target with yet a third agency, perhaps because its personnel are on the ground in the area, or have the local credibility to organize the action. The target individual is subsequently passed to the second agency for transport and processing. In the press releases that follow, the announcement is made that “Agency B has taken the Subject into custody for prosecution.” Pictures are released of the subject being transported by the second agency. The barest details of the arrest are given, perhaps to the extent that the agency’s personnel were there for the arrest (they were -- as support or in contact from the outside perimeter of the event) and with some minor credit given to the local arresting officers. In the public’s eyes, the second, higher-profile agency is the hero. Its leaders and advocates can

then ask for, and receive, further funding that might have otherwise been given to the information-originating agency to better enable its personnel to interact with its sources of information in other, related areas. But the second agency uses those funds to further its own ends and to expand its personnel recruiting and training budgets in areas not or only barely related to the investigations or programs that lead to the gathering of the information on the high-profile target. Subsequently, the first agency's resources are reduced, and the agent gaining the information is transferred and not replaced, the information originator's sources dry up and other useful information is missed or never gathered or never passed on or perhaps is not able to be passed on. Eventually some event happens that might have been preventable had even the status quo been maintained.

Or in another example, an agency might develop information useful in prosecuting a target. However, a second agency is also following and investigating that same individual. Its agents ask for the originator's information, but rather than enable or integrate the first agency into their investigative effort, the second agency's personnel stonewall or even cause the other investigation to be closed. Later the target is arrested and, once again, sole credit is taken by the second agency without acknowledgement of the originator's efforts, even though fruits of that investigation are used in developing the case against the target. And again, the second agency is able to paint itself as the deserving organization for resources.

What comes to pass is something like this:

The CIA's failure to share information on al-Midhar and Alhamzi (hijackers in the 9/11 incident) blinded other government agencies when they encountered the pair. When, for instance, al-Midhar was in Saudi Arabia in June, his visa expired. Since he was not on any watch list, the State Department's consular office in Saudi Arabia routinely issued a new one. When Alhamzi was pulled over for speeding in April 2001 by an Oklahoma state trooper, the policeman ran his driver's license through the database and checked the registration to make sure that there was no arrest warrant and that

the car was not stolen. A listing by the FBI on their terror watch list would have ended Alhamzi's odyssey then, but without any sharing from the CIA, Alhamzi left with just two tickets totaling \$138. (He had not paid them by September 11.)

Even more disturbing was that if the CIA had passed their names as risks to the Transportation Department, they would have been on a list that would have cross-checked them against all airline reservations. Both al-Midhar and Alhamzi used their own names when making reservations on American Airlines Flight 77, which was flown into the Pentagon.

On August 23, almost twenty months after al-Midhar and Alhamzi had entered the U.S., the CIA notified the INS that their names should be placed on the terrorist watch list. The INS ran the names through their computer database and then informed the CIA and the FBI that the men were already in the country. The CIA, of course, already knew this but said nothing.

The FBI, aware for the first time that two suspected terrorists were somewhere in the U.S., curiously never notified Clarke's Counterterrorism Security Group or the White House, either one of which could have mobilized much greater federal resources in hunting the two.³⁷

This sort of behavior leads to interagency distrust and the refusal, later on, of other organizations to assist that agency in both large and small things. Information is withheld or shared only grudgingly, especially as it becomes clear that sharing has become a one-way process and that credit is not going to be given where it is due.

At least two significant messages have been sent at the interagency level as this unfolds. First, within the agency that has received or withheld the information, its members are reinforced in their perception of their superiority and primacy. Their view that they and their agency are the worthy ones and that others are not is validated. This leads to an arrogance and belief that theirs is the agency to be fed, that other agencies exist to serve and work with them. It does not necessarily follow that the receiving agency should also work with and feed intelligence to others, even in return for information that leads to its success.

The second message sent is to the external agencies and is a variant on the first one.

This is that, “You exist to serve us. We’re the lead. You just feed us the information and we’ll handle the problem ourselves.” In effect, there is little working with others, or at least no sharing of the benefits or publicity gained for the information originator’s efforts.

Later, when that second, receiving agency’s agents come under scrutiny of others, even in the execution of their duties, they may well be disadvantaged to the detriment of their activities just because of who they are and for whom they work.

Perception may not quite be reflective of reality, however. A long-time member of the Department of Defense observed to the author that,

The budget is not completely a ‘zero sum game.’ Normally, the competition in the Executive Branch is sensitive to the strategy -- in this case, global in nature. The Department must make a strong case for the capability -- in this case, additional personnel. Finally, there is the possibility, though perhaps slight, that some prioritization can take place to find bill payers in the department. One cultural point, in the government, especially the Executive, is that poaching on the resources of others rarely produces anything more than problems and cuts rather than providing solutions and adds.³⁸

For all the truth in that observation, at the levels where the information sharing should often be going on, the perception of the zero sum game has as much impact as if it were reality. Therefore, agencies act as if it is real.

For another example, “The FBI’s jealousy over its counterintelligence turf, not only vis-à-vis the CIA but also vis-à-vis the military services’ counterintelligence analysis (as well as operations), is a similar symptom of structural problems.”³⁹

Furthermore, as a culture, the Intelligence Community has been accused of obsession both with secrecy and with some degree of its own internal agency version of political correctness, sometimes to the point of apparent stupidity. The Army, a year after September 11, 2001, fired Arab linguists because they were gay, and the Army’s policy is that gays are not to be hired, or if discovered, kept in employment regardless of their utility or need. The

CIA has fewer than 1,100 case officers overseas. For a comparison of national priorities, the FBI has more agents in its New York Field Office.⁴⁰

Finally, “while ‘information sharing’ has become almost a buzzword in the aftermath of 9/11, existing procedures, with each of the intelligence agencies controlling the information they produce, make it difficult to share across the community, much less with other governments or state and local authorities. “More generally, innovations in intelligence *analysis* run smack into existing security procedures, which are designed to limit information to those with a ‘need to know,’”⁴¹ and to prevent its wider sharing. The problem is that insights are likely to be gained from outsiders who come to the information with new perspectives, who have had no perceived need to know before. “The fundamental challenge is reshaping how the U.S. government thinks of information, and how information should be used and controlled.”⁴²

A critical problem of *who’s in charge?*, both of the overall effort and of the various agencies’ outputs continues to vex interagency efforts.

In the past, the concept of a designated lead agency did not carry with it the operational authority to enjoin cooperation. The executive and legislative branches have not seen fit to routinely provide interagency leadership with direct control over the resources necessary for interagency operations.⁴³

The question is how to overcome these problems of the perceived zero-sum game in the interagency and the Intelligence Community and structure the process and organizations to better communicate with each other and to better share information coming to their members? It’s not likely that Congress or the elected leaders and their appointees making the budget will change their stripes or procedures. The interagency will remain, to some degree, a zero-sum game. The solution may be to revise the interagency, to simplify or consolidate it, within certain functions at least.

In general, the Intelligence Community's agencies' structures individually, and in the IC collectively, reflect the way that this group of agencies came into being over time, based on intelligence disciplines that varied in their operational concepts, technologies, applications, and customer communities.

Human Intelligence (HUMINT), for example, at the national level serves national intelligence requirements. Within the armed services, however, HUMINT often serves theater and tactical operational needs.... Imagery Intelligence (IMINT) and Signals Intelligence (SIGINT) have served both national and tactical customers.... SIGINT, in contrast, has developed infrastructures dedicated to specific national systems and targets as well as other infrastructures that support the war fighter more directly.⁴⁴

At the end of the Cold War, and with the rise of the GWOT and its changing intelligence demands, environmental changes for the Intelligence Community and the geopolitical and social world in which it was modeled, have created a need for a much more integrated Intelligence Community system. Indeed, this environmental change has offered a powerful opportunity for considerable restructuring and two significant alterations in function and interaction. This opportunity, if mishandled, might well be missed.

The missions supported by the IC are less and less likely than during the Cold War to be characterized by clear divisions between national, strategic and tactical, political, economic, law enforcement and military intelligence. These varying aspects have, with globalization of crime, economics, trade, military technology, and terror users, become more interrelated and their lines blurred. "For example, a complete picture of another nation's WMD program must convey not only that nation's...relations with nations that may be supplying the technology (or to which it may be supplying technology), but also the electronic intelligence (ELINT) regarding specific systems."⁴⁵

The second change allows for more integration among the IC's components.

Information technology advances present the opportunity for integrating and consolidating some aspects of the United States' national intelligence capabilities, characterized by joint efforts and interplay rather than by the individual infrastructures traditionally associated with each intelligence discipline and agency.

According to a 2004 Armed Forces Communications and Electronics Association (AFCEA) White Paper,

Contemporary information technology enables large enterprises to manage disparate infrastructures uniformly in support of a wide range of customers and products.

A Director of Central Intelligence-led offsite in November 2003 reached similar conclusions. That offsite called for “*expeditious sharing of collected data and full information transparency enabled by tagging data at or as close to the source of data as possible.*” It recognized the need, across the Community, for “*commercial-sector models – Enterprise Management, Enterprise Portfolio Management, and Enterprise Architectures*” as well as “*commercially available...tools [that] can help an analyst discern and understand obscure linkages between individuals, activities, and methods of operation...*” Finally, the offsite called for Community-wide “*tagging standards allow the use of sophisticated “analytic discovery” tools to further refine both queries and answers.*”⁴⁶ (Emphasis is in the original.)

Observations made in this offsite offered the possibility for Community-wide analytic standards and architecture serving an integrated Intelligence Community.⁴⁷

Of course, there are obstacles to significant intelligence structural reorganization. The intelligence community agencies collectively are one. Bureaucratic self-protection has a considerable place in the opposition. Additionally, some Congressional committees have historically presented roadblocks to increases in the powers of the Director of Central Intelligence. For example, the armed services committees tend to prevent significant reduction in military control over intelligence activities.

There is, however, at least one more reason that may explain, in part, why many radical reorganization proposals fail -- or at least it provides a

justification for why they should have failed. That reason is a simple one. Many of the proposals are simply *bad ideas* [emphasis in the original] -- either because they would be achieved at the cost of significant organizational disruption without commensurate benefits, or because they would actually do more harm than good.⁴⁸

What may be required is restructuring on the magnitude of that brought about in the National Security Act of 1947 that created the Central Intelligence Agency. For instance,

The solution to this nonsense argument about raw intelligence versus all-source intelligence is to have both. To do so requires a second model of intelligence analysis in addition to the central processing model demanded by proponents of all-source exclusivity. The distributed processing model...makes it possible for users to receive tailored analysis done close to the decision maker by intelligence analysts familiar with the user's unique needs.⁴⁹

Thus far, reforms proposed for the IC, especially in reaction to the events of September 11, 2001, seem to treat the problems revealed in hearings and investigations of what might have gone wrong in the Intelligence Community primarily as policy matters, ignoring underlying structural issues.⁵⁰ Perhaps the most radical suggestion has been to establish a Department of National Security by merging significant portions of the Departments of Defense, State, Justice, Energy, the Central Intelligence Agency, and the Federal Emergency Management Agency (FEMA) in order to meet future national security challenges and demands.⁵¹

This was partially accomplished in the creation of the Department of Homeland Security (DHS) in 2002. That brought together a number of agencies that were, by and large, law enforcement focused. However, with the exception of the Coast Guard, none of the agencies rolled into the DHS were members of the Intelligence Community. As such, although a consumer of intelligence, there is relatively little experience with the intricacies of the relations within the IC in DHS. This is an aspect of its organizational culture and its

members' networking that can only be overcome with time. The intelligence gathering and analysis functions needed for conduct of the security strategy and operations of the U.S. Government generally remain with the agencies where they were located prior to the President's declaration of the Global War on Terror⁵². Some 80 percent of the Intelligence Community still remains in the Department of Defense. Domestically, most terrorism-related intelligence gathering, analysis, and dissemination continue to reside with the Federal Bureau of Investigation. The Department of Homeland Security started out with only half the tools it needs to conduct its mission.

Of course, the question may be not how to get the organizations to cooperate, but whether the organizations that make up the Intelligence Community should continue to exist in their current state. Large, mature organizations are notoriously difficult to change either structurally or procedurally. The majority of the agencies making up the IC are just that -- large and mature. The recently created Department of Homeland Security may not be considered mature in and of itself, but its component agencies are. The National Counterterrorism Center (NCTC), also new, consists heavily of personnel who were formerly employed by other IC agencies and so they were socialized into organizations not prone to willing information sharing either.

“Every organization has a unique culture that is defined partly by its structure, history, and policies. For that culture to endure, it must be transmitted from current members to new members. This process, known as organizational socialization, is especially important in organizations with strong, insular cultures, as those with weak cultures have less to transmit and will tend to experience culture changes as members come and go.”⁵³

It may be that to bring the intelligence community to heel, its constituent organizations need to be markedly restructured, or even more radically, the IC gathering and analytical functions may need to be brought together under a single head. However,

reshaping both intelligence and security to effectively confront future threats may require considerable change in culture even beyond the organization. These changes, even if ultimately deemed socially, politically, and nationally acceptable, will not come soon. In the near term, a number of smaller proposals can at least ameliorate some of the more immediate problems within the IC.

For example, the 9/11 Commission suggested that reports start with separating information and sources and that they be written at a level that can be relatively easily shared right from the start. “If intelligence consumers wanted more, they could query the system under whatever rules were in place, leaving an audit trail of requests.”⁵⁴ An ongoing problem this would also begin to address is that many potential consumers do not even know what to ask for, or what the right question to ask might be. Perhaps they do not even know whom to ask or if the possibility of the intelligence being available exists.⁵⁵

The opportunity for a smart reform exists just now. The figurative window is open, but no one knows for how long.

The CIA and the FBI successfully fought to avoid being pulled into the Department of Homeland Security, but

The Intelligence Community itself, as in 1947, [still] desperately needs its own structural reforms. They must be done separately from homeland security reorganization, however, or dysfunctions will be increased, not reduced...A great deal is at stake today, not just in intelligence reform, but also in homeland security reform.⁵⁶

Exacerbating the problems surrounding issues of authority and resourcing is the lack of an agreed interagency planning process that might synchronize interagency effort. Decentralized operations in the field require cogent strategies and plans to inform the operator of his agency’s objectives, concepts for operating, and available resources. Agencies will continue to be prone to talking past each other as they plan and program according to different priorities, schedules, and operating areas.⁵⁷

The State Department offers much as an example of interagency planning and operation. Of all the cabinet agencies, it has perhaps the greatest experience operating in the interagency environment. Each embassy has its Country Team, composed of the senior members of all the offices and agencies represented at the embassy. In some places, there are more non-State personnel connected with the mission than there are State employees. Embassies represent, then, a microcosm example of the working interagency. Country teams meet under the leadership of the Ambassador and Deputy Chief of Mission to both discuss the week-to-week operations, make the embassy's long-term plans, and to coordinate embassy efforts in a crisis. The country team could be used as the beginning template for a working interagency process.⁵⁸

The nature of a Country Team, that it is small, that its members are both accustomed to working together and are senior enough to make decisions within their sections, offers both a template for the relationships and the model for information passing. "Dissemination, of course, involves getting usable intelligence products to the appropriate users.... [It] is at root a communications issue."⁵⁹

Lastly, the Department of State, though the oldest of the Cabinet Departments, is and always has been one of the smallest. It continues to be perceived to be made up of some of the best and brightest in the government's bureaucracy due to its selection process. Because of its clientele and remoteness, with its missions located outside U.S. territory and Washington, DC, it is also often viewed as one of the weakest of the Federal Government's departments. It is, in its own way, nonthreatening bureaucratically. It is simply not well-positioned to snatch other agencies' responsibilities and resources. Within this framework, it could be used to manage many of the interagency aspects of the Intelligence Community.

The significant shortcoming in using the Country Team model in the interagency process and structure is that it demands collegiality among the participants. Collegiality is developed through long-term relationship building and networking that may not entirely be affirmed, sustained, or formed simply due to the changeover and assignment cycles of the Interagency's member organizations.

Stable, structured organizational networks and individual agency and even people's roles within those structures are important from both theoretical and applied management perspectives. It is a matter of strategic and operational importance, for example, for organizations to consider their need for liaisons within their own structures and with other agencies that might be working on different aspects of the same problem and where that need for liaison is located. Liaison activities may need to be created formally where they do not exist informally.⁶⁰ It is in this context that the interagency forms task forces and fusion centers.

VI THE ROLE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

In the private sector, the information revolution has forced many commercial organizations to change from their traditional, industrial era hierarchical, top-down, structures to more organic networks of cross-functional teams. However, government agencies, including Intelligence Community, have tended not to fundamentally embrace these changes -- but then, neither have the United States' political leaders.⁶¹

Periodic reorganization takes place within Federal Government agencies anyway. This is a basic fact of bureaucratic and organizational reality. Reorganizations take place serving both political ends and to improve operational abilities -- and hopefully both at the

same time. The debates surrounding changes in organizational missions and their altering their structures to meet those changes support and work toward a variety of programmatic and political ends and objectives. Arguments revolving around centralization and decentralization, or the degree of either that should take place, are significant and critical to the end result and outcome. A centralized structure consolidates power and authority in the hands of a few individuals; decentralizing may expedite work, but it also raises the visibility of particular offices. “Mergers of previously specialized offices can highlight, dilute, or conceal their work. Placing program implementation authority in a weak, low-profile office essentially determines the program’s fate, and therefore is an element of program strategy.”⁶²

The terms *centralization* and *decentralization* (emphasis in the original) refer to the degree to which decision-making authority is confined to the top echelons of the bureau or assigned to the lower echelon offices and officials....Decentralized structures, by definition, permit greater autonomy in the bureau’s subdivisions and make broad participation in some decisions possible...In an extremely decentralized structure, there may be no one watching for new opportunities for the *whole* organization or for new activities requiring cross-program coordination.

Centralization, on the other hand, can be used to achieve greater control, to monitor operations, and to clarify policymaking and communication channels.⁶³

For the moment, demands for centralization seem to be ascendant in the debate. As such, the National Security Act of 2004 created the office of the Director of National Intelligence to overcome a long-standing problem in the Intelligence Community. The “double-hatting [of] the Director of Central Intelligence [in the National Security Act of 1947] as the director of the CIA limited his ability to stand above and orchestrate the whole intelligence community. Instead, he became a prisoner of the CIA and shared its insecurity about control over other agencies’ resources and turf.”⁶⁴

It may be that, with the creation of the DNI’s office, the system demands still more,

and also more radical or extensive reorganization. The DNI may hold the seeds of consolidation for the Intelligence Community. And perhaps that is what it needs, at least where analysis is concerned: a single, all-source analytical site where all the collectors send their information and from which all users may draw on intelligence, both finished and raw. However, a problem in the creation of the office of the Director of National Intelligence (DNI) is that this office now has added yet another bureaucratic staff and layer to the process.

Under the Intelligence Reform and Terrorism Prevention Act of 2004, the DNI serves as the president's chief intelligence adviser, and oversees changing and improving personnel policies and technology programs, at least in principle, across the broad IC. Among the technical programs assigned for management is the creation of a comprehensive 'Information Sharing Environment' in the Interagency. Supposedly the DNI is also the author of the IC budget. In theory, this should be a relatively powerful position.⁶⁵

However, that theoretical power may not truly amount to all that much. The legislation limits the Office of the DNI to a permanent staff of 500 people. Three hundred of these will be transfers from the 'community management' staff at the CIA. Only 150 of the others may be transferred from existing IC agencies. The law also mandates that the DNI's office is not to be located in the White House or at any existing IC facility.⁶⁶ In reality and practice, the DNI has a comparatively small staff and an office location remote from its supposedly subordinate agencies and its primary customers, the policy makers and senior leadership of the U.S. Government.⁶⁷ "In the context of the intelligence community, the DNI has no troops."⁶⁸

A further barrier to any real empowerment of the DNI lies with its budget control, or rather, lack of control.

In principle, DNIs will have considerable programmatic authority: They will develop the National Intelligence Program (NIP) and broad personnel policy for civilians in all the agencies. In that sense, the DNI's authority over the nation's intelligence budget is roughly comparable to that of the Secretary of Defense over total defense spending. The limitations on DNI authority are more apparent at the level of *execution*—for instance, the restriction on moving more than a hundred people to any particular new joint intelligence center. Beyond the hundred, the DNI will, like the DCI before him, have to bargain with the other agency heads. The 5 percent limit also applies to the DNI's authority to *reprogram* budgeted money without congressional approval. To be sure, 5 percent of a big agency budget is a lot of money, especially in the context of the DNI's programming authority.⁶⁹

The law actually restricts the DNI from reprogramming or moving more than five percent of any given agency's budget or \$150 million, whichever is smaller, from one agency in one year.⁷⁰ In the overall scheme of the various intelligence agencies, this amount seems to border on paltry, especially in the context of the United States' trillion-dollar budget. That said, the power to reprogram funds does have considerable symbolic power -- if the DNI is willing to use it. Even a relatively small amount moved can indicate displeasure or desire for a new focus.

VII INTERAGENCY CHANGES IN SYSTEMS AND STRUCTURES

Critical to the Intelligence Community's reorganization, and critical even if no other significant actual reorganization or consolidation or transfer of function takes place, is one single significant reform. Regardless of whatever leadership and legislation demands of the Intelligence Community organizations, they will be able to remain isolated from each other, able to withhold information, keep their own secrets, so long as their communication and analytical information processing formats and architecture remain separate. A standardized, centralized (with multiple, dispersed back-ups) accessible-to-all architecture is key to forcing

their cooperation. Clearance level and need-to-know controls can be enforced through access permissions on the part of individual users. This technological adoption and adaptation may well trigger the organizational change necessary to create a cooperative Intelligence Community.

There are three basic approaches to achieving an information-sharing systems architectural end. In the first, the IC, whether by committee or by DNI direction, would define systems to be used by individual agencies. This approach relies on each agency's own engineering and acquisition programs, practices and methods.

In the second approach, the IC would somehow manage enterprise architecture, design, and acquisitions. The acquisition of integrating capabilities and technologies would be conducted to unify infrastructure.

Both of these approaches are already in use to some extent.⁷¹

The Armed Forces Communications and Electronics Association (AFCEA) has suggested a third approach that is already proven in the private sector and takes

advantage of emerging information technologies as they become available, and focuses...on satisfying a wide range of customers. This model allows for the continued autonomy of major components of an industry. At the same time, the model creates *new business processes* serving a wide variety of participants. The rise of business-to-business (B-to-B) exchanges that link data, create knowledge, and allow for swift transactions among a wide variety of participants, is an example of this model. Some of these exchanges encompass entire industries. For example, Covisint,...[was] formed by DaimlerChrysler, Ford, General Motors and Renault-Nissan...to reduce waste and improve customer response...A host company can use the Covisint community portal, or Covisint can customize a portal that can extend a customer's current enterprise systems out to its suppliers in a safe and secure manner. In essence, the Covisint B-to-B model allows for the flexible configuration of 'extranets' serving a variety of participants.⁷²

This model, although not requiring the complete integration of existing systems, "does require a high degree of cooperation, collaboration, joint development, agreement on

common business processes at a wide variety of points along each participant's value chain, and recognition of the value resulting products bring to customers."⁷³

The challenge in creating such a system lies in how to allow analysts and subsequently policymakers access to information while avoiding information overload. The IC is and will continue to be called upon to balance increasingly capable collection, analysis, and storage systems with the dissemination of data and a realistic understanding of important developments. While doing this, continued precautions will be necessary to preserve civil liberties and American cultural values.

The expense of a single, new system to collect, process, and analyze the huge volumes of information the U.S. Government can obtain and generate is also relevant to discussions of policy at the legislative and budget-making levels.⁷⁴ The short-term costs of information consolidation, while incredibly high, would be ameliorated in the long run by the relative simplicity of having to maintain only one system rather than several and by the sheer volume or bulk of sales that a discount could be demanded of suppliers.

There is no shortage of tool-building going on—at the CIA's In-Q-Tel, and Advanced Technology Programs; at the Intelligence Community's Advanced Research and Development Activity, and Intelligence Information Innovation Center; or with the Pentagon's Defense Advanced Research Projects Agency. The initiatives are focused on mining large data sets but also remembering discarded hypotheses and seeing new patterns, as well as providing analysts with better ways of working together. As yet, however, the initiatives are scattered and are all too often driven by technology. With no clearinghouse for matching what analysts want and what technology can provide, innovations run the risk of remaining just fancy bits of technology, not real advances in analytic method. So, a DNI ought to move to create a focal point for tool-building and innovation in using these tools. If, for instance, all analysts had, more or less, similar workstations, that would facilitate moving them around the Intelligence Community, including into newly created centers. So, too, a focal point for learning lessons would make sense. Now, postmortems, like that over the error of U.S. estimates about WMD in Iraq, are usually conducted in the full glare of publicity and so run more toward assessing blame than learning how to do better.⁷⁵

Another example of an expandable existing data base, the Treasury Department's Treasury Enforcement Communications System (TECS), is already familiar to Federal Law Enforcement agencies and officers. It is thorough and simple. It may be searched with minimal information at the start. A small amount of data leads to a basic page that is linked to multiple subsequent pages containing more in-depth information. TECS has its shortcomings. For example, because it is based on old technology, it is difficult to enter a search using a soundex, or a spelling variant on a name. However, it offers a viable, familiar, in-place starting point for the using community for information entry and sharing. Of course, with all the information available in the system, TECS can overload the user, forcing investigators and analysts to perform the equivalent of a brute-force search when confronted with multiple hits on a query. To overcome this, as well as to make more efficient their investigations, investigative systems personnel and managers in some Federal law enforcement agencies, such as the State Department's Diplomatic Security Service, have been involved in researching and working on architecture and permits to cause investigative data bases to better 'talk to each other' in order to save time and effort in conducting criminal and terrorist investigations and inquiries.

Beyond changing technical systems, overcoming the bureaucratic inertia among competing and complementary agencies has not been and will continue not to be an easy task. Entrenched, mature bureaucracies tend to resist changes to their founding goals or to diversions from their traditional missions. However, because of the nature and character of contemporary national security threats, "there is growing realization in and out of the intelligence community that fusion centers [or other forms of interagency cooperative agreements and practices] can help overcome the deleterious effects of institutional

myopia.”⁷⁶ Further, military, law enforcement and intelligence agencies are all being forced to review and revise how they have historically worked together or failed to work with one another.

An example of how law enforcement and intelligence agencies might operate together is found in Canada, perhaps the United States’ nearest comparison culturally for all the differences among the two nations. There, agencies without law enforcement powers conduct investigations that can result in criminal charges and arrest warrants. Upon conclusion of their investigations, their investigative files and information are turned over to the Royal Canadian Mounted Police, who do have law enforcement authority for service of the resulting warrants. The Mounties, either on their own or with the assistance of the investigating agency, conduct the necessary searches or hunts for the suspects and make the arrests. Beyond this, the Canadian Security Intelligence Service serves as a potential model for use in forming a domestic intelligence program that continues to preserve civil liberties.⁷⁷

In a similar vein to the interagency relationship in Canada, the United States Marshal’s Service receives all warrants from all agencies conducting criminal investigations and has the power to effect arrests pursuant to those warrants. The Marshals are, in fact, the agency with the mandate to make all federal arrests pursuant to warrants resulting from federal criminal investigations. While approximately 70 other federal agencies have arrest authority, most are limited in some manner, usually to warrants or crimes arising from the specific set of statutes they are charged with investigating. For instance, Internal Revenue Service Special Agents investigate tax and revenue code violations; the Bureau of Diplomatic Security investigates passport and visa fraud for the Department of State. The Marshals Service, while not a criminal investigative agency itself, is charged with apprehending the

target of any federal warrant, regardless of what agency conducted the investigation.

As alluded to earlier, others have noted that “surmounting institutional parochialism is a must if the chances for intelligence failures are to be reduced. [They have suggested that] the way to do that without upsetting bureaucratic sensibilities too much is to expand the use of interagency task forces and fusion centers.”⁷⁸ Task forces are groupings of members of multiple agencies charged with focusing on and overcoming a particular problem. For example, the FBI heads Joint Terrorism Task Forces (JTTFs) stationed in cities all over the U.S. JTTFs bring together law enforcement agents and intelligence analysts from both the Interagency and even state and local offices for the purpose of investigating and apprehending terrorism suspects.

Fusion centers are sites and organizations focusing on intelligence and analysis of certain tasks or threats. One of the best known in the current milieu is probably the National Counterterrorism Center. Established in 2004 under the office of the DNI, the “NCTC comprises employees from the CIA, FBI, the Departments of State, Defense, Homeland Security, Energy, Treasury, Agriculture, Transportation, and Health and Human Services, the Nuclear Regulatory Commission, and the US Capitol Hill Police. The Center provides a unique environment to optimize the USG's collective knowledge and formidable capabilities to identify and counter the terrorist threat to the nation.”⁷⁹

Policy on and in the fusion centers already in existence continues to present several problems:

One, there are bureaucratic issues inherent in properly defining a center’s role in the intelligence community, and turf battles often occur. Since the establishment of the first center in 1986, critics in the intelligence community have constantly complained that the centers really are not community organizations at all, since the CIA dominates them.⁸⁰

[On the face of it, overcoming such criticisms appears relatively easy. Using the NCTC as an example or prototype, an initial] step in making the centers more effective would be to move them out of the CIA and put them at a neutral location accessible to all the relevant intelligence agencies. The second step would be to spell out clearly each center's mission, provide each center with its own budget, and establish a personnel system in each center that would link with, but be independent of, specific agency funds and personnel systems. The third step would be to authorize the DNI to provide incentives for people in each of the intelligence agencies to serve in the centers and make such service a positive career move.⁸¹

“Indiscriminately proliferating task forces and fusion centers, however, poses the real danger of defeating the idea of integration.”⁸² The fusion centers are, by their nature, somewhat *ad hoc* constructs. The problem with this is that ‘*ad hoc*cracy’ tends to be a relatively short-term solution to a challenge. The day-to-day working relations in an ad hoc organization such as a task force or fusion center are, by their nature, not formed for the long term. Personnel from multiple agencies bring their agencies’ points of view it is true, but they also bring their agencies’ biases and rules and regulations that may conflict with those of the fusion center or task force -- if that entity has any.

A challenge the individual faces when assigned to a task-organized, ad hoc or otherwise irregular group, sometimes administratively as well as organizationally and culturally may be in answering to the interagency as well as to the individual's own organization and normal chain of command. Just because he or she understands or acts to share information, his or her own superiors may be reluctant or even opposed to certain information or data sharing. On the personnel side, reorganization requires that the Interagency be recognized as a legitimate claimant upon an agency's personnel. As such, those detailed to the fusion centers need to be taken care of and recognized for promotion on par with their counterparts in the agency who do not take the outside positions. The Goldwater-Nichols Department of Defense Reorganization Act of 1986, reorganizing the

Department of Defense to create and institutionalize a joint structure within the military, included the sentence, "Promotion rates of officers on the Joint Staff shall be equal to or greater than the promotion rates of officers on the military headquarters staffs." The intent was to give an incentive to and protect those who took tours and operated in the military version of the interagency, the joint environment.⁸³

Through the fusion centers and among personnel assigned long-term to task forces, members of the Interagency begin forming those informally networked communities of practice that allow professionals to interact, to exchange methodological and institutional information, to post and respond to individual cases and investigations, and to develop *ad hoc* teams of experts for specific problems or tasks. Expanding upon this, creating semi-formalized variations upon these communities of practice "with simple search tools, basic database software, and a simple network visualization interface, any analyst in the Intelligence Community would be able to identify any other expert whose domain specialty was needed to answer a specific question or solve a specific problem."⁸⁴

Such a knowledge management structure would also provide for a degree of professional mentoring within the network and the Intelligence Community. Newcomers would be able to find experts and to establish mutually beneficial relationships. Many agencies already encourage internal mentoring and networking. Improved interagency activities could improve and expand that sort of professional development and widen institutional knowledge. "With appropriate incentives, experts would be encouraged to contribute to the network and make available their time and expertise for the purpose of mentoring."⁸⁵

This sort of networking, mentoring, communication and information sharing among

the Interagency is also a first step toward overcoming a challenge faced by all government agencies: the loss of corporate and institutional knowledge and memory caused by employee attrition and the lack of central knowledge repositories for capturing “lessons learned.” The Department of Defense, the Department of Energy and the National Aeronautics and Space Administration, maintain internal centers for lessons learned for their employees as do many corporations.⁸⁶ Such centers act as information repositories of records and histories of successful and unsuccessful operations and activities. Their intent is to reduce organizational redundancy and error or failure by tracking, analyzing, and reporting after-action reviews and analytic outcome data. Another function these centers help fulfill is the establishment of networks for communities of practice within or among companies, agencies and other organizations.⁸⁷ Improved interfacing architecture would help remedy and expand this aspect of knowledge administration. It would also help in allowing other agencies to vicariously learn from the successes, failures and experiments of their Interagency counterparts.

Architecturally linked communities of practice would include mentoring, analytic practice groups, contacts, and both off- and on-line resources including data bases, information or forums on emerging threats, and methodology for analysis and problem solving. Each community would have or create a central repository of lessons learned, coupled with a comprehensive index available to all, that would be based on spot and after-action reports. These repositories would also include formal reviews of strategic intelligence products to find the reasons underlying both errors and failures and also successes. “These communities could also begin to reshape organizations by rethinking organizational designs, developing more formal socialization programs, testing group configurations for effectiveness, and doing the same for management and leadership practices.”⁸⁸

Finally, in any restructuring of the IC, whether through restructuring agencies, creating new ones, or increasing the number and types of task forces or fusion centers, it is important that domestic intelligence functions should be incorporated with both law enforcement and foreign intelligence activities and analysis where necessary and relevant. The 9/11 terrorist attacks showed that the traditional divides between law enforcement, domestic intelligence, and foreign intelligence is no longer meaningful. That tradition needs replacement with new concepts of intelligence seamlessly linking all aspects of intelligence where the defense of the nation is at stake.⁸⁹

A further barrier to information sharing, whether within the Interagency or with the public in general, lies in the very nature of classified information: that “There are secrets and there are secrets.” Telling the difference between the two, determining what is or should actually be classified, creates the challenge. Coming up with a workable approach to securing intelligence that makes sense to those with classification authority, to those who use the intelligence, and even perhaps to those who are told they have no ‘need to know’ has long been one of the more challenging tasks faced by the executive. The United States government needs the power and authority to keep those secrets that actually matter. The rest of the information it has needs to be accessible by those who can use and benefit from it.⁹⁰ “Secrecy...impedes communication. U.S. intelligence has a track record of overclassifying information, which has impeded the smooth flow of information between producers of intelligence and consumers of intelligence...Information not known cannot be acted upon.”⁹¹

While serving overseas, this author received information relating to a possible threat against a U.S. citizen. During the preparation of his report, he was directed by another

Embassy official, who had some stake in the matter and so had clearing authority on the cable, to increase the classification the author had assigned to it. The official's primary reason, given that the information was somewhat sensitive, was that he had been briefed and taught that, 'when in doubt, classify it.' Within a week, in order to facilitate the threat's investigation by other agencies and governments, the author had, with the concurrence of that same Embassy officer who had directed its classification, downgraded the report to a level where the information could be shared with persons without security clearances but who could assist in investigating the threat.

Critical in interagency organizational cultural reform is the proper classification, clearance and distribution of information. The nature of intelligence, both criminal and non-criminal, requires protection of the means of gathering information and the sources of intelligence. That protection has been significant in limiting the various intelligence agencies' abilities and in justifying inclinations to not communicate with each other. Legal strictures and structures, such as limiting when and where and upon whom a given agency can gather and maintain information and with whom they may share it, have further limited their effectiveness and the usefulness of the information and the ability of others either to use it or to act upon it. For example, the restrictions on the Central Intelligence Agency's gathering and data basing of information on American citizens and other U.S. persons have limited some opportunities in gaining critical intelligence on potential terrorists. It is certainly not beyond the realm of possibility that terrorist organizations may have attempted to recruit U.S. citizens because of their awareness of this limit. Further, limits on sharing information between the intelligence and law enforcement communities are sometimes overly tightly interpreted and applied. These limits have been, as discussed already, pointed

to as one of the governmental failures that enabled the terrorists who perpetrated the 9/11 attacks.

Returning to the architectural aspect of the challenge facing the IC, the ‘need to know’ dilemma does have its solutions. Because of the requirements for discrimination and both limiting who has access and yet distributing information on certain subjects to the people who need it, intelligence and systems personnel have already created dissemination lists of individuals with the requisite qualifications and clearances for receiving intelligence products. As noted earlier, designating a report a TERREP gets it disseminated within the counterterrorism community. The Department of State’s cable system has a series of four-letter tags or distribution codes (the TAGS system) annotated in cable headings. Bearing a given code in its tagging, a cable is automatically distributed to people for whom systems administrators have designated for receipt of that coding. Even with the TAGS system already in place, the Intelligence Community has been slow to take advantage of new information technologies that would enhance that tagging and help to better and more appropriately disseminate intelligence products. Some of that slowness lies with the CIA and NSA, the agencies in charge of clearing and approving systems and methods of distribution. The CIA, citing security reasons, has a long history of resisting the expansion of electronic systems for integrating intelligence sharing.⁹²

VIII MANAGING ORGANIZATIONAL CULTURAL CHANGE

Leadership, as much as administration and management, is significant in changing organizational cultures and to tearing down the barriers created by those cultures. How agency leaders in the bureaucracy go about effecting change is, while a normal part of the

duties of leadership, critical in bettering how the intelligence system works. The legal and regulatory barriers to communication in the Intelligence Community and the Interagency have been eroded, if not completely torn down. Overcoming the remaining barriers demands changing the culture and is vital to the safety of the nation's people if not to the nation itself.

Recognized even at its inception, a principal challenge and mission for the DNI, was and continues to be overcoming organizational culture that interferes with communication among the agencies. The Director of National Intelligence brings a new structure to the Intelligence Community. "Organizational structure influences both the direction and substance of communication...*Vertical* communication occurs between superiors and subordinates; it may flow downward...or upward...*Horizontal* communication links related tasks, work units, and divisions of the organization."⁹³

Changes in culture can be effected through how things are communicated. Within bureaucracies, significant change is usually driven from the top down, whether by executive direction or legislative action. For example, in legislation creating the office of the Director of National Intelligence (DNI), with regard to the FBI's and other agencies' surveillance activities within the U.S., the National Foreign Intelligence Program and National Foreign Intelligence Board have been renamed to reflect the fusion between foreign and domestic intelligence programs to the National Intelligence Board and National Intelligence Program.⁹⁴

The tools for changing and redirecting the inertia inherent in the U.S. Government's bureaucracy are contained in the agencies' leadership's daily message sending and receiving activities. These tools can be described as symbols (the raw material) of communication, patterns (the systematic use of the raw material), and settings (the place of the

communication).⁹⁵

Symbols in this context include, in addition to words and language, how leaders set priorities, what those priorities are, and how they communicate what they believe to be important to their subordinates.

Patterns are the methods by which leaders put their symbols to use. This includes the timing of their messages to their subordinates and how they go about praising or reinforcing the behaviors they want changed.

Settings are exactly that -- where the symbols are applied, and may include who carries out the application -- such as senior leaders or midlevel managers directed to carry it out.

Because bureaucracies, especially those the size of a government, like objects, run largely on inertia, some theorists have suggested that structural shakeups or introducing new processes are not the most effective means to change organizational perspectives. Introducing temporary systems to redirect an organization might be a better way to incrementally effect long-term institutional changes. “Major -- but limited -- shifts in emphasis have been accomplished by public and private bureaucracies through three kinds of temporary focusing mechanisms: single-element focusers, systems of interaction, and dominating values.”⁹⁶

A single-element focuser is an individual or office dealing with one problem or aspect of a problem or target of interest. It works with a limited, temporary focus on one or two major new items.⁹⁷

A system of interaction is “a coherent system of senior management interaction...with the purpose of shifting management attention either to some new direction

or to some new method of reaching overall consensus.” This may be as informal as a regularized management gathering in an informal setting or as formal as regular review sessions among managers and subordinates.⁹⁸

Dominating values are those values and aspects of an organization that a leader actively and overtly works to change. However, a values change is not completely an imposed change or change by fiat, but is one brought about “only when an important change is perceived to be at hand.”⁹⁹

Managers and leaders can begin the reformation of organizational cultures through adopting positions and attitudes that focus on the intentions and beliefs of workers and on the perceptions and language that link one human being to another -- communication. Through their use of symbols, patterns and settings, leaders emphasize their place in the group and highlight goals and missions in their status as co-workers through increasing their interaction with their workers. Taking this sort of intentionalist approach demands that managers be close to their subordinates, no longer treating workers or clients as objects to be motivated or manipulated. Through close communication and contact, they would enhance their power, capacity, and creativity to perform their mission.¹⁰⁰

In the long run, having someone in charge should make for better cooperation among the agencies of the Intelligence Community. But, as several administrations worth of Secretaries of Defense have found in pressing for more “jointness” among the military services, the task is long and arduous. It will likely be no different in the IC, even in an era when better cooperation is demanded. “Jointness“ in the Department of Defense, initially addressed in legislation through the Defense Reform Act of 1948, was not truly legislated

until the 1980s when the Cold War was in its decline.¹⁰¹ At times, some members of the military still seem to struggle mentally with the concept, though in practice many have embraced it, working across branches through both the formal and informal networks that have evolved out of the necessity for cooperative interservice and interagency operations.

Substantial strategic and organizational change, whether intra- or interagency will probably be resisted by those who have spent years doing things in their own, organizationally acculturated ways. This is why it is so very important for leaders to begin working to change culture, preferably before implementing new strategic initiatives. However, as the world speeds up and with crisis upon us, it is too late to change the culture to one of information sharing and interagency cooperation with a future strategic goal in mind. With that ideal already impossible, it is necessary for the leaders to work on altering culture and strategy simultaneously.¹⁰²

Understanding leadership, especially in the group context, is closely related to understanding how organizational cultures are changed. Successfully changing the attitudes and habits of individuals and groups depends greatly on the commitment of the leaders, and those leaders must be good at leading. If leaders, especially the ones respected by the rank and file of an organization, support a change, then that change has a chance. If they do not support change, it probably will not occur.¹⁰³ Those same leaders and managers need to understand, and perhaps do without entirely being told, that the administrative and bureaucratic world is constructed or reconstructed through the actions and interactions of groups and the individuals within those groups. While managers might not always encourage the possibility of change, they must recognize and communicate to their subordinates that existing realities might alter, requiring organizational realities to change as well and that

some change is not only inevitable but necessary.¹⁰⁴ It is, as noted earlier, a part of administrative life.

Those opposed to organizational change, regardless of how it is initiated, may, indeed *must* eventually be overcome, either through marginalization or departure. The latter would be preferred as it takes them out of the picture entirely. The problem is that either of these processes may take time. The marginalization comes only with that person, especially if he or she is established, being moved or failing to rise higher. Departure may come about as retirement, hiring by an outside agency, or transfer. In the latter, the person may, however, retain contacts and even interaction with the parent agency.

Organizational cultural change may take time that is not available, indeed, *is* not available in the Global War on Terror. A further challenge to organizational cultural change is that, when a change is viewed by managers as problematic for the organization's future, management tends to focus on 'the problem' itself rather than its causes. Transforming an organization "from an 'inwardly focused organization' to one that [is] focused on the marketplace and customer solutions" is critical. "Changing an entrenched ... culture and transforming the prevailing mindset ... [is] a process that [takes] years, and its progress [is] often measured in inches."¹⁰⁵

Louis V. Gerstner, CEO of IBM from 1993 to 2002, put forth, broadly, a plan for companies looking to transform their organizational cultures:

- Get the company to look outside of the company for answers...
- To transform the company mindset, consider Gerstner's three keys:
Marketplace Obsession, Speed, and teamwork.
- Understand that genuine cultural change can take years.¹⁰⁶

IX REFORM DEMANDS ARE NOTHING NEW TO THE IC

Throughout its history, the United States' Intelligence Community, coming about as it did through the creation of multiple agencies serving a variety of purposes and using a variety of methods and tools, with little centralized design or overall plan, has and continues to operate in ways that promote competition among its component agencies over information, money, people, other resources, and access. Each of the IC's member agencies has its own capabilities, either operationally or analytically or both, and each produces intelligence unique and relevant to its customer groups. Specialized collection or analysis mechanisms or the information they collect and intelligence they produce become the currency used to outbid or undermine each other in the political, public and bureaucratic arenas. As they try to enhance their power or protect their turf or move their own agendas forward, intelligence agencies miscommunicate or fail to communicate either with each other, with their customers and the consumers of their products, or even within themselves. "Such "non-cooperation" is the leading cause of intelligence failure."¹⁰⁷

Almost from its inception, and even before it was formalized as a "community," reform has been asked or even demanded of the IC. However, it is apparent that it has done little to implement most of the proposals made for it. Certainly, some of the responsibility for this lies with Congress, for it is through legislation that the legal basis for reform is set and directed. However, calls for a strong, central administrator of intelligence prior to the creation of the office of the Director of National Intelligence, largely went ignored until after the terrorist attacks on the United States on September 11, 2001. Except for some relatively minor tweaking of the existing structure, little else was done. For a time, if anything was done to reform the IC, the efforts went to limiting its power and scope of effort. That,

coupled with the inherent resistance of bureaucratic organizations to major change, has been the major source of opposition to greater cohesion. Press reports indicate that despite political pressures in the period since 9/11, the intelligence agencies themselves have continued to attempt to block reforms aimed at reducing turf battles, overcoming legal stumbling blocks, streamlining bureaucracies, increasing information and intelligence sharing and analysis, and imposing greater accountability. There are those who assert that the current presidential administration has already missed the opportunity to retool the nation's Cold War-era intelligence bureaucracies for fighting terrorism.¹⁰⁸

However, the pitfall of going overboard with that sort of retooling is that it potentially ignores other long-term threats. For instance, though the Cold War is over, Russia remains significant militarily and is a continuing figure on the world stage with nuclear weapons and geographic position. China is emerging as both a potential adversary and partner. It is expanding its military and its economy. As such, intelligence relevant to policy with both nations continues to be vital to U.S. interests. Perhaps the U.S. intelligence community needs expansion to cover more contingencies as well as restructuring to fight the war on terror.

For now, these concerns seem to have been set aside by a desire by Congress and the Executive branch to let the system shake itself out for a time before taking the more extreme step of creating additional IC structure in further reaction to the events of 9/11. The IC, while retooling for the GWOT, seems not to have completely let that focus get in the way of maintaining some capability in the realm of other long-term threats.

Bureaucratic leaders appear to have begun to commit to some fundamental changes in mission and practice. They recognize, perhaps better than most, that terrorism is a matter for

intelligence and law enforcement, as well as the military. Through legislation such as the PATRIOT ACT and through subsequent practice, the figurative wall that once separated non-criminal intelligence and law enforcement, including that which existed almost to the point of egregiousness within the FBI, has been all but erased. Agents and analysts learning of or seeking national or international terrorist intelligence are now allowed to share information with colleagues who are investigating criminal cases.¹⁰⁹

However, even as Intelligence Community leaders tentatively sign on to the idea of interagency cooperation, barriers to sharing ideas, information and data continue to arise. Existing security processes and structures, within the IC and other agencies with which it sometimes partners, impede efforts to combine or standardize how they are conducted. They continue to interfere with creating new practices. They continue to bear negatively upon building the systems architectural capacity required to support the level of integration necessary for the IC to truly function effectively. Programs in individual agencies, and within the nation's intelligence infrastructure as a whole, are segmented and fragmented through a wide variety of special access requirements. Interagency distrust of each other's motives and processes continues to impede interagency cooperation.¹¹⁰

Because of this distrust, "realistic expectations must be accompanied by some significant structural changes, the most important of which is to infuse greater cohesion into the intelligence process."¹¹¹ Some of this will be affected by personal and personnel integration as well as by systems and information sharing systems architecture and common databasing.

That distrust contributes to a certain degree of ambivalence about the United States' national security interagency structure and how it operates for leaders, legislators, and

policymakers for reasons both good and bad. America's economic strength and military might, and subsequently, the comparative material wealth of the Intelligence Community has historically provided some latitude for experimentation and duplication of effort in the service of the nation's political goals. It is in this context, and in the context of American social and political society, that a decentralized Intelligence Community is probably the only one that can maintain long-term public support, especially in a form of government where it is possible for the control of the executive and legislative branches of government to be split between two major political parties. For political, philosophical, and practical reasons, the IC will continue to remain decentralized and dispersed in its operations and command and control. A certain degree of competitive analysis and discussion is necessary and important to maintain both the trust and confidence of the American public.

Decentralization of the community helps assure the military maintains its control over its tactical and operational intelligence programs. It also functions to assure Congress that neither the President's chief intelligence adviser nor the President can acquire a threatening concentration of domestic political power. Neither can they monopolize the foreign policy advice being passed to or from the White House.

Because of this, the United States is likely to maintain a relatively decentralized Intelligence Community. Impulses toward centralization and concentration of power are likely to continue to be contained, especially within this political system. That is, at least until some new, greater, more societally and nationally threatening crisis re-aligns the political and bureaucratic players in the process and compels cooperation in what are still politically and socially questionable or unacceptable directions.¹¹²

This ambivalence is likely to endure for the same reasons that created it in the first

place: there is no agreement or acceptable vision for its replacement. Intelligence Community reform efforts and initiatives face approximately the same obstacles that Harry Truman faced in the years immediately after World War II. Now as then, everyone involved in the reform effort has some idea of what reforms are needed, but there are also changes they will not or cannot tolerate. That mix of ideas, desires and objections produces a veto on someone's part to almost every proposal. Ultimately, the reforms that survive the political process are the ones policymakers and legislators dislike the least. However, that ongoing debate over structure and how to manage threat information in the here and now is also likely to keep alive an idea that was first articulated in the aftermath of the Pearl Harbor disaster and has been once again reinforced by the 9/11 attacks. This is that idea that the principles of unity of command, ease of communication, and the view that information is best interpreted and analyzed if it is shared, can all be better served with a greater degree of centralization among the agencies of the Intelligence Community.¹¹³

In the long run, having a Director of National Intelligence in charge of the IC's efforts to improve and centralize management, practice and oversight of the community should make for better cooperation among its component agencies. "But as two generations of Secretaries of Defense have found in pressing for more "jointness" among the military services, the task is long and arduous."¹¹⁴ Creating or forcing cooperation in the Interagency and in the Intelligence Community, with their even-more-than-the-Defense-Department's disparate agencies, organizations and cultures is neither likely to be easy or quick.

X TOWARD DEVELOPING ORGANIZATIONAL CULTURE

In reform efforts directed at the Intelligence Community, developing a strong

interagency organizational culture of cooperation, communication, information, intelligence and analytical conclusion sharing is important because this type of culture serves a variety of useful functions useful to the mission or missions they collectively serve. Successfully creating a new, or at least modifying the existing IC organizational culture, is a critical mission for the DNI for several reasons.

First, cultures help to create the shared interpretation of organizational and interorganizational events that are pertinent to their purpose. Members not only know how they are expected to behave and interact with one another and with their customers, but also how each other thinks. It gives a common ground for language, study, and interpretation and how one might put forth dissent in a manner that will be accepted as valid by other members of the culture.

Second, along with the aforementioned cognitive functions, cultures have emotional impact upon their members. In a manner of speaking, they lend an aura of excitement and can be a source of inspiration to employees in their work lives.

Third, organizational cultures generate commitment by giving members a sense of community through shared experience, beliefs and other common ground. The culture creates and maintains boundaries. It helps define its members as well as outsiders or subgroups who may not be acting properly in relation to the rest of the group.

Fourth, cultures serve as social control mechanisms, formally labeling certain patterns of activity as required, allowed, or prohibited. As its members relate to one another and interact, it exerts some control over what is proper behavior within the organizational context.

Finally, research and writing on organizational cultures indicates that the presence of

a strong internal organizational culture may help to increase productivity among an agency's members.¹¹⁵

It is important for leaders and decision-makers to be aware of an agency's culture as well as its mission and operational stance in order to understand how to both manage and communicate with and within it. Understanding an organization helps bring about confidence in its actions, in its abilities to achieve the goals set for it, and assists in interpreting the messages and information it sends out. Though this does not protect against the unexpected, understanding and relating to the organization helps its leaders and the consumers of its products to better respond to or for it when the unexpected does occur.

XI CENTRALIZATION THREATS

Obviously, careful planning and work must be done. Care must be taken in structuring and organizing a new interagency or operational structure and information-sharing architecture to achieve the necessary balance to ensure the interagency is able to meet the needs of the various agencies using its services. This author is not overly optimistic that it will be done properly. Current political realities and considerations could potentially over-centralize the Intelligence Community and make it structurally unresponsive to anyone outside the presidential administration. They could also effectively cripple it by trying to make it respond to everyone. Either one would make it not only less effective than what is currently out there, but would be counter to the very purpose of the proposed reorganization and restructuring of the intelligence community. Its already mixed structure, with a better information sharing and knowledge management architecture will likely modify its organizational culture at least somewhat. The trend toward interagency centralization with

regard to overall management, common communication, and installation of information processing systems and an improved sharing and distribution architecture, while keeping with its decentralized overall structure, can overcome some of its most severe shortcomings and negative limitations.

Too much effort directed at centralizing and improving poses certain threats, alluded to previously, to the nation. If, as some authors assert, Americans are willing to accept some reduction or lessening in civil liberties in the name of intelligence and law enforcement structural efficiency and effectiveness,¹¹⁶ a hallmark of leadership in this country may be to stand on principle against the masses. Leaders may need to take the principled stand, to be statesmen and women, to protect liberties hard gained and easily lost or given up. Therein lies as much of a long-term danger to this nation as that of terrorist attack. If Americans give up their liberties for safety and security, then perhaps the terrorists will have won in the big picture of the war on terror -- they will have forced Americans to give up a part of themselves. And if they are willing to give up some part of themselves, then perhaps they are willing to give up more. Giving up their hard-won freedoms, Americans could ultimately lose the country and its founding principles and alter the very basis of the Republic's existence.

Be that as it may, American culture and its political system and processes impose legal limits and restrict bureaucratic and, theoretically both executive and legislative freedom of action. That same culture does not necessarily exclude innovation and reform. Decentralization and fragmentation are hallmarks of the United States' society. So are pragmatism and efficiency. "There is no reason to believe that freedom is inconsistent with a culture of greater fusion among agencies for the purposes of efficiency and

effectiveness.”¹¹⁷

That point gives reason for hope. Other democracies, such as Canada, Great Britain and France, have managed to create working intelligence bureaucracies without significantly limiting or impeding upon civil liberties. Granted, most other democracies tend to have more centralized governments than the United States, but they have continued to ensure and protect their peoples’ civil liberties and to have functioning civil societies. A characteristic of democracies’ intelligence systems is, as with the U.S., a separation of domestic law enforcement and both domestic and foreign intelligence gathering and analysis. However, most others seem to have attained a balance and created better mechanisms for the sharing and integration of intelligence among domestic agencies where this is necessary to the security of the state.¹¹⁸

Varying degrees of decentralization and centralization will both continue as aspects of our system. Bureaucratic necessity, driven by national political demands, will see some form of interagency cooperation, most likely in the form of the continued creation of intelligence fusion centers and joint task forces. Some restructuring and even coercion by strong legislative and executive leaders will probably still be necessary as agencies are forced to give up functions they previously held to interagency task forces and new Intelligence Community fusion centers. For example, it may take actual sanctions against the agency or at least some of its employees for old-guard members of the CIA to render their activities in and information garnered for that agency’s Counterterrorism Center (the CTC) to the recently-formed National Counterterrorism Center (the NCTC). Indeed, it may become necessary to take the CTC away from the CIA and give its functions, lock, stock and barrel, to the NCTC to prevent CIA bureaucrats from attempting to undermine the effectiveness of

the new agency, either consciously or unwittingly, as they struggle to hold on to their old ways of operating.

XII CONCLUSION – Interagency Cultures Are Changeable

Organizational cultures exist within the Intelligence Community and in each of the agencies within that community. Further, this series of organizational cultures has, for a variety of reasons, created barriers to interagency communication and information sharing. Whatever those reasons were, whether good or bad, the overarching organizational culture is dysfunctional in its efforts to see to the nation's security.

The bureaucratic and intelligence community's biases toward limited cooperation among themselves as well as with those from outside their boundaries can be overcome. Those biases can be overcome with minimal pain for all involved if those bringing about reform grasp that they are dealing with both an overall subculture and series of organizational cultures that have grown up with and within the agencies that comprise the IC. Elected and appointed leaders who take the time to understand the culture of the Interagency and Intelligence Community, and who attempt to analyze the effects of their intervening on those cultures, will be more effective in their reforms. Effective performance interventions will have a positive effect on the organization's culture and become themselves measurement instruments.¹¹⁹

The improvement of human performance often requires an organization to change its culture, and organizational leaders seldom possess sufficient power to mandate cultural change by edict. At best, management can introduce agents or agencies of change and manage their organization's culture in the same way they manage physical and financial resources. An organization's culture shapes individual behavior by establishing norms and taboos and, ultimately, determines the quality and character of an

organization's products. Culture and product are inseparable, and one cannot be changed without affecting the other. The choice confronting any organization is to manage its institutional culture or to be managed by it.¹²⁰

Much the same can be said of the interagency and the intelligence community agencies. Each has its own organizational culture superimposed upon its members' adherence to the greater culture of the nation. Those cultures have developed, been modified, formed and reformed over the varying histories of the agencies involved. Those organizational cultures, reinforced by technical differences, have caused their members to fail to cooperate and communicate with each other, sometimes in matters critical to the safety of the nation's people.

The barriers to cooperation can be torn down and the intelligence efforts of the agencies of the IC made more unified, even as the separate bureaucracies continue to exist and carry out their individual missions. Tearing down those barriers takes two things: first the leaders of the Interagency must do what they were hired or elected or appointed to do: lead. They must create and demand a culture of communication and sharing of intelligence data. Inherent in this is realizing that the zero-sum game they perceive does not, in reality, exist. Passing that realization to their subordinates, as well as to their peers, is an essential part of their cultural reform mission. Through their application of symbolism and symbols, and the settings in which these tools are used, leaders can change and remake their organizations' cultures. As they push for these changes in information and intelligence sharing, leaders must allow their subordinates to change and to pass along data and analysis that they may instinctively or professionally know needs to be shared. Second, is the adoption of common systems architecture such that the IC's databases are available to all its members. With this, analysts and operators can access the information they need to be

accurate and effective. To bring about both aspects of this reform of the Intelligence Community, its appointed leaders must identify and budget for the resources necessary to enable making concrete efforts. This may require not only refocusing some resources, but also increasing them. The elected leaders must exercise the necessary budget authority and oversight and make the sacrifices or decisions necessary to ensure the cultural reform's successful implementation. But, unless Congress and the Executive work together, the author concludes that we, as a nation, will fail in our efforts to reform our dysfunctional organizational cultures and their muddled environment.

Should our leaders find themselves able to cooperate, there is hope. With reforms successfully in place, the necessity of *ad hoc* muddling through can be replaced by an organized, even consistent approach to managing or, better yet, heading off crises early on or before they start. Informed leaders, operators and analysts who can and will and are willing to communicate, can ensure that intelligence is shared with or is given to those who need it in order to act upon it.

The problems posed by a dysfunctional, uncooperative and disunited organizational culture can be overcome. Organizational culture can be modified and reformed. In spite of perception to the contrary, U.S. Government agencies are not, truly, caught up in a zero-sum game with regard to resources. The tools for change, for cooperation, and communication exist. They even exist in the hands of elected leaders and by the leaders of executive bureaucracy in charge of its agencies and their organizational cultures. It is a matter of whether they can or will utilize those tools effectively and for the greater good of the nation.

NOTES

¹ The idea of government agencies effectively muddling through their operations was first proposed by Charles El Lindblom in “The Science of Muddling Through.” (*Public Administration*, Vol. 19, 1959), pp 59-79.

² The *need to know* refers to the controlled distribution of information to those cleared to act upon it or analyze it or otherwise make or contribute to decisions based upon it. Classified information may be protected because of its source or the method in which it was obtained. Protection can be necessary because, if acted upon, an opponent may be able to determine how or from where or from whom the information was probably obtained.

³ *Weapons of Mass Destruction* or *WMD* is a term commonly applied to nuclear, biological, or chemical weapons.

⁴ Michael A. Turner, *Why Secret Intelligence Fails*. (Dulles, VA: Potomac Books, Inc., 2005), p 2.

⁵ *Ibid.*, p 125.

⁶ The term *Global War on Terror* may be viewed by some as somewhat of a misnomer. Some argue that terror or terrorism is the tactic used and that war may not be waged against a concept or ‘ism.’ In reality, the conflict is with those who utilize terrorism as their primary high-profile tactic against their adversaries. The GWOT is hardly even a war on terror or terrorist organizations as a whole, but, in its current iteration at least, a war against radical interpretations of Islam. However, political sensitivities demand that it not be called an outright war or crusade against Islam or an aspect of the religion and culture and, since radical Islam’s adherents tend to use terrorist tactics and methods, the term will suffice.

⁷ Joint Chiefs of Staff, *U.S. Department of Defense Dictionary of Military Terms*. (New York: Arco Publishing, 1988), p 183.

⁸ *United States Intelligence Community – Who We Are*. (<http://www.intelligence.gov/1-members.shtml>), accessed on February 19, 2006.

⁹ Gregory F. Treverton, “Forward” to Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*. (Washington, DC: Center for the Study of Intelligence, 2005), p xii.

¹⁰ William E. Odom, *Fixing Intelligence: For a More Secure America*. (New Haven, CT: Yale University Press, 2003), pp 196-205.

¹¹ *Posse Comitatus* refers to the use of the military for domestic law enforcement purposes and is tightly controlled under U.S. Statute. The *Posse Comitatus* Act of 1878 has traditionally been viewed as a major barrier to the use of U.S. military forces in planning for homeland defense. In fact, many in uniform believe that the act precludes the use of U.S. military assets in domestic security operations in any but the most extraordinary situations. As is often the case, reality bears little resemblance to the myth for homeland defense planners. Through an erosion of the act’s prohibitions over the past 20 years, *posse comitatus* today is more of a procedural formality than an actual impediment to the use of U.S. military forces in homeland defense. This is discussed in Craig T. Trebilcock, “The Myth of *Posse Comitatus*.” (<http://www.homelandsecurity.org/journal/articles/Trebilcock.htm>.) accessed on February 19, 2006.

¹² Joint Pub 3-08. *Interagency Coordination During Joint Operations, Vol 1*. (9 October 1996), p I-5.

¹³ *Ibid.*, p I-9.

¹⁴ Thomas J. Peters, “Symbols, Patterns, and Settings: An Optimistic Case for Getting Things Done,” in Shafritz and Ott, pp 402- 420, p 406.

¹⁵ Joint Pub 3-08, p vi.

¹⁶ *Ibid.*

¹⁷ Public Law 107-56, October 26, 2001, cited as the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001.”

¹⁸ One way law enforcement agencies have worked around the Third Agency Rule in criminal and terrorist investigations has been through the formation of joint interagency investigative task forces (JTTFs).

¹⁹ Turner, p 55.

²⁰ *Ibid.*, p 373.

²¹ *Ibid.*

²² Meryl Reis Louis, “Organizations as Culture-bearing Milieus,” in Shafritz and Ott, pp 421- 430, p 429.

²³ Jay M. Shafritz and J. Steven Ott. *Classics of Organization Theory, Second Edition.* (Pacific Grove, CA: Brooks/Cole Publishing Company, 1978), p 374.

²⁴ Caren Siehl and Joanne Martin. “The Role of Symbolic Management: How Can Managers Effectively Transmit Organizational Culture?” in Shafritz and Ott, pp 433- 445, p 433-434.

²⁵ *Ibid.*, p 434.

²⁶ *Ibid.*

²⁷ Louis, p 421.

²⁸ Patrick Radden Keefe, *Chatter: Dispatches from the Secret World of Global Eavesdropping.* (New York: Random House, 2005), pp 237-238.

²⁹ Joint Pub 3-08, p I-7.

³⁰ Harold F. Gortner, Julianne Mahler, and Jeanne Bell Nicholson, *Organization Theory: A Public Perspective.* (Chicago: Dorsey Press, 1987), p 178.

³¹ Turner, p 51.

³² *Ibid.*, p 55.

³³ *Ibid.*, p 46.

³⁴ Rolington, Alfred. "Keeping Intelligence Objective." *Jane's Intelligence Review*, December 1, 2005. (http://www4.janes.com/subscribe.jir/doc_view.jsp?K2DocKey=/content1/janesdata/mags), accessed on January 17, 2006.

³⁵ Gortner, Mahler, and Nicholson, p 173.

³⁶ *Ibid.*

³⁷ Gerald Posner, *Why America Slept: The Failure to Prevent 9/11*. (New York: Random House, 2003), pp 178-179.

³⁸ E-mail from USAF Lt Gen (R) Charles Cunningham, JFSC to the author, January 30, 2006.

³⁹ Odom, p 5.

⁴⁰ Keefe, p 237.

⁴¹ Gregory F. Treverton, *Rand Occasional Papers: The Next Steps in Reshaping Intelligence*. (Santa Monica, CA: The Rand Corporation: 2005), p 27.

⁴² *Ibid.*

⁴³ William W. Mendel and David G. Bradford, *Interagency Cooperation: A Regional Model for Overseas Operations*. (Washington, DC: Institute for National Strategic Studies, National Defense University: 1995), p 85.

⁴⁴ Armed Forces Communications and Electronics Association (AFCEA), *National Security and Horizontal Integration*. HI White Paper, 2004. (<http://www.afcea.org/committees/intel/HIWhitePaper>) accessed on February 11, 2006, pp 1-2.

⁴⁵ *Ibid.*, p 2.

⁴⁶ *Ibid.*, pp 2-3.

⁴⁷ *Ibid.*, p 3.

⁴⁸ Jeffrey T. Richelson, *The U.S. Intelligence Community*. (Boulder, CO: Westview Press, 1999), p 2.

⁴⁹ Odom, p. xxviii.

⁵⁰ *Ibid.*, p 7.

⁵¹ William A. Navas, "The National Security Act of 2002," pp 231-244 in Stuart, p 241.

⁵² This is not a formal declaration of war, a power which the President does not have under the U.S. Constitution, Art. 1, sec. 8. As with some crises, some 'wars' referred to by presidents exist because of their way of stating the problem, for example the GWOT, the War on Poverty, the 'moral equivalent of war,' etc. A

crisis is defined as “a crucial or decisive point or situation; a turning point. An unstable situation, in political, social, economic or military affairs, especially one involving an impending, abrupt change (Wiktionary, accessed March 26, 2006).” Some events come to be defined as a crisis, or even a war, in spite of their lack of decisive actions or endings, which holds, by implication, an immediacy both of the situation and of the ability to deal with it satisfactorily in a relatively short period of time. Overstatement is not an issue dealt with in this paper, however.

⁵³ Stephen H. Konya and Rob Johnston. “Organizational Culture: Anticipatory Socialization and Intelligence Analysts,” pp 97-106, in Johnston, p 97.

⁵⁴ Treverton, *Rand Occasional Papers*, p 28.

⁵⁵ *Ibid.*

⁵⁶ Odom, pp xvii-xviii.

⁵⁷ Mendel and Bradford, p 87.

⁵⁸ *Ibid.*

⁵⁹ Odom, p 22.

⁶⁰ Gortner, Mahler, and Nicholson, p 174-175.

⁶¹ Rolington.

⁶² Gortner, Mahler, and Nicholson, p 100.

⁶³ *Ibid.*, pp 106-107.

⁶⁴ Odom, p xv.

⁶⁵ Jason Vest, “Dumb Intelligence: Concerns About the Director of National Intelligence Go Far Beyond John Negroponte’s Bloody Past.” *Boston Phoenix*, February 25 - March 3, 2005. (http://www.bostonphoenix.com/boston/news_features/other_stories/multi-page/documents/04495068.asp), accessed on December 20, 2005.

⁶⁶ At the time of this paper’s writing, the DNI’s office was *temporarily* housed in a newly-constructed Defense Intelligence Agency building in Washington, DC. This arrangement is for the interim until a permanent facility is located or constructed.

⁶⁷ Some historians have made the observation that the degree of influence the State Department and Secretary of State once wielded over foreign policy was diminished by the move from the Old Executive Office Building (now the Eisenhower Executive Office Building) next door to the White House to State’s current location in Washington, DC’s Foggy Bottom area in the 1950s. The Secretary of State’s influence was eclipsed to a large degree by that of the National Security Advisor whose office occupies much of the old State offices. Location and proximity to the seat of power matters even in the republic.

⁶⁸ Vest.

⁶⁹ Treverton, *Rand Occasional Papers*, p 5.

⁷⁰ *Ibid.*

⁷¹ AFCEA, pp 3-4.

⁷² AFCEA, p 5.

⁷³ AFCEA, p 6.

⁷⁴ Jeffery T. Richelson, *The U.S. Intelligence Community*. (Boulder, CO: Westview Press, 1999), p 471.

⁷⁵ Treverton, *Rand Occasional Papers*, p 21.

⁷⁶ Turner, p 150.

⁷⁷ General Michael V. Hayden, Principal Deputy Director of National Intelligence, *Press Conference*, June 29, 2005. (http://www.dni.gov/wmd_recommendation.html), accessed on December 20, 2005.

⁷⁸ Turner, p 150.

⁷⁹ *National Counterterrorism Center: Key Partners*, (http://www.nctc.gov/about_us/key_partners.html), accessed on March 6, 2006.

⁸⁰ Turner, pp 151-152.

⁸¹ *Ibid.*, p 152.

⁸² *Ibid.*, p 154.

⁸³ Hayden.

⁸⁴ Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*. (Washington, DC: Center for the Study of Intelligence, 2005), p 112.

⁸⁵ *Ibid.*

⁸⁶ *Ibid.*

⁸⁷ *Ibid.*

⁸⁸ Gregory F. Treverton, "Forward" to Johnston, p xii.

⁸⁹ Turner, p 153.

⁹⁰ Thomas Powers, *Intelligence Wars: American Secret History from Hitler to al-Qaeda*. (New York: New

York Review Books, 2002), p 343.

⁹¹ Turner, p 54.

⁹² *Ibid.*, pp 118-120.

⁹³ Gortner, Mahler, and Nicholson, p 160.

⁹⁴ Hayden.

⁹⁵ Peters, p 402.

⁹⁶ *Ibid.*, p 413.

⁹⁷ *Ibid.*, p 414.

⁹⁸ *Ibid.*, pp 415-416.

⁹⁹ Peters, Thomas J. "Symbols, Patterns, and Settings: An Optimistic Case for Getting Things Done," in Shafritz and Ott, 402- 420, p 418.

¹⁰⁰ Gortner, Harold F., Julianne Mahler, and Jeanne Bell Nicholson. *Organization Theory: A Public Perspective*. Chicago: Dorsey Press, 1987, p 11.

¹⁰¹ Treverton, *Rand Occasional Papers*, p 1.

¹⁰² Jeffery A. Krames, *What the Best CEOs Know: 7 Exceptional Leaders and their Lessons for Transforming Any Business*. (New York: McGraw-Hill, 2003), p 121.

¹⁰³ Gortner, Mahler, and Nicholson, p 74.

¹⁰⁴ Robert B. Denhardt, *Theories of Public Organization*. (Belmont, CA: Brooks/Cole Publishing Company, 1984), p 183.

¹⁰⁵ Krames, pp 115-117.

¹⁰⁶ Krames, pp 117-118.

¹⁰⁷ Turner, p 14.

¹⁰⁸ Turner, pp 149-150.

¹⁰⁹ Treverton, *Rand Occasional Papers*, p 15.

¹¹⁰ AFCEA, p 7.

¹¹¹ Turner, p 147.

¹¹² Michael Warner, Michael, ed. *Central Intelligence: Origin and Evolution*. (CIA History Staff, Washington, DC: Center for the Study of Intelligence, 2001), pp 17-18.

¹¹³ *Ibid.*, p 17.

¹¹⁴ Treverton, *Rand Occasional Papers*, p 1.

¹¹⁵ Siehl and Martin, pp 434-435.

¹¹⁶ Turner, in notes to p 56 of *Why Secret Intelligence Fails*, claims several polls since September 11, 2001, support this assertion.

¹¹⁷ Turner, p 56.

¹¹⁸ *Ibid.*, p 66.

¹¹⁹ Johnston, p 115.

¹²⁰ *Ibid.*, p 115-116.

BIBLIOGRAPHY

- 9/11 Commission. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: WW. Norton and Company, 2004.
- Alberts, David S., et al. *Understanding Information Age Warfare*. Washington, DC: DoD Command and Control Research Program, 2001.
- Armed Forces Communications and Electronics Association (AFCEA). *National Security and Horizontal Integration*. HI White Paper, 2004, <<http://www.afcea.org/committees/intel/HIWhitePaper>>, accessed on February 11, 2006.
- Bartholomees, Jr., J. Boone, ed. *U.S. Army War College Guide to National Security Policy and Strategy*. Carlisle Barracks, PA: Dept. of National Strategy and Security, U.S. Army War College, 2004.
- Behunin, Scott A. *Homeland Security Advisory System*. Monterey, CA: Naval Postgraduate School, 2004.
- Bergman, Lowell, et al. "Spy Agency Data After Sept. 11 Led FBI to Dead Ends," *The New York Times*. 17 January 2006, Pg 1.
- Best, Jr., Richard A. *Intelligence Community Reorganization: Potential Effects on DoD Intelligence Agencies*. Washington, DC: Congressional Research Service, 2004.
- Boardman, Chase H. "Freedom of Information Policy in the United States." Master's Degree Paper, University of North Dakota, Grand Forks, ND, 1990.
- _____. "The Impact of Open Records and Open Meetings on the Legislative Process." Master's Degree Independent Study, University of North Dakota, Grand Forks, ND, 1990.
- Bogdanos, Matthew F. "Joint Interagency Cooperation: The First Step," *Joint Forces Quarterly*, 37, April 2005. pp 10-18.
- Bowman, Stephen. *When the Eagle Screams: America's Vulnerability to Terrorism*. San Jose, CA: Writer's Club Press, 2001.
- Bryant, Jackie J. *Army Knowledge Management (AKM): Challenges Ahead*. Carlisle Barracks, PA: U.S. Army War College, 2002.
- Cartney, Michael. *The Art of Balancing Information Security and Information Sharing*. Cambridge, MA: Harvard University, 2000.

- Cerami, Joseph R. and James F. Holcomb, eds. *U.S. Army War College Guide to Strategy*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2001.
- Charchlan, Daniel J. *Understanding Culture and Consensus Building: Requisite Competencies for Interagency Operations*. Carlisle Barracks, PA: U.S. Army War College, 2001.
- Chester, Kemp L. *A Goldwater-Nichols for MOOTW?* Newport, RI: Naval War College, 2000.
- Chomsky, Noam. *9-11*. New York: Seven Stories Press, 2002.
- Colyer, Kevin C. *A Command and Control Structure for Joint Interagency Counterterrorism*. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2001.
- Cottrell, David and Eric Harvey. *Leadership Courage: Leadership Strategies for Individual and Organizational Success*. Dallas, TX: Walk the Talk Co. 2004.
- Cunningham, Charles, LTG, USAF (Ret). E-mail to the author, January 30, 2006.
- Curry, Mark L. *The Interagency Process in Regional Foreign Policy: A Monograph*. Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 1994.
- Demac, Donna A. *Keeping America Uninformed: Government Secrecy in the 1980's*. New York: Pilgrim Press, 1984.
- Denhardt, Robert B. *Theories of Public Organization*. Belmont, CA: Brooks/Cole Publishing Company. 1984.
- Dickinson, Lansing E. *The Military Role in Countering Terrorist Use of Weapons of Mass Destruction*. Maxwell Air Force Base, AL: USAF Counterproliferation Center, Air University, 1999.
- Dochnal, Alfred E. *The United States Homeland Defense Against International Terrorist*. Newport, RI: Naval War College, 2001.
- Director of National Intelligence. *The National Intelligence Strategy of the United States of America*. October 2005
- Federal Emergency Management Agency. *International Cooperation in Emergency Preparedness and Disaster Management, Volume I*. Washington, DC, 2000.
- Federal Emergency Management Agency. *International Cooperation in Emergency Preparedness and Disaster Management, Volume II*. Washington, DC, 2000.

- Gortner, Harold F., Julianne Mahler, and Jeanne Bell Nicholson. *Organization Theory: A Public Perspective*. Chicago: Dorsey Press, 1987.
- Gunderson, Jon. "Protecting U.S. National Interests: The Role of the Ambassador and the Country Team." *Special Warfare*, Fall 1998.
- Gutierrez, Michael J. *Intelligence and High Intensity Drug Trafficking Areas (HIDTA's): A Critical Evaluation of the HIDTA Investigative Support Center (ISC)*. Monterrey, CA: Naval Postgraduate School, 2004.
- Hastedt, Glenn P. "CIA's Organizational Culture and the Problem of Reform." *International Journal of Intelligence and Counterintelligence*. Fall 1996.
- Hayden, Gen. Michael V., Principal Deputy Director of National Intelligence, *Press Conference*, June 29, 2005, <http://www.dni.gov/wmd_recommendation.html>, accessed December 20, 2005.
- Hayes, Margaret Daly and Gary F. Wheatley. *Interagency and Political-Military Dimensions of Peace Operations, Haiti: A Case Study*. Washington, DC: Center for Advanced Concepts and Technology: GPO, 1996.
- Hefling, Kimberly. "Army Officer Says 9/11 Terror Cells were ID'd." *The (Norfolk, VA) Virginian-Pilot*. 18 August 2005, A5.
- History and Lessons of Intelligence Failure, The*. <<http://faculty.ncwc.edu/toconnor/431/431lect05.htm>>, accessed on December 28, 2005.
- Johnson, William F. *Operations Logistics for OCONUS Consequence Management: A Joint-Interagency Challenge*. Newport, RI: Naval War College, 1998.
- Johnston, Rob. *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*. Washington, DC: Center for the Study of Intelligence, 2005.
- Joint Chiefs of Staff. *U.S. Department of Defense Dictionary of Military Terms*. New York: Arco Publishing, 1988.
- Joint Military Intelligence College. *Global War on Terrorism: Analyzing the Strategic Threat. Discussion Paper Number 13*. Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, 2004.
- Jones, Christopher R. *Achieving Unity of Effort at the Operational Level through the Interagency Process*. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2005.
- Keefe, Patrick Radden. *Chatter: Dispatches from the Secret World of Global Eavesdropping*. New York: Random House, 2005.

- Keegan, John. *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. New York: Alfred A. Knopf, 2003.
- Krames, Jeffrey A. *What the Best CEOs Know: 7 Exceptional Leaders and their Lessons for Transforming Any Business*. New York: McGraw-Hill, 2003.
- Krawchuk, Fred T. *Combating Terrorism: A Joint Interagency Approach*. Arlington, VA: Institute of Land Warfare, Landpower Essay: 2005.
- Lindblom, Charles E. "The Science of Muddling Through." *Public Administration*, Vol. 19, 1959. pp 59-79.
- Lowman, Warren. *Operations Other Than War: An Interagency Imperative*. Newport, RI: Naval War College, 1994.
- Lynch, Timothy D. *A Suggested Decision-Making Guide for Use by Interagency Working Groups in Developing Policy Recommendations for Complex Contingency Crisis Operations*. Carlisle Barracks, PA: U.S. Army War College, 1997.
- Machiavelli, Nicolo. *The Prince*. Project Gutenberg: File tprnc10.txt, 1998.
- McCreedy, Kenneth O. *Waging Peace: Operations Eclipse I and II -- Some Implications for Future Operations*. Carlisle Barracks, PA: U.S. Army War College, 2004.
- Meat Loaf and Dick Wagner. "Execution Day," *Blind Before I Stop*. Atlantic Recording Corporation, 1986.
- Mendel, William W. and David G. Bradford. *Interagency Cooperation: A Regional Model for Overseas Operations*. Washington, DC: Institute for National Strategic Studies, National Defense University, 1995.
- Miller, Paul David. *The Interagency Process: Engaging America's Full National Security Capabilities*. Cambridge, MA: Institute for Foreign Policy Analysis, 1993.
- Murray, Williamson, ed. *A Nation at War in an Era of Strategic Change*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2004.
- _____. *Transformation Concepts for National Security in the 21st Century*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2002.
- National Counterterrorism Center. <http://www.nctc.gov/about_us/key_partners.html>, accessed on March 6, 2006.
- National Security Council. *CONPLAN: United States Government Interagency Domestic Terrorism Concept of Operation Plan*. Washington, DC, 2001.

- _____. *Handbook for Interagency Management of Complex Contingency Operations*. 1998.
- _____. *National Security Council Interagency Process*. Washington, DC, 1987.
- Odom, William E. *Fixing Intelligence: For a More Secure America*. New Haven, CT: Yale University Press, 2003.
- Odom, William E. and Robert Dujarric. *America's Inadvertent Empire*. New Haven, CT: Yale University Press, 2004.
- "Pentagon, Secret Unit Clash Over 9/11 Issues." *The (Norfolk, VA) Virginian-Pilot*. 16 February 2006, A8.
- Poole, Michele A. *Interagency Management of Complex Contingency Operations: The Impact of Presidential Decision Directive 56*. Monterey, CA: Naval Postgraduate School, 2001.
- Posner, Gerald. *Why America Slept: The Failure to Prevent 9/11*. New York: Random House, 2003.
- Posner, Richard A. *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*. Lanham, MD: Rowman and Littlefield, Publishers, Inc., 2005.
- Powers, Thomas. *Intelligence Wars: American Secret History from Hitler to al-Qaeda*. New York: New York Review Books, 2002.
- Public Law 80-253*, cited as "The National Security Act of 1947 as Amended," U.S. Code. Vol. 402 (2005).
- Public Law 93-579*, cited as "The Privacy Act of 1974. U.S. Code, as Amended," Vol. 5, Sec. 552 (2003).
- Public Law 99-433*, cited as the "Goldwater-Nichols Department of Defense Reorganization Act of 1986."
- Public Law 104-231, Stat 3048*, cited as the "Freedom of Information Act as Amended."
- Public Law 107-56, October 26, 2001*, cited as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001."
- Rast, Vicki J. *Interagency Conflict and United States Intervention Policy: Toward a Bureaucratic Model of Conflict Termination*. Fairfax, VA: George Mason University, 1999.

- _____. *Interagency Fratricide: Policy Failures in the Persian Gulf and Bosnia*. Maxwell Air Force Base, AL: Air University Press, 2004.
- Richelson, Jeffrey T. *The U.S. Intelligence Community*. Boulder, CO: Westview Press, 1999.
- Robinson, William B. *Programs for Improved Politico-Military Capabilities in the Department of State*. Cambridge, MA: Center for International Affairs, Harvard University, 1965.
- Rolington, Alfred. "Keeping Intelligence Objective." *Jane's Intelligence Review*. December 1, 2005, <http://www4.janes.com/subscribe.jir/doc_view.jsp?K2DocKey=/content1/janesdata/mags>, accessed on January 17, 2006.
- Schein, Edgar H. *Organizational Culture and Leadership, 2nd Edition*. San Francisco, CA: Jossey-Bass, 1992.
- Shafritz, Jay M. and J Steven Ott. *Classics of Organization Theory: Second Edition, Revised and Expanded*. Pacific Grove, CA: Brooks/Cole Publishing Company, 1987.
- Sherman, Jason. "The Protective Veil: What's the Best Way to Protect the Nation's Secrets? That's the Talk of the Town." *Armed Forces Journal International*: May 1999.
- Simon, Jr., James M. *Crucified on a Cross of Goldwater-Nichols*. Cambridge, MA: Harvard University Center for Information Policy Research, 2001.
- Stimeare, Ronald R. *Is it Really Possible to Prevent "Interagency Information-Sharing" From Becoming an Oxymoron?* Carlisle Barracks, PA: U.S. Army War College, 2005.
- Straughan, Matt. *Information Operations and Unity of Effort: The Case for a Joint Agency Information Operations Task Force*. Newport, RI: Naval War College, 1997.
- Stroup, Theodore G. "Leadership and Organizational Culture: Actions Speak Louder than Words." *Military Review*. January-February 1996.
- Stuart, Douglas T. ed., *Organizing for National Security*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2000.
- Sullivan, Linda E., Anthony T. Kruzas, eds., *Encyclopedia of Governmental Advisory Organizations*. Detroit, MI: Gale Research Co., 1975.
- Theoharis, Athan G., ed. *A Culture of Secrecy: The Government Versus the People's Right to Know*. Lawrence, KS: University of Kansas Press, 1998.
- Trebilcock, Craig T. "The Myth of *Posse Comitatus*." <<http://www.homelandsecurity>.

- org/journal/articles /Trebilcock.htm>, accessed on February 19, 2006.
- Treverton, Gregory F. *Rand Occasional Papers: The Next Steps in Reshaping Intelligence*. Santa Monica, CA: The Rand Corporation: 2005.
- Turner, Michael A. *Why Secret Intelligence Fails*. Dulles, VA: Potomac Books, Inc., 2005.
- Turner, Stansfield. *Secrecy and Democracy: The CIA in Transition*. Boston, MA: Houghton Mifflin Company, 1985.
- U.S. Central Intelligence Agency. *Director of Central Intelligence Directive 1/7: Security Controls on the Dissemination of Intelligence Information*. 30 June 1998.
- U.S. Congress. House. Committee on Government Reform. Subcommittee on National Security, Veterans Affairs, and International Relations. *Federal Interagency Data-Sharing and National Security: Hearing Before the Subcommittee on National Security, Veterans Affairs, and International Relations of the Committee on Government Reform*. 107th Cong., 1st Sess., 24 July 2001.
- U.S. Congress. Select Committee on Intelligence, U.S. Senate and the Permanent Select Committee on Intelligence, U.S. House of Representatives. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001: Vol 1*. 107th Cong., 2nd Sess., 18-26 September 2002.
- U.S. Congress. Senate. S. 2845, Debate on the National Intelligence Reform Act of 2004. *Congressional Record*, S9700-9720. (27 September 2004). <<http://www.fas.org/irp/news/2004/09/s092704.html>>, accessed December 20, 2005.
- U.S. Department of Defense. *CONPLAN: United States Government Interagency Domestic Terrorism Concept of Operations Plan*. Washington, DC, 2001.
- _____. *Directive Number 3305.5: General Defense Intelligence Program (GDIP) Management*. 9 May 1986.
- _____. *Directive Number 5105.21: Defense Intelligence Agency (DIA)*. 18 February 1997.
- _____. *Directive Number 5143.01: Undersecretary of Defense for Intelligence*. 23 November 2005.
- _____. *Directive Number 8115.01: Information Technology Portfolio Management*. 10 October 2005.
- _____. *Joint Doctrine Capstone and Keystone Primer*. 10 September 2001.
- _____. *Joint Publication 3-26, Homeland Security*. 2 August 2005.

- _____. *Struggle and Stalemate in the Western Sahara*. Washington, DC: Defense Intelligence Agency, 1979.
- _____. Office of the Undersecretary of Defense. *Memorandum for Director, Defense Intelligence Agency, Subject: Information Technology Portfolio Management*. 26 September 2005.
- U.S. Department of the Interior, President's Council on Management Improvement (U.S.), Committee on Organization and Structure. *Streamlining Internal Control Processes and Strengthening Management Controls with Less Effort*. Washington, DC, 1985.
- U.S. General Accounting Office. *Combating Terrorism: Interagency Framework and Agency Programs to Address the Overseas Threat*. Washington, DC, 2003.
- _____. *Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy*. Washington, DC, 2001.
- _____. *Combating Terrorism: Observations on the Nunn-Lugar-Domenici Domestic Preparedness Program*. Washington, DC, 1998.
- _____. *Combating Terrorism: Observations on Crosscutting Issues*. Washington, DC, 1998.
- _____. *Combating Terrorism: Observations on Options to Improve the Federal Response*. Washington, DC, 2001.
- _____. *DoD Personnel: More Consistency Needed in Determining Eligibility for Top Secret Security Clearances*. Washington, DC, 2001.
- United States Intelligence Community. <<http://www.intelligence.gov/1-members.shtml>>, accessed on February 19, 2006.
- U.S. Joint Chiefs of Staff. *Interagency Coordination During Joint Operations. Joint Pub 3-08*. Washington, DC, 1996.
- _____. *U.S. Department of Defense Dictionary of Military Terms*. New York: Arco Publishing, 1988.
- U.S. President. Executive Order. "National Security Information, E.O. 12356." <http://www.epic.org/open_gov/eo_12356.html>, accessed on August 22, 2005.
- _____. Executive Order. "Classified National Security Information, E.O. 12958." *Federal Register* 60, (20 April 1995): 19825. <<http://www.nara.gov/fedreg/eo1995.html>>, accessed on September 11, 2005.

_____. Executive Order. "Amendment to Executive Order 12958, Classified National Security Information, E.O. 12972." *Federal Register* 60, (1 July 1997): 36984. <<http://www.nara.gov/fedreg/eo1995.html>>, accessed on September 11, 2005.

_____. Executive Order. "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, E.O. 13292." *Federal Register* 70, (12 August 2005): 47161. ><http://www.regulations.gov/fredpdfs/05-16031.pdf>>, accessed on September 11, 2005.

_____. Executive Order. "Further Strengthening the Sharing of Terrorism Information to Protect Americans, E.O. 13388."

Vest, Jason. "Dumb Intelligence: Concerns About the Director of National Intelligence Go Far Beyond John Negroponte's Bloody Past." *Boston Phoenix*, February 25 - March 3, 2005, <http://www.bostonphoenix.com/boston/news_features/other_stories/multi-page/documents/04495068.asp>, accessed on December 20, 2005.

Vohryzek-Bolden, Miki and Gayle Olson-Raymer and Jeffrey O. Whamond. *Domestic Terrorism and Incident Management: Issues and Tactics*. Springfield, IL: Charles C. Thomas, Publisher, LTD, 2001.

Warner, Michael, ed. *Central Intelligence: Origin and Evolution*. CIA History Staff, Washington, DC: Center for the Study of Intelligence, 2001.

Wellons, Dave. *Doctrine for Domestic Disaster Response Activities*. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2000.

AUTHOR BIOGRAPHY

The author is a Special Agent in the U.S. Department of State's Diplomatic Security Service. In his 15 years of service, he has served as the Assistant Regional Security Officer in Damascus, Syria, as the Regional Security Officer (RSO) for the Embassy in Bamako, Mali, in the Los Angeles and Washington Field Offices, as a desk officer in the Passport Fraud Investigation Division, and as a Shift Leader on Secretary of State Colin Powell's protective detail. Prior to entering the Joint Forces Staff College Joint Advanced Warfighting School, he was a Senior Watch Officer in the Diplomatic Security Command Center. As the Assistance RSO in Damascus, he received the State Department's Superior Honor Award for his leadership of the Local Guard Force during a mob attack on the Embassy.

Prior to coming to the State Department, the author taught an Introduction to American Government at the University of North Dakota from which he holds a Master's Degree in Public Administration and a Bachelor's Degree in Journalism. After graduating from college in 1983, the author served as a Field Artillery Officer in the U.S. Army in West Germany and as a staff officer in an Engineering Battalion in the North Dakota Army National Guard.

The author is married. He and his wife have two children. Following graduation from the JAWS course, he is scheduled to be posted as the RSO for the U.S. Consulate General in Dubai.